**UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO**
**ESCUELA DE POSGRADO**

**MAESTRÍA EN INGENIERÍA DE SISTEMAS**
**CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE**

**Tesis**

# Propuesta de un modelo de gestión de incidentes de tecnologías de la información para las universidades públicas de la región Amazonas

**para obtener el Grado Académico de:**

**Maestro en ingeniería de sistemas**
**con mención en gerencia de tecnologías de la información y gestión del software**

**AUTORES:**

**Ing. Elger Orlando Silva Barboza**
**https://orcid.org/0009-0002-7358-3481**

**Ing. Roberto Carlos Eyzaguirre Caceres**
**https://orcid.org/0000-0001-5910-9893**

**ASESOR**

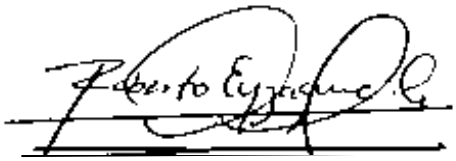
**Dr. Luis Alberto Otake Oyama**
**https://orcid.org/0000-0003-0382-4788**

**LAMBAYEQUE, 2026**

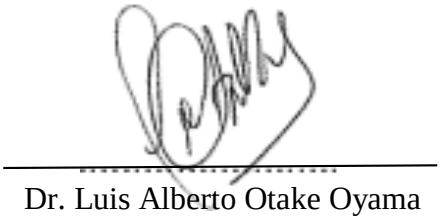
**Propuesta de un modelo de gestión de incidentes de tecnologías de la información para las universidades públicas de la región Amazonas**

PRESENTADA POR:

Ing. Elger Orlando Silva Barboza
AUTOR



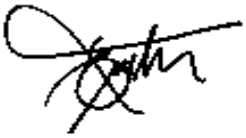
Ing. Roberto Carlos Eyzaguirre Caceres
AUTOR



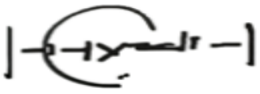
Dr. Luis Alberto Otake Oyama
ASESOR

Presentada a la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el Grado Académico de: MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE.

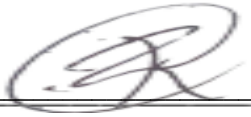
APROBADA POR:



Dr. Ernesto Karlo Celi Arevalo
PRESIDENTE



M.Sc. Omar Wilton Saavedra Salazar
SECRETARIO



M.Sc. Roberto Carlos Arteaga Lora
VOCAL

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

# ACTA DE SUSTENTACIÓN
# N° 007-2026-UI-FICSA

Siendo las 12:00 m horas del día 17 de agosto del 2026 en la sala de sustentaciones de la Facultad de Ingeniería Civil de Sistemas y de Arquitectura se reunieron los miembros de jurado de la Tesis de ***MAESTRIA EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE***; Titulada: **"PROPUESTA DE UN MODELO DE GESTIÓN DE INCIDENTES DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LAS UNIVERSIDADES PÚBLICAS DE LA REGIÓN AMAZONAS"**, designados mediante **Resolución Decanal N°341-2025-UNPRG-FICSA de fecha 9 de mayo del 2025** con la finalidad de Evaluar y Calificar la sustentación de la Tesis de ***MAESTRIA EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE***, conformado por los siguientes docentes:

| | |
|---|---|
| **DR. ING. ERNESTO KARLO CELI AREVALO** | **PRESIDENTE** |
| **MSC. ING. OMAR WILTON SAAVEDRA SALAZAR** | **SECRETARIO** |
| **MSC. ING. ROBERTO CARLOS ARTEAGA LORA** | **VOCAL** |

**Asesorado por DR. ING. LUIS ALBERTO OTAKE OYAMA.**

El acto de sustentación fue autorizado por **Oficio Virtual N° 175-2026-UIFICSA.** La Tesis de ***Maestría en Ingeniería de Sistemas con Mención en Gerencia de Tecnologías de la Información y Gestión del Software*** fue presentada y sustentada por los Tesistas **ROBERTO CARLOS EYZAGUIRRE CACERES Y ELGER ORLANDO SILVA BARBOZA,** tuvo una duración de 120 minutos. Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

| | NUMERO | LETRAS | CALIFICATIVO |
|---|---|---|---|
| **ROBERTO CARLOS EYZAGUIRRE CACERES** | 18 | DIECIOCHO | MUY BUENO |
| **ELGER ORLANDO SILVA BARBOZA** | 19 | DIECINUEVE | MUY BUENO |

**Por lo que quedan APTOS para obtener el Grado Académico de:** *MAESTRO EN INGENIERIA DE SISTEMAS CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE;* **de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil De Sistemas y de Arquitectura de la Universidad Nacional Pedro Ruiz Gallo.**

Siendo las 14:10 horas del mismo día, se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

**DR. ING. ERNESTO KARLO CELI AREVALO**
**PRESIDENTE**

**MSC. ING. OMAR WILTON SAAVEDRA SALAZAR**
**SECRETARIO**

**MSC. ING. ROBERTO CARLOS ARTEAGA LORA**
**VOCAL**

**DR. ING. LUIS ALBERTO OTAKE OYAMA**
**ASESOR**

JHFF/bcm.

## CONSTANCIA DE VERIFICACIÓN DE ORIGINALIDAD

Yo, Dr. Luis Alberto Otake Oyama, en calidad de asesor y usuario revisor de la Tesis de Maestría titulada: *"Propuesta de un Modelo de Gestión de Incidentes de Tecnologías de la Información para las Universidades Públicas de la Región Amazonas"*, cuyos autores son Elger Orlando Silva Barboza, identificado con DNI N.° 47412777, y Roberto Carlos Eyzaguirre Cáceres, identificado con DNI N.° 16751511; declaro que la evaluación efectuada mediante el programa informático correspondiente ha arrojado un porcentaje de similitud del **14 %** conforme se verifica en el Resumen del Reporte Automatizado de Similitudes que se adjunta al presente documento.

Asimismo, el suscrito ha realizado el análisis respectivo del citado reporte, concluyendo que las coincidencias detectadas dentro del porcentaje de similitud permitido no constituyen plagio, evidenciándose que el documento cumple con los principios de integridad científica, así como con las normas y protocolos establecidos para el adecuado uso de citas y referencias bibliográficas.

Finalmente, se adjunta el Recibo Digital correspondiente, para efectos de garantizar la trazabilidad del proceso respectivo.

Lambayeque, 22 de mayo de 2026

**Dr. Luis Alberto Otake Oyama**
**DNI N.° 16755316**
**Asesor**

PROPUESTA DE UN MODELO DE GESTIÓN DE INCIDENTES DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LAS UNIVERSIDADES PÚBLICAS DE LA REGIÓN AMAZONAS

INFORME DE ORIGINALIDAD

| 14% | 13% | 5% | 4% |
|---|---|---|---|
| INDICE DE SIMILITUD | FUENTES DE INTERNET | PUBLICACIONES | TRABAJOS DEL ESTUDIANTE |

FUENTES PRIMARIAS

| | | |
|---|---|---|
| 1 | hdl.handle.net<br>Fuente de Internet | 3% |
| 2 | repositorio.uss.edu.pe<br>Fuente de Internet | 1% |
| 3 | www.coursehero.com<br>Fuente de Internet | 1% |
| 4 | repositorio.ucv.edu.pe<br>Fuente de Internet | 1% |
| 5 | Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD<br>Trabajo del estudiante | <1% |
| 6 | repositoriotec.tec.ac.cr<br>Fuente de Internet | <1% |
| 7 | Submitted to Universidad Privada del Norte<br>Trabajo del estudiante | <1% |
| 8 | repositorio.unprg.edu.pe<br>Fuente de Internet | <1% |
| 9 | repositorioacademico.upc.edu.pe<br>Fuente de Internet | <1% |
| 10 | repositorio.upec.edu.ec<br>Fuente de Internet | <1% |
| 11 | repositorio.unc.edu.pe<br>Fuente de Internet | <1% |

Dr. Luis Alberto Otake Oyama
DNI N.° 16755316
Asesor

turnitin

# Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

| | |
|---|---|
| Autor de la entrega: | Orlando Silva Barboza |
| Titulo del ejercicio: | Quick Submit |
| Titulo de la entrega: | PROPUESTA DE UN MODELO DE GESTIÓN DE INCIDENTES DE ... |
| Nombre del archivo: | Informe_de_tesis__Orlando_Silva_Roberto_Eyzaguirre_V2.1.docx |
| Tamaño del archivo: | 10.33M |
| Total páginas: | 180 |
| Total de palabras: | 44,179 |
| Total de caracteres: | 260,695 |
| Fecha de entrega: | 22-may-2026 11:19a. m. (UTC-0500) |
| Identificador de la entrega: | 2967213185 |

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

ESCUELA DE POSGRADO
MAESTRÍA EN INGENIERIA DE SISTEMAS
CON MENCIÓN EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE

TESIS

"PROPUESTA DE UN MODELO DE GESTIÓN DE INCIDENTES DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LAS UNIVERSIDADES PÚBLICAS DE LA REGIÓN AMAZONAS"

INVESTIGADORES
ING. ELGER ORLANDO SILVA BARBOZA
ING. ROBERTO CARLOS EYZAGUIRRE CÁCERES

ASESOR
MG. LUIS ALBERTO OTAKE OYAMA

LAMBAYEQUE, 2026

**Dr. Luis Alberto Otake Oyama**
**DNI N.° 16755316**
**Asesor**

## DEDICATORIA

Dedico la presente tesis, a mi madre y hermana, por su amor incondicional, esfuerzo constante y apoyo permanente a lo largo de mi formación personal y profesional. Su ejemplo de perseverancia y fortaleza ha sido mi mayor inspiración para alcanzar cada una de mis metas.

Asimismo, a toda mi familia, quienes con su confianza, cariño y motivación me impulsaron a continuar y culminar satisfactoriamente esta etapa de crecimiento profesional.

**(E.O.S.B)**

A mi querida familia, a mi esposa Milagros e hijos Diego y Carlos, a mi madre Esperanza cuyo amor incondicional, paciencia y comprensión han sido la fuerza que me impulsó a continuar incluso en los momentos más difíciles.

Sus palabras de ánimo, su compañía silenciosa y su confianza absoluta en mí iluminaron cada paso de este camino.

**(R.C.E.C)**

## AGRADECIMIENTOS

Expreso mi más sincero agradecimiento a mi familia, por el apoyo incondicional, la confianza y el respaldo brindado durante el desarrollo de esta investigación y a lo largo de mi formación académica.

De manera especial, agradezco al Mg. Luis Alberto Otake Oyama, asesor de la presente tesis, por su orientación, conocimientos, dedicación y valiosos aportes académicos, los cuales fueron fundamentales para la culminación satisfactoria de este trabajo de investigación.

Finalmente, agradezco a todas las personas que, de una u otra manera, contribuyeron y acompañaron el desarrollo de esta tesis de maestría.

**(E.O.S.B)**

Deseo expresar mi más profundo y sincero agradecimiento a mi familia por su apoyo incondicional.

Al Mg. Luis Alberto Otake Oyama, quien nos ha brindado su apoyo y orientación con su asesoría en esta investigación.

**(R.C.E.C)**

## ÍNDICE GENERAL

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

## RESUMEN

La presente investigación abordó la problemática de la gestión inadecuada de incidentes de tecnologías de la información en el entorno universitario, caracterizada por la ausencia de procesos estandarizados, la atención reactiva, la falta de trazabilidad y la dependencia del conocimiento individual del personal técnico. Esta situación generaba demoras en la atención, baja calidad del servicio y riesgos para la continuidad de servicios críticos como el sistema académico, aulas virtuales y plataformas institucionales.

En cuanto a los fundamentos teóricos, el estudio se sustentó principalmente en el marco de buenas prácticas de ITIL 4, especialmente en la práctica de gestión de incidentes, orientada a restaurar el servicio en el menor tiempo posible. Asimismo, se incorporaron conceptos relacionados con la gestión de servicios de TI, la mejora continua, la gestión del conocimiento y el uso de métricas como MTTR y FCR, los cuales permitieron estructurar un modelo integral alineado a estándares internacionales.

Desde el punto de vista metodológico, la investigación fue de tipo aplicada, con enfoque cualitativo y diseño no experimental de corte transversal. Se desarrolló en cuatro fases: diagnóstico de la situación actual, identificación de brechas respecto a ITIL 4, diseño del modelo propuesto y validación mediante juicio de expertos. Para esta última fase se utilizó un instrumento estructurado que evaluó criterios de cobertura, comprensibilidad, consistencia interna y pertinencia institucional. Las técnicas investigativas utilizadas fueron: análisis de procesos, interpretación de prácticas, comparativa con ITIL, diseño de una propuesta y la validación de la misma mediante juicio experto.

Los resultados evidenciaron la existencia de brechas significativas en la gestión actual, lo que justificó el diseño de un modelo que integra componentes organizativos y operativos, como el Punto Único de Contacto, niveles de soporte, procesos estandarizados y base de conocimientos. La validación experta mostró altos niveles de aceptación, con promedios superiores a 4.5 en todos los criterios evaluados, lo que confirma la viabilidad, coherencia y aplicabilidad del modelo en el contexto universitario.


**Palabras clave:** gestión de incidentes, ITIL 4, servicios de TI, mesa de ayuda, mejora continua.

**ABSTRACT**

The present research addressed the problem of inadequate IT incident management in the university environment, characterized by the absence of standardized processes, a reactive approach, lack of traceability, and strong dependence on individual technical knowledge. This situation led to delays in response times, reduced service quality, and risks affecting the continuity of critical services such as academic systems, virtual learning platforms, and institutional services.

From a theoretical perspective, the study was primarily based on the ITIL 4 framework, particularly the incident management practice, which focuses on restoring services as quickly as possible. Additionally, concepts related to IT service management, continual improvement, knowledge management, and performance metrics such as MTTR and FCR were incorporated. These foundations enabled the development of a structured and comprehensive model aligned with international best practices.

Methodologically, the research followed an applied approach with a qualitative focus and a non-experimental cross-sectional design. The study was conducted in four stages: diagnosis of the current situation, identification of gaps compared to ITIL 4, design of the proposed model, and validation through expert judgment. For validation, a structured instrument was used to assess criteria such as coverage, comprehensibility, internal consistency, and institutional relevance. The research techniques employed included process analysis, interpretation of practices, comparison with ITIL, the design of a proposal, and its validation through expert judgment.

The results revealed significant gaps in the existing incident management practices, which justified the development of a model integrating both organizational and operational components, including a Single Point of Contact (Service Desk), support levels, standardized processes, and a knowledge base. Expert validation showed high levels of acceptance, with average scores above 4.5 across all evaluation criteria, confirming the feasibility, coherence, and applicability of the proposed model in the university context.

**Keywords:** incident management, ITIL 4, IT services, service desk, continual improvement.

# INTRODUCCIÓN

En la actualidad, el desarrollo de las organizaciones se encuentra fuertemente condicionado por el uso intensivo de las tecnologías de la información (TI) como soporte de sus procesos. Este escenario ha llevado a que las áreas de TI dejen de enfocarse únicamente en la gestión de infraestructura tecnológica y comiencen a orientarse hacia la provisión de servicios, tanto para usuarios internos como externos. No obstante, este cambio no siempre ha sido acompañado por una visión clara de valor, lo que ha generado inversiones poco justificadas o sobredimensionadas, muchas veces sin considerar de manera adecuada los riesgos asociados (Marulanda, et.al. 2019).

En ese mismo contexto, las estrategias de gestión de TI han venido transitando desde un enfoque centrado en proyectos hacia un enfoque basado en servicios. Mientras que el primero buscaba ampliar capacidades tecnológicas y habilitar nuevas funcionalidades, el segundo se orienta a asegurar la calidad, continuidad y eficiencia de los servicios ofrecidos, considerando de forma más explícita variables como el costo, el riesgo y la satisfacción del usuario (Baud, 2016). Este cambio, aunque necesario, no ha sido sencillo de implementar en muchas organizaciones.

Diversos estudios han demostrado que la adopción adecuada de tecnologías de la información puede generar beneficios significativos en términos de eficiencia operativa, toma de decisiones y generación de valor. Sin embargo, cuando su implementación no se gestiona correctamente, los efectos pueden ser contraproducentes, afectando la continuidad de los servicios e incluso la confianza de los usuarios. En ese sentido, los modelos organizacionales actuales han comenzado a priorizar enfoques basados en el ciclo de vida del servicio, dejando en un segundo plano las visiones estrictamente funcionales o por procesos.

La gestión de servicios de TI se ha consolidado así como un componente clave en la generación de valor organizacional. Este valor no solo se expresa en términos de utilidad para la organización, sino también en la capacidad de garantizar servicios confiables, oportunos y seguros para los usuarios. En otras palabras, no basta con que el servicio funcione; debe hacerlo bajo condiciones de calidad, disponibilidad y continuidad que respondan a las expectativas del entorno.

En este marco, la cultura de gestión de servicios se sostiene en tres pilares fundamentales: el alineamiento con las necesidades del usuario, la mejora continua de la calidad del servicio y el control de los costos operativos asociados (Marulanda et al., 2019). No obstante, lograr este equilibrio implica enfrentar múltiples desafíos, especialmente cuando los procesos no están formalmente definidos o carecen de mecanismos de control adecuados.

Uno de los aspectos más críticos dentro de esta gestión es el tratamiento de los incidentes de TI. La capacidad de una organización para detectar, registrar, analizar y resolver incidentes de manera oportuna influye directamente en la percepción de calidad del servicio. Sin embargo, en la práctica, muchas organizaciones aún operan bajo esquemas informales, donde los incidentes se atienden de manera reactiva y sin un registro sistemático, lo que limita el aprendizaje organizacional y la prevención de recurrencias.

Cuando los incidentes no son gestionados adecuadamente, las soluciones suelen enfocarse únicamente en restaurar el servicio sin analizar las causas subyacentes del problema. Esta situación incrementa la probabilidad de reincidencia y puede ocasionar impactos operativos, económicos y de seguridad más severos para la organización (ISO/IEC 27035-1, 2016; Axelos, 2019).

En relación con ello, marcos de referencia como ITIL han proporcionado lineamientos ampliamente aceptados para la gestión de servicios de TI, incluyendo la gestión de incidentes. ITIL propone un enfoque flexible y adaptable que permite a las organizaciones estructurar sus procesos en función de sus necesidades, promoviendo una mayor eficiencia operativa y un mejor control de los recursos tecnológicos (Baud, 2016). Sin embargo, su adopción efectiva requiere un proceso de adaptación contextual que muchas veces no se logra de manera adecuada.

A nivel internacional, se ha evidenciado que la ausencia de sistemas formales de gestión de incidentes puede generar consecuencias significativas, como la pérdida de información crítica, la disminución de la productividad y el incremento de los costos operativos (ISO/IEC 27035-1, 2016). Asimismo, según Axelos (2019), una gestión deficiente de incidentes impacta directamente en la disponibilidad de los servicios, afectando la experiencia del usuario y la reputación institucional.

En el ámbito educativo, particularmente en las universidades públicas, estas problemáticas adquieren una dimensión aún más relevante. Las universidades públicas dependen cada vez más de los sistemas y servicios tecnológicos para sostener procesos académicos, administrativos y de investigación, por lo que la indisponibilidad de dichos servicios puede afectar directamente la continuidad institucional y la experiencia de los usuarios (Orozco & Tovar, 2018; Nugroho & Fianty, 2023).

En el caso específico de las Universidades Públicas de la región Amazonas, se ha observado que la gestión de incidentes de TI enfrenta múltiples limitaciones. La ausencia de un modelo estructurado ha dado lugar a situaciones recurrentes de interrupción de servicios, pérdida de información y retrasos en la atención de problemas. Estas deficiencias no solo afectan la eficiencia operativa, sino que también inciden en la calidad de los servicios brindados a la comunidad universitaria.

A partir de las entrevistas y revisión documental realizadas durante el diagnóstico institucional, se identificaron diversas problemáticas, entre ellas procesos poco transparentes, infraestructura tecnológica inadecuada, estrategias de gestión inconsistentes, deficiencias en la coordinación entre áreas, así como la ausencia de normativas actualizadas. A ello se suma una limitada integración de sistemas y un bajo nivel de concientización del personal respecto al uso adecuado de las tecnologías de la información.

En relación con la gestión de incidentes, las entrevistas y revisión de procedimientos institucionales permitieron evidenciar la inexistencia de procesos formalmente definidos, la ausencia de un Punto Único de Contacto y el uso de mecanismos informales para el reporte y seguimiento de incidentes. Asimismo, el registro de incidentes en herramientas básicas como hojas de cálculo dificulta su seguimiento, análisis y aprovechamiento como fuente de conocimiento organizacional.

Esta situación pone en evidencia una brecha importante entre las prácticas actuales de las universidades públicas de la región Amazonas y las recomendaciones establecidas por marcos de referencia como ITIL. Dicha brecha no solo es operativa, sino también

conceptual, ya que refleja la ausencia de un modelo que integre de manera coherente los elementos funcionales y estructurales necesarios para una gestión eficiente de incidentes.
En ese sentido, la presente investigación se orienta a responder la siguiente interrogante: ***¿qué elementos funcionales y estructurales debe tener un modelo de gestión de incidentes de tecnologías de la información basado en ITIL como soporte de la operación de los servicios de TI en las universidades públicas de la región Amazonas?***

El propósito central de la presente investigación fue ***desarrollar una propuesta de modelo de gestión de incidentes de tecnologías de la información que integre elementos funcionales y estructurales, tomando como base las buenas prácticas del marco referencial ITIL***. Este modelo se planteó como un soporte para la operación de los servicios de TI en las Universidades Públicas de la Región Amazonas, considerando sus condiciones reales, limitaciones operativas y el nivel actual de madurez en la gestión de servicios.

Para alcanzar este objetivo general, en primer lugar se buscó *identificar los problemas y debilidades presentes en los procesos académicos que brindan servicios a la comunidad universitaria*. Este objetivo resultó necesario porque permitió entender cómo las deficiencias en la gestión de TI no se limitan a lo técnico, sino que terminan afectando directamente actividades académicas clave. En varios casos, los problemas no eran evidentes a simple vista, sino que estaban relacionados con prácticas informales o poco documentadas.

En una segunda etapa, *se analizó la forma en que se gestionaban los incidentes de tecnologías de la información dentro de dichos procesos*. Este análisis no solo se centró en describir lo que se hacía, sino en contrastarlo con las buenas prácticas propuestas por ITIL. De esta manera, fue posible identificar brechas concretas, algunas más críticas que otras, que explicaban por qué los tiempos de respuesta eran altos o por qué ciertos incidentes se repetían con frecuencia.
A partir de ello, se planteó como siguiente objetivo el *diseño de los elementos funcionales y estructurales de una mesa de ayuda al usuario*. Esta decisión no fue casual, ya que se observó que una de las principales limitaciones era la falta de un punto centralizado para la gestión de incidentes. La mesa de ayuda se concibió entonces como un componente clave para ordenar la atención, mejorar la comunicación y evitar la dispersión de los reportes.

De manera complementaria, *se definieron criterios para la clasificación y priorización de los incidentes, así como para el escalonamiento de su atención*. Este objetivo permitió establecer una lógica más clara para decidir qué incidentes atender primero y cómo asignar los recursos disponibles. En la práctica, se notó que muchas decisiones se tomaban de forma improvisada, lo que generaba retrasos innecesarios o un uso poco eficiente del personal técnico.

Otro de los objetivos consistió en *diseñar el flujo de trabajo del proceso de gestión de incidentes a través de la mesa de ayuda*. Este flujo buscó ordenar las actividades desde el registro inicial hasta la resolución y cierre del incidente. No se trató solo de dibujar un proceso ideal, sino de construir uno que pudiera ser realmente aplicable en el contexto de las universidades analizadas, incluso con sus limitaciones actuales.

Finalmente, se propuso *validar el modelo de gestión de incidentes mediante un juicio de expertos*, considerando criterios como Cobertura del modelo, Comprensibilidad, Consistencia interna y Pertinencia institucional. Esta validación permitió obtener una mirada externa sobre la propuesta, lo que ayudó a identificar posibles ajustes antes de su aplicación. En cierto modo, fue una forma de contrastar la propuesta con la experiencia de profesionales que ya han trabajado en este tipo de entornos.

La presente investigación se justifica, en primer lugar, desde su pertinencia, ya que responde a una necesidad concreta identificada en las Universidades Públicas de la Región Amazonas. Estas instituciones dependen cada vez más de los servicios de tecnologías de la información para el desarrollo de sus funciones académicas y administrativas. Sin embargo, como se ha evidenciado, la gestión de incidentes no ha evolucionado al mismo ritmo, lo que genera interrupciones frecuentes y afecta la continuidad de los servicios.

Desde una perspectiva de relevancia, el estudio cobra importancia porque aborda un problema que no solo impacta en el ámbito tecnológico, sino también en la calidad del servicio educativo. Cuando un sistema académico falla o no está disponible, las consecuencias se trasladan directamente a estudiantes, docentes y personal administrativo. Esto puede traducirse en retrasos, pérdida de información o incluso en la percepción negativa sobre la institución. En ese sentido, mejorar la gestión de incidentes

no es un tema técnico aislado, sino un factor que influye en la experiencia de toda la comunidad universitaria.

Asimismo, la investigación adquiere relevancia al proponer una solución estructurada basada en buenas prácticas reconocidas internacionalmente, como ITIL. No obstante, lo valioso en este caso no es solo la adopción del marco, sino su adaptación a un contexto específico, donde existen limitaciones de recursos, alta rotación de personal y, en algunos casos, ausencia de cultura organizacional orientada a servicios. Este ajuste contextual es clave, porque muchos modelos fallan precisamente por intentar aplicarse de manera genérica.

En cuanto al aporte a la ciencia, el estudio contribuye a reducir una brecha en el conocimiento relacionada con la aplicación práctica de modelos de gestión de incidentes en entornos universitarios públicos de regiones con menor desarrollo tecnológico. Si bien existen múltiples estudios sobre gestión de servicios de TI, pocos abordan de manera específica la realidad de instituciones públicas en contextos regionales como el de Amazonas, donde las condiciones operativas son distintas a las de grandes organizaciones o universidades con mayor nivel de madurez tecnológica (Ferreira, 2021; Dzemydienė et al., 2024; Nugroho & Fianty, 2023).

En ese sentido, la propuesta desarrollada no solo tiene un valor aplicado, sino también teórico, ya que integra conceptos de gestión de servicios, gestión de incidentes y adaptación contextual. De alguna manera, intenta demostrar que es posible implementar modelos basados en estándares internacionales sin perder de vista la realidad local (Axelos, 2019; Baud, 2016).

Finalmente, la investigación aporta una base que puede ser utilizada en futuros estudios o en procesos de mejora institucional dentro de otras universidades públicas con características similares. Aunque no pretende ser un modelo definitivo, sí ofrece una referencia estructurada que puede ser ajustada, ampliada o incluso cuestionada en otros contextos. Y eso, en cierta forma, también forma parte del avance del conocimiento.

# DISEÑO TEÓRICO

## 1.1. Antecedentes

Dzemydienė, Turskienė y Šileikienė (2024) desarrollaron un estudio orientado a proponer un enfoque de gestión de incidentes TIC para una institución educativa a partir de las recomendaciones de ITIL 4. El problema que abordaron estuvo relacionado con la necesidad de resolver incidentes de manera más rápida, con menor impacto sobre los usuarios y con procedimientos más claros. Teóricamente, el trabajo se sustentó en la práctica de incident management de ITIL 4, en la priorización por impacto y urgencia, en el uso de Help Desk y en la construcción de una base de conocimiento para documentar soluciones. Metodológicamente, las autoras reportaron una investigación experimental en una institución educativa, registrando incidentes mediante un sistema Help Desk. Entre sus resultados, destacaron que el enfoque propuesto permitió estructurar el proceso desde el registro, clasificación y priorización hasta la resolución, el reporte y la ampliación de la base de conocimiento; además, concluyeron que muchas debilidades previas se asociaban a procedimientos no previstos, deficiencias de registro, falta de entrenamiento y escasa cultura institucional de gestión de incidentes.

Palilingan y Batmetan (2018) estudiaron la gestión de incidentes en un sistema de información académica, partiendo del problema de que muchos incidentes no eran tratados de forma adecuada y terminaban afectando la continuidad del servicio. Como fundamento principal emplearon el framework ITIL, específicamente técnicas derivadas de la sección Service Operation, para organizar la atención de incidentes. En términos metodológicos, el artículo se presenta como un estudio aplicado orientado a encontrar una forma adecuada de gestionar incidentes en sistemas académicos. Sus hallazgos fueron bastante concretos: reportaron que 84.5% de los incidentes podían ser atendidos rápida y apropiadamente y que el 15.5% restante debía escalarse, concluyendo que el modelo permitía administrar mejor los recursos y sostener un servicio académico más eficiente.

En nuestra revisión, otro antecedente relevante es el de Orozco y Tovar (2018), quienes propusieron un modelo de gestión de incidentes basado en ITIL para instituciones de educación superior en Barranquilla y su área metropolitana. El

problema identificado fue que los procesos de atención de incidentes en las universidades eran básicamente reactivos y no se apoyaban en estándares o mejores prácticas del sector. En el plano teórico, el estudio combinó ITIL con una mirada sistémica de la infraestructura y de la calidad del servicio. Metodológicamente, los autores definieron su trabajo como una investigación de tipo holístico, de nivel comprensivo, proyectivo, diseño transeccional contemporáneo, uso de triangulación y validación por juicio de expertos. Como resultado, obtuvieron un modelo sistémico basado en buenas prácticas que, según señalan, aporta beneficios para la gestión de incidentes en universidades y ordena el flujo del proceso bajo una lógica más formal.

Pereira, et.al (2021) abordaron el problema desde otra perspectiva, centrada en el desempeño temporal del proceso de incident management dentro de la gestión de servicios TI. Su investigación se apoyó en la relación entre Business Process Management (BPM) e ITSM, incorporando además referencias a ITIL y simulación de procesos. En cuanto al método, los autores desarrollaron un estudio de caso orientado a mejorar el tiempo de ejecución del proceso de gestión de incidentes, usando una herramienta de simulación de procesos de negocio. Sus resultados identificaron tres prácticas con mayor potencial de mejora: automatización de actividades, eliminación de actividades e integración tecnológica, y mostraron que su aplicación eliminaba el esfuerzo requerido en el primer nivel de soporte y reducía en 10.7% el tiempo promedio de procesamiento en el segundo nivel.

Por su parte, Nugroho y Fianty (2023) analizaron el uso de principios de ITIL para mejorar el funcionamiento diario de una división de TI a través del help desk y la gestión de incidentes. El problema estudiado giró en torno a la necesidad de estandarizar flujos de atención y elevar la eficiencia del servicio. Teóricamente, se apoyaron en IT governance, ITIL, IT helpdesk e incident management; metodológicamente, recopilaron datos de correos electrónicos entre usuarios y el área de TI, además de entrevistas, y utilizaron el método ITIL Maturity Level (ITML) para evaluar el estado del proceso. Los resultados mostraron que el help desk alcanzó un puntaje de 3.5, mientras que incident management obtuvo 2, por debajo del nivel esperado de cumplimiento; aun así, el estudio concluyó que la gestión de incidentes sí permitía estandarizar flujos de trabajo y sostener el desempeño del servicio, aunque todavía con brechas de madurez importantes.

En el contexto peruano, Loayza-Uyehara (2016) desarrolló un modelo de gestión de incidentes para una entidad estatal, motivado por el aumento de requerimientos de servicios TI y por problemas concretos como la falta de tratamiento de severidades, la ausencia de tiempos de respuesta y restauración, y la duplicidad de registros. El estudio se sustentó en las buenas prácticas de ITIL y en la articulación con una herramienta de service management. Desde el punto de vista metodológico, el autor describe un proceso de revisión y aplicación de los componentes del modelo para diseñar una propuesta ajustada a la entidad. Entre los principales resultados, se reportó la implementación de un nuevo modelo y una herramienta de soporte, así como una disminución de 52.2% en los incidentes registrados en el primer trimestre de 2015 respecto del tercer trimestre de 2014, lo que fue interpretado como una mejora asociada a una mejor gestión de incidentes.

Pita (2022) evaluó el efecto de implementar un Service Desk bajo ITIL en la Universidad Nacional de la Amazonía Peruana. El problema de partida fue que el área responsable atendía incidentes sin procedimientos formales, sin herramientas adecuadas y sin metas definidas, generando malestar e insatisfacción entre los usuarios. En lo teórico, la tesis se apoyó en ITIL, KPIs de gestión de incidentes, SLA y medición de percepción y satisfacción. Metodológicamente, se trató de una investigación cuantitativa aplicada, con diseño preexperimental de pretest y postest, utilizando todos los incidentes reportados, fichas de registro, cálculo de KPIs y encuestas a usuarios. Los resultados mostraron mejoras en los cinco KPIs propuestos, incrementos significativos en percepción y satisfacción, y un aumento de incidentes resueltos dentro del SLA de 47.52% a 80.20%; en consecuencia, el autor concluyó que el desarrollo del Service Desk mejoró la gestión de incidentes de TI en la UNAP.

Finalmente, Guerra Cabrera (2021) estudió el impacto de implementar un sistema Service Desk basado en tecnologías web en la Universidad Nacional de Cajamarca, focalizándose en la atención de incidencias de hardware y software de su unidad de soporte informático. El problema estuvo asociado a la necesidad de mejorar los procesos actuales y reducir los tiempos de atención. Como base teórica, el trabajo tomó las fases de ITIL vinculadas al registro, categorización, priorización, diagnóstico

inicial, gestión de tareas, resolución y cierre del incidente. En el plano metodológico, se trató de una investigación evaluativa con implementación, desarrollada con la metodología IPEE para identificar requerimientos y responsables del proyecto. Sus resultados mostraron una reducción promedio del 43% en los tiempos de proceso y un 63.3% de satisfacción de usuarios, concluyendo que el sistema impactó positivamente en la atención de incidencias dentro de la universidad.

## 1.2. Estado de arte

### 1.2.1. En relación a los fundamentos teóricos aplicados

En la literatura revisada, el principal sustento teórico para la gestión de incidentes de TI ha sido el marco de referencia **ITIL**, tanto en su versión v3 como en ITIL 4, aunque con una clara predominancia de la primera. En términos generales, los estudios coinciden en considerar la gestión de incidentes como un proceso orientado a restaurar el servicio en el menor tiempo posible, minimizando el impacto sobre el negocio o los usuarios.

Dzemydienė et al. (2024) fundamentaron su propuesta en ITIL 4, incorporando conceptos como la priorización basada en impacto y urgencia, el uso de un punto único de contacto (Service Desk) y la gestión del conocimiento como elemento clave para evitar la recurrencia de incidentes. En una línea similar, Palilingan y Batmetan (2018) utilizaron ITIL como base para estructurar la atención de incidentes en sistemas académicos, aunque desde una perspectiva más alineada con ITIL v3 y su enfoque en la operación del servicio.

Otros estudios, como el de Orozco y Tovar (2018), complementaron ITIL con un enfoque sistémico, considerando la interacción entre procesos, infraestructura y usuarios dentro de las instituciones de educación superior. Esta integración permitió ampliar la visión más allá del proceso de incident management, incorporando elementos de gestión organizacional.

Asimismo, Pereira et al. (2021) realizaron una articulación entre IT Service Management y **Business Process Management (BPM)**, destacando la importancia de modelar y optimizar los procesos de gestión de incidentes desde una lógica de eficiencia operativa. Por su parte, Nugroho y Fianty (2023) abordaron el marco ITIL

desde una perspectiva de madurez, utilizando el modelo ITIL Maturity Level para evaluar el nivel de implementación de las prácticas.

En el contexto peruano, Loayza-Uyehara (2016), Pita Astengo (2022) y Guerra Cabrera (2021) se basaron principalmente en ITIL v3, incorporando además conceptos como acuerdos de nivel de servicio (SLA), indicadores de desempeño (KPIs) y herramientas de service desk, lo que refleja una adopción más operativa que estratégica del marco.

Se evidencian que, aunque existe un consenso en torno al uso de ITIL como marco teórico principal, su aplicación varía significativamente en función del contexto, y en muchos casos no se incorpora aún la lógica más reciente de ITIL 4, especialmente en entornos universitarios públicos.

### 1.2.2. En relación a los métodos de investigación aplicados

En cuanto a los métodos de investigación, se observa una diversidad de enfoques, aunque con predominio de estudios aplicados y orientados a la solución de problemas concretos.

Dzemydienė et al. (2024) emplearon un enfoque experimental, aplicando directamente el modelo propuesto en un entorno educativo, lo que permitió observar cambios en la gestión de incidentes en tiempo real. Este tipo de aproximación resulta valiosa porque permite validar las propuestas en contextos reales, aunque también depende de condiciones específicas de implementación.

Por otro lado, Pereira et al. (2021) utilizaron un estudio de caso apoyado en simulación de procesos, lo que les permitió analizar el impacto de distintas mejoras antes de su implementación. Este enfoque aporta una visión más analítica, aunque menos cercana a la operación real.

En contraste, Orozco y Tovar (2018) desarrollaron una investigación de tipo proyectivo con validación por expertos, lo que les permitió construir un modelo teórico-práctico sin necesidad de implementarlo completamente. De manera similar, Loayza-

Uyehara (2016) siguió una lógica de desarrollo de propuesta basada en análisis documental y aplicación de buenas prácticas.

En el caso de investigaciones en universidades peruanas, como las de Pita Astengo (2022) y Guerra Cabrera (2021), se utilizaron enfoques cuantitativos aplicados, incluyendo diseños preexperimentales y evaluaciones de impacto. Estos estudios midieron variables como tiempos de atención, niveles de satisfacción y cumplimiento de SLA, lo que permitió evidenciar mejoras concretas tras la implementación de soluciones.

Finalmente, Nugroho y Fianty (2023) adoptaron un enfoque evaluativo basado en niveles de madurez, utilizando entrevistas y análisis documental para determinar el estado actual de la gestión de incidentes.

Los métodos aplicados reflejan una tendencia hacia la investigación aplicada, con énfasis en la mejora de procesos, aunque con una limitada integración entre evaluación, diseño e implementación en un mismo estudio.

### 1.2.3. Soluciones implementadas en la gestión de incidentes

En relación con las soluciones propuestas, los antecedentes coinciden en la implementación de tres componentes principales: **estructuración del proceso de gestión de incidentes, implementación de service desk y uso de herramientas tecnológicas de soporte**.

Dzemydienė et al. (2024) desarrollaron una solución basada en ITIL 4 que incluyó la formalización del proceso completo de gestión de incidentes, desde el registro hasta la resolución, incorporando además una base de conocimiento para documentar soluciones recurrentes. Esta propuesta permitió mejorar la organización del proceso, aunque dependía en gran medida de la disciplina en el registro de información.

Palilingan y Batmetan (2018) propusieron un modelo enfocado en la correcta categorización y escalamiento de incidentes dentro de sistemas académicos, logrando mejorar la eficiencia en la atención. Sin embargo, su solución se centró más en el proceso que en la integración con herramientas tecnológicas avanzadas.

Por su parte, Orozco y Tovar (2018) plantearon un modelo sistémico que integraba la gestión de incidentes con otros procesos de TI, proponiendo una estructura organizacional más clara y alineada con ITIL. Esta solución aportó una visión más integral, aunque no se evidenció su implementación completa.

En el ámbito de la optimización de procesos, Pereira et al. (2021) propusieron mejoras específicas como la automatización de actividades, la eliminación de tareas redundantes y la integración de sistemas, lo que permitió reducir tiempos de atención y mejorar la eficiencia operativa.

En el contexto peruano, las soluciones implementadas por Loayza-Uyehara (2016), Pita Astengo (2022) y Guerra Cabrera (2021) se centraron principalmente en la implementación de **service desk** apoyados en herramientas tecnológicas. Estas soluciones incluyeron la definición de flujos de atención, la asignación de roles, la incorporación de SLA y el uso de indicadores de desempeño. Los resultados evidenciaron mejoras en los tiempos de respuesta, reducción de incidentes y aumento en la satisfacción de los usuarios.

### 1.2.4. Síntesis comparativa y brecha de conocimiento

A partir del análisis realizado, se puede observar que existe una base teórica sólida en torno al uso de ITIL para la gestión de incidentes, así como una variedad de enfoques metodológicos orientados a la mejora de procesos. Asimismo, las soluciones implementadas han demostrado ser efectivas en términos de eficiencia operativa y satisfacción del usuario.

No obstante, también se identifican limitaciones importantes. En primer lugar, la mayoría de los estudios se basa en ITIL v3, lo que evidencia una baja adopción de ITIL 4 en contextos reales. En segundo lugar, muchas propuestas se centran en componentes específicos, como el service desk o la automatización, sin integrar de manera completa un modelo estructurado que articule todos los elementos necesarios para la gestión de incidentes.

Finalmente, existe una escasa producción científica enfocada específicamente en universidades públicas de contextos regionales como la región Amazonas. Las condiciones particulares de estas instituciones, como: limitaciones de recursos, alta rotación de personal y ausencia de procesos formales, no han sido abordadas de manera suficiente en los estudios revisados.

En ese sentido, la presente investigación busca cubrir esta brecha mediante el desarrollo de un modelo de gestión de incidentes basado en ITIL, incorporando tanto elementos funcionales como estructurales, y adaptándolo a las características específicas de las universidades públicas de la región Amazonas. De alguna manera, se intenta no solo aplicar un marco teórico, sino aterrizarlo a una realidad que, en la práctica, suele quedar fuera de los modelos tradicionales.

## 1.3. Fundamento teórico

### 1.3.1. Gestión de servicios de TI como base para la continuidad de los servicios tecnológicos

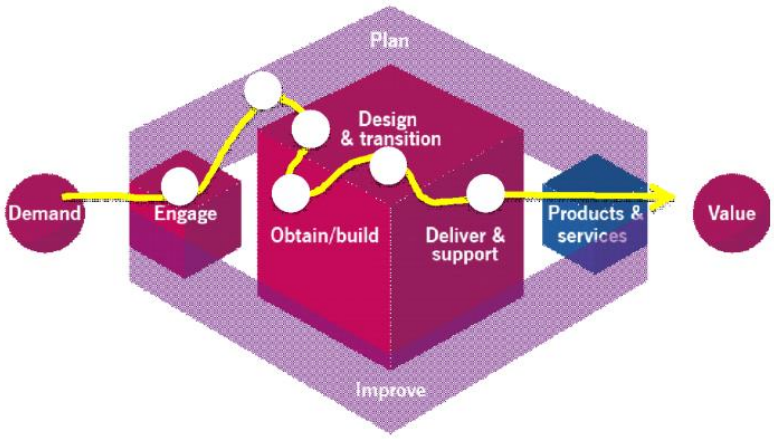
La Gestión de Servicios de Tecnologías de la Información, conocida como IT Service Management (ITSM), puede entenderse como un enfoque estructurado que organiza, controla y mejora la forma en que se diseñan y entregan los servicios de TI dentro de una organización. En este sentido, Trinidad et al. (2021) señalan que ITSM se basa en procesos orientados a asegurar que los servicios tecnológicos realmente aporten valor a los objetivos del negocio. No se trata únicamente de mantener sistemas funcionando, sino de garantizar que esos sistemas respondan a necesidades concretas. Por eso, más que una función operativa, ITSM se posiciona como un componente estratégico dentro de la organización, aunque en la práctica muchas veces todavía se le siga viendo como soporte.

De acuerdo con lo planteado por Trinidad, la adopción de marcos de referencia como ITIL, ISO/IEC 20000 o CMMI-SVC ha demostrado ser un factor clave para mejorar la calidad de los servicios de TI, incrementar la satisfacción de los usuarios y optimizar los costos asociados. Sin embargo, estos beneficios no se logran de forma automática. Requieren una implementación que considere no solo procesos bien definidos, sino también aspectos humanos, como la motivación del personal, sus competencias y el nivel de compromiso con la mejora continua. En ese sentido, ITSM

funciona como un enlace entre la operación diaria de TI y los resultados que realmente importan a la organización, tales como la continuidad del servicio, los tiempos de respuesta o la percepción de calidad por parte de los usuarios.

Desde otra perspectiva, Harjanto y Aji (2024) abordan ITSM a partir de su relación con la gestión de activos de TI (ITAM), destacando que los recursos tecnológicos no existen de manera aislada, sino que están directamente vinculados a la prestación de servicios. En su estudio cualitativo desarrollado en una empresa de ciberseguridad, los autores evidencian que cuando los activos se gestionan bajo los principios de ITIL 4 y su enfoque de cadena de valor del servicio (Service Value Chain), se logra un mayor control sobre los costos, una reducción de riesgos operativos y una mejora en la reputación organizacional. Esto ocurre porque la organización es capaz de demostrar trazabilidad, cumplimiento y un uso responsable de sus recursos tecnológicos, algo que, aunque suene básico, no siempre se logra en entornos reales.

Figura 1. Componentes de la cadena de valor del servicio en el marco ITIL 4



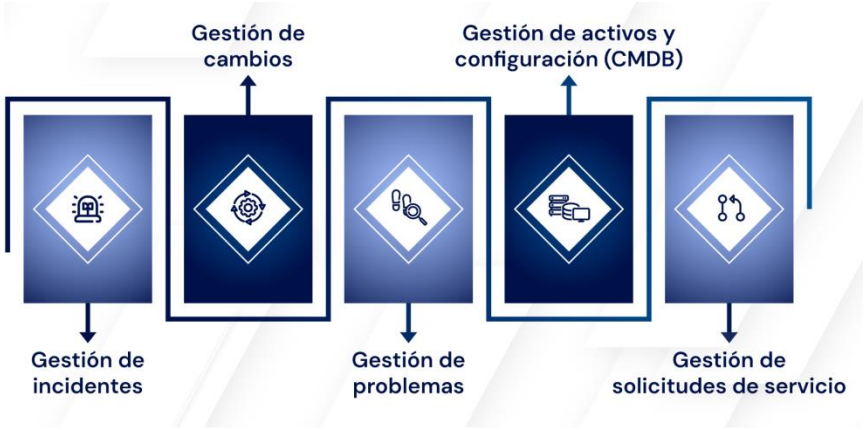

Nota: Obtenido de Harjanto y Aji (2024)

La relación entre ITSM y los procesos del negocio se vuelve aún más evidente cuando se analiza la evolución del marco ITIL hacia su versión más reciente. Según explica Agutter (2020), ITIL se mantiene como el referente más extendido en la gestión de servicios de TI, pero su enfoque ha cambiado de manera significativa, pasando de una visión centrada en procesos a un modelo basado en un sistema de valor que puede integrarse con otras prácticas de gestión. Este cambio no es menor, ya que implica dejar de ver a TI como un conjunto de actividades aisladas y empezar a

entenderla como parte de un sistema más amplio que genera valor para la organización.

Del mismo modo, Agutter (2020) también señala que el modelo operativo digital de ITIL 4 ha sido diseñado para apoyar a los equipos de TI en la creación, entrega y operación de productos y servicios que realmente se alineen con la estrategia del negocio. Esto sugiere que ITSM, cuando se interpreta desde ITIL 4, va más allá de un simple conjunto de procesos documentados; se trata más bien de una forma de estructurar y conectar flujos de valor entre TI y las distintas áreas de la organización. Dicho de otro modo, no es solo “cómo se hacen las cosas”, sino cómo esas actividades terminan generando resultados que sí importan, algo que en muchos casos todavía no se logra del todo en la práctica.

Figura 2. Estructura de prácticas de la gestión de servicios de TI en ITIL 4




Nota: Obtenido de Agutter (2020)

En el ámbito de la seguridad de la información, la literatura más reciente deja bastante claro que ya no es viable tratarla como un componente independiente de la gestión de servicios. En esa línea, Sekti (2025) plantea que la seguridad ha pasado a ser un elemento central dentro del ITSM, impulsado en gran medida por la creciente dependencia de las organizaciones respecto a la infraestructura digital. El autor enfatiza que principios como la confidencialidad, la integridad y la disponibilidad no deberían gestionarse de manera aislada, sino integrarse dentro del ciclo de vida de los servicios de TI. Esto implica articular la gestión de riesgos, la respuesta a incidentes, el cumplimiento normativo y los controles de seguridad como parte del

mismo sistema de gestión, y no como algo que se añade después cuando surgen problemas.

Siguiendo esa misma lógica, Sekti (2025) también propone un conjunto de estrategias orientadas a proteger los servicios de TI desde un enfoque más preventivo. Entre ellas se incluyen la implementación de controles proactivos, la evaluación constante de vulnerabilidades y la planificación de respuestas ante incidentes, siempre alineadas con los objetivos organizacionales y los requisitos regulatorios. Esta perspectiva resulta particularmente relevante en el contexto universitario, donde la gestión de incidentes no solo implica resolver fallas técnicas, sino también resguardar información sensible, como datos académicos, administrativos o de investigación, y asegurar la continuidad de servicios críticos. A veces se subestima este punto, pero la caída de un sistema de matrícula o de un aula virtual puede generar un impacto bastante serio en la operación institucional.

Por otro lado, Harjanto y Aji (2024) evidencian que ciertas prácticas específicas de ITSM, como la gestión de activos de TI (IT Asset Management) bajo ITIL 4, tienen efectos que van más allá de lo operativo. En su estudio, muestran que una adecuada gestión de activos no solo mejora el control financiero, sino que también fortalece la ciberseguridad, al reducir vulnerabilidades, asegurar la actualización de los sistemas y controlar el uso de licencias. Aunque su enfoque se centra en los activos, el razonamiento puede extenderse a otros procesos de ITSM, incluida la gestión de incidentes, ya que todos comparten el mismo marco conceptual y el mismo principio de alineación con los objetivos del negocio.

Estos aportes permiten entender que ITSM no se limita a la gestión de servicios desde una perspectiva operativa, sino que constituye un enfoque integral orientado a procesos, alineado con la estrategia organizacional e interconectado con la seguridad de la información. En la práctica, este enfoque se materializa principalmente a través de marcos como ITIL 4, que ofrecen una estructura flexible para integrar estos elementos, aunque su implementación completa todavía representa un reto en muchos entornos institucionales.

### 1.3.2. Enfoque de ITIL 4 en la gestión de servicios de tecnologías de la información

En la publicación *ITIL Foundation: ITIL 4 Edition* (Axelos, 2020), se presenta ITIL 4 como una evolución de las prácticas tradicionales de gestión de servicios, incorporando un cambio importante en la forma de entender cómo se genera valor. En este contexto, se introduce el concepto de **Service Value System (SVS)** como el eje central del modelo. El SVS no se limita a describir procesos, sino que integra principios guía, mecanismos de gobernanza, la cadena de valor del servicio, prácticas de gestión y la mejora continua. Según Axelos (2020), este sistema permite visualizar cómo todos los componentes de la organización se articulan para transformar la demanda en valor. En otras palabras, ya no se trata solo de ejecutar actividades, sino de entender cómo estas se conectan y contribuyen al resultado final, lo cual redefine la forma en que se concibe la gestión de servicios.

Desde una perspectiva más aplicada, Ferreira (2021) explica que ITIL 4 reorganiza la gestión de servicios de TI alrededor del SVS y de la **Service Value Chain (SVC)**, proponiendo una estructura más flexible y orientada al valor. El autor señala que este enfoque incorpora elementos clave como las cuatro dimensiones de la gestión de servicios, los principios guía y el conjunto de prácticas ITIL, lo que permite analizar de manera más integral la relación entre TI y el negocio. Esta visión resulta útil porque facilita no solo la implementación de prácticas como incident management, sino también la evaluación de variables como el valor percibido del servicio, el nivel de alineamiento estratégico o la madurez organizacional. En ese sentido, ITIL 4 no solo organiza procesos, sino que también ofrece una base conceptual para estudiar cómo los servicios de TI impactan en los resultados del negocio.

Por otro lado, Santosa y Mulyana (2023) muestran que ITIL 4 puede utilizarse más allá del ámbito operativo, específicamente como un marco conceptual para el diseño de arquitecturas de gestión de servicios. En su investigación, los autores desarrollan una arquitectura empresarial basada en ITIL 4 y el framework TOGAF, con el objetivo de estructurar la gestión de servicios en organizaciones de mediano y gran tamaño. Este enfoque permite organizar dominios como negocio, datos, aplicaciones y procesos bajo una lógica coherente, lo que facilita la construcción de artefactos como catálogos de servicios, modelos de datos o diagramas funcionales.

De esta manera, ITIL 4 no solo guía la operación diaria, sino que también sirve como base para el diseño estructural de sistemas de gestión de servicios que luego pueden ser evaluados o implementados en contextos reales.

### 1.3.3. La gestión de incidentes como práctica operativa en ITIL 4

Dentro del marco ITIL 4, la gestión de incidentes se considera una de las prácticas más relevantes a nivel operativo, ya que está directamente relacionada con la capacidad de mantener la continuidad del servicio. Según la guía oficial *ITIL 4 Practice Guide: Incident Management*, el propósito de esta práctica es “minimizar el impacto negativo de los incidentes mediante la restauración rápida de la operación del servicio a un nivel acordado” (Axelos, 2020). Esta definición deja entrever dos aspectos importantes: por un lado, que los incidentes son parte inevitable del funcionamiento de los servicios de TI, y por otro, que su tratamiento debe ser organizado y orientado a resultados. En este sentido, el valor no solo está en diseñar buenos servicios, sino en asegurar que estos sigan funcionando incluso cuando ocurren fallas.

En cuanto a su estructura, Axelos (2020) describe un conjunto de actividades que conforman el ciclo de vida del incidente, entre ellas la detección, registro, clasificación, priorización, diagnóstico, resolución y cierre. Estas etapas permiten mantener un control adecuado sobre cada incidente y asegurar que se gestione de acuerdo con su nivel de impacto. Además, ITIL 4 introduce la diferenciación entre incidentes comunes y **major incidents**, aquellos que afectan servicios críticos o a un gran número de usuarios. Para estos casos, se plantea la necesidad de roles específicos y mecanismos de coordinación más rigurosos. Esta distinción resulta especialmente relevante en el contexto universitario, donde la caída de un sistema clave puede tener consecuencias inmediatas en la operación académica.

Dzemydienė et al. (2024) aportan evidencia empírica que complementa este enfoque teórico, particularmente en entornos educativos. En su estudio, destacan que los servicios tecnológicos en instituciones académicas requieren altos niveles de disponibilidad debido a su rol en actividades de enseñanza, investigación y gestión administrativa. Las autoras señalan que la gestión de incidentes basada en ITIL 4 es fundamental para garantizar la continuidad de estos servicios (Dzemydienė et al.,

2024). Como parte de su propuesta, desarrollan un algoritmo que integra mecanismos de detección temprana, clasificación y priorización de incidentes, lo que permite al personal técnico diferenciar rápidamente entre eventos de distinta criticidad. Este tipo de enfoque demuestra que ITIL 4 puede adaptarse a contextos específicos mediante herramientas y reglas operativas concretas.

Un aspecto adicional que resalta en el trabajo de Dzemydienė et al. (2024) es la incorporación de automatización y soporte algorítmico en la gestión de incidentes. Las autoras sostienen que, en entornos con alta carga operativa, depender únicamente de la intervención manual puede resultar insuficiente, por lo que recomiendan el uso de herramientas inteligentes que permitan anticipar fallas y analizar patrones de comportamiento. Esta idea se alinea con lo planteado por Axelos (2020), quien destaca que la efectividad de la gestión de incidentes depende de la combinación de procesos definidos, personal capacitado y herramientas tecnológicas adecuadas. Es decir, no basta con tener un proceso bien diseñado si no se cuenta con los medios para ejecutarlo de manera eficiente.

Desde otra perspectiva, Nugroho y Fianty (2023) analizan la gestión de incidentes a partir de su nivel de madurez organizacional, utilizando un modelo de autoevaluación basado en ITIL. Su estudio evidencia que muchas organizaciones presentan deficiencias en aspectos como la documentación de procesos, la definición de niveles de servicio y la integración con otras prácticas como problem management. Estas limitaciones terminan afectando la eficiencia del servicio y generando tiempos de respuesta inconsistentes. Los autores concluyen que la aplicación de buenas prácticas de ITIL permite mejorar la integración de procesos, fortalecer el cumplimiento de acuerdos de nivel de servicio y aumentar la satisfacción de los usuarios. Aunque su análisis se basa en ITIL v3, los principios evaluados siguen siendo aplicables en ITIL 4, lo que facilita su adaptación a contextos como el de las universidades públicas.

### 1.3.4. Componentes estructurales de la gestión de incidentes en ITIL 4

De acuerdo con la guía oficial *ITIL®4 Practice Guide: Incident Management*, la gestión de incidentes no debe entenderse únicamente como una secuencia de actividades, sino como una práctica que se sostiene sobre una estructura más amplia e

interrelacionada. En este sentido, Axelos (2020) señala que dicha práctica se apoya en las cuatro dimensiones de la gestión de servicios: organización y personas, información y tecnología, socios y proveedores, y flujos de valor y procesos. Esta visión permite comprender que la gestión de incidentes no es un proceso aislado, sino un sistema donde intervienen distintos elementos que deben estar alineados. Como lo indica el propio Axelos (2020), se trata de una práctica fundamental cuya finalidad es restaurar el servicio en el menor tiempo posible, lo que impacta directamente en la satisfacción del usuario, la confianza en el proveedor y el valor generado.

Uno de los aspectos más claros en cuanto a la estructura de esta práctica se encuentra en la definición de sus entradas, actividades y salidas. Axelos (2020) describe que la gestión de incidentes se alimenta de múltiples fuentes de información, entre ellas datos de monitoreo, reportes de usuarios, información de configuración, inventarios de activos, catálogos de servicios, acuerdos de nivel de servicio (SLA) y registros previos de incidentes o problemas. A partir de estos insumos, se desarrollan actividades clave como la detección, el registro, la clasificación, el diagnóstico y la resolución. El proceso culmina con resultados concretos, como la restauración del servicio, la actualización de registros y la generación de información para la mejora continua. En conjunto, este flujo evidencia que la gestión de incidentes no solo resuelve problemas, sino que transforma información en conocimiento útil para la organización.

Adicionalmente, la guía introduce elementos estructurales más específicos que permiten estandarizar la gestión de incidentes. Entre ellos destacan los modelos de incidente, definidos como enfoques reutilizables para tratar incidentes recurrentes, lo que permite reducir tiempos de respuesta y evitar improvisaciones (Axelos, 2020). También se considera la gestión de incidentes mayores, que requieren una estructura organizativa distinta, incluyendo la asignación de un coordinador especializado, equipos dedicados y mecanismos de comunicación más estrictos. A esto se suman las denominadas *workarounds*, que permiten ofrecer soluciones temporales mientras se resuelve la causa raíz. Estos componentes evidencian que la práctica no solo se basa en actividades, sino en estructuras que facilitan su ejecución en distintos niveles de complejidad.

Desde una perspectiva aplicada, Dzemydienė et al. (2024) muestran cómo estos elementos pueden adaptarse a un entorno educativo. En su propuesta, destacan la necesidad de definir procedimientos claros, asignar responsables y utilizar herramientas tecnológicas que respalden la gestión de incidentes. Su modelo incorpora un enfoque algorítmico que integra detección temprana, clasificación y priorización, apoyado en sistemas de soporte a la decisión. Esto permite diferenciar entre eventos informativos e incidentes reales, optimizando el uso de los recursos disponibles. En este contexto, los elementos estructurales incluyen no solo procesos, sino también reglas de decisión, matrices de priorización y mecanismos formales de registro.

Las autoras también enfatizan que, en instituciones educativas, la continuidad de los servicios tecnológicos requiere una estructura sólida que combine roles, procesos y tecnología de manera coherente. Por ello, su propuesta integra componentes como el Service Desk, herramientas de monitoreo y repositorios de conocimiento, permitiendo detectar incidentes de forma automatizada, gestionarlos según su nivel de criticidad y documentarlos para su análisis posterior (Dzemydienė et al., 2024). Esta integración refleja lo planteado por Axelos (2020), quien indica que la gestión de incidentes se articula con distintas actividades de la cadena de valor del servicio, como *engage*, *deliver and support* o *improve*, y se relaciona con otras prácticas como *monitoring and event management* o *change enablement*.

Por otro lado, Ramadhan (2024) aporta una visión complementaria al analizar la gestión de incidentes desde la perspectiva de la formalización de procedimientos. En su estudio, basado en ITIL 4, se propone la descomposición del proceso en siete etapas, a partir de las cuales se diseñan procedimientos operativos estándar (SOP) para la atención de incidentes en un sistema de biblioteca digital. Además, el autor utiliza una matriz RACI para definir responsabilidades, lo que permite clarificar quién ejecuta, quién decide, quién apoya y quién debe ser informado en cada fase. Este enfoque evidencia que los elementos estructurales también incluyen mecanismos de gobernanza y documentación formal que facilitan la implementación del proceso.

El mismo estudio muestra que la incorporación de formularios, procedimientos documentados y mecanismos de evaluación contribuye a mejorar la capacidad de

gestión de incidentes (Ramadhan, 2024). Esto se alinea con el concepto de *Practice Success Factors* (PSF) propuesto por Axelos (2020), que agrupa los componentes necesarios para asegurar el éxito de la práctica. En el caso de Incident Management, estos factores incluyen la detección temprana de incidentes, su resolución eficiente y la mejora continua del proceso. En la práctica, estos factores integran personas, procesos, información y tecnología, funcionando como bloques que sostienen la efectividad del modelo.

A partir de lo expuesto, se puede afirmar que los componentes estructurales de la gestión de incidentes en ITIL 4 comprenden un conjunto articulado de elementos. En primer lugar, se identifican las entradas, que incluyen información proveniente de monitoreo, usuarios y sistemas de gestión. En segundo lugar, se reconoce un flujo de actividades claramente definido, que va desde la detección hasta el cierre del incidente. En tercer lugar, se generan salidas que aportan valor, como la restauración del servicio y el aprendizaje organizacional. A ello se suma una estructura organizativa con roles definidos, el uso de artefactos formales como modelos de incidente o SOP, y la presencia de factores de éxito que integran todos estos componentes. En conjunto, estos elementos permiten entender la gestión de incidentes no como un procedimiento aislado, sino como una práctica estructurada que sostiene la operación de los servicios de TI.

### 1.3.5. La mesa de ayuda como eje operativo en la gestión de incidentes de TI

Dentro del marco de gestión de servicios, la mesa de ayuda (service desk) se configura como un componente esencial para articular la atención de incidentes y solicitudes. Según la guía de ITIL 4 Foundation, su propósito principal es capturar y canalizar la demanda relacionada con incidentes y solicitudes de servicio (Axelos, 2020). En términos prácticos, esto significa que la mesa de ayuda actúa como el punto de entrada formal hacia los servicios de TI, concentrando la interacción con los usuarios, registrando los eventos reportados y coordinando la respuesta con los equipos técnicos. De esta manera, permite mantener un control centralizado sobre cómo se gestionan los problemas que afectan la operación de los servicios digitales.

Mahardika (2022) refuerza esta idea al describir la mesa de ayuda como el “single point of contact (SPOC)” entre el proveedor del servicio y el usuario, destacando su

función como puente de comunicación entre ambas partes. El autor explica que, a través del service desk, se registran y gestionan incidentes, solicitudes de servicio y requerimientos de acceso, además de servir como interfaz con otros procesos de la operación del servicio. Desde esta perspectiva, la mesa de ayuda no puede reducirse a un simple centro de atención técnica; más bien, constituye un servicio visible que define, en gran medida, la experiencia del usuario con el área de TI. Cuando esta función presenta fallas, el impacto se extiende a todo el modelo de gestión, ya que se pierde un punto confiable para organizar y priorizar la demanda.

En esa misma línea, Mahardika (2022) detalla que las funciones del service desk incluyen actividades como la recepción y registro de incidentes, su clasificación, la asignación de prioridades, el escalamiento cuando corresponde, la búsqueda de soluciones y la comunicación constante con los usuarios sobre el estado de sus solicitudes. Asimismo, debe interactuar con otras prácticas ITIL, como la gestión de problemas o cambios, y proporcionar información a la gerencia sobre el desempeño del servicio. Esto evidencia que la mesa de ayuda actúa como un habilitador organizacional, ya que traduce las buenas prácticas en acciones concretas, con responsables definidos, flujos de información claros y métricas que pueden ser evaluadas.

En el contexto de ITIL 4, la relevancia del service desk se amplía al integrarse dentro de la cadena de valor del servicio. Axelos (2020) señala que esta práctica participa en múltiples flujos de valor, especialmente en aquellos donde existe interacción directa con los usuarios. De este modo, contribuye a actividades como *engage* y *deliver and support*, asegurando que la comunicación sea efectiva y que los incidentes sean gestionados de manera consistente. En el caso de un modelo de gestión de incidentes aplicado a universidades, esto implica que la mesa de ayuda se convierte en el punto central desde el cual se gestionan incidencias relacionadas con sistemas académicos, plataformas virtuales o servicios administrativos.

Dzemydienė et.al. (2024) evidencian esta función en el ámbito educativo, señalando que la complejidad de las infraestructuras tecnológicas en las instituciones requiere un service desk centralizado que permita responder de manera eficiente a los incidentes. En su estudio, las autoras destacan que este componente integra

información proveniente de distintos sistemas, como plataformas de aprendizaje, repositorios documentales y servicios administrativos, facilitando la coordinación de la respuesta ante fallas. Sin este punto central, sostienen, resulta difícil mantener la continuidad de los servicios tecnológicos que soportan los procesos académicos.

Además, Dzemydienė et al. (2024) plantean un enfoque en el que la mesa de ayuda cumple un rol clave dentro de un algoritmo de gestión de incidentes. En este modelo, el service desk no solo recibe y registra información, sino que también participa en la clasificación, priorización y derivación de los incidentes hacia los equipos correspondientes. Esto confirma que la mesa de ayuda funciona como un habilitador tanto a nivel técnico como organizacional, ya que permite integrar los distintos componentes del proceso y evitar que la gestión de incidentes se realice de manera fragmentada o descoordinada.

### 1.3.6. Criterios de clasificación y priorización de incidentes en ITIL 4

Dentro de ITIL 4, la clasificación y priorización de incidentes se consideran elementos fundamentales para organizar la atención de los servicios de TI. Según la *ITIL 4 Incident Management Practice Guide*, antes de asignar una prioridad es necesario evaluar variables como el impacto y la urgencia, aunque estas por sí solas no constituyen la priorización (Axelos, 2020). En realidad, funcionan como insumos que permiten tomar decisiones más informadas sobre el orden de atención de los incidentes. La guía también plantea que los incidentes deben gestionarse dentro de un backlog compartido, donde la prioridad se define considerando el impacto en el negocio, los tiempos establecidos en los SLA y la disponibilidad de recursos.

Desde un enfoque aplicado, Dzemydienė et al. (2024) señalan que, en entornos educativos con infraestructuras tecnológicas complejas, resulta necesario desarrollar mecanismos que permitan gestionar los incidentes de acuerdo con niveles de prioridad claramente definidos. En su propuesta, los incidentes se clasifican inicialmente según el tipo de servicio o componente afectado, como servidores, redes o aplicaciones, y posteriormente se priorizan considerando la criticidad del servicio y el nivel de afectación a los usuarios. Este enfoque incorpora reglas de decisión que permiten diferenciar entre eventos informativos, incidentes menores y fallas críticas, facilitando una gestión más eficiente.

Otro aspecto relevante del modelo planteado por Dzemydienė et al. (2024) es el uso de herramientas tecnológicas que automatizan parte del proceso de clasificación y priorización. En su caso, emplean un sistema de gestión que permite registrar los incidentes, categorizarlos y asignarlos automáticamente al grupo técnico correspondiente. Esto reduce la carga operativa del personal y mejora la consistencia en la toma de decisiones, evitando que la priorización dependa exclusivamente del criterio individual.

Por su parte, Zahrothul Ain y Safitri (2023) abordan la problemática desde una perspectiva más tecnológica, destacando las limitaciones de los procesos manuales en la clasificación y priorización de incidentes. Las autoras señalan que la asignación incorrecta de categorías o prioridades puede generar retrasos en la atención y afectar la calidad del servicio. Para enfrentar este problema, proponen el uso de técnicas de *machine learning* que permitan automatizar la identificación de la categoría, el grupo responsable y el nivel de prioridad de cada incidente. Sus resultados muestran que es posible mejorar la precisión en la clasificación y acelerar la toma de decisiones, lo que contribuye a una gestión más eficiente y alineada con las prácticas de ITIL (Zahrothul Ain & Safitri, 2023).

### 1.3.7. Mecanismos de escalamiento en la gestión de incidentes de TI

El escalamiento puede entenderse como el mecanismo formal mediante el cual un incidente es transferido a otro nivel de atención cuando no puede resolverse con los recursos o capacidades disponibles en el nivel inicial. En el marco de ITIL 4, esta práctica resulta clave para asegurar el cumplimiento de los niveles de servicio, ya que permite mantener la continuidad operativa frente a situaciones que superan la capacidad de respuesta inmediata. Como señala Axelos (2020), la finalidad de la gestión de incidentes es reducir al mínimo el impacto negativo mediante la restauración rápida del servicio, lo cual requiere procesos claros de asignación, reasignación y coordinación entre distintos niveles de soporte. En la práctica, esta rapidez difícilmente se logra sin una estructura de escalamiento bien definida.

El escalamiento funcional representa el mecanismo más habitual en la operación diaria de los servicios de TI. Consiste en transferir el incidente a un nivel de soporte con mayor especialización técnica, como cuando un incidente pasa del service desk

a un equipo de segundo o tercer nivel. Sembina et al. (2022) ilustran este enfoque mediante un modelo de tres niveles basado en ITIL, donde los incidentes simples son atendidos en primera línea, los más complejos se derivan a niveles intermedios y los críticos son gestionados por equipos especializados. A través de simulaciones y modelado de procesos, los autores evidencian que esta estructura mejora significativamente el cumplimiento de los acuerdos de nivel de servicio, incrementando la tasa de resolución dentro del SLA. Este resultado sugiere que una adecuada definición de niveles de soporte no solo ordena el trabajo, sino que también impacta directamente en la eficiencia del servicio.

Por otro lado, el escalamiento jerárquico responde a una lógica distinta, ya que no se centra en la capacidad técnica, sino en la necesidad de tomar decisiones a nivel organizacional. Este tipo de escalamiento se activa cuando el incidente tiene un alto impacto en el negocio, compromete servicios críticos o requiere autorizaciones especiales. Kanellopoulos (2024), en su estudio sobre respuesta a incidentes en el sector marítimo, muestra cómo los protocolos de escalamiento jerárquico permiten involucrar a la alta dirección en la toma de decisiones estratégicas, como la suspensión de operaciones o la notificación a entidades externas. El autor advierte que, sin este tipo de escalamiento, las organizaciones tienden a reaccionar con lentitud ante incidentes críticos, lo que incrementa los riesgos y prolonga los tiempos de recuperación.

Desde la perspectiva de ITIL 4, ambos tipos de escalamiento se integran dentro de los flujos de valor del servicio, formando parte del diseño operativo de la gestión de incidentes. Axelos (2020) señala que los incidentes deben ser gestionados en función de su tipo y nivel de impacto, lo que implica definir rutas de escalamiento tanto funcional como jerárquico. En este sentido, el estudio de Sembina et al. (2022) puede interpretarse como una validación práctica de este enfoque, al demostrar que la claridad en los criterios de escalamiento contribuye a reducir tiempos de resolución y mejorar la disponibilidad de los servicios.

De manera complementaria, la literatura en ciberseguridad refuerza la importancia del escalamiento jerárquico como un componente esencial de la resiliencia organizacional. Kanellopoulos (2024) plantea que los planes de respuesta efectivos

combinan roles claramente definidos, protocolos de escalamiento y ejercicios de simulación que permiten a la organización actuar de manera coordinada frente a incidentes complejos. Esta lógica es trasladable al ámbito de los servicios de TI, donde el escalamiento funcional asegura que los incidentes sean atendidos por personal capacitado, mientras que el escalamiento jerárquico garantiza que las decisiones críticas se tomen en el momento oportuno.

### 1.3.8. Indicadores y métricas para la evaluación de la gestión de incidentes

Las métricas y los indicadores constituyen el principal medio para evaluar el desempeño de los procesos de gestión de incidentes, permitiendo transformar la operación en información medible y analizable. En este contexto, Cadena et al. (2020) destacan que, ante el incremento de amenazas y vulnerabilidades, el uso adecuado de métricas se vuelve fundamental para gestionar incidentes y proteger los activos de información. En su estudio, los autores clasifican los indicadores en función de dimensiones como costo, calidad y tiempo de servicio, y los relacionan con estándares internacionales como ISO 27004 y NIST 800-55. Esto evidencia que la medición no se limita a contar incidentes, sino a evaluar la eficacia y eficiencia del proceso en su conjunto.

En la misma línea, Cadena et al. (2020) retoman un principio ampliamente difundido en la gestión de servicios: aquello que no se define no puede medirse, y lo que no se mide difícilmente puede mejorarse. Aplicado a la gestión de incidentes en ITIL 4, este principio implica que la organización debe establecer con claridad conceptos como tiempo de respuesta, nivel de impacto o esfuerzo de recuperación. Sin estas definiciones, resulta complicado evaluar el desempeño del proceso o justificar decisiones relacionadas con la asignación de recursos. El estudio propone además una tipificación de métricas que incluye indicadores de detección, respuesta, costos y resiliencia, los cuales pueden integrarse en sistemas de monitoreo y control.

Un ejemplo aplicado de este enfoque se presenta en el trabajo de Najjarpour et al. (2025), quienes diseñan un panel de control para la gestión de servicios de TI en hospitales docentes. En su propuesta, se estructuran más de cien indicadores distribuidos en diferentes áreas, como hardware, software, redes y sistemas de información. Los autores explican que estos indicadores se basan en marcos como

ITIL y COBIT, lo que permite alinear la medición con estándares reconocidos. El panel desarrollado facilita el monitoreo en tiempo real, la generación de reportes y el soporte a la toma de decisiones, tanto a nivel operativo como estratégico.

Aunque el estudio de Najjarpour et al. (2025) se desarrolla en el sector salud, sus aportes resultan plenamente aplicables al contexto universitario. En ambos casos, los servicios de TI son críticos para la operación institucional y requieren un seguimiento constante. El estudio demuestra que la implementación de un sistema estructurado de indicadores permite identificar tendencias, detectar problemas recurrentes y evaluar el cumplimiento de los niveles de servicio. En ese sentido, un modelo de gestión de incidentes que no incorpore métricas claras corre el riesgo de quedarse en un plano teórico, mientras que un sistema de indicadores alineado con ITIL 4 facilita la mejora continua y la toma de decisiones basada en evidencia.

## 1.4. Categorías de análisis de la investigación

La denominación “Categorías de análisis de la investigación” resulta más coherente con el enfoque cualitativo adoptado en el estudio, debido a que la investigación no se orientó a medir variables mediante indicadores cuantificables ni a establecer relaciones estadísticas entre ellas, como ocurre en los enfoques cuantitativos. El propósito de la investigación fue comprender, interpretar y analizar las prácticas actuales de gestión de incidentes de tecnologías de la información en las universidades públicas de la región Amazonas, así como diseñar un modelo basado en ITIL 4 adaptado a dicho contexto institucional. En este sentido, el análisis se desarrolló a partir de categorías temáticas y aspectos interpretativos relacionados con procesos, roles, prácticas operativas y componentes organizativos, los cuales fueron estudiados mediante entrevistas, revisión documental y análisis comparativo.

No se utilizó el término “operacionalización de variables” para no generar inconsistencia metodológica con la naturaleza cualitativa y propositiva del estudio, mientras que la expresión “categorías de análisis” representa de manera más adecuada la lógica interpretativa y descriptiva empleada durante el desarrollo de la investigación.

### 1.4.1. Definición conceptual de las categorías de análisis

**Categoría de análisis 1: Gestión actual de incidentes de tecnologías de la información en las universidades públicas de la región Amazonas**

Esta categoría de análisis comprende las prácticas, procedimientos, mecanismos de atención y formas organizativas actualmente utilizadas por las universidades públicas de la región Amazonas para gestionar incidentes relacionados con los servicios de tecnologías de la información. Incluye la manera en que los incidentes son detectados, reportados, registrados, clasificados, atendidos y resueltos dentro de las áreas responsables de soporte tecnológico.

Asimismo, esta categoría considera los actores involucrados, los canales de comunicación utilizados, los criterios aplicados para priorizar incidentes y los mecanismos existentes para el escalamiento y seguimiento de los casos reportados. Desde una perspectiva cualitativa, permite comprender cómo se desarrolla realmente la gestión de incidentes en el contexto institucional, identificando fortalezas, limitaciones operativas y brechas respecto a las buenas prácticas propuestas por ITIL 4.

**Categoría de análisis 2: Modelo de gestión de incidentes de TI basado en ITIL 4**

Esta categoría corresponde a la propuesta de un modelo estructurado de gestión de incidentes fundamentado en las buenas prácticas de ITIL 4 y adaptado al contexto operativo y organizacional de las universidades públicas de la región Amazonas. El modelo integra componentes organizativos y operativos orientados a mejorar la continuidad, trazabilidad y calidad de los servicios de TI.

Dentro de esta categoría se consideran aspectos relacionados con la implementación de una Mesa de Ayuda como Punto Único de Contacto, la definición de roles y niveles de soporte, los procedimientos de registro, clasificación, priorización, escalamiento, resolución y cierre de incidentes, así como la incorporación de métricas, mecanismos de comunicación y gestión del conocimiento institucional. La categoría también comprende los elementos orientados a la mejora continua y la validación técnica del modelo mediante juicio de expertos.

### 1.4.2. Estructuración operativa de las categorías de análisis

**Categoría de análisis 1: Gestión actual de incidentes de tecnologías de la información en las universidades públicas de la región Amazonas**

La presente categoría fue abordada mediante el análisis cualitativo de las prácticas y procesos utilizados actualmente para la gestión de incidentes de tecnologías de la información en las universidades públicas estudiadas. Para ello, se emplearon técnicas como la revisión documental, las entrevistas semiestructuradas y el análisis comparativo de procesos vinculados a la atención de incidentes de TI.

La información recopilada permitió identificar la forma en que se ejecutaban actividades relacionadas con el registro, clasificación, priorización, escalamiento, resolución y cierre de incidentes, así como las limitaciones organizativas y operativas existentes. Posteriormente, estas prácticas fueron contrastadas con los lineamientos y recomendaciones establecidos por ITIL 4, permitiendo reconocer brechas, debilidades y oportunidades de mejora en la gestión institucional de incidentes.

**Categoría de análisis 2: Modelo de gestión de incidentes de TI basado en ITIL 4**

Esta categoría se desarrolló a través del diseño estructurado de un modelo de gestión de incidentes alineado con las buenas prácticas de ITIL 4 y contextualizado a la realidad de las universidades públicas de la región Amazonas. Su construcción comprendió el diseño de componentes organizativos y funcionales necesarios para fortalecer la atención y control de incidentes de TI.

El desarrollo de esta categoría incluyó la definición de flujos operativos, criterios de clasificación y priorización, mecanismos de escalamiento funcional y jerárquico, establecimiento de roles y niveles de soporte, implementación conceptual de una Mesa de Ayuda y diseño de mecanismos de gestión del conocimiento y métricas de desempeño.

Finalmente, el modelo propuesto fue sometido a un proceso de validación mediante juicio de expertos especializados en gestión de servicios de TI, ITIL 4 y seguridad de la información, quienes evaluaron la cobertura del modelo, su comprensibilidad, consistencia interna y pertinencia institucional.

Tabla 1. Estructuración operativa de las categorías de análisis de la investigación

| Categoría de análisis | Subcategorías de análisis | Aspectos específicos analizados | Técnicas de recojo de información | Instrumentos utilizados |
|---|---|---|---|---|
| Diagnóstico de la gestión actual de incidentes de TI | Registro y atención de incidentes | Forma de recepción de incidentes, documentación existente, tiempos de atención, trazabilidad y seguimiento | Entrevista semiestructurada y revisión documental | Guía de entrevista y matriz documental |
| | Clasificación y priorización | Criterios utilizados para categorizar incidentes, definición de prioridades, manejo de incidentes críticos | Entrevista y análisis comparativo | Guía de entrevista y matriz de análisis ITIL 4 |
| | Escalamiento y resolución | Procedimientos de derivación, niveles de soporte existentes, resolución de incidentes recurrentes y críticos | Entrevista y revisión documental | Guía de entrevista y ficha documental |
| | Cierre y seguimiento | Validación con usuarios, documentación de soluciones, control post-incidente y reaperturas | Entrevista | Guía de entrevista |
| | Gestión del conocimiento | Uso de manuales, procedimientos, repositorios técnicos y reutilización del conocimiento | Entrevista y revisión documental | Guía de entrevista y matriz documental |
| | Gestión de métricas | Existencia de indicadores, seguimiento de SLA, tiempos de resolución y reportes operativos | Revisión documental y entrevista | Matriz documental y guía de entrevista |
| | Comunicación con usuarios | Mecanismos de comunicación institucional, notificaciones y atención al usuario | Entrevista | Guía de entrevista |
| Análisis organizativo de la gestión de incidentes | Estructura organizacional de TI | Organización de la OTI, distribución de responsabilidades y soporte técnico | Revisión documental y entrevista | Matriz documental y guía de entrevista |
| | Roles y responsabilidades | Funciones del personal técnico, responsables de procesos y niveles de soporte | Entrevista | Guía de entrevista |

| | | | | |
|---|---|---|---|---|
| | Recursos tecnológicos y operativos | Herramientas ITSM, infraestructura tecnológica, sistemas institucionales y recursos de soporte | Revisión documental | Ficha de análisis documental |
| Evaluación comparativa con ITIL 4 | Gestión de incidentes según ITIL 4 | Correspondencia entre prácticas institucionales y lineamientos de ITIL 4 | Análisis comparativo documental | Matriz comparativa ITIL 4 |
| | Mesa de Ayuda y Punto Único de Contacto | Existencia de SPOC, canales de atención y centralización de incidentes | Revisión documental y entrevista | Matriz comparativa y guía de entrevista |
| | Escalamiento funcional y jerárquico | Coherencia de los flujos de escalamiento con ITIL 4 | Análisis documental | Matriz comparativa ITIL 4 |
| | Gestión del conocimiento y mejora continua | Uso de base de conocimientos y mecanismos de aprendizaje organizacional | Revisión documental | Matriz comparativa |
| Diseño del modelo de gestión de incidentes | Componentes estructurales del modelo | Diseño de la Mesa de Ayuda, roles, niveles de soporte, métricas y base de conocimientos | Análisis documental y modelamiento | Matriz de diseño del modelo |
| | Componentes funcionales del modelo | Registro, clasificación, priorización, escalamiento, resolución y cierre de incidentes | Modelamiento de procesos | Diagramas BPMN y matrices operativas |
| | Flujos operativos del proceso | Secuencia operativa de atención de incidentes y articulación entre niveles de soporte | Modelamiento de procesos | Diagramas BPMN |
| | Gestión de incidentes mayores | Declaración, atención, comunicación y seguimiento de incidentes críticos | Análisis comparativo y modelamiento | Matriz de incidentes mayores |
| | Gestión del conocimiento institucional | Estructura y utilización de la base de conocimientos | Diseño documental | Matriz de contenidos KB |
| Validación del modelo propuesto | Cobertura del modelo | Nivel en que el modelo integra los componentes necesarios para la gestión de incidentes | Juicio de expertos | Instrumento de validación |

| | | | | |
|---|---|---|---|---|
| | Comprensibilidad | Claridad de los flujos, roles, procedimientos y documentación | Juicio de expertos | Instrumento de validación |
| | Consistencia interna | Coherencia entre componentes organizativos, operativos y lineamientos ITIL 4 | Juicio de expertos | Instrumento de validación |
| | Pertinencia institucional | Adaptación del modelo a las necesidades y condiciones de las universidades analizadas | Juicio de expertos | Instrumento de validación |

# DISEÑO METODOLÓGICO

## 2.1. Enfoque de la investigación

La investigación presentó un enfoque cualitativo, debido a que buscó comprender y analizar la forma en que se gestionaban los incidentes de tecnologías de la información en las universidades públicas estudiadas, Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (UNTRM) y en la Universidad Nacional Intercultural Fabiola Salazar Leguía de Bagua (UNIFSLB), identificando limitaciones operativas, organizativas y funcionales para posteriormente diseñar una propuesta basada en ITIL 4.

## 2.2. Tipo de investigación

La investigación fue de tipo aplicada, porque se orientó al diseño de una propuesta de solución frente a una problemática identificada en la gestión de incidentes de TI.

## 2.3. Diseño de la investigación

El diseño fue descriptivo–propositivo, debido a que inicialmente se analizó la situación actual de la gestión de incidentes y posteriormente se desarrolló un modelo de gestión basado en ITIL 4 adaptado al contexto universitario.

El estudio no se orientó a manipular variables ni a realizar experimentación, sino a analizar prácticas existentes, revisar documentación institucional y contrastar estos hallazgos con las buenas prácticas de ITIL 4.

## 2.4. Método de la investigación

El método principal utilizado fue el analítico–documental, el cual permitió examinar de manera detallada los procesos actuales de gestión de incidentes en la UNTRM y la UNIFSLB, identificando sus principales limitaciones y puntos críticos. Este análisis se complementó con un enfoque comparativo, mediante el cual se contrastaron las prácticas observadas con los lineamientos propuestos por ITIL 4, específicamente en la práctica de Incident Management.

Asimismo, se incorporó el método de validación por expertos, dado que el modelo propuesto no solo debía ser coherente desde el punto de vista teórico, sino también

viable en la práctica. A través de este método, se recogieron valoraciones especializadas que permitieron ajustar y fortalecer la propuesta final.

## 2.5. Población y muestra

Los participantes de la investigación estuvieron conformados por personal relacionado con la gestión y soporte de los servicios de tecnologías de la información en las universidades públicas de la región Amazonas consideradas en el estudio, específicamente en las áreas responsables de las operaciones tecnológicas y soporte institucional. Se incluyó personal técnico y administrativo vinculado a la atención, seguimiento y resolución de incidentes de TI, debido a que poseen experiencia directa sobre el funcionamiento real de los procesos tecnológicos institucionales.

En coherencia con el enfoque cualitativo de la investigación, la selección de participantes se realizó mediante un criterio intencional, priorizando a aquellos actores que contaban con conocimiento, experiencia y participación activa en la gestión de incidentes y en la operación de servicios tecnológicos críticos. Esta selección permitió obtener información contextual, detallada y pertinente sobre las prácticas utilizadas, las limitaciones existentes y las necesidades operativas de las instituciones analizadas.

Asimismo, participaron especialistas externos en calidad de evaluadores del modelo propuesto. La selección de estos expertos se efectuó mediante muestreo intencional, considerando criterios como experiencia profesional en gestión de servicios de TI, ITIL 4, seguridad de la información y gestión de procesos tecnológicos. La participación de estos especialistas permitió realizar la validación técnica y metodológica del modelo diseñado, fortaleciendo su pertinencia y coherencia respecto a las buenas prácticas internacionales.

## 2.6. Técnicas e instrumentos de recolección de información

Las técnicas empleadas permitieron recopilar información cualitativa y documental necesaria para comprender la situación actual y sustentar la propuesta del modelo. Estas técnicas se aplicaron de manera complementaria, lo que permitió triangular la información y obtener una visión más completa del problema.

### 2.6.1. Entrevista semiestructurada

La entrevista semiestructurada fue la técnica principal para recoger información directa sobre la gestión de incidentes en la UNTRM y la UNIFSLB. A través de esta técnica se exploraron las percepciones del personal de TI respecto a cómo se registran los incidentes, qué criterios se utilizan para clasificarlos y priorizarlos, cómo se realiza el escalamiento y cuáles son las principales dificultades en la atención.

El instrumento utilizado fue una guía de preguntas abiertas (Ver Anexo 1), organizada en función de los componentes del proceso de gestión de incidentes. Las entrevistas se dirigieron a personal técnico y administrativo involucrado en el soporte de TI, lo que permitió obtener información de la realidad operativa de la gestión de incidentes. En algunos casos, las respuestas evidenciaron diferencias entre lo que se supone que debería hacerse y lo que realmente ocurre en la práctica.

### 2.6.2. Revisión documental

Con el propósito de evaluar el nivel de formalización de la gestión de incidentes, se realizó una revisión documental detallada en ambas universidades. Esta técnica permitió analizar documentos institucionales como manuales de funciones, lineamientos de TI, registros de incidentes, reportes de soporte, catálogos de servicios y cualquier otra evidencia relacionada con la gestión tecnológica.

La guía de revisión documental (Ver Anexo 2) se orientó a identificar si existían políticas y procedimientos formales, si se habían definido roles y responsabilidades, si se realizaba seguimiento de los incidentes y si las herramientas utilizadas permitían registrar y controlar adecuadamente la información. Este análisis permitió identificar vacíos importantes, tanto a nivel normativo como operativo, que sustentaron la necesidad de proponer un modelo más estructurado.

### 2.6.3. Matriz comparativa ITIL 4 vs situación actual

Como parte del análisis, se elaboró una matriz comparativa entre los elementos clave de ITIL 4 Incident Management y la situación observada en la UNTRM y la UNIFSLB (Ver Anexo 3). Esta matriz permitió identificar de manera más ordenada las brechas existentes, tales como la falta de criterios formales de priorización, debilidades en el

registro de incidentes, ausencia de rutas claras de escalamiento y limitada utilización de métricas.

El uso de esta herramienta fue importante porque ayudó a estructurar el diagnóstico y, al mismo tiempo, sirvió como base para definir los componentes que debía incluir el modelo propuesto.

### 2.6.4. Instrumento de juicio de expertos

Una vez diseñado el modelo de gestión de incidentes basado en ITIL 4, se procedió a su validación mediante la técnica de juicio de expertos. Para ello, se utilizó una matriz de evaluación (Ver Anexo 4) que permitió analizar la propuesta desde diferentes criterios.

a. La suficiencia permitió verificar si el modelo incluía los elementos necesarios, tanto funcionales como estructurales, para una adecuada gestión de incidentes.
b. La claridad evaluó qué tan comprensible resultaba el modelo en términos de su estructura, diagramas y descripciones.
c. La coherencia analizó la consistencia interna del modelo y su alineación con las buenas prácticas de ITIL 4.
d. La relevancia permitió determinar si el modelo respondía a las necesidades reales de la UNTRM y la UNIFSLB.

El instrumento utilizó una escala de valoración de 1 a 5, donde 1 representaba un nivel muy bajo y 5 un nivel muy alto. Además, se incluyó un espacio para observaciones cualitativas, lo que permitió recoger sugerencias que ayudaron a mejorar la versión final del modelo.

### 2.6.5. Procedimiento de análisis de la información

La información obtenida mediante entrevistas semiestructuradas, revisión documental y análisis comparativo fue procesada mediante un análisis temático de contenido. Inicialmente, la información recopilada fue organizada según las categorías de análisis definidas en la investigación, tales como registro de incidentes, priorización, escalamiento, roles de soporte y gestión del conocimiento.

Posteriormente, se identificaron patrones, coincidencias, debilidades y prácticas recurrentes presentes en las universidades analizadas. Estos hallazgos fueron contrastados con las buenas prácticas propuestas por ITIL 4, permitiendo reconocer brechas funcionales y organizativas en la gestión actual de incidentes.

Finalmente, los resultados fueron interpretados de manera descriptiva y analítica, estableciendo relaciones entre las necesidades identificadas y los componentes propuestos en el modelo de gestión de incidentes.

### 2.6.6. Validez y consistencia de los instrumentos cualitativos

Los instrumentos utilizados en la investigación fueron elaborados y adaptados tomando como referencia las buenas prácticas propuestas por ITIL 4 para la gestión de incidentes de tecnologías de la información, así como los objetivos y categorías de análisis definidos en la investigación. Su construcción se orientó a recopilar información relacionada con los procesos reales de atención de incidentes, los mecanismos de escalamiento, la organización del soporte y las prácticas de gestión de servicios presentes en las universidades estudiadas.

Asimismo, se aplicó triangulación de fuentes mediante el uso complementario de entrevistas, revisión documental y análisis comparativo con las recomendaciones de ITIL 4, con la finalidad de fortalecer la consistencia interpretativa de los hallazgos obtenidos.

La definición de las categorías de análisis y de los instrumentos de recopilación de información mantuvo correspondencia con los objetivos de investigación y con los fundamentos teóricos del estudio, asegurando coherencia entre el problema investigado, el proceso de análisis y el diseño del modelo propuesto.

# RESULTADOS DE LA INVESTIGACIÓN

## 3.1. Análisis diagnóstico de la gestión de tecnologías de la información

### 3.1.1. Análisis diagnóstico de la gestión de tecnologías de la información en la UNTRM

En la UNTRM, el documento más importante hallado para entender la función TIC es el Reglamento de Organización y Funciones (ROF) 2025. Allí se define a la Oficina de Tecnologías de la Información como órgano de apoyo dependiente del Rectorado, responsable de gestionar y administrar integralmente las tecnologías de la información. Además, sus funciones incluyen formular y evaluar el Plan Estratégico de Tecnologías de Información (PETI), implementar el Plan de Gobierno Digital, administrar licencias de software, promover la automatización y digitalización de procesos, administrar infraestructura y red de datos, gestionar seguridad de la información, brindar soporte tecnológico y gestionar riesgos asociados a sistemas, infraestructura y servicios TI. Este ROF es clave porque muestra que, al menos en el plano normativo, la universidad sí reconoce casi todos los componentes que luego se relacionan con una gestión formal de incidentes: planeamiento, infraestructura, seguridad, soporte, continuidad y riesgo.

Otro documento encontrado es el Mapa de Procesos Institucional 2025. En ese documento, la gestión de TI aparece como el proceso de soporte *S04. Gestión de Tecnología de la Información, cuyo objetivo es "proporcionar y mantener soluciones tecnológicas seguras, innovadoras y sostenibles" para fortalecer la gestión institucional, mejorar servicios académicos y administrativos y promover la transformación digital*. El mismo mapa lista como productos de ese proceso cosas bastante concretas: estaciones de trabajo habilitadas, backup de información, mantenimiento preventivo y correctivo, aplicaciones desarrolladas, portal web actualizado y plan de gobierno digital. Eso demuestra que en la UNTRM la función TIC no está pensada solo como soporte reactivo, sino como un proceso institucional con entregables reconocidos. Sin embargo, el mismo mapa no hace visible un subproceso explícito de gestión de incidentes. Esto significa que la gestión de TI está reconocida, pero no necesariamente desagregada en prácticas operativas especializadas.

El Manual de Organigrama Estructural 2025 confirma además que la Oficina de Tecnologías de la Información ocupa un lugar de segundo nivel organizacional dentro de los órganos de administración interna. Esto es relevante porque le da una posición formal relativamente fuerte dentro de la estructura universitaria y la ubica cerca de otros órganos clave para la modernización, como planeamiento, calidad y secretaría general. Esta ubicación es favorable para implementar un modelo de gestión de incidentes, porque facilita articulación con procesos académicos, administrativos y de gobierno. Aun así, el organigrama no muestra subunidades internas especializadas dentro de la OTI; eso podría traducirse en una concentración funcional mayor y, probablemente, en menor separación entre gobierno TI, infraestructura, soporte y desarrollo.

También se encontró el PEI 2023-2030 de la UNTRM. En este documento aparece como acción estratégica la idea de “Plan de Gobierno Digital implementado para la comunidad universitaria”, lo que muestra que la transformación digital sí está incorporada al planeamiento institucional. Sin embargo, no se cuenta todavía con el Plan de Gobierno Digital ni con el PETI. Esta situación no permite realizar la trazabilidad de las acciones relacionadas con la gestión de las TIC o analizar la formalidad de los procesos.

### 3.1.2. Análisis diagnóstico de la gestión de tecnologías de la información en la UNIFSLB

En la UNIFSLB, la documentación revisada deja ver una estructura TIC más desagregada. El ROF y el organigrama muestran a la Oficina de Tecnologías de la Información con cuatro unidades internas: Unidad de Gobierno y Tecnologías de la Información, Unidad de Infraestructura, Redes y Comunicaciones, Unidad de Desarrollo de Software y Unidad de Soporte Técnico Informático. Esta estructura sugiere una separación funcional más madura entre gobierno TI, infraestructura, desarrollo y soporte. Desde el punto de vista de gestión de incidentes, eso facilitaría definir niveles de atención, escalamiento funcional y responsabilidades diferenciadas, algo que suele ser difícil cuando todo recae en una sola oficina sin subdivisiones visibles.

La UNIFSLB también tiene un documento explícito de Plan de Gobierno Digital 2023-2025, aprobado por resolución de comisión organizadora en julio de 2023. El documento se vincula al Decreto Legislativo 1412 y muestra que la universidad ya viene organizando su gobernanza digital mediante comité y plan específico. Esto significa que se cuenta con un instrumento concreto de planificación digital, no solo una mención dentro del ROF o del PEI, interpretándose como una señal de mayor madurez en la formalización del direccionamiento digital, al menos a nivel documental.

De la revisión de los documentos de seguimiento del POI y en los resultados vinculados al PEI, aparece de forma reiterada la acción estratégica *AEI.04.06: "Gobierno Digital implementado para la comunidad universitaria"*. Además, el POI 2025 y su seguimiento muestran actividades concretas ejecutadas por la OTI, como mantenimiento preventivo de impresoras y fotocopiadoras, y también se recupera la elaboración de documentos como la política de redes. Esto da a entender que el gobierno digital en la UNIFSLB se traduce en actividades operativas y documentos de soporte. Esta situación es relevante porque acerca la planeación TIC a la operación diaria, donde se producen y atienden los incidentes.

Otro hallazgo importante es la Resolución Presidencial N.° 264-2025-UNIFSLB, relacionada con el Plan de Implementación de GLPI para la gestión eficiente del inventario de activos tecnológicos. El documento indica que la implementación de GLPI permitiría mejorar la trazabilidad de los equipos, el control centralizado de incidencias y la eficiencia en los procesos de gestión de activos, y además precisa que el plan contiene acciones, cronograma y recursos para optimizar la administración y control de activos tecnológicos. Se entiende que el GLPI no solo sirve para inventario, sino también como una plataforma usada para mesa de ayuda y gestión de tickets. Esto es evidencia concreta de que la UNIFSLB apunta a un modelo formal de incident management.

También se encontró una serie de documentos formales relacionados con el uso de TI en los procedimientos institucionales. La directiva para formular y aprobar reglamentos, directivas y planes establece que, una vez aprobados, los documentos deben remitirse a la Oficina de Tecnologías de la Información para su publicación,

lo que le da a la OTI un papel operativo en la difusión normativa institucional. A esto se suma una directiva de mesa de partes virtual, que le asigna a la OTI la responsabilidad de asegurar la disponibilidad, integridad y disponibilidad de la información. Esto relaciona a la OTI con funciones de seguridad y continuidad informacional en los servicios digitales que brinda la universidad.

Tabla 2. Comparación analítica de la documentación institucional en relación con la gestión de incidentes de TI

| Categoría de documento | Información esperada | Hallazgos UNTRM | Hallazgos UNIFSLB |
|---|---|---|---|
| **Procedimientos de TI** | Existencia de un procedimiento formal documentado para la gestión de incidentes que detalle etapas, responsables y flujo de atención | - No se identifica un procedimiento formal de gestión de incidentes.<br>- No se evidencian fases definidas ni flujos estructurados de atención.<br>- No se describen mecanismos de escalamiento ni cierre formal.<br>- La atención de incidentes parece depender de prácticas operativas no documentadas.<br>- Se evidencia una ausencia significativa de formalización del proceso. | - No se identifica un procedimiento formal específico de gestión de incidentes.<br>- No se describen fases ni flujos completos del proceso. Sin embargo, la existencia de unidades diferenciadas (soporte, infraestructura, desarrollo) sugiere una base organizativa que podría facilitar su implementación.<br>- La gestión sigue siendo mayormente reactiva, aunque con mejores condiciones estructurales que la UNTRM. |
| **MOF / ROF / Plan de Gobierno Digital** | Definición de funciones, responsabilidades y roles vinculados a la gestión de servicios TI y atención a usuarios | - El ROF define funciones amplias de la OTI: soporte, seguridad, infraestructura y planeamiento.<br>- No se asignan roles específicos para la gestión de incidentes.<br>- No existe diferenciación de niveles de soporte.<br>- Las funciones están definidas de forma general, no operativa. | - Se identifican roles más desagregados dentro de la OTI (gobierno TI, soporte, infraestructura, desarrollo).<br>- Existe Plan de Gobierno Digital formalizado. Sin embargo, los roles no están definidos específicamente para incident managemen.<br>- No se establecen responsabilidades claras para registro, priorización o seguimiento de incidentes. |
| **Reglamentos o lineamientos de TI** | Presencia de criterios operativos para la atención de incidentes: categorización, niveles de prioridad, tiempos de respuesta y protocolos | - No se identifican lineamientos específicos para la gestión de incidentes.<br>- No existen criterios de clasificación ni priorización.<br>- No se definen tiempos de atención ni escalamiento.<br>- Los documentos se enfocan en objetivos generales de TI y seguridad. | - -No se identifican lineamientos específicos de incident management.<br>- Existen documentos vinculados a gobierno digital y políticas de red.<br>- No se traducen en criterios operativos como impacto, urgencia o SLA.<br>- No hay protocolos formales de escalamiento o priorización. |
| **Registros o evidencias operativas de incidentes** | Existencia de reportes estructurados que evidencien tipos de incidentes, frecuencia, tiempos de atención y resolución | - No se encontró un registro formal de incidentes.<br>- Los incidentes se infieren de manera indirecta (fallas de red, sistemas, energía, seguridad).<br>- No existe trazabilidad ni historial documentado.<br>- No se evidencian tiempos de respuesta ni cierres formales. | - No se identifica un repositorio formal de incidentes.<br>- Se evidencian problemas operativos similares (infraestructura, sistemas, conectividad).<br>- La futura implementación de GLPI sugiere intención de formalizar el registro.<br>- Actualmente no hay trazabilidad estructurada ni métricas de atención. |
| **Herramientas tecnológicas de soporte TI** | Uso de plataformas para gestión de tickets, monitoreo de infraestructura y repositorios de conocimiento técnico | - No se evidencia uso de herramientas ITSM o sistemas de tickets.<br>- El monitoreo es básico, asociado a infraestructura (firewall, red).<br>- No existe base de conocimiento formal.<br>- La gestión depende principalmente de recursos técnicos sin integración de soporte. | - Se identifica la implementación planificada de GLPI como herramienta de gestión de activos e incidencias.<br>- Esto representa un avance hacia un sistema ITSM.<br>- Aún no se evidencia un uso consolidado de base de conocimiento.<br>- El monitoreo sigue siendo limitado, pero con potencial de mejora. |

## 3.2. Evaluación de la gestión actual de incidentes de TI

### 3.2.1. Evaluación de la gestión actual de incidentes de TI en la UNTRM desde la perspectiva de los responsables de TI

Como parte del trabajo de campo, se llevaron a cabo entrevistas semiestructuradas dirigidas a personal clave de la Oficina de Tecnologías de la Información (OTI) de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas. La primera se realizó con el responsable de la administración de la infraestructura tecnológica (red institucional, conectividad, servidores y seguridad perimetral), mientras que la segunda estuvo orientada a la responsable de la gestión y operación de los sistemas académicos y administrativos, entre ellos el sistema de matrícula, aulas virtuales, sistemas de gestión académica y plataformas administrativas.

A partir del análisis conjunto de ambas entrevistas, fue posible identificar cómo se viene gestionando, en la práctica, la atención de incidentes de TI en la UNTRM, evidenciando una serie de debilidades que permiten entender mejor la necesidad de un modelo formal basado en ITIL 4.

**a. Incidentes frecuentes**

Respecto a los incidentes más frecuentes, los entrevistados coincidieron en que los problemas más recurrentes están asociados a la conectividad de red, fallas en equipos de comunicación y caídas intermitentes de los sistemas académicos, especialmente en periodos críticos como matrícula o evaluaciones. El responsable de infraestructura señaló que existen tramos de red que ya presentan desgaste y switches que operan al límite de su capacidad, lo que provoca interrupciones parciales en distintas áreas. Por su parte, la responsable de aplicaciones indicó que el acceso a plataformas como el aula virtual o el sistema académico suele degradarse cuando hay alta concurrencia, lo que genera múltiples reportes simultáneos de usuarios.

**b. Detección de incidentes**

En relación con la detección de incidentes, se observó que ésta se realiza principalmente de forma reactiva. Es decir, la mayoría de incidentes se identifican cuando los usuarios reportan el problema. No se cuenta con herramientas de

monitoreo proactivo que permitan anticipar fallas o generar alertas tempranas. En algunos casos, el área de infraestructura logra identificar caídas de servicios mediante revisiones manuales, pero esto no forma parte de un sistema estructurado.

**c. Registro de incidentes**

Respecto al registro de incidentes, ambos entrevistados coincidieron en que no existe un mecanismo centralizado ni formal. Los incidentes suelen comunicarse por llamadas telefónicas, mensajes de WhatsApp o correos electrónicos, y en muchos casos no quedan registrados. Algunos técnicos llevan sus propios apuntes o archivos personales, pero no existe un repositorio institucional que permita hacer seguimiento o análisis histórico. Esto limita seriamente la trazabilidad de los incidentes y dificulta la identificación de patrones o problemas recurrentes.

**d. Procedimiento para la gestión de incidentes**

En cuanto a la existencia de un procedimiento formal, se confirmó que no hay un documento aprobado que establezca cómo se deben gestionar los incidentes. La atención depende en gran medida de la experiencia del personal y de la urgencia percibida en cada caso. Esto podría generar variabilidad en la forma de atención, ya que cada técnico aplica su propio criterio, lo que a veces funciona… pero otras veces termina generando demoras o soluciones temporales.

**e. Punto único de contacto**

Un aspecto crítico identificado fue la ausencia de un punto único de contacto (Service Desk). No existe una mesa de ayuda como tal. Los usuarios suelen contactar directamente a los técnicos que conocen, lo que provoca una atención dispersa y poco controlada. En palabras de uno de los entrevistados, “hay días en que llegan problemas por todos lados y no hay forma de ordenarlos”. Esta situación también genera duplicidad de reportes y, en algunos casos, incidentes que no son atendidos oportunamente.

**f. Asignación de los incidentes**

Sobre la asignación de incidentes, se evidenció que esta no sigue un esquema estructurado. El incidente es atendido por quien lo recibe inicialmente, incluso si no

es el más adecuado para resolverlo. En ocasiones se deriva a otro técnico, pero sin un flujo definido. Esto refleja la ausencia de una estructura basada en niveles de soporte, lo cual coincide con lo observado en la práctica.

**g. Niveles de soporte**

Al consultar sobre los niveles de soporte, los entrevistados indicaron que no están formalmente definidos. Existe una diferenciación implícita basada en la experiencia del personal, pero no hay una clasificación clara (nivel 1, nivel 2, nivel 3) ni roles establecidos para cada tipo de incidente. Esto limita la eficiencia en la atención y genera sobrecarga en ciertos técnicos.

**h. Clasificación y priorización de los incidentes**

En cuanto a la clasificación y priorización, se confirmó que no se utilizan criterios formales. Los incidentes se atienden en función de la urgencia percibida o de la presión de los usuarios afectados. Por ejemplo, los problemas en matrícula o sistemas académicos suelen recibir atención inmediata, pero no porque exista una matriz de impacto y urgencia definida, sino por la importancia evidente del proceso. Esto implica que la priorización es subjetiva y puede variar según el contexto.

**i. Escalonamiento de los incidentes**

Respecto al escalamiento, se identificó que el escalamiento funcional ocurre de manera informal cuando un técnico reconoce que no puede resolver el problema y busca apoyo en otro colega. Sin embargo, no existen rutas definidas ni tiempos establecidos. En cuanto al escalamiento jerárquico, este solo se activa en situaciones críticas, generalmente cuando autoridades académicas intervienen, pero sin un protocolo claro que regule este proceso.

**j. Herramientas para la gestión de incidentes**

En relación con las herramientas utilizadas, se evidenció la ausencia de plataformas ITSM. No se utiliza un sistema de tickets ni herramientas integradas para la gestión de incidentes. El monitoreo de infraestructura se realiza mediante funciones básicas de los equipos de red, pero sin una visión centralizada. Sin embargo, se mencionó

la intención de implementar herramientas como GLPI en el futuro, lo que podría representar un avance importante.

**k. Base de conocimientos**

Otro aspecto relevante es que no existe una base de conocimiento. Las soluciones a incidentes no se documentan de manera sistemática, por lo que el conocimiento queda en la experiencia individual del personal. Esto podría generar dependencia de ciertos técnicos y dificulta la estandarización de la atención.

**l. Cierre de los incidentes**

En cuanto al cierre de incidentes, no se identificó un proceso formal. En muchos casos, el incidente se considera resuelto cuando el usuario deja de reportar el problema, pero no se realiza una validación estructurada ni se registra el cierre. Esto afecta la calidad del servicio y la confiabilidad de la información.

**m. Métricas e indicadores para la gestión de incidentes**

Tampoco se evidenció el uso de métricas o indicadores. No se miden tiempos de atención, resolución ni niveles de servicio, lo que impide evaluar el desempeño del proceso o identificar oportunidades de mejora.

**n. Otras debilidades**

Finalmente, los entrevistados coincidieron en señalar diversas limitaciones estructurales, entre ellas: infraestructura tecnológica con componentes obsoletos, problemas eléctricos recurrentes, falta de herramientas especializadas, ausencia de procedimientos y una carga operativa elevada. También se mencionaron incidentes relacionados con seguridad de la información, como intentos de acceso no autorizado, los cuales se gestionan de forma aislada, sin integración con un proceso formal de gestión de incidentes.

En conjunto, los hallazgos permiten concluir que la gestión de incidentes en la UNTRM se desarrolla bajo un enfoque predominantemente reactivo, con baja formalización, limitada trazabilidad y sin alineación con las buenas prácticas de ITIL 4. Esta situación evidencia una brecha importante que justifica plenamente el

desarrollo de un modelo estructurado que permita organizar, estandarizar y mejorar la atención de incidentes en la universidad.

### 3.2.2. Evaluación de la gestión actual de incidentes de TI en la UNIFSLB desde la perspectiva de los responsables de TI

En el caso de la Universidad Nacional Intercultural Fabiola Salazar Leguía de Bagua (UNIFSLB), se realizaron entrevistas a dos actores clave: el responsable de soporte e infraestructura tecnológica y el encargado de los sistemas académicos y administrativos. A diferencia de la UNTRM, se percibió una ligera intención de organización en algunos procesos, aunque todavía sin una formalización clara ni alineación con estándares como ITIL 4.

#### a. Incidentes frecuentes

Los entrevistados indicaron que los problemas más comunes están asociados a la conectividad en sedes descentralizadas, fallas en el acceso al sistema académico institucional, denominado *Sistema Integrado de Gestión Académico Universitario (SIGAU)*, y dificultades en el uso del aula virtual basada en Moodle, especialmente en zonas donde la conectividad es limitada. También se mencionaron incidentes recurrentes en el sistema de biblioteca digital y en los servicios de autenticación de usuarios (Active Directory), lo que afecta el acceso a múltiples plataformas institucionales.

#### b. Detección de incidentes

Se evidenció que, al igual que en la UNTRM, esta ocurre mayormente cuando los usuarios reportan fallas. Sin embargo, el responsable de infraestructura mencionó que se realizan revisiones periódicas del estado de los servidores mediante herramientas básicas como paneles del sistema operativo y verificaciones manuales del firewall. Aun así, no existe un sistema automatizado de monitoreo ni generación de alertas, lo que limita la capacidad de anticiparse a fallas críticas.

#### c. Registro de incidentes

Si bien actualmente no existe un sistema institucional plenamente implementado, se mencionó que se encuentra en proceso de adopción una herramienta como GLPI

para la gestión de incidencias. Mientras tanto, los incidentes se registran de -forma parcial en hojas de cálculo compartidas y correos electrónicos. Esto podría generar cierta trazabilidad, aunque incompleta, ya que muchos incidentes menores no son registrados.

**d. Procedimiento para la gestión de incidentes**

Los entrevistados señalaron que no existe un documento aprobado que regule la gestión de incidentes. No obstante, indicaron que internamente manejan ciertas "pautas de trabajo" no documentadas, especialmente en el área de soporte. Estas pautas dependen de la experiencia del personal y no están estandarizadas, lo que genera diferencias en la forma de atención entre técnicos.

**e. Punto único de contacto**

Se indicó que existe un correo institucional destinado al soporte técnico (soporte@unifslb.edu.pe), pero su uso no es generalizado. Muchos usuarios continúan reportando incidentes por canales informales como llamadas o mensajes directos. Esto podría generar una situación híbrida donde existe un canal formal, pero no es reconocido ni utilizado como único medio oficial.

**f. Asignación de los incidentes**

Se observó que existe cierta intención de organización, ya que los incidentes registrados en los archivos compartidos suelen asignarse al técnico disponible. Sin embargo, no hay un sistema automatizado ni reglas claras de asignación. En algunos casos, los incidentes quedan pendientes si no se realiza seguimiento manual, lo que evidencia debilidades en la gestión del flujo de trabajo.

**g. Niveles de soporte**

Se identificó que existe una separación funcional entre el área de soporte técnico, infraestructura y desarrollo de sistemas. Sin embargo, esta división no está formalizada como niveles de soporte (nivel 1, 2, 3). En la práctica, los incidentes escalan hacia personal con mayor conocimiento, pero sin una estructura definida ni tiempos establecidos.

**h. Clasificación y priorización de los incidentes**

Los entrevistados indicaron que no existe una taxonomía formal. Sin embargo, mencionaron que de manera empírica diferencian entre incidentes “urgentes” y “no urgentes”, priorizando aquellos que afectan servicios académicos como el SIGAU o el aula virtual. Aun así, no se utilizan matrices de impacto y urgencia, lo que hace que la priorización sea subjetiva y variable.

**i. Escalonamiento de los incidentes**

Se observó que el escalamiento funcional ocurre de manera más frecuente que en la UNTRM, debido a la existencia de equipos diferenciados. No obstante, este proceso no está documentado. El escalamiento jerárquico se presenta únicamente en casos críticos, como caídas del sistema académico durante procesos de matrícula, donde intervienen autoridades académicas. Sin embargo, no existe un protocolo formal para estos casos.

**j. Herramientas para la gestión de incidentes**

Se evidenció un avance incipiente con la intención de implementar GLPI, lo que representa una oportunidad importante. Actualmente, el monitoreo de servidores se realiza de forma manual y no existe una integración de herramientas que permita una gestión centralizada de incidentes.

**k. Base de conocimientos**

En cuanto a la documentación de soluciones, los entrevistados indicaron que algunas soluciones se comparten entre técnicos de manera informal, pero no existe una base de conocimiento estructurada. Esto podría generar dependencia del conocimiento individual y dificulta la estandarización.

**l. Cierre de los incidentes**

Se indicó que no existe un procedimiento formal. En algunos casos se confirma con el usuario si el problema fue resuelto, pero esto no se documenta. En otros casos, simplemente se asume que el incidente ha sido solucionado.

**m. Métricas e indicadores para la gestión de incidentes**

Se evidenció que no se generan indicadores formales. No se mide el tiempo de resolución ni la cantidad de incidentes atendidos, lo que limita la capacidad de evaluar el desempeño del área de TI.

**n. Otras debilidades**

Se identificaron limitaciones importantes, entre ellas: conectividad limitada en zonas interculturales, dependencia de infraestructura externa, falta de herramientas especializadas, ausencia de procedimientos formalizados y limitada capacitación en marcos de referencia como ITIL. También se mencionaron incidentes relacionados con seguridad, como accesos indebidos o configuraciones vulnerables, que no se gestionan dentro de un proceso integrado.

## 3.3. Análisis de las limitaciones en la gestión de incidentes de TI en los servicios académicos y administrativos

### 3.3.1. Análisis de las limitaciones en la gestión de incidentes de TI en los servicios académicos y administrativos de la UNTRM

Los procesos académicos y administrativos de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (UNTRM) dependen de manera directa de diversos servicios tecnológicos que soportan su operación diaria. Entre los principales se identifican:

- Para el ámbito académico: el Sistema Integrado de Gestión Académica (SIGA-UNTRM), la plataforma de Aula Virtual basada en Moodle, el Sistema de Gestión de Investigación (SGI-UNTRM) para el registro de tesis y proyectos, el servicio de verificación de similitud académica (Turnitin), la Biblioteca Virtual institucional, el Repositorio Institucional Amazónico (RIA-UNTRM) y el correo institucional;
- En el ámbito administrativo: el Sistema Integrado de Administración Financiera (SIAF), así como los sistemas internos de tesorería, contabilidad, logística y gestión de planillas.

Adicionalmente, la universidad en su sede de Bagua Chica cuenta aproximadamente con entre 450 y 500 terminales de trabajo (computadoras de

escritorio y laptops), distribuidas entre laboratorios de las carreras de Ingeniería de Sistemas, Ingeniería Mecánica Eléctrica, Ingeniería en Ciberseguridad e Ingeniería Mecatrónica, así como oficinas administrativas y dependencias académicas.
Se identificaron una serie de debilidades tanto a nivel estructural como operativo, las cuales afectan la continuidad, calidad y seguridad de los servicios de TI que soportan estos procesos.

**a. Ausencia de un proceso formal de gestión de incidentes**

Se evidenció que la universidad no cuenta con un procedimiento institucional documentado que regule el registro, tratamiento y cierre de incidentes de TI. Esta situación genera:

- Una gestión predominantemente reactiva, sin capacidad de anticipación.
- Atención desorganizada, basada en comunicación informal (llamadas, mensajes o contacto directo).
- Falta de trazabilidad, lo que impide identificar incidentes recurrentes.
- Imposibilidad de evaluar el desempeño del área, debido a la ausencia de indicadores.

Esta debilidad afecta directamente procesos críticos como matrícula, registro de notas, gestión de investigación y trámites administrativos, los cuales dependen de la disponibilidad de plataformas tecnológicas.

**b. Limitaciones en la infraestructura tecnológica y su mantenimiento**

El análisis de la infraestructura tecnológica evidenció condiciones que incrementan el riesgo de fallas operativas:

- Equipos de red (switches y enlaces de fibra) con signos de desgaste o capacidad limitada.
- Segmentos de red con cableado estructurado deteriorado, especialmente en laboratorios.
- Configuraciones en el firewall que no han sido completamente optimizadas.

- Servidores instalados en ambientes con condiciones térmicas no siempre adecuadas.
- Sistemas de respaldo energético (UPS) con capacidad reducida frente a cortes prolongados.

Estas condiciones afectan la disponibilidad de servicios académicos y los sistemas administrativos, especialmente en momentos de alta demanda.

**c. Problemas recurrentes en terminales de trabajo (usuarios finales)**

Uno de los aspectos más críticos identificados está relacionado con los equipos de usuario final:

- Algunas computadoras con bajo rendimiento debido a hardware desactualizado (memoria RAM insuficiente, discos mecánicos).
- Sistemas operativos no estandarizados o con configuraciones inconsistentes.
- Equipos sin mantenimiento preventivo periódico.
- Instalación de software no autorizado que genera conflictos o vulnerabilidades.
- Fallas frecuentes en laboratorios (equipos que no encienden, lentitud, errores de sistema).

Esto podría generar que los usuarios experimenten problemas como:

- Dificultad para acceder al SIGA-UNTRM o al aula virtual.
- Lentitud al cargar aplicaciones académicas.
- Pérdida de sesiones o bloqueos inesperados.

En muchos casos, los incidentes reportados por usuarios no son fallas del sistema central, sino problemas locales en sus equipos, lo que complica el diagnóstico.

**d. Deficiencias en la red de datos y comunicaciones**

Se identificaron problemas importantes en la red institucional:

- Cobertura irregular de la red inalámbrica en algunas facultades.

- Saturación del ancho de banda en horarios pico.
- Latencia elevada en accesos simultáneos a plataformas.
- Pérdida intermitente de conectividad en laboratorios.

Además, en sedes o ambientes con alta densidad de usuarios, la red presenta caídas parciales que afectan el desarrollo normal de clases y actividades académicas.

Estas condiciones generan:

- Interrupciones en el uso del aula virtual.
- Dificultad para acceder a sistemas en tiempo real.
- Retrasos en procesos administrativos.

**e. Problemas de acceso a sistemas y bases de datos**

Se evidenciaron inconsistencias en el acceso a los sistemas institucionales:

- Caídas del SIGA-UNTRM durante procesos de matrícula o registro de notas.
- Lentitud en consultas a bases de datos, especialmente en horarios de alta demanda.
- Errores de autenticación en usuarios (credenciales no sincronizadas).
- Accesos denegados por configuraciones inconsistentes en permisos.

Estos problemas generan malestar en los usuarios y afectan directamente la continuidad de los procesos académicos.

**f. Debilidades en la seguridad de la información**

Se identificaron diversas vulnerabilidades que pueden comprometer la integridad y confidencialidad de la información institucional:

- Uso de contraseñas poco robustas y ausencia de políticas de gestión de accesos.
- Equipos con protección antivirus desactualizada.
- Configuraciones de red con niveles de exposición innecesarios.

- Falta de un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente implementado.

Estas debilidades representan un riesgo para activos críticos como los registros académicos, los proyectos de investigación almacenados en el SGI-UNTRM y los datos personales de estudiantes y docentes.

**g. Problemas en la continuidad operativa (energía y climatización)**

La operación de los servicios tecnológicos se ve afectada por condiciones físicas del entorno:

- Fluctuaciones de energía eléctrica que generan interrupciones inesperadas.
- Sistemas de climatización insuficientes para garantizar condiciones estables en la sala de servidores.

Esto puede ocasionar reinicios no planificados, degradación del hardware y caídas de servicios clave, afectando directamente la continuidad de los procesos académicos y administrativos.

**h. Carencia de herramientas especializadas para la gestión de incidentes**

Se constató que la UNTRM no dispone de herramientas formales para la gestión de incidentes, tales como:

- Sistemas de gestión de tickets.
- Plataformas de mesa de ayuda (Service Desk).
- Sistemas de monitoreo centralizado.
- Repositorios de conocimiento técnico.

La ausencia de estas herramientas limita la capacidad de organización del trabajo, el seguimiento de incidentes y la mejora continua del servicio.

**i. Alta dependencia de sistemas académicos críticos**

Los procesos académicos dependen en gran medida de plataformas como el SIGA-UNTRM y el aula virtual. Durante el análisis se evidenció que:

- Estos sistemas presentan caídas o degradación bajo alta carga.
- Existen problemas de conectividad que afectan el acceso en momentos clave.
- Se generan inconsistencias en la información debido a consultas o configuraciones inadecuadas.

Esto impacta directamente en la matrícula, evaluación académica y gestión docente, generando retrasos y malestar en la comunidad universitaria.

**j. Dependencia del conocimiento individual del personal técnico**

Se identificó que la gestión de incidentes depende en gran medida de la experiencia individual de los técnicos:

- No existen procedimientos estandarizados.
- La asignación de incidentes no considera especialización.
- Las soluciones no se documentan de manera sistemática.

Esto podría generar inconsistencias en la atención, riesgo ante rotación de personal y dificultades para mejorar los procesos.

**k. Falta de definición de roles y niveles de soporte**

No se evidenció una estructura formal de niveles de soporte. La organización actual no distingue claramente entre:

- Atención inicial de incidentes.
- Soporte técnico especializado.
- Responsables de servicios críticos.

Esto provoca sobrecarga en determinados técnicos y retrasos en la resolución de incidentes.

**l. Escalamiento no estructurado**

El escalamiento de incidentes se realiza de manera informal:

- Se deriva a otro técnico cuando el problema supera la capacidad inicial.
- No existen criterios definidos para escalar incidentes críticos.
- La intervención de niveles jerárquicos ocurre solo en situaciones de presión institucional.

Esto incrementa el riesgo en incidentes de alto impacto y limita la capacidad de respuesta organizada.

**m. Ausencia de monitoreo preventivo**

Finalmente, se evidenció que no existen mecanismos de monitoreo proactivo que permitan anticipar fallas en la infraestructura:

- No se detectan oportunamente caídas de red o saturación de recursos.
- No se monitorean condiciones críticas como temperatura o uso de servidores.
- No se identifican intentos de intrusión de forma sistemática.

Esto mantiene a la organización en un estado reactivo frente a los incidentes.

Con las observaciones identificadas, se elaboró la tabla resumen de los resultados del diagnóstico de la gestión de incidentes de TI en la UNTRM en base a los hallazgos, la misma que se muestra a continuación:

Tabla 3. Matriz de contraste entre ITIL 4 y la situación actual de la gestión de incidentes de TI en la UNTRM

| **Componente de ITIL 4** | **Referencia en ITIL 4** | **Situación observada en UNTRM (causas y efectos)** | **Solución propuesta basada en ITIL 4** | **Nivel de brecha** |
|---|---|---|---|---|
| Registro de incidencias | Todo incidente debe registrarse en un sistema centralizado y estructurado. | **Causa:** No existe sistema de registro. **Efecto:** Pérdida de trazabilidad, repetición de incidentes, imposibilidad de análisis. | Implementación de herramienta ITSM con registro obligatorio de tickets. | No implementado |
| Punto único de contacto (Service Desk) | Centraliza la comunicación con usuarios y controla el ciclo de vida del incidente. | **Causa:** Múltiples canales informales (WhatsApp, llamadas). **Efecto:** Desorden, duplicidad de incidentes, pérdida de solicitudes. | Implementar mesa de ayuda institucional (SPOC) con canales formales. | Inexistente |
| Categorización de incidentes | Clasificación estructurada por tipo, categoría y subcategoría. | **Causa:** No hay taxonomía definida. **Efecto:** Dificultad para analizar tendencias y asignar recursos. | Definir catálogo de categorías de incidentes alineado a servicios TI. | Ausente |
| Priorización de incidentes | Basada en impacto y urgencia. | **Causa:** Priorización subjetiva. **Efecto:** Incidentes críticos no siempre atendidos primero. | Implementar matriz impacto–urgencia con niveles de prioridad. | Inexistente |
| Estructura de niveles de soporte | Definición de niveles 1, 2 y 3 con funciones claras. | **Causa:** No existe estructura formal. **Efecto:** Sobrecarga de técnicos y atención ineficiente. | Definir niveles de soporte y roles asociados. | No definido |
| Escalamiento técnico (funcional) | Derivación a niveles especializados según complejidad. | **Causa:** Escalamiento informal. **Efecto:** Retrasos en resolución y mala asignación. | Definir flujos de escalamiento técnico por tipo de incidente. | Ausente |
| Escalamiento organizacional (jerárquico) | Escalamiento a niveles de decisión para incidentes críticos. | **Causa:** Solo ocurre por presión externa. **Efecto:** Respuesta tardía ante incidentes mayores. | Definir protocolo de incidentes críticos (Major Incident). | Inexistente |
| Gestión de la resolución | Documentación de soluciones para reutilización. | **Causa:** No se documentan soluciones. **Efecto:** Dependencia del conocimiento individual. | Implementar base de conocimiento institucional. | Ausente |
| Cierre de incidentes | Validación con usuario y registro formal del cierre. | **Causa:** No hay proceso de cierre. **Efecto:** Incidentes no | Establecer procedimiento formal de cierre con validación. | No implementado |

| Componente de ITIL 4 | Referencia en ITIL 4 | Situación observada en UNTRM (causas y efectos) | Solución propuesta basada en ITIL 4 | Nivel de brecha |
|---|---|---|---|---|
| | | verificados, baja calidad del servicio. | | |
| Monitoreo y gestión de alertas | Detección proactiva mediante herramientas. | **Causa:** Monitoreo manual limitado.<br>**Efecto:** Incidentes detectados tardíamente. | Implementar herramientas de monitoreo (red, servidores, servicios). | Bajo |
| Herramientas ITSM | Plataforma integrada para gestión de incidentes. | **Causa:** No existen herramientas especializadas.<br>**Efecto:** Gestión manual, desorganizada. | Implementar GLPI u otra herramienta ITSM. | Ausente |
| Indicadores de desempeño | Métricas como MTTR, SLA, incidentes recurrentes. | **Causa:** No se mide el proceso.<br>**Efecto:** No hay mejora continua ni control de calidad. | Definir KPIs y panel de control de incidentes. | Inexistente |
| Definición de roles | Roles claros documentados en la organización. | **Causa:** Roles genéricos no operativos.<br>**Efecto:** Confusión en responsabilidades. | Definir roles específicos (Service Desk, soporte, coordinador). | Difuso |
| Formalización del proceso | Procedimiento documentado y aprobado. | **Causa:** No existe proceso formal.<br>**Efecto:** Variabilidad en la atención. | Documentar proceso completo de incident management. | Ausente |
| Gestión de incidentes de seguridad | Integración con seguridad de la información. | **Causa:** Gestión aislada de incidentes de seguridad.<br>**Efecto:** Riesgo alto de vulneraciones. | Integrar incident management con seguridad (SGSI). | Inexistente |
| Gestión de terminales de usuario final | ITIL sugiere control de activos y soporte al usuario. | **Causa:** Equipos obsoletos, sin mantenimiento.<br>**Efecto:** Lentitud, fallas, incidentes frecuentes. | Implementar gestión de activos (ITAM) y mantenimiento preventivo. | Deficiente |
| Gestión de red y conectividad | ITIL integra monitoring y capacity management. | **Causa:** Saturación, cableado deteriorado.<br>**Efecto:** Caídas de red y servicios. | Implementar monitoreo, segmentación y mejora de red. | Bajo |
| Gestión de acceso a sistemas | Control de accesos y disponibilidad del servicio. | **Causa:** Problemas de autenticación y BD.<br>**Efecto:** Usuarios sin acceso a sistemas críticos. | Integrar gestión de identidades y control de accesos. | Limitado |

### 3.3.2. Análisis de las limitaciones en la gestión de incidentes de TI en los servicios académicos y administrativos de la UNIFSLB

En la UNIFSLB, los servicios tecnológicos que soportan los procesos académicos y administrativos se articulan principalmente a través del Sistema Integrado de Gestión Académico Universitario (SIGAU-UNIFSLB), la plataforma de Aula Virtual (Moodle), el Sistema de Biblioteca Digital, el repositorio institucional, el correo institucional, así como los sistemas administrativos vinculados al SIAF, logística y recursos humanos.

A nivel de infraestructura, la universidad cuenta con una cantidad estimada de entre 200 y 350 terminales de trabajo, distribuidas en oficinas administrativas, laboratorios de cómputo y espacios académicos. Sin embargo, debido a su ubicación geográfica y condiciones de conectividad, presenta particularidades que influyen directamente en la gestión de incidentes.

Del análisis documental y entrevistas realizadas, se identificaron una serie de debilidades tanto a nivel estructural como operativo en la Universidad Nacional Intercultural Fabiola Salazar Leguía de Bagua (UNIFSLB), las cuales afectan la continuidad, calidad y seguridad de los servicios de TI que soportan los procesos académicos y administrativos.

**a. Ausencia de un proceso formal de gestión de incidentes**

Se evidenció que la universidad no cuenta con un procedimiento institucional formalmente aprobado que regule el registro, tratamiento y cierre de incidentes de TI. Si bien existen algunas prácticas internas, estas no están documentadas ni estandarizadas. Esto podría generar:

- Una gestión parcialmente organizada, pero no consistente entre áreas.
- Atención basada en criterios individuales del personal técnico.
- Registros incompletos o dispersos de incidentes.
- Dificultad para generar indicadores o reportes confiables.

Esta situación impacta directamente en procesos críticos como matrícula en el Sistema Integrado de Gestión Académico Universitario (SIGAU-UNIFSLB), el uso del aula virtual y los servicios administrativos.

**b. Limitaciones en la infraestructura tecnológica y su mantenimiento**

El análisis evidenció que la infraestructura tecnológica presenta restricciones importantes:

- Equipos de red con capacidad limitada para soportar crecimiento de usuarios.
- Dependencia de enlaces de conectividad con variabilidad en la calidad del servicio.
- Configuraciones de red y firewall no completamente optimizadas.
- Servidores con recursos limitados frente a demandas crecientes.
- Sistemas de respaldo energético con cobertura parcial.

Estas condiciones afectan la disponibilidad de servicios como el SIGAU, Moodle y sistemas administrativos, especialmente en horarios de alta demanda.

**c. Problemas recurrentes en terminales de trabajo (usuarios finales)**

Se identificaron problemas frecuentes en los equipos de usuario final, estimados entre 200 y 350 terminales distribuidos en laboratorios, oficinas y áreas académicas:

- Equipos con configuraciones heterogéneas (distintos sistemas operativos y versiones).
- Varios laboratorios con computadoras con bajo rendimiento en laboratorios académicos.
- Falta de mantenimiento preventivo periódico. No se cuenta con un plan de mantenimiento preventivo
- En varias terminales se encontraron el uso de software no estandarizado.

- Fallas recurrentes en equipos compartidos por estudiantes.

Esto podría generar:

- Dificultades para acceder al SIGAU o al aula virtual.
- Lentitud en el uso de plataformas académicas.
- Interrupciones durante clases o evaluaciones.

En muchos casos, los incidentes reportados tienen origen en el equipo del usuario y no en el sistema central, lo que dificulta su diagnóstico.

**d. Deficiencias en la red de datos y comunicaciones**

Uno de los aspectos más críticos en la UNIFSLB está relacionado con la conectividad:

- Cobertura inalámbrica irregular en distintos ambientes.
- Limitaciones de ancho de banda, especialmente en sedes alejadas.
- Latencia elevada en accesos a plataformas institucionales.
- Caídas intermitentes de red en laboratorios y oficinas.

Estas condiciones generan:

- Interrupciones en el uso del aula virtual.
- Problemas para acceder a plataformas académicas en tiempo real.
- Retrasos en actividades administrativas y académicas.

Este problema se ve acentuado por el contexto geográfico y la dispersión de usuarios.

**e. Problemas de acceso a sistemas y bases de datos**

Se evidenciaron inconsistencias en el acceso a los sistemas institucionales:

- Lentitud en el SIGAU durante procesos de matrícula.
- Fallas en autenticación de usuarios en plataformas institucionales.
- Problemas de sincronización de credenciales.
- Accesos restringidos o incorrectamente configurados.

Esto podría generar:

- Dificultad de acceso para estudiantes y docentes.
- Retrasos en procesos académicos.
- Incremento de reportes de soporte.

**f. Debilidades en la seguridad de la información**

El análisis identificó riesgos importantes en materia de seguridad:

- Uso de credenciales compartidas en algunos casos.
- Equipos sin actualizaciones de seguridad constantes.
- Falta de controles formales de acceso.
- Ausencia de un SGSI institucional formal.

Esto compromete la confidencialidad e integridad de información académica y administrativa.

**g. Problemas en la continuidad operativa (energía y climatización)**

Se identificaron limitaciones en las condiciones físicas de operación:

- Cortes de energía eléctrica que afectan la disponibilidad de servicios.
- Sistemas de climatización limitados en la sala de servidores.

Esto podría generar:

- Interrupciones inesperadas en los sistemas.
- Riesgo de daño en equipos.
- Afectación en la continuidad de servicios académicos.

**h. Carencia de herramientas especializadas para la gestión de incidentes**

Se evidenció que la universidad se encuentra en una etapa inicial en el uso de herramientas ITSM:

- Uso incipiente de herramientas como GLPI, aún no institucionalizado.
- Ausencia de mesa de ayuda formal.
- Falta de monitoreo centralizado.
- No existe base de conocimiento estructurada.

Esto limita la eficiencia del proceso y la capacidad de mejora continua.

**i. Alta dependencia de sistemas académicos críticos**

Los procesos académicos dependen principalmente del SIGAU y Moodle. Se observó que:

- Estos sistemas presentan lentitud bajo alta concurrencia.
- Existen problemas de acceso en momentos críticos.
- Se generan interrupciones que afectan el desarrollo académico.

Esto impacta en los procesos de matrícula, evaluaciones y gestión docente, generando insatisfacción en la comunidad universitaria.

**j. Dependencia del conocimiento individual del personal técnico**

Se identificó que:

- Las soluciones no se documentan formalmente.
- La atención depende del conocimiento del técnico.
- No existe estandarización en la resolución de incidentes.

Esto podría generar:

- Variabilidad en la calidad del servicio.
- Riesgo ante ausencia o rotación del personal.

**k. Falta de definición de roles y niveles de soporte**

No existe una estructura formal de niveles de soporte, aunque sí una diferenciación funcional:

- Soporte técnico
- Infraestructura
- Sistemas

Sin embargo, esto no está definido bajo un esquema estructurado, lo que genera:

- Dificultades en la asignación de incidentes.
- Sobrecarga en ciertos perfiles técnicos.

**l. Escalamiento no estructurado**

El escalamiento ocurre de manera informal:

- Se deriva el incidente según conocimiento del personal.
- No existen criterios definidos para escalamiento crítico.
- No hay tiempos establecidos.

Esto podría generar:

- Retrasos en incidentes complejos.
- Falta de control en incidentes de alto impacto.

**m. Ausencia de monitoreo preventivo**

Finalmente, se evidenció que la gestión tiene un enfoque reactivo:

- No existen herramientas automatizadas de monitoreo.
- No se detectan fallas antes de que impacten al usuario.
- No se monitorean variables críticas de infraestructura.

Tabla 4. Matriz de contraste entre ITIL 4 y la situación actual de la gestión de incidentes de TI en la UNIFSLB

| **Componente de ITIL 4** | **Referencia conceptual en ITIL 4** | **Situación observada en UNIFSLB (causas y efectos)** | **Solución propuesta basada en ITIL 4** | **Nivel de brecha** |
|---|---|---|---|---|
| Registro de incidencias | Registro estructurado en repositorio centralizado. | **Causa:** Registro parcial en Excel y correos. **Efecto:** Información incompleta y análisis limitado. | Consolidar registro en herramienta ITSM (GLPI). | Parcial |
| Punto único de contacto (Service Desk) | Canal único de interacción con usuarios. | **Causa:** Uso combinado de correo, llamadas y contacto directo. **Efecto:** Desorganización y duplicidad. | Formalizar mesa de ayuda y canal único institucional. | Informal |
| Categorización de incidentes | Clasificación estructurada de incidentes. | **Causa:** No hay taxonomía formal. **Efecto:** Dificultad para | Definir catálogo de incidentes por servicios. | Ausente |

| | | | | |
|---|---|---|---|---|
| | | gestionar y analizar incidentes. | | |
| Priorización de incidentes | Basada en impacto y urgencia. | **Causa:** Priorización empírica. **Efecto:** Atención desigual y subjetiva. | Implementar matriz impacto–urgencia. | Débil |
| Estructura de niveles de soporte | Definición clara de niveles de atención. | **Causa:** Separación funcional no formalizada. **Efecto:** Ineficiencia en atención. | Formalizar niveles de soporte (1, 2, 3). | Parcial |
| Escalamiento técnico (funcional) | Derivación estructurada a niveles especializados. | **Causa:** Escalamiento informal entre áreas. **Efecto:** Retrasos y falta de control. | Definir rutas de escalamiento técnico. | Poco estructurado |
| Escalamiento organizacional (jerárquico) | Escalamiento para incidentes críticos. | **Causa:** Solo ocurre en crisis. **Efecto:** Respuesta tardía en incidentes mayores. | Definir protocolo de incidentes críticos. | Incipiente |
| Gestión de la resolución | Documentación de soluciones. | **Causa:** Conocimiento no documentado. **Efecto:** Dependencia del personal. | Crear base de conocimiento institucional. | Limitado |
| Cierre de incidentes | Validación con usuario. | **Causa:** Cierre informal o implícito. **Efecto:** Falta de control de calidad. | Establecer procedimiento de cierre formal. | Parcial |
| Monitoreo y gestión de alertas | Detección proactiva de incidentes. | **Causa:** Monitoreo manual básico. **Efecto:** Incidentes detectados tardíamente. | Implementar monitoreo automatizado. | Bajo |
| Herramientas ITSM | Uso de herramientas integradas. | **Causa:** GLPI en fase inicial. **Efecto:** Gestión aún no consolidada. | Implementar completamente herramienta ITSM. | En implementación |
| Indicadores de desempeño | Métricas para evaluar gestión. | **Causa:** No existen KPIs. **Efecto:** No hay control ni mejora continua. | Definir indicadores (MTTR, SLA, etc.). | Inexistente |
| Definición de roles | Roles claramente definidos. | **Causa:** Roles generales sin detalle operativo. **Efecto:** Ambigüedad en responsabilidades. | Definir roles específicos en gestión de incidentes. | Parcial |

| | | | | |
|---|---|---|---|---|
| Formalización del proceso | Documentación del proceso. | **Causa:** No existe procedimiento formal. **Efecto:** Variabilidad en la atención. | Documentar proceso ITIL 4 adaptado. | Ausente |
| Gestión de incidentes de seguridad | Integración con seguridad. | **Causa:** Gestión separada y reactiva. **Efecto:** Riesgo de vulneraciones. | Integrar con prácticas de seguridad TI. | Limitado |
| Gestión de terminales de usuario final | Control y mantenimiento de equipos. | **Causa:** Equipos con mantenimiento irregular. **Efecto:** Fallas frecuentes en usuarios. | Implementar gestión de activos (ITAM). | Deficiente |
| Gestión de red y conectividad | Gestión de capacidad y disponibilidad. | **Causa:** Conectividad limitada y variable. **Efecto:** Caídas frecuentes de servicios. | Mejorar infraestructura y monitoreo de red. | Bajo |
| Gestión de acceso a sistemas | Control de accesos y disponibilidad. | **Causa:** Problemas de autenticación y sincronización. **Efecto:** Usuarios sin acceso a sistemas. | Implementar gestión de identidades. | Limitado |

## 3.4. Configuración de los componentes funcionales y organizativos de la mesa de ayuda

### 3.4.1. Finalidad del diseño de los componentes funcionales y organizativos de la mesa de ayuda

El diseño de los componentes funcionales y estructurales de una Mesa de Ayuda tuvo como objetivo principal establecer un mecanismo institucional que permita gestionar de manera ordenada y eficiente los incidentes de tecnologías de la información que afectan tanto a los procesos académicos como administrativos. En esencia, se buscó pasar de una atención improvisada, dispersa y dependiente de personas específicas, hacia un proceso estructurado, con reglas claras y resultados más predecibles.

La implementación de la Mesa de Ayuda se concibe como una forma de reorganizar la atención de incidentes, permitiendo que estos sean gestionados bajo un esquema definido que garantice su registro, seguimiento y resolución. De esta manera, se pretende asegurar la trazabilidad de cada caso, reducir los tiempos de respuesta y

ofrecer un servicio más consistente a la comunidad universitaria, algo que actualmente no siempre ocurre.

Desde el punto de vista funcional, la Mesa de Ayuda está pensada como el canal central a través del cual los usuarios interactúan con el área de tecnologías de la información. Es decir, se convierte en el punto único de contacto, desde donde se recepcionan, clasifican y derivan los incidentes siguiendo criterios previamente establecidos. Esto permite evitar la dispersión de solicitudes, disminuir la dependencia del conocimiento individual de los técnicos y reducir la pérdida de información que suele darse cuando no existe un sistema formal.

En términos estructurales, el diseño propone organizar claramente los roles, definir niveles de soporte y establecer rutas de escalamiento. Con ello, se busca determinar con mayor precisión quién debe atender cada tipo de incidente, en qué momento y bajo qué condiciones. Este enfoque resulta clave para asegurar que incidentes de alto impacto, como interrupciones de sistemas académicos, fallas en la red, problemas en servidores o eventos de seguridad, sean atendidos con la prioridad que realmente requieren, evitando afectar procesos críticos como matrícula, evaluaciones o trámites administrativos.

Finalmente, la Mesa de Ayuda se plantea como un elemento fundamental para fortalecer la gestión de los servicios de TI dentro de la universidad. Su diseño se alinea con las buenas prácticas de ITIL 4, permitiendo no solo mejorar la atención de incidentes, sino también sentar las bases para una gestión más madura, orientada a resultados, con indicadores claros y capacidad de mejora continua.

### 3.4.2. Determinación de brechas frente a las buenas prácticas de ITIL 4

A partir del diagnóstico efectuado sobre la manera en que actualmente se atienden los incidentes de tecnologías de la información, se llevó a cabo una evaluación comparativa entre la realidad observada y los lineamientos establecidos por ITIL 4. Este análisis permitió reconocer con claridad las principales brechas existentes, poniendo en evidencia diferencias importantes entre la gestión actual (marcada por

prácticas poco estructuradas) y el nivel de organización, formalización y control que propone este marco de referencia.

En ese sentido, las brechas identificadas se convierten en un insumo clave para el desarrollo del modelo propuesto, ya que orientan de forma concreta los aspectos que requieren ser fortalecidos, normalizados o incorporados, con el fin de avanzar hacia una gestión más ordenada, medible y alineada con buenas prácticas internacionales.

Tabla 5. Brechas en la gestión de incidentes de TI en las universidades UNTRM y UNIFSLB frente a las buenas prácticas de ITIL 4

| **Componente de la gestión de incidentes (ITIL 4)** | **Lineamientos recomendados por ITIL 4** | **Situación evidenciada en UNTRM y UNIFSLB** | **Tipo de brecha identificada** |
|---|---|---|---|
| **Registro de incidentes** | Los incidentes deben almacenarse de forma estructurada en un sistema centralizado que permita su seguimiento. | El registro es inexistente o parcial. En UNTRM no hay registro formal; en UNIFSLB se usan hojas de cálculo y correos de manera incompleta. | Brecha crítica: trazabilidad limitada o inexistente. |
| **Punto único de contacto (Service Desk)** | Debe existir un canal único que centralice la recepción y seguimiento de incidentes. | No existe mesa de ayuda formal. Los usuarios recurren a contactos directos o múltiples canales informales. | Brecha estructural: falta de centralización en la atención. |
| **Clasificación de incidentes** | Se requiere una categorización estandarizada que facilite la gestión y análisis. | No hay clasificación formal; se realiza de manera empírica según criterio del técnico. | Brecha metodológica: ausencia de taxonomía definida. |
| **Priorización de incidentes** | La prioridad debe establecerse según impacto y urgencia previamente definidos. | La priorización es subjetiva, basada en presión del usuario o percepción del técnico. | Brecha operativa: inexistencia de criterios objetivos. |
| **Asignación de incidentes** | Debe responder a roles definidos y niveles de soporte establecidos. | La asignación depende de quién recibe el incidente; no hay reglas claras ni automatización. | Brecha organizativa: asignación improvisada. |
| **Niveles de soporte** | ITIL propone niveles estructurados (primer, segundo y tercer nivel). | No existen niveles formalizados; solo diferenciación informal entre técnicos. | Brecha de diseño: estructura de soporte no definida. |

| | | | |
|---|---|---|---|
| **Escalamiento funcional** | Debe existir un procedimiento técnico claro para derivar incidentes complejos. | El escalamiento se realiza de forma informal entre técnicos. | Brecha funcional: falta de rutas definidas. |
| **Escalamiento jerárquico** | Se deben establecer mecanismos para gestionar incidentes críticos. | Solo ocurre en situaciones de presión institucional; no hay criterios formales. | Brecha de gobernanza: inexistencia de gestión de incidentes mayores. |
| **Resolución de incidentes** | Las soluciones deben documentarse para reutilización futura. | Las soluciones no se documentan; dependen del conocimiento del personal. | Brecha de conocimiento: ausencia de base de datos de soluciones. |
| **Cierre de incidentes** | Debe existir validación del usuario y registro formal del cierre. | No hay cierre formal; en muchos casos se asume que el problema se resolvió. | Brecha de control: cierre no gestionado. |
| **Monitoreo y alertas** | Se deben utilizar herramientas para detección proactiva de fallas. | El monitoreo es limitado o manual; los incidentes se detectan cuando el usuario reporta. | Brecha tecnológica: enfoque reactivo. |
| **Herramientas ITSM** | Se recomienda el uso de plataformas integradas para gestionar incidentes. | En UNTRM no existen herramientas; en UNIFSLB hay uso incipiente de GLPI. | Brecha tecnológica: implementación insuficiente. |
| **Indicadores de desempeño** | Se deben definir métricas para evaluar eficiencia del proceso. | No existen indicadores ni reportes de desempeño. | Brecha analítica: falta de medición. |
| **Roles y responsabilidades** | Los roles deben estar claramente definidos y documentados. | Roles generales sin relación directa con la gestión de incidentes. | Brecha organizacional: responsabilidades poco claras. |
| **Documentación del proceso** | El proceso debe estar formalizado mediante procedimientos y manuales. | No existe documentación formal del proceso en ninguna de las universidades. | Brecha documental: proceso no institucionalizado. |
| **Gestión de incidentes de seguridad** | Debe integrarse con la gestión de seguridad de la información. | Los incidentes de seguridad se gestionan de forma aislada. | Brecha transversal: falta de integración TI–seguridad. |

El análisis comparativo entre la situación actual de la gestión de incidentes en la UNTRM y la UNIFSLB, frente a las buenas prácticas propuestas por ITIL 4, permitió identificar un conjunto de brechas que explican, de manera bastante clara, las dificultades que ambas instituciones enfrentan en la operación de sus servicios tecnológicos.

a. En primer lugar, se observa una brecha estructural significativa, relacionada con la ausencia de elementos básicos como una mesa de ayuda, un sistema de registro centralizado y una definición clara de roles y niveles de soporte. Esta carencia impide organizar adecuadamente la atención de incidentes y genera una dependencia excesiva de la iniciativa individual del personal técnico.

b. Se evidencia una brecha operativa y metodológica, vinculada a la falta de criterios estandarizados para clasificar, priorizar y escalar incidentes. Como resultado, la atención se vuelve inconsistente, con decisiones que varían según el contexto o la percepción del momento, lo que afecta la calidad del servicio.

c. Finalmente, se identifica una brecha tecnológica y analítica, reflejada en la ausencia o implementación incipiente de herramientas ITSM, sistemas de monitoreo y métricas de desempeño. Esto limita la capacidad de las universidades para anticipar fallas, evaluar su gestión y mejorar continuamente.

### 3.4.3. Definición de los componentes operativos y organizacionales de la mesa de ayuda

A continuación se presenta la propuesta integral de los componentes que conforman la Mesa de Ayuda (Service Desk), diseñada con el propósito de atender las debilidades identificadas en el diagnóstico de la gestión de incidentes de tecnologías de la información en las universidades analizadas, y de alinearse con las buenas prácticas establecidas por ITIL 4.

La propuesta busca estructurar un modelo que permita ordenar la atención de incidentes, mejorar la trazabilidad y fortalecer la calidad del servicio brindado a la comunidad universitaria. La propuesta se organiza en una tabla que diferencia dos grandes grupos de componentes: por un lado, los elementos estructurales, que representan la base organizativa y los recursos necesarios para el funcionamiento de la Mesa de Ayuda; y por otro, los elementos funcionales, que describen las actividades, procesos y acciones que deben ejecutarse para gestionar adecuadamente los incidentes.

Esta diferenciación permite comprender no solo cómo debe estar conformada la Mesa de Ayuda, sino también cómo debe operar en la práctica para garantizar una gestión eficiente, consistente y alineada con estándares internacionales.

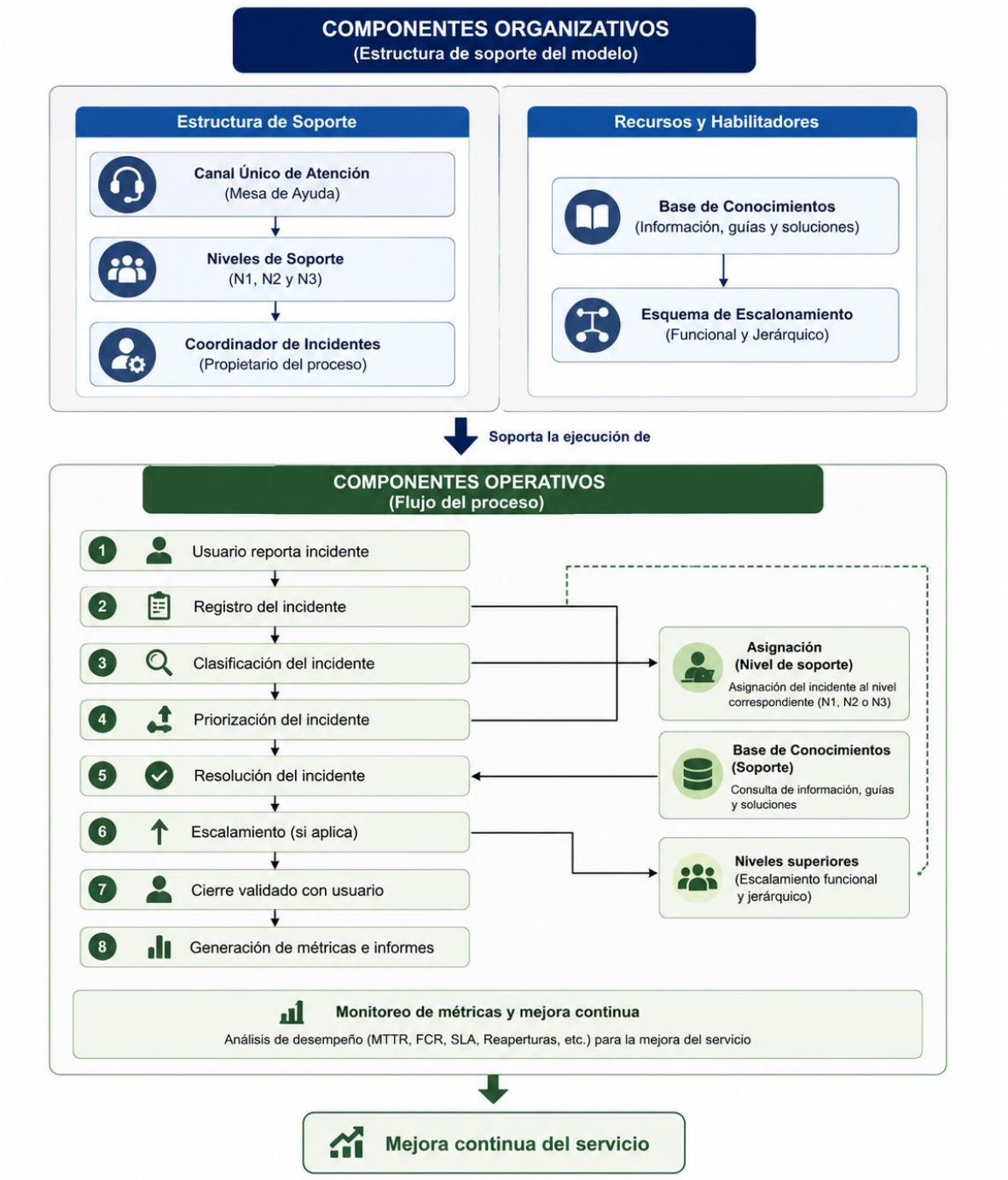
Los componentes organizativos y operativos incluidos en la propuesta fueron definidos a partir de las brechas identificadas durante el diagnóstico institucional y de las recomendaciones establecidas por ITIL 4 para la práctica de gestión de incidentes. La incorporación de elementos como la Mesa de Ayuda, los niveles de soporte y las métricas de desempeño responde a la necesidad de mejorar la trazabilidad, coordinación y continuidad de los servicios tecnológicos universitarios.

Tabla 6. Propuesta integrada de componentes organizativos y operativos de la mesa de ayuda para la UNTRM y UNIFSLB

| **Naturaleza del componente** | **Componente propuesto** | **Descripción alineada al modelo ITIL 4 y al contexto universitario de la UNTRM y UNIFSLB** |
|---|---|---|
| **Organizativo** | Canal único institucional de atención | La Mesa de Ayuda se establece como el único punto oficial para la recepción de incidentes y solicitudes de TI. Centraliza la comunicación de estudiantes, docentes y personal administrativo, eliminando el uso de canales informales (llamadas, mensajes, contacto directo) y permitiendo un control completo de los casos. |
| **Organizativo** | Estructura de soporte por niveles | Se define una organización por niveles de atención:<br>Nivel 1: recepción, registro y resolución de incidentes básicos.<br>Nivel 2: atención especializada (redes, sistemas, bases de datos).<br>Nivel 3: soporte avanzado (desarrollo, proveedores externos o expertos). Esto permite distribuir mejor la carga de trabajo y reducir tiempos de resolución. |
| **Organizativo** | Coordinador de gestión de incidentes | Responsable de supervisar el cumplimiento del proceso, coordinar escalamientos, analizar tendencias y proponer mejoras. Actúa como enlace entre la operación técnica y la gestión institucional, asegurando alineación con ITIL 4. |
| **Organizativo** | Plataforma de gestión de servicios (ITSM) | Implementación de una herramienta (por ejemplo, GLPI) que permita gestionar el ciclo completo del incidente: registro, clasificación, priorización, asignación, seguimiento y cierre. Facilita la generación de reportes y métricas clave. |
| **Organizativo** | Repositorio de conocimiento institucional | Espacio donde se documentan soluciones, guías técnicas y preguntas frecuentes. Permite reutilizar soluciones, reducir tiempos de atención y disminuir la dependencia del conocimiento individual. |
| **Organizativo** | Esquema formal de escalamiento | Definición de rutas claras para el escalamiento técnico (por especialidad) y jerárquico (para incidentes críticos). Asegura que los incidentes de alto impacto sean gestionados con prioridad y coordinación adecuada. |

| | | |
|---|---|---|
| **Operativo** | Registro estructurado de incidentes | Todos los incidentes se documentan en la herramienta ITSM con información estándar: usuario, servicio afectado, descripción, fecha, categoría, prioridad y solución. Permite trazabilidad completa y análisis posterior. |
| **Operativo** | Clasificación estandarizada | Los incidentes se categorizan según una taxonomía definida (red, hardware, software, acceso, seguridad, servicios académicos, etc.), lo que facilita su análisis y correcta asignación. |
| **Operativo** | Priorización basada en criterios objetivos | Se utiliza una matriz de impacto y urgencia para definir la prioridad de cada incidente, evitando decisiones subjetivas y garantizando atención oportuna a los servicios críticos. |
| **Operativo** | Asignación controlada de incidentes | La herramienta ITSM distribuye los incidentes según categoría, nivel de soporte y carga de trabajo, evitando la asignación informal y mejorando la eficiencia del equipo técnico. |
| **Operativo** | Resolución documentada | Cada incidente resuelto se registra junto con su solución, permitiendo alimentar la base de conocimiento y reducir la recurrencia de problemas. |
| **Operativo** | Escalamiento gestionado | Los incidentes que no pueden resolverse en el nivel inicial se derivan automáticamente al nivel correspondiente, siguiendo reglas definidas de tiempo y complejidad. |
| **Operativo** | Cierre validado del incidente | El incidente se considera cerrado únicamente cuando el usuario confirma que el servicio ha sido restablecido, asegurando calidad en la atención. |
| **Operativo** | Monitoreo y generación de indicadores | Se generan métricas como tiempo promedio de resolución (MTTR), volumen de incidentes, cumplimiento de SLA y tasa de reincidencia, permitiendo evaluar el desempeño y apoyar la toma de decisiones. |
| **Operativo** | Comunicación activa con usuarios | En situaciones críticas, la Mesa de Ayuda informa de manera oportuna a la comunidad universitaria sobre el estado de los servicios, reduciendo incertidumbre y mejorando la percepción del servicio. |

Figura 3. Esquema de estructural y operativo de la propuesta



### 3.4.4. Configuración de los componentes organizativos de la mesa de ayuda

A continuación se desarrolla la definición y estructuración de los principales componentes organizativos que conforman la Mesa de Ayuda propuesta, los cuales permiten establecer las bases para una gestión ordenada y sostenible de los incidentes de tecnologías de la información en las universidades analizadas.

Estos componentes determinan cómo se distribuyen las responsabilidades, cómo se canaliza la comunicación y cómo se garantiza la continuidad de los servicios tecnológicos.

#### a. Canal único institucional de atención (Single Point of Contact – SPOC)

**Finalidad del canal único de atención**

El canal único de atención tiene como propósito considerarse como el medio oficial a través del cual se gestionan todos los incidentes y solicitudes relacionadas con los servicios de tecnologías de la información. Con ello, se busca sustituir el esquema actual, caracterizado por múltiples vías informales donde los usuarios recurren directamente a técnicos específicos, generando desorden y falta de control.

La implementación de este punto centralizado permitirá organizar de manera más coherente la atención de incidentes, alineando el soporte tecnológico con las necesidades reales de los procesos académicos y administrativos.

Los beneficios que se persiguen con este componente son los siguientes:

- Estructurar la atención de TI en función de los servicios críticos que soportan las actividades universitarias.
- Contribuir a la continuidad operativa de plataformas académicas y administrativas clave, así como de la infraestructura tecnológica que las sustenta.
- Disminuir la dependencia del conocimiento individual del personal técnico, promoviendo una gestión más institucionalizada.

- Establecer un proceso ordenado para el registro, clasificación, priorización y resolución de incidentes.
- Generar información confiable que sirva de base para la toma de decisiones en la gestión de tecnologías de la información.

**Estructura organizativa del canal único de atención**

El canal único de atención propuesto oes el componente central dentro del modelo de gestión de incidentes, cuya organización responde a las necesidades operativas de las universidades analizadas. Su diseño busca integrar funciones, roles y herramientas en un entorno controlado que permita gestionar de manera eficiente las solicitudes de soporte tecnológico.

A continuación, se presenta la configuración organizativa planteada. La definición de un Punto Único de Contacto se fundamenta en las recomendaciones de ITIL 4 relacionadas con la función del service desk como mecanismo centralizado para la recepción, seguimiento y coordinación de incidentes.

Tabla 7. Configuración organizativa del canal único de atención institucional

| Componente organizativo | Descripción funcional |
|---|---|
| Ubicación institucional del canal de atención | Se establece como una unidad operativa dentro de la Oficina de Tecnologías de la Información (OTI), alineada a los lineamientos de gobierno digital institucional. Depende directamente de la jefatura de TI y su formalización debe realizarse mediante un documento normativo interno. |
| Equipo de atención inicial | Conformado por personal de primer nivel encargado de recepcionar, registrar y atender incidentes básicos. Puede organizarse por áreas funcionales (académica, administrativa, soporte general) para mejorar la distribución de la demanda. |
| Responsables de coordinación y control | Incluye un coordinador de atención encargado de supervisar tiempos de respuesta, derivaciones y cumplimiento del proceso, así como un responsable del proceso de incidentes orientado al seguimiento de indicadores y mejora continua. |
| Canales de atención integrados | Se consideran múltiples medios de acceso: plataforma digital, línea telefónica institucional y atención presencial. Este último canal es relevante en contextos donde el acceso digital no es uniforme. |
| Plataforma de gestión de incidentes (ITSM) | Herramienta tecnológica que permite administrar de forma integral los incidentes de servicios académicos, administrativos e infraestructura. Debe facilitar el registro, seguimiento, priorización y generación de reportes. |

| | |
|---|---|
| Repositorio de soluciones y conocimiento | Espacio centralizado donde se documentan soluciones, procedimientos e instructivos de uso de sistemas institucionales. Su actualización debe ser periódica para mantener su utilidad operativa. |
| Recursos tecnológicos de soporte | Incluye estaciones de trabajo dedicadas, herramientas de monitoreo, sistemas de registro de incidentes y acceso a utilidades de diagnóstico para red, servidores y servicios críticos. |

### Operatividad del canal único de atención

El canal único no solo cumple una función organizativa, sino que también ejecuta un conjunto de actividades clave dentro del proceso de gestión de incidentes. Estas funciones permiten asegurar que cada incidente sea tratado de manera consistente, desde su registro hasta su cierre.

A continuación, se describen las principales funciones operativas:

Tabla 8. Funciones operativas del canal único de atención en la gestión de incidentes

| Componente operativo | Descripción de la actividad |
|---|---|
| Registro formal de incidentes | Todo incidente es documentado mediante un formato estandarizado dentro del sistema ITSM, garantizando consistencia en la información recopilada. |
| Clasificación estructurada | Los incidentes se organizan según categorías definidas (sistemas académicos, plataformas virtuales, redes, seguridad, infraestructura, equipos, software, entre otros), lo que facilita su análisis y tratamiento. |
| Determinación de prioridad | Se establece un nivel de prioridad basado en el impacto y la urgencia del incidente, considerando momentos críticos del calendario académico y la afectación del servicio. |
| Asignación de casos | Los incidentes son distribuidos al personal correspondiente según su naturaleza y nivel de complejidad, evitando asignaciones improvisadas. |
| Gestión de escalamiento | Cuando un incidente supera la capacidad de atención inicial, se deriva al nivel de soporte adecuado o a instancias superiores, siguiendo criterios previamente definidos. |
| Comunicación con usuarios | Se mantiene informada a la comunidad universitaria sobre el estado de los servicios, especialmente en situaciones de alto impacto o interrupciones relevantes. |
| Cierre con validación | El incidente se da por concluido únicamente cuando el usuario confirma que el servicio ha sido restablecido de manera satisfactoria. |
| Generación de indicadores de desempeño | Se registran y analizan métricas como tiempos de atención, volumen de incidentes y niveles de servicio, lo que permite evaluar el desempeño y mejorar el proceso. |

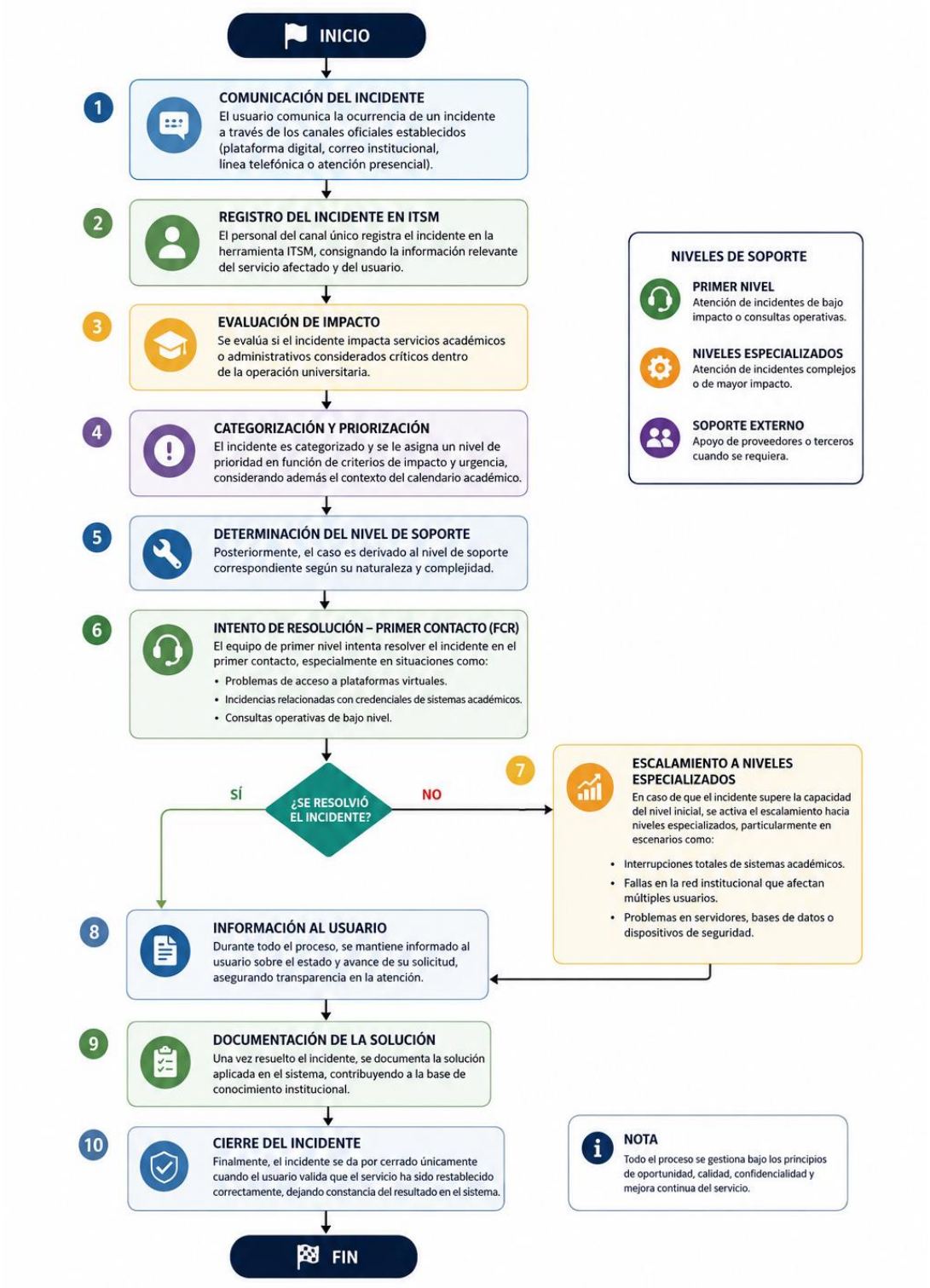
**Secuencia operativa del canal único de atención en la gestión de incidentes**

El funcionamiento del canal único de atención se desarrolla a través de una secuencia organizada de actividades que permiten gestionar los incidentes de manera controlada, desde su reporte inicial hasta su cierre definitivo. Este flujo busca asegurar consistencia en la atención, trazabilidad de los casos y alineación con las buenas prácticas de ITIL 4.

A continuación, se describe el proceso operativo propuesto:

1. El usuario comunica la ocurrencia de un incidente a través de los canales oficiales establecidos, tales como la plataforma digital, correo institucional, línea telefónica o atención presencial.
2. El personal del canal único registra el incidente en la herramienta ITSM, consignando la información relevante del servicio afectado y del usuario.
3. Se evalúa si el incidente impacta servicios académicos o administrativos considerados críticos dentro de la operación universitaria.
4. El incidente es categorizado y se le asigna un nivel de prioridad en función de criterios de impacto y urgencia, considerando además el contexto del calendario académico.
5. Posteriormente, el caso es derivado al nivel de soporte correspondiente según su naturaleza y complejidad.
6. El equipo de primer nivel intenta resolver el incidente en el primer contacto (First Contact Resolution), especialmente en situaciones como:
    - Problemas de acceso a plataformas virtuales.
    - Incidencias relacionadas con credenciales de sistemas académicos.
    - Consultas operativas de bajo nivel.
7. En caso de que el incidente supere la capacidad del nivel inicial, se activa el escalamiento hacia niveles especializados, particularmente en escenarios como:
    - Interrupciones totales de sistemas académicos.
    - Fallas en la red institucional que afectan múltiples usuarios.
    - Problemas en servidores, bases de datos o dispositivos de seguridad.
8. Durante todo el proceso, se mantiene informado al usuario sobre el estado y avance de su solicitud, asegurando transparencia en la atención.
9. Una vez resuelto el incidente, se documenta la solución aplicada en el sistema, contribuyendo a la base de conocimiento institucional.
10. Finalmente, el incidente se da por cerrado únicamente cuando el usuario valida que el servicio ha sido restablecido correctamente, dejando constancia del resultado en el sistema.

Figura 4. Flujograma del proceso de gestión de incidentes



**b. Estructura de roles y responsabilidades según niveles de soporte**

La gestión de incidentes propuesta se apoya en una organización por niveles de soporte, donde cada uno cumple funciones específicas dentro del proceso. Esta distribución permite ordenar la atención, mejorar los tiempos de respuesta y asegurar que cada incidente sea tratado según su complejidad. Los perfiles asociados a cada nivel se detallan en el Anexo 5.

**Nivel 1 – Atención inicial y soporte básico**

Este nivel constituye el primer punto de intervención dentro del proceso de gestión de incidentes. Su función principal es atender los casos más frecuentes y de menor complejidad, aplicando procedimientos previamente definidos y documentados.

Responsabilidades principales:

- Recibir los incidentes a través del canal único de atención.
- Registrar la información en la herramienta ITSM de manera completa y uniforme.
- Clasificar los incidentes según la categorización institucional (sistemas académicos, red, seguridad, plataformas virtuales, entre otros).
- Establecer la prioridad utilizando criterios de impacto y urgencia.
- Resolver incidentes básicos en el primer contacto (First Contact Resolution), apoyándose en guías y base de conocimiento.
- Derivar los casos que no puedan resolverse hacia el siguiente nivel de soporte.
- Mantener informado al usuario sobre el estado de su solicitud.
- Aportar información relevante para la actualización de la base de conocimiento institucional.

Perfil sugerido

Personal técnico de la OTI con conocimientos generales en soporte informático, manejo de sistemas académicos y uso de herramientas institucionales.

**Nivel 2 – Soporte especializado en infraestructura y servicios**

Este nivel se encarga de atender incidentes que requieren un mayor grado de especialización técnica, especialmente aquellos relacionados con la infraestructura tecnológica y los sistemas institucionales.

Responsabilidades principales

- Resolver incidentes asociados a redes, servidores, bases de datos y plataformas digitales.
- Atender problemas en sistemas académicos y administrativos que demanden análisis técnico.
- Identificar causas recurrentes y proponer acciones correctivas.
- Documentar soluciones complejas para su posterior reutilización.
- Escalar casos al nivel superior cuando se requiera intervención externa o altamente especializada.

Áreas involucradas

- Redes y comunicaciones
- Infraestructura y virtualización
- Seguridad informática
- Administración de bases de datos
- Gestión de aplicaciones institucionales

**Nivel 3 – Soporte avanzado y atención de incidentes críticos**

Este nivel interviene en situaciones de alta complejidad que superan las capacidades del equipo interno, incluyendo incidentes críticos o estructurales que afectan directamente la continuidad del servicio.

Responsabilidades principales

- Resolver fallas complejas en sistemas académicos o administrativos que involucren lógica de negocio o integridad de datos.
- Atender incidentes de seguridad de alto impacto, como accesos no autorizados o vulneraciones.
- Ejecutar intervenciones técnicas en componentes críticos de la infraestructura.

- Coordinar con proveedores tecnológicos para soporte especializado.
- Validar soluciones definitivas y actualizaciones de sistemas.
- Documentar soluciones estratégicas orientadas a evitar recurrencias.

Perfil sugerido

- Desarrolladores de sistemas institucionales
- Proveedores de software y plataformas digitales
- Especialistas externos en infraestructura o seguridad
- Soporte técnico de fabricantes de hardware

Competencias requeridas por nivel de soporte

Para asegurar el adecuado funcionamiento del modelo, cada nivel debe contar con un conjunto de competencias específicas, tanto técnicas como operativas y actitudinales. Estas competencias permiten garantizar una atención eficiente, coherente y alineada con las buenas prácticas de ITIL 4.

La matriz detallada de competencias por nivel se presenta en el Anexo correspondiente. La segmentación de niveles de soporte se estableció considerando la complejidad técnica de los incidentes, el grado de especialización requerido y las prácticas de escalamiento funcional propuestas por ITIL 4.

Tabla 9. Matriz de capacidades requeridas por niveles de soporte en la gestión de incidentes de TI

| **Área de competencia** | **Nivel 1 – Soporte inicial** | **Nivel 2 – Soporte especializado** | **Nivel 3 – Soporte avanzado / externo** |
|---|---|---|---|
| Dominio general de tecnologías de información | Manejo básico de equipos, sistemas operativos, red y plataformas institucionales (sistemas académicos, aula virtual, correo). | Conocimiento especializado en infraestructura tecnológica: redes, servidores, bases de datos y sistemas institucionales. | Dominio experto en tecnologías críticas: seguridad avanzada, arquitectura de sistemas, desarrollo y plataformas de misión crítica. |
| Capacidad de diagnóstico de incidentes | Identificación de síntomas y recopilación ordenada de información del incidente. | Análisis técnico detallado para identificar causas raíz y evaluar impacto. | Evaluación profunda de incidentes complejos o estructurales mediante herramientas avanzadas. |

| | | | |
|---|---|---|---|
| Manejo de herramientas de gestión (ITSM) | Registro, categorización y priorización de incidentes en la plataforma. | Actualización de estados, documentación técnica y seguimiento del incidente. | Análisis de tendencias, documentación de soluciones estratégicas y mejora del sistema. |
| Interacción con usuarios y equipos | Comunicación clara con usuarios, especialmente en contextos de alta demanda académica. | Coordinación técnica con otros especialistas y áreas involucradas. | Comunicación a nivel estratégico con autoridades y proveedores externos. |
| Capacidad de resolución de incidentes | Resolución de problemas básicos: accesos, configuraciones simples, soporte operativo. | Solución de incidentes de complejidad media y alta relacionados con infraestructura y sistemas. | Implementación de soluciones definitivas, correcciones estructurales y mejoras tecnológicas. |
| Comprensión del proceso de gestión de incidentes | Conocimiento del flujo básico del proceso y sus etapas principales. | Comprensión integral del proceso, incluyendo análisis técnico y mejora. | Dominio completo del modelo ITIL 4 y su integración con otros procesos de gestión. |
| Gestión del conocimiento institucional | Consulta de guías y procedimientos disponibles. | Generación y actualización de contenido en la base de conocimiento. | Validación técnica de información crítica y generación de conocimiento especializado. |
| Gestión del escalamiento | Identificación de casos que requieren derivación. | Ejecución del escalamiento técnico hacia niveles superiores. | Activación de escalamiento jerárquico en incidentes críticos o de alto impacto. |
| Competencias interpersonales | Habilidades de comunicación, empatía y atención al usuario. | Trabajo colaborativo, análisis crítico y enfoque en solución de problemas. | Liderazgo técnico, toma de decisiones y gestión de situaciones complejas. |

**Asignación de responsabilidades en el proceso de gestión de incidentes (Matriz RACI)** La matriz RACI planteada se construyó tomando como referencia las actividades principales del proceso de gestión de incidentes basado en ITIL 4, así como los roles definido en los distintos niveles de soporte. Su finalidad es establecer con claridad quién ejecuta cada actividad, quién supervisa su cumplimiento, quién debe ser consultado y quién debe mantenerse informado durante el proceso.

Para la correcta interpretación de la matriz, se consideran los siguientes criterios:

**R (Responsible):** Responsable directo de ejecutar la actividad.

**A (Accountable):** Responsable final de que la actividad se complete adecuadamente.
**C (Consulted):** Participa brindando soporte o asesoría técnica.
**I (Informed):** Debe ser informado sobre el desarrollo o resultado de la actividad.

La asignación de responsabilidades se diseñó para evitar duplicidad de funciones, mejorar la coordinación operativa y establecer mecanismos claros de trazabilidad y escalamiento.

Tabla 10. Distribución de responsabilidades del proceso de gestión de incidentes en la mesa de ayuda

| **Actividad del proceso** | **Nivel 1 – Soporte inicial** | **Nivel 2 – Soporte especializado** | **Nivel 3 – Soporte avanzado / externo** | **Coordinador del proceso de incidentes** | **Usuarios (académicos y administrativos)** |
|---|---|---|---|---|---|
| Recepción del incidente | R | I | I | A | I |
| Registro en sistema ITSM | R | I | I | A | I |
| Clasificación del incidente | R | C | I | A | I |
| Determinación de prioridad | R | C | I | A | I |
| Resolución inicial (FCR) | R | I | I | A | I |
| Análisis técnico | I | R | C | A | I |
| Resolución de incidentes complejos | I | C | R | A | I |
| Escalamiento técnico | R | A | I | C | I |
| Escalamiento a nivel institucional (incidentes críticos) | A | C | C | R | I |
| Comunicación con usuarios | R | I | I | A | C |

| Actividad del proceso | Nivel 1 – Soporte inicial | Nivel 2 – Soporte especializado | Nivel 3 – Soporte avanzado / externo | Coordinador del proceso de incidentes | Usuarios (académicos y administrativos) |
|---|---|---|---|---|---|
| Documentación en base de conocimiento | R | R | C | A | I |
| Validación del cierre | R | C | I | A | R |
| Generación de indicadores (MTTR, FCR, etc.) | I | I | I | R / A | I |
| Mejora continua del proceso | C | C | C | R / A | I |

A partir de la matriz presentada, se pueden identificar varios aspectos clave en la organización del proceso:

- El Nivel 1 concentra la mayor parte de las actividades operativas, lo que permite una atención más ágil y organizada de los incidentes desde su registro hasta su seguimiento inicial.
- El Nivel 2 cumple un rol fundamental en la resolución técnica especializada, evitando que los incidentes complejos saturen el primer nivel y asegurando un tratamiento adecuado según su naturaleza.
- El Nivel 3 interviene en situaciones puntuales que requieren conocimientos avanzados o soporte externo, lo que optimiza el uso de recursos internos.
- El coordinador del proceso de incidentes actúa como responsable de la supervisión integral, garantizando el cumplimiento del modelo, la generación de métricas y la mejora continua del servicio.
- Los usuarios de las áreas académicas y administrativas participan activamente validando el cierre de los incidentes y contribuyendo con un reporte oportuno, lo cual resulta clave para la efectividad del proceso.

**c. Rol de coordinación del proceso de gestión de incidentes de TI**

Dentro de la estructura propuesta para la gestión de incidentes, proponemos la incorporación de un rol clave encargado de asegurar la correcta operación, supervisión y mejora del proceso. Este rol resulta fundamental para evitar la

desarticulación de esfuerzos, garantizar el cumplimiento de los lineamientos establecidos y mantener la coherencia del modelo en toda la organización.

A continuación, se describe la propuesta del rol responsable del proceso:

**Denominación del rol institucional**

Coordinador de Gestión de Incidentes de Tecnologías de la Información (CGI-TI)

**Características del puesto**

- Ubicación organizacional: Oficina de Tecnologías de la Información (OTI)
- Dependencia jerárquica: Jefatura de la OTI
- Relaciones de coordinación:
    - Canal único de atención (Service Desk / Nivel 1)
    - Equipos especializados (Nivel 2)
    - Soporte avanzado o proveedores externos (Nivel 3)
    - Área de seguridad digital
    - Dependencias académicas y administrativas

**Finalidad del rol**

El propósito de este puesto es asegurar que el proceso de gestión de incidentes se ejecute de manera ordenada, controlada y alineada con las buenas prácticas de ITIL 4. Asimismo, busca garantizar la continuidad de los servicios tecnológicos críticos que soportan las actividades académicas y administrativas, contribuyendo al cumplimiento de los lineamientos de gobierno digital institucional.

**Responsabilidades principales**

- Supervisar el cumplimiento del proceso de gestión de incidentes en todas sus etapas, desde el registro hasta el cierre.
- Coordinar los mecanismos de escalamiento, tanto a nivel técnico como organizacional, especialmente en situaciones de alto impacto.

- Verificar que los incidentes sean correctamente clasificados, priorizados y cerrados conforme a los criterios establecidos.
- Analizar indicadores de desempeño (tiempos de resolución, tasa de resolución en primer contacto, volumen de incidentes, recurrencia, entre otros) para identificar patrones y oportunidades de mejora.
- Elaborar reportes periódicos dirigidos a la jefatura de la OTI y a la alta dirección cuando corresponda.
- Promover la mejora continua del proceso y del funcionamiento de la mesa de ayuda.
- Asegurar la alineación del proceso con ITIL 4, las políticas de seguridad de la información y los lineamientos de gobierno digital.
- Coordinar con el área de seguridad digital en la gestión de incidentes relacionados con ciberseguridad.

**Capacidades requeridas**

- Conocimiento sólido del marco ITIL 4, especialmente en la práctica de gestión de incidentes.
- Habilidades en gestión de procesos y análisis de indicadores.
- Capacidad de coordinación interáreas y comunicación institucional efectiva.
- Pensamiento analítico orientado a la mejora continua.
- Comprensión del entorno universitario y de los lineamientos de transformación digital.

**Ubicación dentro de la estructura organizativa**

El rol propuesto se integra dentro de la estructura de tecnologías de la información de la siguiente manera:

→ Alta Dirección / Rectorado
  → Jefatura de Tecnologías de la Información
    → Coordinador de Gestión de Incidentes de TI (CGI-TI)
      → Equipo de atención inicial (Nivel 1 – Mesa de Ayuda)
        → Equipo especializado (Nivel 2 – Infraestructura y sistemas)
          → Soporte avanzado (Nivel 3 – expertos o proveedores)

**Mecanismo de seguimiento y control del proceso**

Para garantizar el adecuado funcionamiento del proceso de gestión de incidentes, el coordinador debe ejecutar un esquema continuo de seguimiento basado en el análisis de información operativa.

Este esquema incluye la revisión periódica de indicadores, la identificación de incidentes recurrentes, la evaluación del cumplimiento de los niveles de servicio y la definición de acciones correctivas o de mejora. Asimismo, implica la generación de reportes que permitan evidenciar el desempeño del proceso y sustentar decisiones orientadas a optimizar la gestión de los servicios de TI.

**d. Base de conocimientos del proceso de gestión de incidentes**

Otro de los elementos clave del proceso de gestión de incidentes es la Base de Conocimiento, la cual se concibe como un repositorio estructurado, validado y de uso obligatorio para la atención de incidentes de TI en la Universidad. Su finalidad es registrar, organizar y reutilizar el conocimiento técnico y operativo, permitiendo reducir tiempos de atención, aumentar la resolución en primer contacto y promover la autogestión responsable de la comunidad universitaria.

**Estructura propuesta para la Base de Conocimientos**

Para el diseño de la base de conocimientos se debe tener en cuenta que los servicios considerados son los siguientes:

- Sistema de Información Académica (SIA)
- Aula Virtual - Moodle
- Servicio de verificación de duplicidad de documentos académicos y de investigación (Turnitin)
- Servicio de registro de tesis y proyectos de investigación
- Servicio de Biblioteca virtual
- Servicio de Repositorio institucional de investigaciones
- Plataforma de correo institucional
- Sistemas de gestión administrativa (SIAF, tesorería, contabilidad y planillas)

- Red de datos (cableado, switches, antenas)
- Seguridad en la red y las comunicaciones
- Servidores y almacenamiento – Servidores físicos
- Servidores y almacenamiento en la nube (Servicios de terceros)
- Energía y climatización de sala de servidores
- Equipos de laboratorio
- Equipos terminales de laboratorios de cómputo
- Equipos terminales de áreas administrativas
- Software académico
- Software de ofimática

**e. Gestión del conocimiento como soporte al proceso de incidentes de TI**

Un componente fundamental dentro del modelo de gestión de incidentes es la gestión del conocimiento, la cual se materializa a través de una base institucional estructurada que almacena información técnica y operativa relevante para la atención de incidencias. Este repositorio no solo cumple una función de almacenamiento, sino que actúa como un recurso estratégico para mejorar la eficiencia del proceso.

La base de conocimiento se plantea como un sistema organizado, validado y de uso obligatorio por parte del personal de soporte, cuyo objetivo es facilitar la reutilización de soluciones, reducir los tiempos de atención, incrementar la tasa de resolución en el primer contacto y fomentar, en la medida de lo posible, la autogestión por parte de los usuarios.

**Organización propuesta de la base de conocimiento**

Para el diseño de este repositorio, se debe considerar que los servicios tecnológicos que soportan las actividades académicas y administrativas constituyen el eje central de organización del conocimiento. En ese sentido, la base debe estructurarse en función de los principales servicios institucionales, entre los cuales se incluyen:

- Sistemas académicos (registro, matrícula, notas, gestión docente).

- Plataformas de aprendizaje virtual (aulas virtuales basadas en LMS).
- Servicios de gestión de investigación (registro de tesis, repositorios institucionales).
- Herramientas de apoyo académico (control de originalidad de documentos, bibliotecas digitales).
- Servicios de comunicación institucional (correo electrónico y plataformas colaborativas).
- Sistemas administrativos (gestión financiera, contable y de recursos humanos).
- Infraestructura de red y comunicaciones (cableado, equipos de red, conectividad).
- Seguridad de la información (controles de acceso, incidentes de ciberseguridad).
- Infraestructura tecnológica (servidores físicos, virtualización y servicios en la nube).
- Condiciones operativas (energía eléctrica, climatización de centros de datos).
- Equipamiento tecnológico (laboratorios de cómputo y equipos de usuario final).
- Software institucional y herramientas de ofimática.

Esta organización permite que el conocimiento se clasifique de acuerdo con los servicios que realmente impactan la operación universitaria, facilitando su consulta y aplicación durante la atención de incidentes.

**Contenido esperado en la base de conocimiento**

Para cada uno de los servicios identificados, la base de conocimiento debe contener información estructurada que permita comprender, diagnosticar y resolver incidentes de manera eficiente. Esto incluye, entre otros elementos:

- Descripción del servicio y su funcionamiento general.
- Tipos de incidentes más frecuentes asociados al servicio.
- Procedimientos de solución paso a paso.

- Guías rápidas de atención para el personal de soporte.
- Instructivos orientados a usuarios finales (cuando aplique).
- Identificación de causas comunes y acciones preventivas.
- Relación con otros servicios o dependencias tecnológicas.
- Registro de soluciones previamente aplicadas y validadas.

La estructura de contenidos de la base de conocimientos fue diseñada considerando los incidentes recurrentes identificados durante el diagnóstico y las recomendaciones de ITIL 4 sobre gestión del conocimiento y mejora continua, los mismos que se muestran en las tablas 11, 12 y 13.

Tabla 11. Tipología de contenidos para la gestión del conocimiento en la mesa de ayuda

| Categoría de contenido | Descripción funcional | Ejemplos aplicados a las universidades analizadas |
|---|---|---|
| **Consultas frecuentes (nivel básico)** | Conjunto de preguntas y respuestas orientadas a resolver dudas comunes que no implican un impacto significativo en la operación. Están dirigidas principalmente a usuarios finales y buscan facilitar la autogestión, reduciendo la necesidad de intervención del soporte técnico. | - ¿Por qué no se visualizan las notas en el sistema académico?<br>- ¿Qué hacer si la plataforma virtual no carga correctamente?<br>- ¿Por qué no aparece el porcentaje de similitud en Turnitin?<br>- ¿En qué fecha se habilita el proceso de matrícula?<br>- ¿Cómo solicitar acceso a la red inalámbrica institucional? |
| **Instructivos de solución rápida** | Documentos breves que detallan acciones específicas que el usuario puede ejecutar por cuenta propia para resolver incidencias simples. Su propósito es mejorar la experiencia del usuario y disminuir la carga operativa del primer nivel de soporte. | - Pasos para recuperar el acceso a la plataforma virtual<br>- Procedimiento para restablecer la contraseña institucional<br>- Verificación del estado de un curso en el LMS<br>- Guía para envío correcto de trabajos en Turnitin<br>- Acceso remoto al sistema académico |
| **Documentación de soluciones recurrentes** | Registros técnicos que describen la resolución de incidentes que ocurren con frecuencia. Incluyen descripción del problema, causa identificada y procedimiento de solución, con el fin de estandarizar la atención y reducir tiempos de respuesta. | - Solución a interrupciones del sistema académico en matrícula<br>- Corrección de errores en módulos de evaluación<br>- Recuperación de conectividad inalámbrica en áreas específicas<br>- Mejora de rendimiento del aula virtual en evaluaciones<br>- Corrección de integración entre plataformas académicas |

| Categoría de contenido | Descripción funcional | Ejemplos aplicados a las universidades analizadas |
|---|---|---|
| **Listas de verificación técnica** | Herramientas estructuradas que permiten al personal técnico realizar diagnósticos de manera ordenada, evitando omisiones y asegurando consistencia en la atención, especialmente en incidentes de infraestructura. | - Verificación de conectividad por áreas académicas<br>- Revisión de disponibilidad del sistema académico<br>- Validación de servicios antes de procesos críticos<br>- Revisión de configuraciones de seguridad<br>- Control de condiciones ambientales en servidores |
| **Protocolos operativos para incidentes críticos** | Documentos formales que establecen los pasos a seguir ante incidentes de alto impacto. Incluyen responsabilidades, flujos de escalamiento y controles, siendo de cumplimiento obligatorio para garantizar la continuidad del servicio. | - Procedimiento de atención de fallas del sistema académico<br>- Protocolo de gestión de incidentes en plataformas virtuales<br>- Creación y gestión de cuentas institucionales<br>- Procedimiento de respaldo de información crítica<br>- Gestión de incidentes mayores |
| **Comunicados preventivos y alertas** | Mensajes orientados a anticipar situaciones que puedan afectar los servicios, como mantenimientos, sobrecarga o riesgos de seguridad. Su finalidad es preparar tanto a usuarios como a personal técnico, reduciendo el impacto de posibles incidentes. | - Recomendaciones ante alta demanda del sistema académico<br>- Avisos de mantenimiento del aula virtual<br>- Interrupciones programadas por trabajos técnicos<br>- Alertas de seguridad ante accesos no autorizados<br>- Recomendaciones ante fallas eléctricas |

Como parte del diseño de la base de conocimiento propuesta, se planteó un conjunto inicial de registros orientados a documentar los incidentes más recurrentes que afectan los servicios académicos y administrativos. Esta información sirve como punto de partida para estandarizar la atención, facilitar el diagnóstico y mejorar la capacidad de respuesta del personal técnico.

La estructura propuesta organiza el conocimiento en función del servicio afectado, el tipo de incidente, los síntomas identificables, las posibles causas, así como las acciones recomendadas para su resolución. Además, se incorpora el nivel de soporte requerido y un rango estimado de atención, lo que permite orientar tanto la asignación de recursos como la priorización operativa.

Tabla 12. Registro base de incidentes y conocimiento técnico asociado por tipo de servicio

| Evento reportado | Servicio comprometido | Naturaleza del incidente | Manifestaciones observadas | Posible origen | Acciones sugeridas de atención | Ruta de atención | Tiempo aproximado de solución |
|---|---|---|---|---|---|---|---|
| Interrupción del sistema académico | Sistema académico institucional | Disponibilidad | Acceso denegado, lentitud o cierre de sesión | Saturación de recursos | N1: verificar alcance.<br>N2: revisar servicios.<br>N3: ajustar capacidad | N1 → N2 → N3 | 30 min – 4 h |
| Bajo rendimiento en plataforma virtual durante evaluaciones | Plataforma LMS institucional | Rendimiento | Lentitud al cargar o enviar tareas | Alta concurrencia / configuración | N1: validar entorno.<br>N2: revisar servicios y módulos | N1 → N2 | 30 min – 2 h |
| No generación de reporte de similitud | Herramienta de control de originalidad | Integración | Informe no disponible | Fallas externas del proveedor | N1: validar envío.<br>N2: verificar integración.<br>N3: escalar a proveedor | N1 → N2 → N3 | 1 – 24 h |
| Error en registro de trabajos de investigación | Sistema de gestión de investigación | Aplicación | Fallas al guardar información | Datos incorrectos o error del sistema | N1: validar datos.<br>N2: revisar sistema.<br>N3: ajuste técnico | N1 → N2 → N3 | 30 min – 2 h |
| Restricción de acceso a biblioteca digital | Biblioteca virtual | Acceso | Usuario no puede ingresar | Problemas de autenticación | N1: validar credenciales.<br>N2: revisar servicio | N1 → N2 | 15 – 60 min |
| Repositorio institucional fuera de servicio | Repositorio académico | Disponibilidad | Contenido no accesible | Fallas en servidor o almacenamiento | N1: registrar.<br>N2: revisar infraestructura | N1 → N2 | 30 min – 3 h |
| Problemas en envío/recepción de correos | Plataforma de mensajería institucional | Acceso | Correos no enviados o rebotados | Fallas del servicio o bloqueo | N1: validar cuenta.<br>N2: revisar servidor | N1 → N2 | 15 – 90 min |
| Caída de sistemas administrativos | Sistemas de gestión interna | Disponibilidad | Procesos detenidos | Fallas en red o servidor | N1: registrar.<br>N2: revisar entorno.<br>N3: soporte especializado | N1 → N2 → N3 | 1 – 6 h |
| Falta de conectividad en áreas académicas | Infraestructura de red | Conectividad | Sin acceso a red | Fallas eléctricas o equipos | N1: validar alcance.<br>N2: revisar equipos.<br>N3: proveedor | N1 → N2 → N3 | 1 – 6 h |

| Evento reportado | Servicio comprometido | Naturaleza del incidente | Manifestaciones observadas | Posible origen | Acciones sugeridas de atención | Ruta de atención | Tiempo aproximado de solución |
|---|---|---|---|---|---|---|---|
| Bloqueo de cuentas institucionales | Seguridad digital | Seguridad | Usuario sin acceso | Intentos fallidos o alertas | N1: validar identidad.<br>N2: desbloqueo | N1 → N2 | 15 – 90 min |
| Servidor institucional sin respuesta | Infraestructura física | Hardware | Servicios caídos | Fallas técnicas o temperatura | N2: diagnóstico.<br>N3: intervención especializada | N2 → N3 | 2 – 8 h |
| Indisponibilidad de servicios en la nube | Servicios externos | Dependencia externa | Aplicaciones inaccesibles | Fallas del proveedor | N2: verificar estado.<br>N3: coordinar proveedor | N2 → N3 | Variable |
| Aumento de temperatura en centro de datos | Condiciones operativas | Continuidad | Alertas térmicas | Fallas de climatización | N2: revisión técnica.<br>N3: soporte externo | N2 → N3 | 2 – 8 h |
| Equipos de laboratorio inoperativos | Equipamiento académico | Hardware | Equipos no encienden | Fallas eléctricas o físicas | N1: verificación.<br>N2: mantenimiento | N1 → N2 | 1 – 4 h |
| Equipos de cómputo con fallas de sistema | Terminales de laboratorio | Software | No inicia el sistema | Daño en sistema operativo | N1: diagnóstico.<br>N2: reinstalación | N1 → N2 | 1 – 3 h |
| Equipos administrativos con bajo rendimiento | Terminales administrativas | Hardware/Software | Lentitud general | Software desactualizado | N1: limpieza.<br>N2: optimización | N1 → N2 | 30 min – 2 h |
| Aplicaciones académicas no ejecutan | Software institucional | Aplicación | Error al iniciar | Problemas de licencia | N1: validar.<br>N2: reinstalar | N1 → N2 | 30 min – 2 h |
| Fallas en herramientas ofimáticas | Software de oficina | Aplicación | Errores en documentos | Configuración dañada | N1: guía rápida.<br>N2: reinstalación | N1 → N2 | 15 – 60 min |

Tabla 13. Estructura inicial de contenidos de la base de conocimiento según servicio y tipo de incidencia

| Servicio tecnológico | Naturaleza del evento | Consultas frecuentes (usuario) | Instructivos de autosolución | Documentación técnica de solución | Listas de verificación | Protocolos operativos | Avisos preventivos |
|---|---|---|---|---|---|---|---|
| Sistema académico institucional | Disponibilidad | ¿Por qué no puedo ingresar al sistema? | Validación de acceso en periodos críticos | Recuperación ante caída total del sistema | Verificación de servicios activos | Plan de contingencia en matrícula | Notificación por alta demanda |
| Sistema académico institucional | Rendimiento | ¿Por qué el sistema está lento? | Recomendaciones en horas pico | Ajuste de desempeño del sistema | Control de consumo de recursos | Escalamiento por saturación | Advertencia de sobrecarga |
| Plataforma virtual de aprendizaje | Acceso | ¿Por qué no aparecen mis cursos? | Ingreso correcto al entorno virtual | Corrección de accesos masivos | Validación de integración con sistema académico | Restablecimiento de acceso | Avisos en evaluaciones |
| Plataforma virtual de aprendizaje | Funcionalidad | ¿Por qué no puedo enviar tareas? | Procedimiento para envío correcto | Solución a fallas en evaluaciones | Revisión de plugins y servicios | Atención a fallas en exámenes | Alertas previas a evaluaciones |
| Herramienta de similitud académica | Integración | ¿Por qué no aparece el reporte? | Verificación del envío correcto | Corrección de integración con plataforma virtual | Validación del servicio externo | Coordinación con proveedor | Avisos de indisponibilidad |
| Sistema de gestión de investigación | Aplicación | ¿Por qué no se registra mi trabajo? | Registro correcto de información | Corrección de errores de validación | Verificación de formularios y base de datos | Soporte a registros académicos | Alertas en procesos de titulación |
| Biblioteca digital | Acceso | ¿Por qué no puedo acceder a recursos? | Acceso remoto a la biblioteca | Solución a bloqueos de acceso | Validación de autenticación | Restablecimiento de accesos | Avisos por vencimiento de licencias |
| Repositorio institucional | Disponibilidad | ¿Por qué no carga el repositorio? | Verificación de disponibilidad | Restauración del servicio | Revisión de almacenamiento | Recuperación del repositorio | Avisos de mantenimiento |
| Correo institucional | Acceso | ¿Por qué no puedo enviar correos? | Configuración del correo | Recuperación de cuentas bloqueadas | Validación de servicios de correo | Gestión ante caída del servicio | Alertas de seguridad |

| Servicio tecnológico | Naturaleza del evento | Consultas frecuentes (usuario) | Instructivos de autosolución | Documentación técnica de solución | Listas de verificación | Protocolos operativos | Avisos preventivos |
|---|---|---|---|---|---|---|---|
| Sistemas administrativos | Disponibilidad | ¿Por qué no funciona el sistema? | Recomendaciones ante fallas | Resolución de interrupciones | Verificación de servicios | Continuidad operativa administrativa | Alertas en cierres contables |
| Infraestructura de red | Conectividad | ¿Por qué no tengo conexión? | Validación de conexión local | Recuperación de red por áreas | Revisión de equipos de red | Restauración de conectividad | Alertas por fallas eléctricas |
| Seguridad digital | Seguridad | ¿Por qué mi cuenta fue bloqueada? | Gestión segura de credenciales | Atención a incidentes de seguridad | Revisión de eventos de seguridad | Gestión de incidentes de seguridad | Alertas de amenazas |
| Infraestructura de servidores | Hardware | ¿Por qué el sistema no responde? | Acciones básicas ante fallas | Resolución de fallas técnicas | Verificación de recursos físicos | Recuperación de servidores | Alertas térmicas |
| Servicios en la nube | Dependencia externa | ¿El servicio externo está caído? | Verificación de estado del proveedor | Gestión de fallas externas | Validación de SLA | Escalamiento con proveedor | Alertas del proveedor |
| Energía y climatización | Continuidad | ¿Por qué se apagaron los sistemas? | Recomendaciones ante cortes | Solución a fallas ambientales | Verificación de UPS y climatización | Plan de contingencia | Alertas de temperatura |
| Equipos de laboratorio | Hardware | ¿Por qué no funciona el equipo? | Verificación básica de encendido | Reparación de equipos | Revisión de hardware | Mantenimiento correctivo | Alertas por fallas recurrentes |
| Terminales de laboratorio | Hardware/Software | ¿Por qué no ejecuta el software? | Reinicio y validación | Reinstalación de sistema | Validación del sistema operativo | Procedimiento estándar | Alertas masivas |
| Equipos administrativos | Hardware/Software | ¿Por qué el equipo está lento? | Recomendaciones de uso | Optimización del sistema | Validación de rendimiento | Soporte técnico administrativo | Alertas por obsolescencia |
| Software académico | Aplicación | ¿Por qué no inicia el sistema? | Ejecución correcta | Corrección de licencias | Validación de instalación | Soporte especializado | Alertas de vencimiento |
| Software de oficina | Aplicación | ¿Por qué falla el programa? | Guía de solución básica | Corrección de errores | Validación de configuración | Reinstalación del software | Alertas de actualización |

**f. Definición del esquema de escalamiento en la gestión de incidentes**

El modelo planteado incorpora un mecanismo de escalamiento técnico estructurado, orientado a asegurar que cada incidente sea atendido por el nivel de soporte que cuente con las capacidades adecuadas para su resolución. Este enfoque responde a la necesidad de evitar soluciones improvisadas y garantizar una atención progresiva, organizada y eficiente.

El esquema se fundamenta en un escalamiento de tipo funcional, donde la atención de un incidente es transferida desde un nivel operativo inicial hacia equipos con mayor especialización, en función de la complejidad del problema. Este tránsito no implica pérdida de control, ya que el seguimiento del incidente se mantiene durante todo su ciclo de vida, asegurando trazabilidad y responsabilidad sobre su resolución.

**Criterios para la activación del escalamiento técnico**

Tal como se desarrolló en los fundamentos teóricos, el escalamiento funcional se activa cuando el incidente presenta condiciones que superan la capacidad de atención del primer nivel. Entre las situaciones más representativas se identifican las siguientes:

- Cuando no es posible resolver el incidente en el primer contacto con el usuario.
- Cuando se requiere intervención técnica especializada o acceso a componentes restringidos.
- Cuando el incidente compromete servicios críticos, infraestructura sensible o aplicaciones institucionales clave.

En estos escenarios, el incidente debe ser derivado de manera oportuna al nivel correspondiente, evitando retrasos innecesarios y reduciendo el impacto en la operación de los servicios.

**Lógica de progresión del escalamiento por niveles**

El modelo establece una progresión ordenada entre niveles de soporte (Nivel 1 → Nivel 2 → Nivel 3), donde cada uno cumple un rol específico dentro del proceso de atención. Este flujo permite distribuir la carga de trabajo de forma más eficiente y asegurar que los incidentes complejos sean tratados por personal con mayor dominio técnico.

A diferencia de una atención improvisada, este esquema define claramente las rutas de derivación, manteniendo la continuidad del proceso y evitando la duplicidad de esfuerzos. Además, el escalamiento no se basa únicamente en la dificultad percibida, sino en criterios definidos previamente según el tipo de servicio afectado.

**Propuesta de escalamiento técnico según tipo de servicio**

Dado que los incidentes no tienen la misma naturaleza ni requieren las mismas competencias, el modelo propone que el escalamiento se estructure en función del servicio involucrado. Esto permite asignar de manera más precisa los recursos técnicos y reducir tiempos de diagnóstico.

En este sentido, cada categoría de servicio (sistemas académicos, plataformas virtuales, infraestructura de red, seguridad, entre otros) cuenta con una ruta de escalamiento definida, en la que se identifican los niveles responsables y los puntos de derivación. Esta organización facilita una atención más coherente, evita decisiones arbitrarias y fortalece la alineación con las buenas prácticas de ITIL 4.

Tabla 14. Esquema de derivación técnica de incidentes según servicio y nivel de soporte

| **Clasificación del incidente** | **Servicio impactado** | **Nivel de atención inicial** | **Derivación técnica especializada (Nivel intermedio)** | **Intervención experta (Nivel avanzado)** |
|---|---|---|---|---|
| Interrupción del servicio | Sistema académico institucional | Nivel 1 – Atención inicial (Service Desk) | Especialista en aplicaciones académicas y servidores | Desarrollador o proveedor del sistema |
| Degradación del desempeño | Sistema académico institucional | Nivel 1 – Atención inicial | Especialista en bases de datos y rendimiento | Arquitecto de soluciones o experto TI |
| Problemas de acceso | Plataforma virtual educativa | Nivel 1 – Atención inicial | Especialista en LMS institucional | Soporte especializado del proveedor |
| Fallas funcionales | Plataforma virtual educativa | Nivel 1 – Atención inicial | Especialista en aplicaciones educativas | Equipo experto en plataforma |
| Problemas de integración | Herramientas externas académicas | Nivel 1 – Atención inicial | Especialista en integración de servicios | Proveedor externo del servicio |
| Errores de aplicación | Sistemas de gestión de investigación | Nivel 1 – Atención inicial | Especialista en sistemas institucionales | Desarrollador del sistema |
| Restricciones de acceso | Biblioteca digital | Nivel 1 – Atención inicial | Especialista en autenticación | Proveedor de contenido digital |
| Caídas del servicio | Repositorio institucional | Nivel 1 – Atención inicial | Especialista en almacenamiento y servidores | Soporte experto en infraestructura |
| Fallas en mensajería | Correo institucional | Nivel 1 – Atención inicial | Especialista en servicios de correo | Proveedor del servicio |
| Interrupción operativa | Sistemas administrativos | Nivel 1 – Atención inicial | Especialista en sistemas administrativos | Soporte externo especializado |
| Problemas de conectividad | Infraestructura de red | Nivel 1 – Atención inicial | Especialista en redes y comunicaciones | Proveedor de telecomunicaciones |
| Incidentes de seguridad | Seguridad digital | Nivel 1 – Atención inicial | Especialista en ciberseguridad | Consultor especializado |
| Fallas en infraestructura | Servidores físicos | Nivel 2 – Soporte especializado | Especialista en hardware y sistemas operativos | Proveedor o fabricante |
| Problemas en servicios cloud | Servicios en la nube | Nivel 1 – Atención inicial | Especialista en gestión cloud | Proveedor de servicios en la nube |

| Clasificación del incidente | Servicio impactado | Nivel de atención inicial | Derivación técnica especializada (Nivel intermedio) | Intervención experta (Nivel avanzado) |
|---|---|---|---|---|
| Incidentes de continuidad | Energía y climatización | Nivel 2 – Soporte especializado | Especialista en infraestructura crítica | Proveedor técnico externo |
| Fallas en equipos académicos | Equipos de laboratorio | Nivel 1 – Atención inicial | Especialista en soporte técnico | Proveedor de hardware |
| Problemas en estaciones de laboratorio | Equipos de cómputo académico | Nivel 1 – Atención inicial | Especialista en sistemas operativos | Soporte técnico especializado |
| Problemas en equipos administrativos | Equipos administrativos | Nivel 1 – Atención inicial | Especialista en soporte TI | Soporte técnico avanzado |
| Fallas en software institucional | Software académico | Nivel 1 – Atención inicial | Especialista en software académico | Proveedor/licenciante |
| Errores en software de oficina | Herramientas ofimáticas | Nivel 1 – Atención inicial | Especialista en soporte de software | Soporte técnico especializado |

El esquema propuesto consolida un modelo de derivación basado en la especialización técnica, el cual busca que cada incidente sea canalizado, desde su registro inicial, hacia el equipo con mayor capacidad para resolverlo. De esta forma, se evita que la atención dependa de la disponibilidad o criterio individual del personal, reduciendo la improvisación y asegurando una respuesta más consistente y eficiente.

Este enfoque contribuye a ordenar la operación del soporte técnico, mejorar la asignación de recursos y garantizar que los incidentes sean tratados conforme a su complejidad real. Además, fortalece la trazabilidad del proceso, ya que cada derivación queda registrada dentro del flujo de atención.

**Definición de condiciones para la identificación de incidentes críticos (Major Incidents)**

Resulta fundamental establecer criterios claros que permitan reconocer oportunamente aquellos incidentes que, por su magnitud, requieren una gestión prioritaria y coordinada. La ausencia de estos criterios suele generar respuestas

tardías, decisiones desordenadas y una alta dependencia del juicio subjetivo del personal.

La delimitación previa de estos escenarios críticos permite activar de manera inmediata mecanismos formales de escalamiento, coordinación inter áreas y comunicación institucional. Esto es especialmente relevante en entornos universitarios, donde la interrupción de servicios como matrícula, plataformas virtuales, sistemas académicos o redes institucionales puede afectar directamente a un gran número de usuarios y comprometer la continuidad de las actividades académicas.

Asimismo, la identificación oportuna de incidentes críticos facilita la asignación prioritaria de recursos, la participación de especialistas o proveedores externos y, cuando es necesario, la intervención de niveles directivos. En conjunto, estas acciones contribuyen a reducir los tiempos de recuperación del servicio (MTTR), minimizar el impacto institucional y fortalecer la gobernanza de los servicios tecnológicos, en concordancia con las buenas prácticas de ITIL 4.

Tabla 15. Parámetros para la clasificación de incidentes críticos en servicios de TI

| **Factor de evaluación** | **Descripción del criterio** | **Condición para clasificación como incidente crítico** |
|---|---|---|
| Impacto en actividades académicas | Afectación a procesos como matrícula, evaluaciones, registro de notas o titulación | Interrupción total o afectación significativa del servicio |
| Impacto en procesos administrativos | Incidencia en operaciones clave de gestión institucional | Detención parcial o total de procesos críticos |
| Alcance de usuarios afectados | Número de personas impactadas por el incidente | Afectación a más del 30% de la comunidad usuaria |
| Tiempo de indisponibilidad | Duración del incidente sin solución efectiva | Más de 2 horas en servicios esenciales |
| Riesgos de seguridad de la información | Posible exposición, alteración o pérdida de datos | Evidencia o sospecha fundamentada de vulneración |
| Afectación a infraestructura crítica | Incidentes relacionados con servidores, energía o climatización | Fallas que comprometen la continuidad operativa |

| | | |
|---|---|---|
| Frecuencia del incidente | Repetición del mismo evento en periodos cortos | Ocurrencia reiterada (más de 3 veces en un mes) |
| Nivel de exposición institucional | Posible impacto reputacional o mediático | Alta visibilidad o riesgo de afectación institucional |

**Regla operativa para la declaración de incidentes críticos**

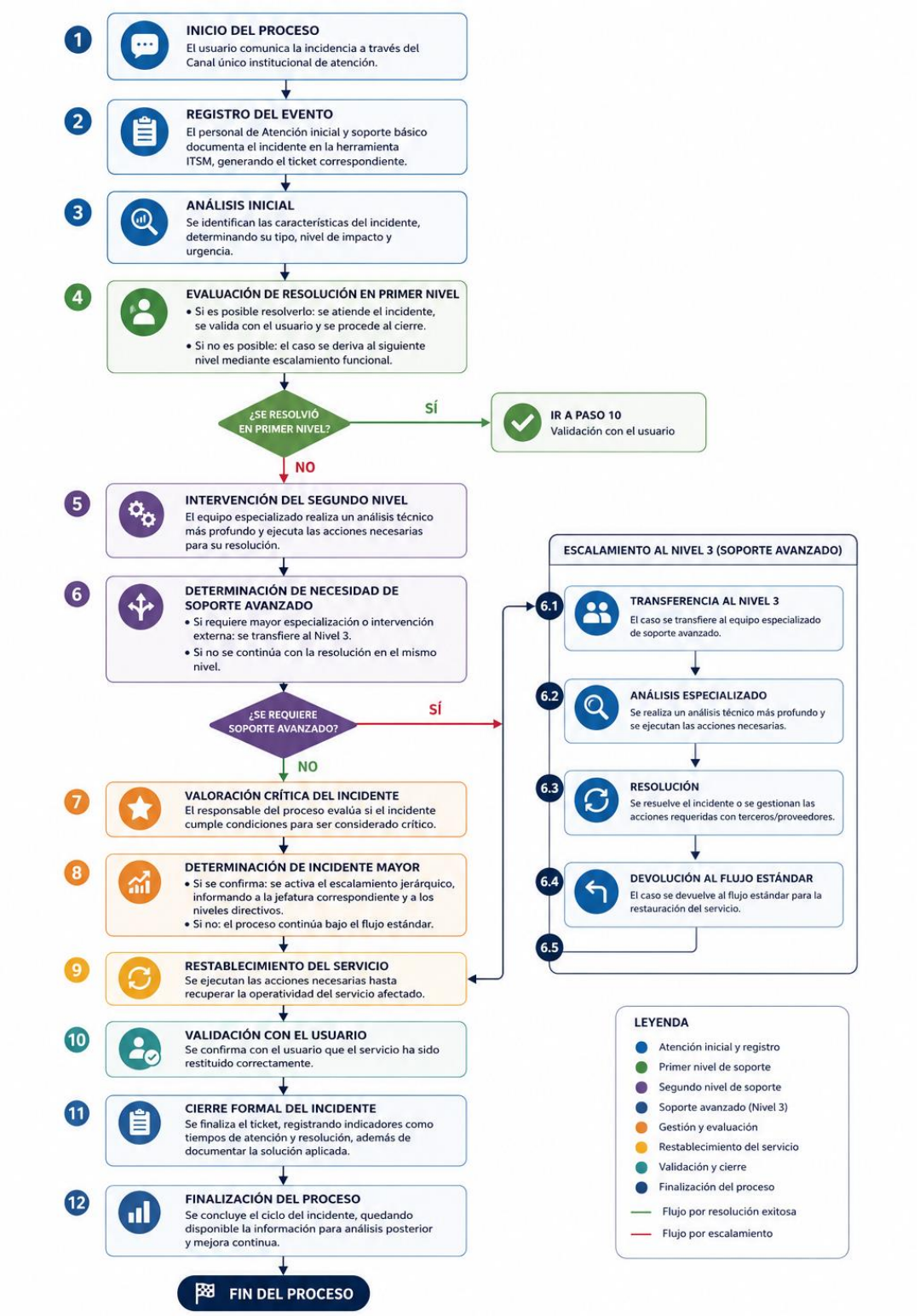
Como criterio de aplicación, se establece que un incidente debe ser clasificado como crítico cuando se cumplan simultáneamente al menos dos de los factores definidos. Esta decisión será responsabilidad del encargado de la gestión de incidentes, quien deberá activar de inmediato los mecanismos de atención prioritaria, escalamiento y comunicación institucional correspondientes.

**Secuencia operativa del proceso de escalamiento**

A continuación, se describe la dinámica planteada para el escalamiento, tanto en su dimensión técnica como organizativa, dentro del modelo propuesto:

1. **Inicio del proceso**
   El usuario comunica la incidencia a través del Canal único institucional de atención.
2. **Registro del evento**
   El personal de Atención inicial y soporte básico documenta el incidente en la herramienta ITSM, generando el ticket correspondiente.
3. **Análisis inicial**
   Se identifican las características del incidente, determinando su tipo, nivel de impacto y urgencia.
4. **Evaluación de resolución en primer nivel**
   - **Si es posible resolverlo:** se atiende el incidente, se valida con el usuario y se procede al cierre.
   - **Si no es posible:** el caso se deriva al siguiente nivel mediante escalamiento funcional.
5. **Intervención del segundo nivel**
   El equipo especializado realiza un análisis técnico más profundo y ejecuta las acciones necesarias para su resolución.
6. **Determinación de necesidad de soporte avanzado**
   - **Si requiere mayor especialización o intervención externa:** se transfiere al Nivel 3.
   - **Si no:** se continúa con la resolución en el mismo nivel.
7. **Valoración de criticidad del incidente**
   El responsable del proceso evalúa si el incidente cumple condiciones para ser considerado crítico.
8. **Determinación de incidente mayor**
   - **Si se confirma:** se activa el escalamiento jerárquico, informando a la jefatura correspondiente y a los niveles directivos.
   - **Si no:** el proceso continúa bajo el flujo estándar.
9. **Restablecimiento del servicio**
   Se ejecutan las acciones necesarias hasta recuperar la operatividad del servicio afectado.
10. **Validación con el usuario**
    Se confirma con el usuario que el servicio ha sido restituido correctamente.
11. **Cierre formal del incidente**
    Se finaliza el ticket, registrando indicadores como tiempos de atención y resolución, además de documentar la solución aplicada.
12. **Finalización del proceso**
    Se concluye el ciclo del incidente, quedando disponible la información para análisis posterior y mejora continua

Figura 5. Secuencia operativa del proceso de escalamiento



### 3.4.5. Definición de los componentes operativos de la mesa de ayuda

**a. Estandarización del registro de incidentes de TI**

El registro estructurado de incidentes se concibe como un mecanismo formal que permite capturar, de manera uniforme y obligatoria, la información relacionada con los eventos que afectan los servicios tecnológicos en las universidades (UNTRM y UNIFSLB). Su propósito principal es asegurar que cada incidente quede documentado desde el momento en que es reportado hasta su resolución final, evitando vacíos de información y garantizando consistencia en el proceso.

La implementación de este registro contribuye a dejar atrás prácticas informales, como la atención basada únicamente en llamadas, mensajes o comunicaciones no documentadas, las cuales dificultan el seguimiento y control de los incidentes. En ese sentido, el registro estructurado fortalece la gestión institucional de los servicios de TI, alineándose con las buenas prácticas de ITIL 4 y con los lineamientos de gobierno digital.

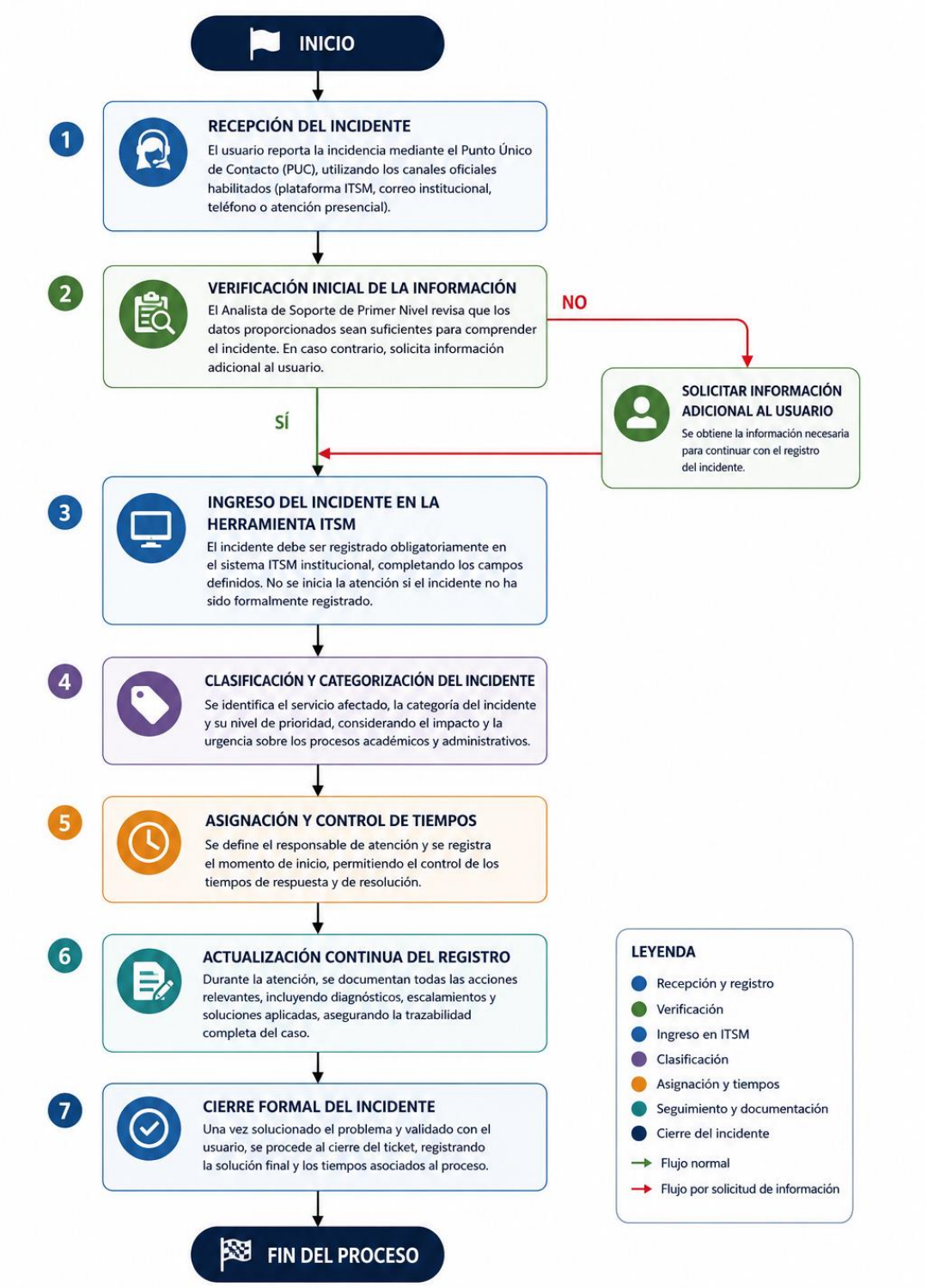
Además, este componente se convierte en el eje de la trazabilidad del proceso, ya que permite reconstruir la secuencia de atención de cada incidente, identificar responsables y medir de forma objetiva los tiempos de respuesta y solución. De igual forma, facilita la construcción de un historial confiable, útil para analizar patrones, detectar incidentes recurrentes y orientar decisiones de mejora continua.

**Secuencia operativa para el registro de incidentes**

El registro de incidentes forma parte integral del proceso de gestión y se desarrolla a través de las siguientes actividades:

1. **Recepción del incidente**
   El usuario reporta la incidencia mediante el Punto Único de Contacto (PUC), utilizando los canales oficiales habilitados (plataforma ITSM, correo institucional, teléfono o atención presencial).
2. **Verificación inicial de la información**
   El Analista de Soporte de Primer Nivel revisa que los datos proporcionados sean suficientes para comprender el incidente. En caso contrario, solicita información adicional al usuario.
3. **Ingreso del incidente en la herramienta ITSM**
   El incidente debe ser registrado obligatoriamente en el sistema ITSM institucional, completando los campos definidos. No se inicia la atención si el incidente no ha sido formalmente registrado.
4. **Clasificación y categorización del incidente**
   Se identifica el servicio afectado, la categoría del incidente y su nivel de prioridad, considerando el impacto y la urgencia sobre los procesos académicos y administrativos.
5. **Asignación y control de tiempos**
   Se define el responsable de atención y se registra el momento de inicio, permitiendo el control de los tiempos de respuesta y de resolución.
6. **Actualización continua del registro**
   Durante la atención, se documentan todas las acciones relevantes, incluyendo diagnósticos, escalamientos y soluciones aplicadas, asegurando la trazabilidad completa del caso.
7. **Cierre formal del incidente**
   Una vez solucionado el problema y validado con el usuario, se procede al cierre del ticket, registrando la solución final y los tiempos asociados al proceso

Figura 6. Secuencia operativa para el registro de incidentes



**Definición de la estructura del registro de incidentes**

La estructura del registro establece el conjunto de campos obligatorios que deben completarse en cada incidente, asegurando que la información sea homogénea y útil para su análisis posterior. Este conjunto de datos constituye la base para la gestión operativa, el control del servicio y la generación de indicadores.

Tabla 16. Estructura de datos para el registro de incidentes en la mesa de ayuda

| Elemento de información | Detalle del contenido registrado |
|---|---|
| Fecha y hora de registro | Fecha y hora exacta en que el incidente es ingresado al sistema ITSM. |
| Identificación del usuario | Datos del usuario que reporta el incidente (nombre, código institucional u otro identificador). |
| Área o dependencia involucrada | Unidad académica o administrativa afectada (facultad, escuela profesional, oficina, etc.). |
| Servicio tecnológico comprometido | Plataforma o servicio impactado (sistema académico, aula virtual, red institucional, correo, entre otros). |
| Tipificación del incidente | Clasificación del evento según su naturaleza (acceso, disponibilidad, rendimiento, seguridad, infraestructura, etc.). |
| Nivel de criticidad | Grado de prioridad definido a partir del impacto y la urgencia (bajo, medio, alto o crítico). |
| Descripción del problema | Detalle de los síntomas o comportamientos reportados por el usuario. |
| Tiempo de inicio de atención | Intervalo entre el registro del incidente y el inicio de su tratamiento. |
| Responsable de atención | Nivel de soporte o especialista asignado para la resolución del incidente. |
| Registro de acciones ejecutadas | Secuencia cronológica de actividades realizadas durante el proceso de atención. |
| Resultado de la intervención | Descripción de la solución implementada para restablecer el servicio. |
| Marca temporal de cierre | Fecha y hora en que el incidente es concluido formalmente. |
| Duración total del incidente | Tiempo total transcurrido desde el registro hasta la solución definitiva. |
| Estado del caso | Situación actual del incidente (registrado, en proceso, escalado, resuelto o cerrado). |
| Confirmación del usuario | Validación del usuario respecto a la correcta solución del incidente. |

**b. Categorización de incidentes**

La definición de una taxonomía estructurada para la categorización de incidentes tiene como propósito establecer un esquema uniforme que permita identificar, ordenar y tratar de manera consistente los eventos que afectan los servicios de tecnologías de la información en las universidades analizadas. Este enfoque facilita que todos los actores involucrados utilicen un mismo criterio al momento de registrar, interpretar y gestionar un incidente, reduciendo ambigüedades y mejorando la coordinación operativa.

Asimismo, la categorización estandarizada permite optimizar la asignación de los casos al nivel de soporte correspondiente, garantizar una priorización coherente basada en impacto y urgencia, y activar de manera oportuna los mecanismos de escalamiento definidos en el modelo. Desde una perspectiva analítica, esta estructura también posibilita consolidar información histórica confiable, lo que favorece el análisis de tendencias, la identificación de incidentes recurrentes y la implementación de acciones de mejora continua alineadas con ITIL 4.

**Esquema propuesto de categorización de incidentes**

A continuación, se presenta una propuesta de clasificación inicial de incidentes, organizada según los principales servicios tecnológicos identificados en las universidades UNTRM y UNIFSLB:

Tabla 17. Taxonomía de incidentes por servicio TI en universidades públicas (UNTRM – UNIFSLB)

| Dominio del servicio TI | Naturaleza del incidente | Descripción del evento | Punto de atención inicial | Ruta de escalamiento técnico |
|---|---|---|---|---|
| Sistema Académico Institucional (SIGA / Académico) | Interrupción del servicio | Imposibilidad de acceso o caída total del sistema en periodos críticos (matrícula, consultas). | Nivel 1 (PUC) | Nivel 2 → Nivel 3 |

| Dominio del servicio TI | Naturaleza del incidente | Descripción del evento | Punto de atención inicial | Ruta de escalamiento técnico |
|---|---|---|---|---|
| Sistema Académico Institucional | Degradación del rendimiento | Lentitud significativa en procesos como matrícula, registro de notas o consultas. | Nivel 1 | Nivel 2 |
| Plataforma de Aprendizaje Virtual (Moodle institucional) | Problemas de acceso | Usuarios no pueden ingresar a cursos, evaluaciones o recursos virtuales. | Nivel 1 | Nivel 2 |
| Plataforma de Aprendizaje Virtual | Fallas funcionales | Errores en evaluaciones, carga de tareas o integración con herramientas externas. | Nivel 1 | Nivel 2 → Nivel 3 |
| Sistemas antiplagio / servicios externos (Turnitin u otros) | Integración externa | No se generan reportes o el servicio presenta indisponibilidad parcial o total. | Nivel 1 | Nivel 2 → Nivel 3 |
| Sistemas de gestión de investigación (repositorios / tesis) | Error de aplicación | Fallas al registrar, consultar o validar información académica. | Nivel 1 | Nivel 2 → Nivel 3 |
| Biblioteca digital y recursos académicos | Restricción de acceso | Imposibilidad de acceder a bases de datos o contenido digital. | Nivel 1 | Nivel 2 |
| Repositorios institucionales | Indisponibilidad | Plataforma no accesible o errores en visualización de documentos. | Nivel 1 | Nivel 2 |
| Correo institucional | Fallas de comunicación | Problemas en envío, recepción o autenticación de cuentas. | Nivel 1 | Nivel 2 |
| Sistemas administrativos (ERP, SIGA administrativo, planillas) | Interrupción operativa | Paralización de procesos administrativos críticos. | Nivel 1 | Nivel 2 → Nivel 3 |

| Dominio del servicio TI | Naturaleza del incidente | Descripción del evento | Punto de atención inicial | Ruta de escalamiento técnico |
|---|---|---|---|---|
| Infraestructura de red (LAN/WAN, WiFi institucional) | Problemas de conectividad | Pérdida parcial o total de conexión en sedes, facultades o áreas. | Nivel 1 | Nivel 2 → Nivel 3 |
| Seguridad informática y comunicaciones | Incidentes de seguridad | Intentos de intrusión, accesos indebidos o compromisos de cuentas. | Nivel 1 | Nivel 2 → Nivel 3 |
| Plataformas de servidores físicos | Fallas de infraestructura | Caída de servidores, saturación o problemas de hardware. | Nivel 2 | Nivel 3 |
| Servicios en la nube (hosting, SaaS institucional) | Indisponibilidad externa | Fallas en servicios provistos por terceros. | Nivel 1 | Nivel 2 → Nivel 3 |
| Energía y climatización del datacenter | Riesgos de continuidad | Problemas eléctricos o térmicos que afectan la operación de servicios. | Nivel 2 | Nivel 3 |
| Equipamiento de laboratorios académicos | Fallas de hardware | Equipos inoperativos que afectan prácticas académicas. | Nivel 1 | Nivel 2 |
| Estaciones de trabajo (laboratorios) | Problemas de software/hardware | Fallas en sistema operativo, aplicaciones o periféricos. | Nivel 1 | Nivel 2 |
| Equipos informáticos administrativos | Problemas operativos | Fallas que afectan la ejecución de procesos administrativos. | Nivel 1 | Nivel 2 |
| Software especializado académico | Error de aplicación | Problemas en software técnico utilizado en carreras (ingenierías, etc.). | Nivel 1 | Nivel 2 |
| Herramientas de ofimática institucional | Incidentes de uso | Fallas en aplicaciones como procesadores de texto, hojas de cálculo, etc. | Nivel 1 | Nivel 2 |

**c. Definición del esquema de priorización de incidentes de TI**

La priorización de incidentes basada en la combinación de impacto y urgencia tiene como finalidad organizar la atención de los eventos tecnológicos de acuerdo con su nivel real de afectación sobre los procesos académicos y administrativos, evitando que la gestión dependa del orden de llegada o de presiones informales por parte de los usuarios.

Este enfoque permite optimizar el uso de los recursos técnicos disponibles, garantizando que los incidentes que afectan servicios críticos —como plataformas académicas, sistemas administrativos, redes institucionales o seguridad digital— sean atendidos con mayor inmediatez. Asimismo, contribuye a fortalecer la continuidad operativa, reducir riesgos institucionales y mejorar la transparencia en la toma de decisiones dentro del proceso de gestión de incidentes.

**Valoración del impacto de los incidentes**

La definición de una escala de impacto resulta esencial para estimar de manera objetiva el grado de afectación que un incidente genera sobre los servicios institucionales. Este criterio evalúa la magnitud de la interrupción considerando variables como la cantidad de usuarios afectados, la criticidad del servicio comprometido y el nivel de afectación a las actividades académicas o administrativas.

La ausencia de una escala estructurada conduce a decisiones subjetivas y a una asignación ineficiente de recursos. En cambio, una categorización estandarizada permite uniformizar criterios entre los niveles de soporte, facilitar comparaciones entre incidentes y generar información confiable para el análisis de tendencias y la mejora continua.

Las escalas de impacto y urgencia fueron construidas tomando como referencia las recomendaciones de ITIL 4 para la priorización de incidentes, adaptándolas al contexto operativo universitario y a los servicios críticos identificados durante el diagnóstico.

Tabla 18. Escala propuesta de evaluación del impacto de incidentes en servicios TI universitarios

| Nivel | Categoría de impacto | Descripción operativa |
|---|---|---|
| 5 | Muy alto (crítico) | Interrupción total de servicios esenciales (plataformas académicas, red institucional, seguridad), afectando a gran parte de la comunidad o comprometiendo datos institucionales. |
| 4 | Alto | Afectación considerable en procesos clave (evaluaciones, matrícula, trámites administrativos), impactando múltiples áreas o facultades. |
| 3 | Moderado | Interrupción parcial que afecta a grupos específicos (facultad, laboratorio o unidad administrativa). |
| 2 | Bajo | Incidente limitado a pocos usuarios o funcionalidades secundarias, con alternativas disponibles. |
| 1 | Muy bajo | Evento menor sin impacto significativo en la operación institucional. |

**Evaluación de la urgencia de atención**

La urgencia se relaciona con la rapidez requerida para atender un incidente, considerando el tiempo disponible antes de que su impacto aumente o genere consecuencias mayores. Este criterio permite anticipar escenarios críticos, especialmente en contextos sensibles del calendario académico.

La incorporación de esta escala evita respuestas improvisadas y favorece una gestión más equitativa y predecible, alineada con los principios de ITIL 4.

Tabla 19. Escala propuesta de evaluación de la urgencia en la atención de incidentes

| Nivel | Categoría de urgencia | Descripción operativa |
|---|---|---|
| 5 | Inmediata | Requiere atención urgente para evitar interrupción de servicios críticos o daño significativo. |
| 4 | Alta | Debe atenderse en corto plazo para evitar escalamiento del incidente. |
| 3 | Media | Puede resolverse dentro de la jornada sin afectar gravemente la operación. |
| 2 | Baja | Atención programable sin impacto relevante en el servicio. |
| 1 | Planificada | Puede incluirse en mantenimiento o mejora programada. |

**Determinación de la prioridad del incidente**

La prioridad se establece mediante la combinación de los niveles de impacto y urgencia, lo que permite definir el orden de atención de los incidentes dentro del sistema de gestión. Este mecanismo garantiza coherencia en la toma de decisiones, evitando criterios subjetivos y alineando la operación con las buenas prácticas de ITIL 4.

Tabla 20. Matriz de priorización de incidentes (Impacto × Urgencia)

| Impacto \ Urgencia | 5 Inmediata | 4 Alta | 3 Media | 2 Baja | 1 Planificada |
|---|---|---|---|---|---|
| **5 Crítico** | Prioridad 1 | Prioridad 1 | Prioridad 2 | Prioridad 2 | Prioridad 3 |
| **4 Alto** | Prioridad 1 | Prioridad 2 | Prioridad 2 | Prioridad 3 | Prioridad 3 |
| **3 Moderado** | Prioridad 2 | Prioridad 2 | Prioridad 3 | Prioridad 3 | Prioridad 4 |
| **2 Bajo** | Prioridad 2 | Prioridad 3 | Prioridad 3 | Prioridad 4 | Prioridad 4 |
| **1 Muy bajo** | Prioridad 3 | Prioridad 3 | Prioridad 4 | Prioridad 4 | Prioridad 4 |

A partir de la matriz de priorización definida para la gestión de incidentes de TI, se establecen lineamientos claros para la toma de decisiones en la atención de los eventos reportados. En este sentido:

Los incidentes clasificados como de prioridad 1 requieren atención inmediata, activando mecanismos de respuesta urgente y, de ser necesario, procedimientos de escalamiento jerárquico debido a su alto impacto sobre los servicios institucionales.

Los incidentes con prioridad 2 deben ser gestionados de manera preferente por el nivel especializado de soporte, asegurando una resolución oportuna mediante la intervención de personal técnico con competencias específicas.

Los incidentes de prioridad 3 y 4 son atendidos inicialmente por el nivel operativo de soporte, organizando su resolución en función de la disponibilidad y la planificación del servicio.

**d. Mecanismo de asignación inteligente de incidentes de TI**

El establecimiento de un esquema de asignación automática o asistida tiene como propósito optimizar la distribución de los incidentes dentro del sistema de

gestión, asegurando que cada caso sea atendido por el recurso técnico más idóneo desde el momento de su registro. Este enfoque contribuye a reducir los tiempos de atención y resolución (MTTR), mejorar la resolución en el primer contacto (FCR) y fortalecer la trazabilidad del proceso.

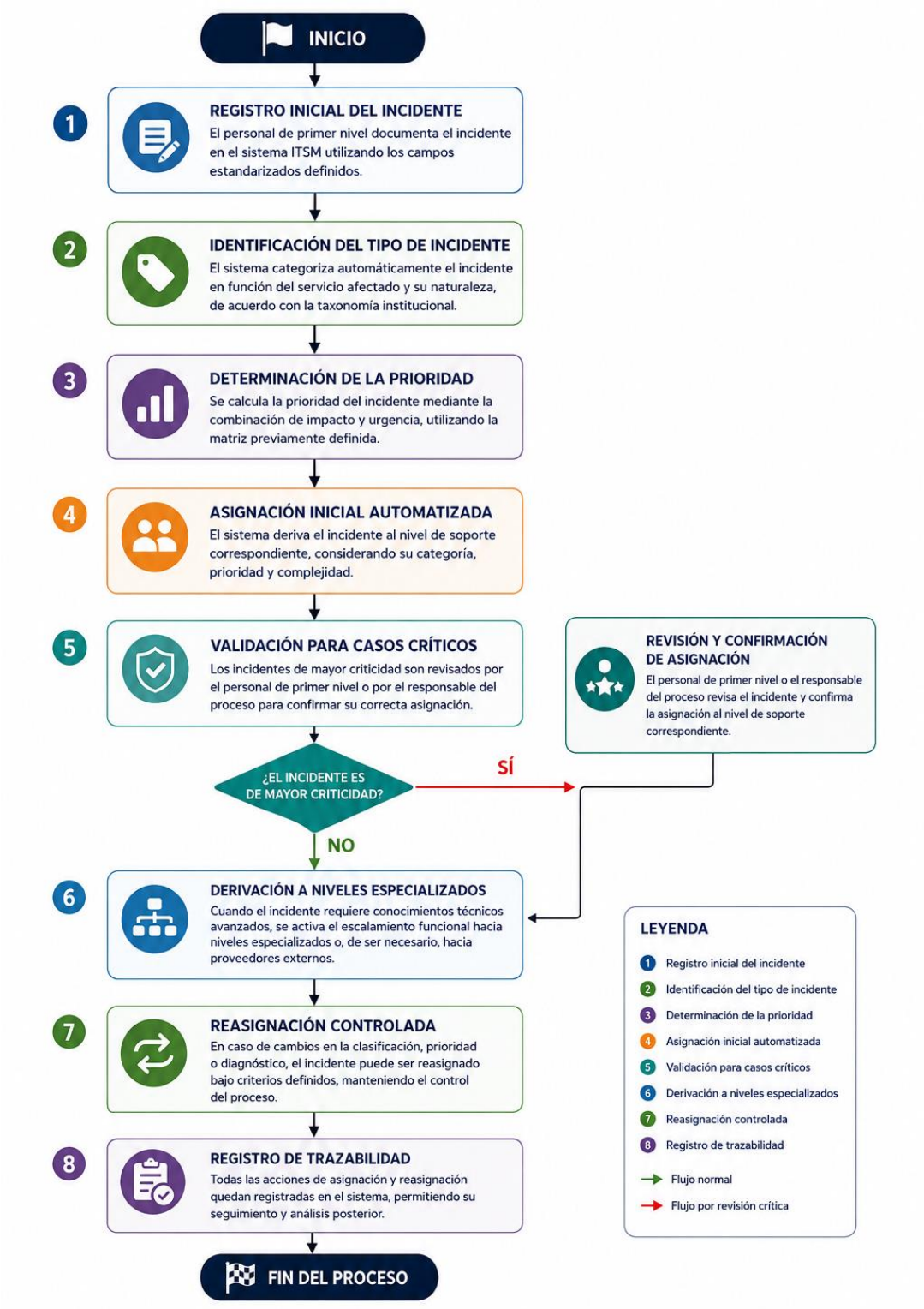
En el contexto de las universidades analizadas, donde convergen múltiples servicios tecnológicos críticos, como: sistemas académicos, plataformas virtuales, infraestructura de red, servicios administrativos y mecanismos de seguridad, la asignación manual basada en criterios individuales genera ineficiencias, retrasos y variabilidad en la calidad del servicio. En contraste, la implementación de reglas de asignación basadas en taxonomías, niveles de prioridad y rutas de escalamiento permite una gestión más objetiva, predecible y alineada con ITIL 4.

**Secuencia operativa para la asignación de incidentes**

El proceso de asignación se ejecuta mediante el sistema ITSM integrado al Canal único institucional de atención, combinando automatización con validación técnica en casos críticos. La secuencia propuesta es la siguiente:

1. **Registro inicial del incidente**
   El personal de primer nivel documenta el incidente en el sistema ITSM utilizando los campos estandarizados definidos.
2. **Identificación del tipo de incidente**
   El sistema categoriza automáticamente el incidente en función del servicio afectado y su naturaleza, de acuerdo con la taxonomía institucional.
3. **Determinación de la prioridad**
   Se calcula la prioridad del incidente mediante la combinación de impacto y urgencia, utilizando la matriz previamente definida.
4. **Asignación inicial automatizada**
   El sistema deriva el incidente al nivel de soporte correspondiente, considerando su categoría, prioridad y complejidad.
5. **Validación para casos críticos**
   Los incidentes de mayor criticidad son revisados por el personal de primer nivel o por el responsable del proceso para confirmar su correcta asignación.
6. **Derivación a niveles especializados**
   Cuando el incidente requiere conocimientos técnicos avanzados, se activa el escalamiento funcional hacia niveles especializados o, de ser necesario, hacia proveedores externos.
7. **Reasignación controlada**
   En caso de cambios en la clasificación, prioridad o diagnóstico, el incidente puede ser reasignado bajo criterios definidos, manteniendo el control del proceso.
8. **Registro de trazabilidad**
   Todas las acciones de asignación y reasignación quedan registradas en el sistema, permitiendo su seguimiento y análisis posterior

Figura 7. Secuencia operativa para la asignación de incidentes



**Criterios operativos para la asignación de incidentes**

Para asegurar una gestión eficiente, la asignación de incidentes se rige por las siguientes reglas:

- La asignación debe basarse en la categoría del servicio afectado y el tipo de incidente identificado.
- La prioridad definida por la matriz impacto–urgencia determina el nivel de atención requerido.
- Los incidentes simples o de baja complejidad deben resolverse en el primer nivel de soporte, promoviendo la resolución en el primer contacto.
- Los incidentes que superen las capacidades del nivel inicial deben ser derivados al nivel especializado correspondiente, evitando retrasos innecesarios.
- Los incidentes que involucren servicios críticos o dependencias externas deben ser escalados oportunamente al nivel avanzado o proveedores.
- Toda asignación debe garantizar la trazabilidad completa del incidente, evitando pérdidas de información o duplicidad de esfuerzos.

**e. Gestión de soluciones estandarizadas y documentación del conocimiento**

La estandarización y registro de las soluciones aplicadas a los incidentes tiene como objetivo garantizar que cada intervención técnica genere evidencia clara, estructurada y reutilizable dentro de la organización. Este enfoque evita la dependencia del conocimiento individual, reduce la improvisación en la atención y facilita la replicabilidad de las soluciones en escenarios similares.

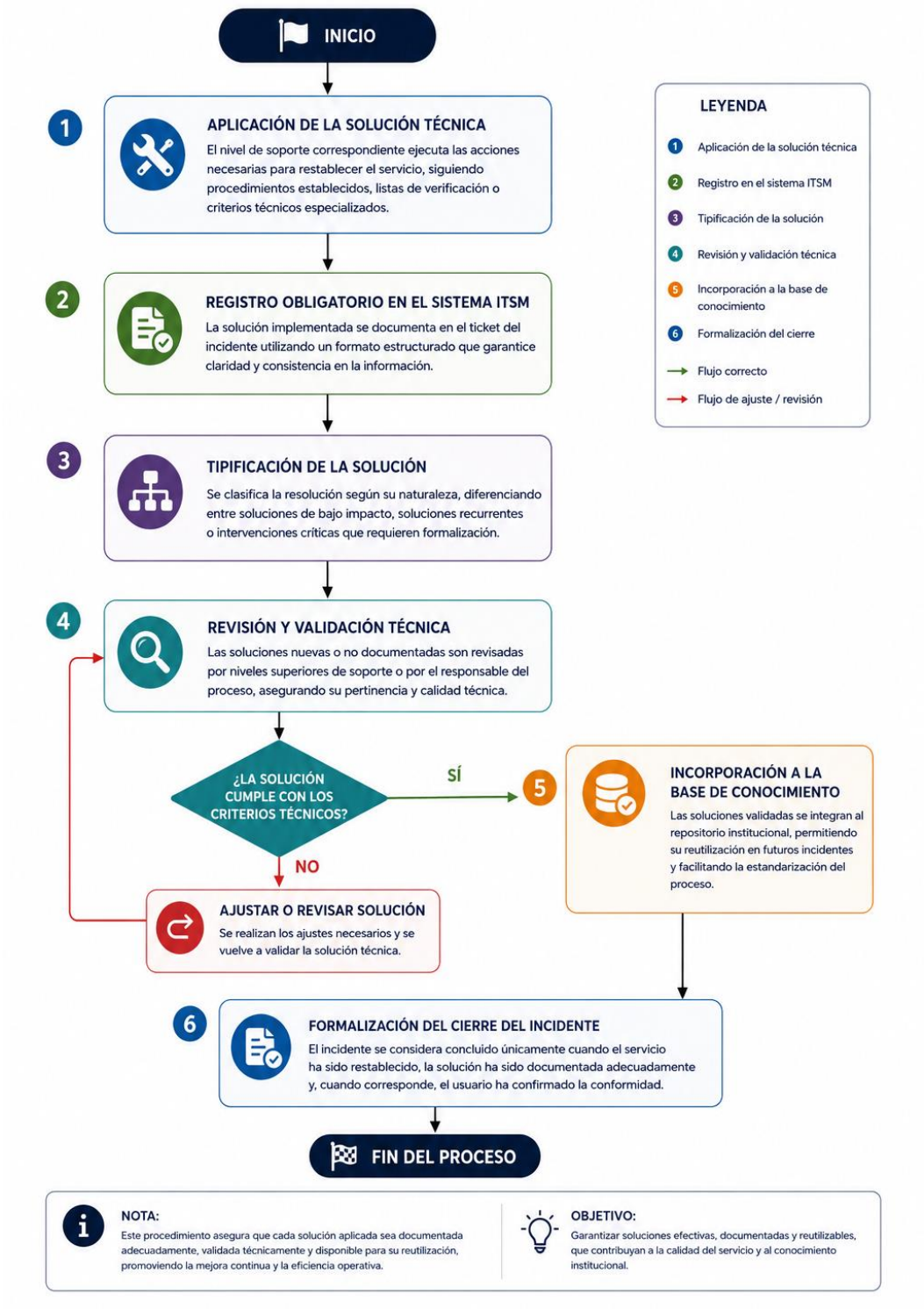
Asimismo, la documentación sistemática de las resoluciones permite convertir cada incidente atendido en un activo de conocimiento institucional, fortaleciendo la continuidad operativa y promoviendo la mejora continua del proceso de gestión de incidentes. En el contexto de las universidades analizadas, donde los servicios tecnológicos soportan actividades académicas críticas, este componente resulta clave para disminuir la recurrencia de fallas, optimizar los tiempos de resolución (MTTR) y aumentar la capacidad de resolución en el primer contacto (FCR).

**Procedimiento para la gestión estructurada de soluciones**

El proceso de documentación de soluciones se integra al ciclo de vida del incidente y se desarrolla mediante las siguientes actividades:

1. **Aplicación de la solución técnica**
   El nivel de soporte correspondiente ejecuta las acciones necesarias para restablecer el servicio, siguiendo procedimientos establecidos, listas de verificación o criterios técnicos especializados.
2. **Registro obligatorio en el sistema ITSM**
   La solución implementada se documenta en el ticket del incidente utilizando un formato estructurado que garantice claridad y consistencia en la información.
3. **Tipificación de la solución**
   Se clasifica la resolución según su naturaleza, diferenciando entre soluciones de bajo impacto, soluciones recurrentes o intervenciones críticas que requieren formalización.
4. **Revisión y validación técnica**
   Las soluciones nuevas o no documentadas son revisadas por niveles superiores de soporte o por el responsable del proceso, asegurando su pertinencia y calidad técnica.
5. **Incorporación a la base de conocimiento**
   Las soluciones validadas se integran al repositorio institucional, permitiendo su reutilización en futuros incidentes y facilitando la estandarización del proceso.
6. **Formalización del cierre del incidente**
   El incidente se considera concluido únicamente cuando el servicio ha sido restablecido, la solución ha sido documentada adecuadamente y, cuando corresponde, el usuario ha confirmado la conformidad

Figura 8. Procedimiento para la gestión estructurada de soluciones



**Estructura mínima para el registro de soluciones**

Para garantizar uniformidad en la documentación, cada resolución de incidente debe registrarse considerando al menos los siguientes elementos:

- Identificación del incidente y del servicio afectado
- Descripción del problema y síntomas observados
- Diagnóstico técnico realizado
- Causa raíz identificada (cuando sea posible)
- Acciones ejecutadas para la solución
- Resultado obtenido y estado final del servicio
- Nivel de soporte que intervino
- Recomendaciones o medidas preventivas

**f. Formalización del cierre de incidentes en el proceso ITSM**

El cierre formal del incidente representa la etapa final del ciclo de gestión y tiene como objetivo asegurar que el servicio afectado haya sido restablecido de manera efectiva, que la solución implementada se encuentre correctamente registrada y que exista validación por parte del usuario o del área afectada. Este proceso permite consolidar la trazabilidad del incidente, evitar cierres prematuros y fortalecer la generación de conocimiento organizacional.

En entornos universitarios analizados, donde los servicios tecnológicos soportan procesos críticos como matrícula, evaluaciones, gestión académica y operaciones administrativas, la formalización del cierre adquiere un rol fundamental. La ausencia de un cierre estructurado genera inconsistencias operativas, dificulta la medición del desempeño del servicio y limita la capacidad de mejora continua dentro del modelo de gestión de incidentes.

**Requisitos para la finalización del incidente**

Un incidente podrá ser concluido formalmente únicamente cuando se verifique el cumplimiento de los siguientes criterios:

- El servicio afectado ha sido completamente restablecido y validado técnicamente.
- La solución implementada se encuentra registrada de manera estructurada en el sistema ITSM.

- Se ha documentado el diagnóstico, la causa y las acciones ejecutadas.
- El usuario o área afectada ha confirmado la conformidad, o se ha cumplido el periodo establecido para dicha validación.
- El incidente ha sido vinculado a la base de conocimiento cuando corresponde, contribuyendo a la reutilización de soluciones.

**Secuencia operativa para el cierre del incidente**

El proceso de cierre se desarrolla mediante las siguientes actividades:

1. **Verificación técnica del servicio**
   El nivel de soporte responsable valida que el servicio funcione correctamente y sin incidencias residuales.
2. **Registro completo de la intervención**
   Se consolida la información del incidente en el sistema ITSM, incluyendo diagnóstico, acciones ejecutadas, tiempos y solución final.
3. **Confirmación del usuario**
   Se notifica al usuario sobre la solución implementada, otorgándole un plazo definido para validar la conformidad.
4. **Actualización del repositorio de conocimiento**
   Cuando el incidente presenta valor recurrente o lecciones relevantes, se documenta o actualiza el contenido correspondiente en la base de conocimientos.
5. **Cierre administrativo del caso**
   El personal del primer nivel ejecuta el cierre formal en el sistema, dejando evidencia completa del proceso.
6. **Revisión posterior (si aplica)**
   En incidentes de alta criticidad, el responsable del proceso realiza una revisión del cierre para validar su calidad y consistencia.

Figura 9. Secuencia operativa para el cierre del incidente

**Participación de roles en el cierre del incidente**

- Soporte de primer nivel: ejecuta el cierre formal del incidente y gestiona la comunicación con el usuario.
- Soporte especializado: valida técnicamente las soluciones en incidentes de mayor complejidad.
- Nivel experto o proveedores: certifican la resolución en casos críticos o estructurales.
- Responsable del proceso de incidentes: supervisa cierres relevantes y analiza indicadores asociados al desempeño del proceso.

**Condiciones para la reapertura de incidentes**

La reapertura de un incidente constituye un mecanismo de control que permite garantizar la calidad real de la solución implementada. En entornos complejos, es posible que una solución aparente no sea definitiva, por lo que este mecanismo evita cierres inconsistentes y protege la continuidad del servicio.

Desde el enfoque de ITIL 4, la reapertura contribuye a mantener la confiabilidad del proceso, asegurando que los indicadores de desempeño reflejen la realidad operativa y que no se consoliden soluciones incompletas o temporales.

Un incidente previamente cerrado podrá reabrirse cuando se presenten las siguientes situaciones:

- El servicio vuelve a presentar fallas dentro del periodo de validación establecido.
- El usuario indica que la solución no resolvió completamente el problema.
- Se identifican inconsistencias o vacíos en la documentación registrada.
- Se evidencia que la causa raíz no fue correctamente tratada.

**g. Sistema de medición del desempeño y reportes de gestión de incidentes**

La implementación de un esquema de medición del desempeño tiene como propósito evaluar de manera objetiva la eficacia del proceso de gestión de incidentes, identificar patrones de comportamiento, anticipar riesgos operativos y sustentar la toma de decisiones estratégicas en el ámbito de las tecnologías de la información.

En el contexto de las universidades analizadas, donde los servicios digitales soportan procesos críticos (matrícula, evaluación, gestión académica, investigación y administración), el uso de indicadores permite evolucionar desde un enfoque reactivo hacia un modelo de gestión basado en evidencia, alineado con los principios de mejora continua de ITIL 4.

Los indicadores propuestos que se muestran en las tablas, 21, 22 y 23 fueron seleccionados debido a su amplio uso en ITSM e ITIL 4 para evaluar la eficiencia operativa, la calidad del servicio y la capacidad de respuesta ante incidentes.

Tabla 21. Indicadores de desempeño operativo del proceso de incidentes

| **Métrica clave** | **Método de cálculo** | **Frecuencia de evaluación** | **Responsable de seguimiento** |
|---|---|---|---|
| Tiempo promedio de resolución (MTTR) por servicio y prioridad | Suma de tiempos de resolución / número total de incidentes resueltos (segmentado) | Mensual | Responsable del proceso de incidentes |
| Resolución en primer contacto (FCR) | (Incidentes resueltos en el primer nivel / total de incidentes) × 100 | Mensual | Equipo de soporte de primer nivel |
| Distribución de incidentes por categoría | Conteo de incidentes clasificados por tipo de servicio y naturaleza del incidente | Semanal / Mensual | Responsable del proceso |
| Cumplimiento de niveles de servicio (SLA) | (Incidentes atendidos dentro del tiempo objetivo / total de incidentes) × 100 | Mensual | Jefatura TI / responsable del proceso |
| Tasa de reapertura de incidentes | (Incidentes reabiertos / incidentes cerrados) × 100 | Mensual | Responsable del proceso |

Tabla 22. Indicadores de calidad del servicio de soporte

| **Métrica de calidad** | **Método de evaluación** | **Frecuencia** | **Responsable** |
|---|---|---|---|
| Nivel de satisfacción del usuario | Promedio de calificaciones obtenidas en encuestas post-atención | Mensual | Soporte de primer nivel |
| Incidencia de problemas recurrentes | Conteo de incidentes repetitivos por servicio en un periodo determinado | Mensual | Responsable del proceso |

| | | | |
|---|---|---|---|
| Uso y actualización de la base de conocimiento | Número de consultas, artículos creados o actualizados por periodo | Mensual | Soporte especializado |

Tabla 23. Indicadores de riesgo y continuidad del servicio

| Métrica de control | Método de cálculo | Frecuencia | Responsable |
|---|---|---|---|
| Incidentes de alta criticidad | Número de incidentes mayores, duración e impacto asociado | Trimestral | Responsable del proceso / Jefatura TI |
| Eventos de seguridad | Conteo de incidentes de seguridad y tiempo promedio de contención | Mensual / Trimestral | Especialista en seguridad |
| Nivel de disponibilidad de servicios críticos | (Tiempo total de operación – tiempo de indisponibilidad) / tiempo total × 100 | Trimestral | Responsable del proceso |

**h. Estrategia de comunicación anticipada y seguimiento de incidentes**

La comunicación anticipada y oportuna con los usuarios tiene como finalidad reducir la incertidumbre, mejorar la percepción del servicio y facilitar la gestión de expectativas antes, durante y después de la ocurrencia de incidentes tecnológicos. En entornos universitarios, donde los sistemas digitales soportan actividades críticas, informar adecuadamente resulta tan relevante como la resolución técnica del incidente.

**Períodos clave del proceso de comunicación**

El modelo propuesto contempla distintos momentos de interacción informativa:

1. **Comunicación preventiva**

   Difusión de alertas sobre periodos de alta demanda, mantenimientos programados o riesgos identificados.
2. **Notificación de incidentes**

   Aviso inmediato ante la detección de fallas o degradación en servicios críticos.
3. **Seguimiento del incidente**

   Actualización periódica del estado del incidente, especialmente en casos de alta criticidad.
4. **Confirmación de restablecimiento**

Comunicación oficial cuando el servicio ha sido recuperado.

5. **Retroalimentación y aprendizaje**

   Difusión de recomendaciones, buenas prácticas y guías de autogestión.

Tabla 24. Canales institucionales de comunicación para la gestión de incidentes

| Medio de comunicación | Uso principal |
|---|---|
| Correo institucional | Canal oficial para notificaciones formales |
| Plataformas académicas (SIA, aula virtual) | Publicación de alertas mediante banners informativos |
| Portal web o intranet institucional | Difusión del estado de los servicios y comunicados generales |
| Sistema ITSM (Mesa de ayuda) | Notificaciones automáticas sobre el estado del incidente |

Tabla 25. Tipología de mensajes en la gestión de incidentes

| Tipo de comunicación | Descripción |
|---|---|
| Alertas preventivas | Avisos anticipados sobre riesgos, mantenimientos o alta demanda |
| Notificación de incidente | Comunicación inicial sobre la interrupción o degradación del servicio |
| Actualizaciones de estado | Información periódica sobre avances y tiempos estimados de solución |
| Aviso de restablecimiento | Confirmación de recuperación del servicio |
| Recomendaciones técnicas | Orientaciones y guías disponibles en la base de conocimiento |

## 3.5. Validación del marco de trabajo para la gestión de incidentes

### 3.5.1. Propósito del proceso de validación del modelo propuesto

El proceso de validación del modelo de gestión de incidentes de tecnologías de la información tuvo como finalidad comprobar su solidez metodológica y su pertinencia técnica, en función de criterios como Cobertura del modelo, Comprensibilidad, Consistencia interna y Pertinencia institucional.

Esta validación se orientó a evaluar si el modelo propuesto incorpora adecuadamente las buenas prácticas establecidas en el marco de referencia ITIL 4,

particularmente en las actividades de registro, clasificación, priorización, escalamiento, resolución y cierre de incidentes. Asimismo, se buscó determinar si los elementos estructurales y funcionales planteados son viables para su implementación en entornos como la UNTRM y la UNIFSLB.

Para tal fin, se utilizó la técnica de juicio de expertos, considerando la opinión especializada de profesionales con experiencia en gestión de servicios de TI, seguridad de la información y gobierno de tecnologías.

### 3.5.2. Criterios para la selección de especialistas evaluadores

La selección de los expertos se realizó considerando criterios que garantizan la idoneidad y experiencia en la temática abordada. En ese sentido, se definieron las siguientes condiciones:

a. Con experiencia profesional vinculada a la gestión de TI, gestión de servicios de TI, seguridad de la información o auditoría de TI.
b. Acreditar una trayectoria mínima de cinco años en áreas relacionadas con ITSM, ITIL, gestión de incidentes o gestión de riesgos tecnológicos.

En base a estos criterios, se seleccionaron cuatro especialistas, quienes participaron en la evaluación del modelo propuesto, aportando una visión técnica y práctica sobre su diseño y aplicabilidad.

La participación de cuatro especialistas para la evaluación del modelo propuesto se consideró suficiente debido a la naturaleza cualitativa y especializada del proceso de validación. En investigaciones basadas en juicio experto y validación de contenido mediante el coeficiente V de Aiken, no se requiere un número elevado de participantes, sino evaluadores con experiencia y conocimiento específico sobre la temática analizada (Nurjanah, et.al, 2023). Así mismo, Aiken (1985) establece que este método puede aplicarse con un número reducido de jueces expertos, siempre que estos posean competencias relacionadas con el objeto de evaluación. Asimismo, estudios recientes sobre validación de instrumentos mediante V de Aiken han utilizado entre tres y siete expertos para garantizar la consistencia y pertinencia de la valoración realizada.

Tabla 26. Caracterización de los expertos participantes en la validación del modelo de gestión de incidentes

| Aspecto evaluado | Experto 1 | Experto 2 | Experto 3 | Experto 4 |
|---|---|---|---|---|
| **Nombre completo** | Celi Arévalo Ernesto | Zocón Alva Oscar | Jeffry Stokely Musayón Díaz | Jessie Bravo Jaico |
| **Formación académica y certificaciones** | Ingeniero en Computación e Informática; Maestro en Informática y Sistemas; Doctor en Administración; certificaciones en ciencia de datos e ISO 27001 | Ingeniero de Computación y Sistemas; Maestro en Ingeniería de Sistemas; certificaciones en ITIL e ISO 27001; especialización en gestión de proyectos (PMI) | Ingeniero de Sistemas; Maestrías en Dirección de TI y Administración; formación en proyectos de inversión | Ingeniero en Computación e Informática; Maestría en Informática y Multimedia; Maestría en administración con mención en gerencia Empresarial; Doctora en Ciencias de la Computación y Sistemas |
| **Campo de especialización profesional** | Auditoría de TI, sistemas de gestión de seguridad de la información, docencia universitaria | Consultoría en seguridad de la información, gestión de proyectos y auditoría TI | Gestión de proyectos tecnológicos, metodologías ágiles, redes y gestión de riesgos | Especialización en Auditoría de Tecnologías de la Información y Seguridad Informática; Implementador Líder en ISO 27001 |
| **Experiencia profesional (años)** | 30 | 25 | 24 | 30 |
| **Trayectoria destacada** | Dirección académica, auditoría externa en TI en entidades financieras | Docencia universitaria y consultoría en seguridad y gestión de proyectos | Dirección de proyectos en entidades como SUNAT y sector privado internacional | Directora del programa académico de Ingeniería de Computación e Informática – UNPRG. |
| **Entidad o entorno laboral** | Consultor independiente y docente en universidades | Consultor independiente y docente universitario | Sector financiero y tecnológico (gestión de proyectos TI) | Docente en universidades Líder del GI Transformación Digital - UNPRG |

### 3.5.3. Diseño del instrumento para la validación del modelo de gestión de incidentes

Con el propósito de validar el modelo propuesto, se diseñó un instrumento de evaluación dirigido a especialistas en gestión de servicios de TI, el cual permitió recoger valoraciones técnicas sobre la calidad y aplicabilidad del modelo de gestión de incidentes.

El instrumento fue estructurado como un cuestionario, orientado a analizar si los componentes del modelo propuesto cumplen con las buenas prácticas establecidas en ITIL 4, considerando tanto los elementos operativos del proceso (registro, clasificación, priorización, escalamiento, resolución y cierre), como los elementos organizativos (roles, mesa de ayuda, métricas y base de conocimiento).

Los componentes sometidos a validación fueron seleccionados por representar los elementos funcionales y estructurales esenciales del proceso de gestión de incidentes basado en ITIL 4.

Tabla 27. Componentes evaluados del modelo de gestión de incidentes basado en ITIL 4

| Dimensión del modelo de incidentes | Elementos evaluados |
|---|---|
| **Gestión operativa de incidentes** | Registro estructurado de incidentes en el sistema ITSM |
| | Clasificación de incidentes según taxonomía institucional |
| | Priorización basada en impacto y urgencia |
| | Asignación a niveles de soporte definidos |
| | Procedimientos de resolución de incidentes |
| | Cierre formal con validación del usuario |
| **Gestión organizativa del proceso** | Definición de roles y responsabilidades en la gestión de incidentes |
| | Implementación de la Mesa de Ayuda como punto único de contacto |
| | Definición de niveles de soporte (Nivel 1, Nivel 2 y Nivel 3) |
| | Establecimiento de flujos de escalamiento funcional y jerárquico |
| **Gestión del conocimiento y mejora continua** | Implementación de una base de conocimiento institucional |
| | Documentación de soluciones y lecciones aprendidas |

| | |
|---|---|
| | Generación de métricas (MTTR, FCR, SLA, reincidencia) |
| | Uso de indicadores para la mejora continua del proceso |

### 3.5.4. Criterios de evaluación del modelo

Para la valoración de los componentes del modelo se emplearon los siguientes criterios, alineados al enfoque de la investigación:

a. **Cobertura del modelo:** Evalúa si el modelo incluye todos los elementos necesarios para gestionar incidentes de manera integral.
b. **Comprensibilidad:** Determina el nivel de claridad en la definición de procesos, roles y flujos.
c. **Consistencia interna:** Analiza la coherencia entre los componentes del modelo y su alineación con ITIL 4.
d. **Pertinencia institucional:** Valora la adecuación del modelo al contexto y necesidades de las universidades analizadas.

### 3.5.5. Escala de valoración utilizada

Se empleó una escala ordinal de cinco niveles para la evaluación de cada criterio:

| Nivel | Interpretación |
|---|---|
| 1 | Muy deficiente |
| 2 | Deficiente |
| 3 | Aceptable |
| 4 | Bueno |
| 5 | Excelente |

### 3.5.6. Procedimiento de aplicación del instrumento de validación del modelo

Para llevar a cabo la validación del modelo de gestión de incidentes de tecnologías de la información, se siguió un procedimiento estructurado que permitió garantizar la participación informada de los especialistas y la consistencia en la recolección de datos. Dicho procedimiento se desarrolló en las siguientes etapas:

1. **Coordinación inicial con los especialistas**

   Se estableció comunicación directa con los expertos mediante contacto telefónico, con el objetivo de solicitar su participación en el proceso de validación. Durante esta etapa se explicó el alcance, propósito y relevancia de la investigación.

2. **Presentación del modelo y entrega del instrumento**

   Se realizaron sesiones virtuales en las que se expuso el modelo propuesto, detallando sus componentes estructurales y funcionales. Posteriormente, se remitió a cada experto una copia del modelo junto con el instrumento de evaluación correspondiente, a fin de facilitar su análisis.

3. **Recopilación y procesamiento de las evaluaciones**

   Los especialistas remitieron los instrumentos debidamente llenados. Las valoraciones obtenidas fueron organizadas y procesadas, permitiendo calcular promedios y consolidar los resultados de la evaluación.

### 3.5.7. Resultados del proceso de validación del modelo

A partir de las valoraciones emitidas por los expertos respecto al modelo de gestión de incidentes propuesto, se elaboró una matriz consolidada que consolida los resultados obtenidos en función de los criterios de evaluación establecidos.

Tabla 28. Resultados consolidados de la validación del modelo de gestión de incidentes basado en ITIL 4 mediante juicio de expertos

| Dimensión del modelo evaluada | Componente del modelo de gestión de incidentes | Evaluador | Cobertura del modelo | Comprensibilidad | Consistencia interna | Pertinencia institucional |
|---|---|---|---|---|---|---|
| **Gestión operativa de incidentes** | Definición del proceso de registro de incidentes | Experto 1 | 5.00 | 5.00 | 4.00 | 4.00 |
| | | Experto 2 | 5.00 | 5.00 | 4.00 | 5.00 |
| | | Experto 3 | 4.00 | 5.00 | 4.00 | 4.00 |
| | | Experto 4 | 4.00 | 5.00 | 4.00 | 4.00 |
| | | **Promedio** | **4.25** | **5.00** | **4.00** | **4.25** |
| | Estructura de clasificación y categorización de incidentes | Experto 1 | 4.00 | 4.00 | 4.00 | 4.00 |
| | | Experto 2 | 5.00 | 4.00 | 4.00 | 5.00 |
| | | Experto 3 | 4.00 | 5.00 | 5.00 | 4.00 |
| | | Experto 4 | 4.00 | 5.00 | 4.00 | 4.00 |
| | | **Promedio** | **4.25** | **4.50** | **4.25** | **4.25** |
| | Modelo de priorización basado en impacto y urgencia | Experto 1 | 5.00 | 5.00 | 4.00 | 5.00 |
| | | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 5.00 | 5.00 | 4.00 | 4.00 |
| | | Experto 4 | 5.00 | 4.00 | 4.00 | 5.00 |
| | | **Promedio** | **5.00** | **4.75** | **4.25** | **4.75** |
| | Procedimiento de resolución de incidentes | Experto 1 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 5.00 | 4.00 | 5.00 | 4.00 |
| | | Experto 4 | 5.00 | 5.00 | 5.00 | 4.00 |
| | | **Promedio** | **5.00** | **4.75** | **5.00** | **4.50** |
| | Procedimiento de escalamiento funcional y jerárquico | Experto 1 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 4 | 5.00 | 5.00 | 5.00 | 4.00 |
| | | **Promedio** | **5.00** | **5.00** | **5.00** | **4.75** |
| | Proceso de cierre formal de incidentes | Experto 1 | 4.00 | 4.00 | 5.00 | 4.00 |
| | | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 4.00 | 4.00 | 4.00 | 4.00 |
| | | Experto 4 | 4.00 | 5.00 | 5.00 | 5.00 |
| | | **Promedio** | **4.25** | **4.50** | **4.75** | **4.50** |
| | **Promedio de la dimensión** | | **4.55** | **4.70** | **4.45** | **4.45** |
| **Gestión organizativa del servicio de incidentes** | Implementación de la Mesa de Ayuda (PUC) | Experto 1 | 5.00 | 5.00 | 4.00 | 4.00 |
| | | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 5.00 | 5.00 | 5.00 | 4.00 |
| | | Experto 4 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | **Promedio** | **5.00** | **5.00** | **4.75** | **4.50** |
| | Definición de roles y niveles de soporte | Experto 1 | 4.00 | 5.00 | 4.00 | 4.00 |
| | | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 4 | 5.00 | 5.00 | 5.00 | 4.00 |
| | | **Promedio** | **4.75** | **5.00** | **4.75** | **4.50** |
| | Integración de métricas e indicadores (MTTR, FCR, SLA) | Experto 1 | 4.00 | 4.00 | 4.00 | 4.00 |
| | | Experto 2 | 4.00 | 4.00 | 4.00 | 4.00 |
| | | Experto 3 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 4 | 5.00 | 5.00 | 4.00 | 4.00 |
| | | **Promedio** | **4.50** | **4.50** | **4.25** | **4.25** |
| | **Promedio de la dimensión** | | **4.75** | **4.83** | **4.58** | **4.42** |
| | | Experto 1 | 5.00 | 5.00 | 4.00 | 5.00 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Gestión del conocimiento y mejora continua** | Implementación de la base de conocimientos | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 4 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | **Promedio** | **5.00** | **5.00** | **4.75** | **5.00** |
| | Uso de la base de conocimientos para mejora continua | Experto 1 | 5.00 | 4.00 | 5.00 | 5.00 |
| | | Experto 2 | 5.00 | 5.00 | 5.00 | 5.00 |
| | | Experto 3 | 4.00 | 4.00 | 5.00 | 4.00 |
| | | Experto 4 | 5.00 | 4.00 | 5.00 | 5.00 |
| | | **Promedio** | **4.75** | **4.25** | **5.00** | **4.75** |
| | **Promedio de la dimensión** | | **4.88** | **4.63** | **4.88** | **4.88** |
| **Resultado global del modelo** | — | — | **4.73** | **4.72** | **4.64** | **4.58** |

### 3.5.8. Cálculo del coeficiente de concordancia entre expertos

El cálculo del coeficiente de concordancia entre expertos es importante porque permite verificar el grado de consistencia y acuerdo en las valoraciones emitidas durante el proceso de validación, de tal manera que asegure que los resultados no dependan de opiniones aisladas o subjetivas, sino de un consenso técnico confiable. Este análisis aportó solidez metodológica a la investigación, ya que evidencia que los criterios evaluados, como: la cobertura, comprensibilidad, consistencia interna y pertinencia del modelo, han sido valorados de manera homogénea por especialistas con experiencia en el área. Para su interpretación, un alto nivel de concordancia respalda la confiabilidad del instrumento y del modelo propuesto, reduce el sesgo individual y fortalece la validez de las conclusiones.

**Coeficiente V de Aiken**

El coeficiente V de Aiken es una medida estadística utilizada para evaluar la validez de contenido de un instrumento o modelo a partir del juicio de expertos. La aplicación de este coeficiente permitió determinar en qué medida los evaluadores coinciden en que los ítems o componentes analizados fueron adecuados, relevantes o representativos respecto al objetivo del estudio (Aguilar-Barojas, 2022).

Este coeficiente se calculó a partir de las calificaciones otorgadas por los expertos en una escala ordinal, tipo Likert, utilizando una escala de cinco niveles, donde:

- 1 = Muy deficiente
- 2 = Deficiente
- 3 = Aceptable
- 4 = Bueno
- 5 = Excelente

El valor del coeficiente V oscila entre 0 y 1, donde valores cercanos a 1 indican una alta validez de contenido, es decir, un mayor consenso entre los expertos respecto a la calidad del modelo evaluado.

Para el cálculo del coeficiente se utilizó la siguiente fórmula:

$$V = \frac{\sum s}{n(c-1)}$$

Donde:
vm (valor mínimo): Es el valor más bajo de la escala, en este caso 1.
ce: Es la calificación dada por el experto.
s = ce − vm: Es el ajuste de las puntuaciones para que comiencen desde 0.
n: número de expertos, en este caso es 4
c: número de categorías de la escala, en este caso es 5

El numerador (∑s) representa la valoración total ajustada y el denominador n(c−1) representa el máximo posible. Por eso, V siempre queda entre 0 y 1.

Para el cálculo se tomó los promedios obtenidos para cada criterio evaluado, que se muestran en la tabla 28:

$$Cobertura = \frac{4.73 - 1}{4} = \frac{3.73}{4} = 0.93$$

$$Comprensibilidad = \frac{4.72 - 1}{4} = \frac{3.72}{4} = 0.93$$

$$Consistencia = \frac{4.64 - 1}{4} = \frac{3.64}{4} = 0.91$$

$$Pertinencia = \frac{4.58 - 1}{4} = \frac{3.58}{4} = 0.90$$

La escala de interpretación del Coeficiente V de Aiken según Aguilar-Barojas (2022) se muestra a continuación:

Tabla 29. Valor del coeficiente V de Aiken

| Valor del coeficiente V de Aiken | Interpretación |
|---|---|
| 0.00 – 0.20 | Muy baja validez |
| 0.21 – 0.40 | Baja validez |
| 0.41 – 0.60 | Validez moderada |
| 0.61 – 0.80 | Alta validez |
| 0.81 – 1.00 | Muy alta validez |

Estando todos los valores entre 0.90 y 0.93, significa que los expertos coinciden fuertemente en que el modelo es adecuado y que el contenido del modelo es pertinente, completo y bien definido.

**Coeficiente W de Kendall**

El coeficiente W de Kendall es una medida de concordancia o acuerdo entre evaluadores, que permite identificar el nivel de consistencia en las valoraciones emitidas por un grupo de expertos sobre un conjunto de ítems o criterios.

Con este coeficiente no se evalúa la validez del contenido (como lo hace el coeficiente V de Aiken), sino el grado en que los expertos coincidieron en sus juicios. Se basa en la transformación de las calificaciones en rangos y su análisis conjunto (Gómez, 2022).

El valor de W también se encuentra en un rango de 0 a 1, donde:

- 0 indica ausencia de acuerdo entre los expertos
- 1 indica acuerdo total

Para su cálculo se utilizó las mismas valoraciones anteriores mediante escalas ordinales tipo Likert de 1 a 5, aunque el coeficiente opera internamente con rangos derivados de dichas puntuaciones. Valores altos de W (mayores a 0.80) indican una concordancia fuerte o muy alta, lo que refuerza la confiabilidad de los resultados obtenidos mediante juicio de expertos.

La fórmula utilizada fue:

$$W = \frac{12S}{m^2(n^3 - n)}$$

Donde:

m = número de expertos (4)

n = número de ítems evaluados

S = variabilidad de los rangos

Los resultados obtenidos en el anexo 6, son:

Tabla 30. Resultados por criterio del coeficiente W de Kendall

| Criterio evaluado | W de Kendall | Interpretación |
|---|---|---|
| Cobertura del modelo | 0.46 | Concordancia moderada |
| Comprensibilidad | 0.68 | Concordancia alta |
| Consistencia interna | 0.55 | Concordancia moderada |
| Pertinencia institucional | 0.67 | Concordancia alta |

Y según la escala de interpretación siguiente:

| Valor de W | Nivel de concordancia |
|---|---|
| 0.00 – 0.20 | Muy baja |
| 0.21 – 0.40 | Baja |
| 0.41 – 0.60 | Moderada |
| 0.61 – 0.80 | Alta |
| 0.81 – 1.00 | Muy alta |

Se tiene que el coeficiente W de Kendall indica que los expertos coincidieron ampliamente en sus valoraciones sobre los componentes del modelo.

### 3.5.9. Análisis de resultados por criterio de evaluación

**a. Cobertura del modelo**

- En relación con el criterio de **cobertura del modelo**, se obtuvo un promedio global de **4.73**, lo cual evidencia un nivel alto de valoración por parte de los expertos. Este resultado indica que el modelo propuesto contempla de manera suficiente los componentes necesarios para una adecuada gestión de incidentes de TI basada en ITIL 4.

- A nivel de dimensiones, se observó que la **gestión del conocimiento y mejora continua** alcanzó el valor más alto (4.88), lo que refleja que la base de conocimientos y su aprovechamiento fueron considerados elementos sólidos y completos dentro del modelo. Asimismo, la **gestión organizativa del servicio de incidentes** presentó una valoración de 4.75, destacando

especialmente la implementación de la Mesa de Ayuda con una puntuación perfecta (5.00), lo cual demuestra que la estructura organizativa propuesta es percibida como integral y adecuada.

- Por otro lado, la **gestión operativa de incidentes** obtuvo un valor ligeramente menor (4.55), lo que sugiere que, si bien los procesos definidos (registro, clasificación, priorización, resolución y cierre) son completos, podrían existir oportunidades de mejora en la precisión o detalle de algunos componentes, particularmente en el registro y cierre de incidentes.

**b. Comprensibilidad**

- Respecto al criterio de **comprensibilidad**, el modelo alcanzó un promedio global de **4.72**, evidenciando que los expertos consideraron que la propuesta es clara, entendible y bien estructurada.

- La dimensión mejor valorada fue la **gestión organizativa del servicio de incidentes** (4.83), lo que indica que los roles, niveles de soporte y la estructura de la Mesa de Ayuda fueron definidos de manera clara y sin ambigüedades. En particular, la Mesa de Ayuda y la definición de roles obtuvieron puntuaciones máximas (5.00), reflejando una adecuada representación organizativa.

- La **gestión operativa de incidentes** obtuvo un promedio de 4.70, destacando el procedimiento de escalamiento (5.00), lo cual evidencia que el flujo de atención y derivación de incidentes es fácilmente interpretable. Sin embargo, el proceso de clasificación y el cierre formal presentan valores ligeramente menores, lo que podría indicar la necesidad de simplificar o clarificar ciertos aspectos operativos.

- En contraste, la **gestión del conocimiento y mejora continua** obtuvo un valor de 4.63, siendo el criterio más bajo dentro de este indicador, particularmente en el uso de la base de conocimientos (4.25). Esto sugiere que, aunque la estructura de la base de conocimientos es clara, su

aplicación práctica o integración en el proceso podría requerir mayor especificación.

**c. Consistencia interna**

- En cuanto a la **consistencia interna**, el modelo alcanzó un promedio global de **4.64**, lo cual refleja una adecuada coherencia entre sus componentes y alineación con las buenas prácticas de ITIL 4.

- La dimensión con mejor desempeño fue la **gestión del conocimiento y mejora continua** (4.88), lo que evidencia que existe una fuerte integración entre la base de conocimientos y el proceso de gestión de incidentes. Asimismo, el uso de la base de conocimientos obtuvo una puntuación máxima (5.00), lo que indica que los expertos perciben este componente como coherente y bien articulado.

- La **gestión organizativa** obtuvo un valor de 4.58, lo que sugiere una buena relación entre los roles, niveles de soporte y métricas, aunque con ligeras oportunidades de mejora en la integración de indicadores.

- Por su parte, la **gestión operativa de incidentes** presentó el valor más bajo (4.45), lo cual podría indicar que, si bien los procesos están correctamente definidos, algunos elementos (como la relación entre clasificación, priorización y cierre) podrían reforzarse para asegurar una mayor coherencia interna.

**d. Pertinencia institucional**

- Respecto al criterio de **pertinencia institucional**, el modelo obtuvo un promedio global de **4.58**, evidenciando que es considerado adecuado y aplicable al contexto universitario.

- La dimensión mejor valorada fue la **gestión del conocimiento y mejora continua** (4.88), lo que demuestra que los expertos consideran que la implementación de una base de conocimientos es altamente relevante para mejorar la gestión de incidentes en la universidad.

- La **gestión organizativa del servicio de incidentes** obtuvo un valor de 4.42, lo que indica que, aunque la estructura propuesta (PUC, roles, niveles) es pertinente, podrían existir desafíos prácticos en su implementación dentro del contexto institucional, posiblemente asociados a recursos, cultura organizacional o madurez tecnológica.

- Finalmente, la **gestión operativa de incidentes** alcanzó un valor de 4.45, evidenciando que los procesos definidos son adecuados para la realidad de la institución, aunque podrían requerir ajustes para adaptarse plenamente a las condiciones operativas actuales.

**e. Valoración global de la propuesta**

- En conjunto, los resultados muestran que el modelo presenta una **alta aceptación por parte de los expertos en todos los criterios evaluados**, destacando especialmente su **cobertura y comprensibilidad**. Asimismo, la **gestión del conocimiento** emerge como el componente más sólido del modelo, mientras que los aspectos operativos y organizativos, aunque bien valorados, presentan **oportunidades de mejora en su articulación e implementación práctica**.

Estos resultados respaldan la **viabilidad técnica y metodológica del modelo propuesto**, evidenciando que se encuentra alineado con ITIL 4 y que responde de manera adecuada al contexto universitario, constituyéndose como una propuesta pertinente para fortalecer la gestión de incidentes de TI.

## DISCUSIÓN DE RESULTADOS

Los resultados obtenidos en la presente investigación evidenciaron que las universidades públicas de la región Amazonas presentan limitaciones importantes en la gestión de incidentes de tecnologías de la información, especialmente relacionadas con la ausencia de procedimientos formalizados, mecanismos de priorización estandarizados, criterios definidos de escalamiento y estructuras organizativas orientadas específicamente a la gestión de incidentes. A partir de ello, se diseñó un modelo de gestión de incidentes basado en ITIL 4, adaptado al contexto operativo universitario de la UNTRM y la UNIFSLB, incorporando componentes funcionales y organizativos alineados a las necesidades identificadas durante el diagnóstico.

Estos resultados guardan relación con lo planteado por Cáceres Castillo (2019), quien identificó que muchas organizaciones implementan prácticas de soporte TI de manera reactiva y poco estructurada, generando tiempos elevados de atención y baja trazabilidad de los incidentes. La coincidencia principal radica en que ambas investigaciones reconocen la necesidad de formalizar los procesos de atención mediante buenas prácticas de ITSM. Sin embargo, el presente estudio se diferencia porque no se limita a analizar deficiencias operativas generales, sino que desarrolla un modelo específicamente contextualizado para universidades públicas, considerando servicios críticos académicos como matrícula, aulas virtuales, gestión de tesis y plataformas institucionales.

De manera similar, Céspedes-Garbanzo (2024) concluyó que la incorporación de prácticas ITIL mejora la organización del soporte tecnológico y contribuye a optimizar la continuidad de los servicios. La similitud con la presente investigación se observa en la importancia otorgada al service desk, los flujos de atención y la gestión documentada de incidentes. No obstante, el aporte diferencial de esta tesis radica en que el modelo propuesto no solo define procesos operativos, sino que integra mecanismos de priorización, matrices de escalamiento funcional y jerárquico, criterios para incidentes mayores, métricas de desempeño (MTTR, FCR y SLA) y una base de conocimientos estructurada para contextos universitarios públicos con limitaciones organizativas y tecnológicas particulares.

Asimismo, los resultados coinciden con lo desarrollado por Cadena et al. (2020), quienes destacan que las métricas operativas permiten evaluar el desempeño real de los procesos

de gestión de incidentes y facilitan la mejora continua. En ambos casos se reconoce la importancia de indicadores como MTTR y FCR para medir eficiencia operativa. Sin embargo, mientras Cadena et al. centran su análisis en métricas de rendimiento aplicables a entornos organizacionales generales, la presente investigación incorpora dichas métricas dentro de un modelo integral adaptado a los servicios críticos universitarios, vinculando además los indicadores con mecanismos de gobernanza, comunicación proactiva y continuidad operativa.

Por otro lado, los hallazgos obtenidos presentan relación con lo señalado por Najjarpour et al. (2025), quienes proponen el uso de indicadores y paneles de control para fortalecer la supervisión de servicios tecnológicos. La similitud se encuentra en la necesidad de monitorear continuamente el comportamiento de los incidentes para apoyar la toma de decisiones. Sin embargo, el estudio desarrollado en la UNTRM y la UNIFSLB amplía este enfoque al incorporar criterios organizativos, procedimientos de cierre formal, mecanismos de reapertura de incidentes y gestión del conocimiento, elementos que no fueron abordados de manera integrada en el antecedente referido.

En relación con los fundamentos teóricos, los resultados obtenidos evidencian una alta correspondencia con las prácticas propuestas por Axelos (2019, 2020) para ITIL 4, especialmente en lo relacionado con la gestión de incidentes, la función del service desk, el escalamiento funcional y la mejora continua. El modelo desarrollado adopta estos principios, pero los adapta a la realidad de universidades públicas regionales, donde existen restricciones de recursos, estructuras organizativas menos especializadas y una fuerte dependencia de servicios académicos digitales. En este sentido, el aporte diferencial de la investigación no radica únicamente en aplicar ITIL 4, sino en contextualizar sus prácticas dentro de un entorno universitario público peruano, aspecto poco desarrollado en investigaciones previas.

Del mismo modo, existe concordancia con la ISO/IEC 27035-1:2016 respecto a la necesidad de gestionar incidentes de forma estructurada, documentada y trazable. Sin embargo, mientras la norma plantea lineamientos generales para la gestión de incidentes de seguridad de la información, la presente investigación desarrolla procedimientos operativos concretos orientados a la continuidad de servicios académicos y administrativos

universitarios, incorporando criterios de priorización, matrices de roles, mecanismos de comunicación y estructuras de soporte multinivel.

Finalmente, los resultados de la validación mediante juicio de expertos fortalecen el aporte diferencial del estudio. Los valores obtenidos en cobertura del modelo (4.73), comprensibilidad (4.72), consistencia interna (4.64) y pertinencia institucional (4.58) evidencian que el modelo no solo mantiene coherencia con ITIL 4, sino que además resulta aplicable y pertinente para el contexto universitario evaluado. Esto diferencia la propuesta de otros antecedentes que se enfocaron principalmente en implementaciones genéricas de ITSM o evaluaciones teóricas, sin desarrollar modelos específicamente orientados a las necesidades operativas y organizativas de universidades públicas regionales.

# CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

1. Se concluyó que la gestión de incidentes de tecnologías de la información en el contexto analizado se caracterizaba por un enfoque predominantemente reactivo, con ausencia de procesos formalizados, escasa estandarización en el registro y atención de incidentes, y una alta dependencia del conocimiento individual del personal técnico. Asimismo, se evidenció la inexistencia de un punto único de contacto, lo que generaba dispersión en la atención, pérdida de trazabilidad y dificultades para el control y seguimiento de los incidentes. Estas condiciones reflejaron una brecha significativa respecto a las buenas prácticas establecidas por ITIL 4.

2. Se determinó que las principales brechas se concentraban en la falta de estructuración del proceso de gestión de incidentes, la inexistencia de roles claramente definidos, la ausencia de mecanismos de priorización basados en impacto y urgencia, y la carencia de procedimientos formales de escalamiento, resolución y cierre. Adicionalmente, se identificó una limitada generación de métricas y una inexistente gestión del conocimiento, lo cual impedía la mejora continua. Estas brechas evidenciaron una desalineación considerable entre la práctica institucional y el marco de referencia ITIL 4.

3. El modelo propuesto logró integrar de manera estructurada y coherente los componentes organizativos y operativos necesarios para una adecuada gestión de incidentes de TI. Este incluyó la implementación de un Punto Único de Contacto de la Mesa de Ayuda, la definición de roles y niveles de soporte, la estandarización de procesos (registro, clasificación, priorización, escalamiento, resolución y cierre), la incorporación de una base de conocimientos y la definición de métricas de desempeño. El diseño permitió articular todos los elementos bajo un enfoque alineado a ITIL 4, orientado a la eficiencia, trazabilidad y mejora continua.

4. El modelo propuesto presenta un alto nivel de validez técnica y metodológica, evidenciado en las valoraciones obtenidas en los criterios de cobertura (4.73), comprensibilidad (4.72), consistencia interna (4.64) y pertinencia institucional (4.58). Los expertos coincidieron en que el modelo es completo, claro, coherente y aplicable

al contexto universitario, destacando especialmente la solidez de la base de conocimientos y la estructura organizativa propuesta. No obstante, se identificaron oportunidades de mejora en la integración operativa y en la implementación práctica de algunos componentes.

5. El modelo de gestión de incidentes de tecnologías de la información basado en ITIL 4 constituye una propuesta viable, pertinente y técnicamente sólida para mejorar la gestión de los servicios de TI en el contexto universitario. El modelo permite superar las debilidades identificadas en el diagnóstico inicial, al establecer procesos estandarizados, roles definidos, mecanismos de control y seguimiento, y una gestión basada en conocimiento y métricas. Asimismo, su validación por expertos respalda su aplicabilidad y contribución a la continuidad operativa, la calidad del servicio y la gobernanza de las tecnologías de la información, consolidándose como una herramienta efectiva para la modernización de la gestión de incidentes en la institución.

**Recomendaciones**

1. Desarrollar estudios posteriores de tipo aplicado o experimental que permitan implementar el modelo de gestión de incidentes propuesto en un entorno institucional real (por ejemplo, en la UNIFSLB u otra universidad pública), con el fin de evaluar su desempeño en condiciones operativas. Estos estudios deberían medir indicadores como MTTR, FCR, cumplimiento de SLA, satisfacción del usuario y reducción de incidentes recurrentes, comparando los resultados antes y después de la implementación. Esto permitiría validar no solo la pertinencia teórica del modelo, sino también su impacto práctico en la mejora de la calidad del servicio de TI.

**2.** Ampliar el alcance de la investigación mediante estudios que articulen el modelo propuesto con otros procesos clave de ITIL 4, como gestión de problemas, gestión de cambios y gestión de niveles de servicio, así como con marcos de seguridad de la información como ISO/IEC 27001 o ISO/IEC 27005. Esta integración permitiría evolucionar hacia un enfoque más integral de gestión de servicios y riesgos, evaluando cómo la gestión de incidentes se relaciona con la prevención de incidentes, la gestión de vulnerabilidades y la continuidad del negocio. De esta manera, se contribuiría a consolidar un modelo más robusto y alineado con las necesidades de gobernanza de TI en el contexto universitario.

## REFERENCIAS CONSULTADAS


Aguilar-Barojas, J. F. (2022). *Validez de contenido de juicio por expertos para la construcción de instrumentos de medición*. Revista Científica de Metodología y Evaluación, 12(2), 45–58.

Agutter, C. (2020). *ITIL® 4 essentials: Your essential guide for the ITIL 4 Foundation exam and beyond* (2.ª ed.). IT Governance Publishing.

Aiken, L. R. (1985). *Three coefficients for analyzing the reliability and validity of ratings*. Educational and Psychological Measurement, 45(1), 131–142.

Axelos. (2019). *ITIL® Foundation: ITIL 4 Edition*. TSO. International Organization for Standardization. (2016). *ISO/IEC 27035-1: Information technology — Security techniques — Information security incident management*. ISO.

Axelos. (2020). *ITIL® 4 practice guide: Incident management*. Axelos Limited.

Baud (2016). *Gestión de servicios TI con ITIL*. Editorial ENI.

Cáceres Castillo, C. A. (2019). *Desarrollo de un modelo de gestión de incidentes basado en ITIL v3.0 para el área de Facilities Management de la empresa Tgestiona* [Tesis de licenciatura, Universidad Peruana de Ciencias Aplicadas].

Cadena, A., Gualoto, F., Fuertes, W., Tello-Oquendo, L., Andrade, R., Tapia, F., & Torres, J. (2020). Metrics and indicators of information security incident management: A systematic mapping study. En Á. Rocha & R. P. Pereira (Eds.), *Developments and advances in defense and security* (pp. 507–519). Springer. https://doi.org/10.1007/978-981-13-9155-2_40

Céspedes-Garbanzo, K. (2024). *Propuesta de implementación del proceso de Gestión de Incidentes, basado en ITIL para Inversiones TB S.A* [Tesis del Instituto Tecnológico de Costa Rica].

Dzemydienė, D., Turskienė, S., & Šileikienė, I. (2024). An approach of ICT incident management based on ITIL 4 methodology recommendations. *Baltic Journal of Modern Computing, 12*(3), 286–303. https://doi.org/10.22364/bjmc.2024.12.3.05

Ferreira, S. F. (2021). The importance of the ITIL framework in managing Information and Communication Technology services. *International Journal of Advanced Engineering Research and Science, 8*(5), 292–296. https://doi.org/10.22161/ijaers.85.35

Gómez, N. B. (2022). El estadígrafo Kendall y su aplicación. Un ejemplo práctico. *Revista Científica Multidisciplinaria*, 4(2), 45–58.

Guerra Cabrera, J. L. (2021). *Impacto de un sistema Service Desk basado en tecnologías web en el proceso de atención de incidencias de hardware y software de la Unidad Técnica de Soporte Informático de la Universidad Nacional de Cajamarca* [Tesis de pregrado, Universidad Nacional de Cajamarca]. Repositorio Institucional UNC.

Harjanto, A., & Aji, R. F. (2024). Improving IT assets management with ITIL 4 framework. *Jurnal Ilmu Komputer dan Informasi (Journal of Computer Science and Information), 17*(2), 127–143. http://dx.doi.org/10.21609/jiki.v17i2.1195

Hasan, M. N. (2021). *Design and implementation of an automated IT incident management system for small and medium-sized enterprises* [Diploma thesis, Tallinn University of Technology].

ISO/IEC. (2016). *ISO/IEC 27035-1: Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. International Organization for Standardization.

Kanellopoulos, A. N. (2024). Enhancing cyber security and counterintelligence in the shipping industry. *National Security and the Future, 25*(1), 137–154. https://doi.org/10.37458/nstf.25.1.6

Kirilov, L., & Mitev, Y. (2022). Key performance indicators to improve e-Mail service quality through ITIL framework. En D. Borissova et al. (Eds.), *Recent advances in computational optimization* (pp. 79–93). Springer. https://doi.org/10.1007/978-3-031-06839-3_5

Loayza Uyehara, A. A. (2015). *Modelo de gestión de incidentes, aplicando ITIL v3.0 en un organismo del Estado peruano* [Tesis de licenciatura, Universidad de Lima].

Loayza-Uyehara, A. A. (2016). Modelo de gestión de incidentes para una entidad estatal. *Interfases, 9*, 221–254. https://doi.org/10.26439/interfases2016.n009.1247

Mahardika, D. (2022). Service desk in perspective of Information Technology Infrastructure Library 3rd-version. *Engineering Science Letter, 1*(2), 47–50. http://dx.doi.org/10.56741/esl.v1i02.142

Marulanda, C., López, M., & Cuesta, F. (2019). Gestión de servicios de TI y generación de valor organizacional. *Revista de Ingeniería*, 24(2), 45–58.

Najjarpour, M., Azizi, A., & Azizi, A. (2025). Determining key performance indicators for the operational dashboard of the IT unit at educational hospitals. *TJT, 2*(2), 36–47. https://doi.org/10.32592/TJT.2025.2.2.36

Ninaraqui Pelaiza, J. G. (2020). *Modelo de gestión de incidencias para mejorar la eficacia de los servicios TI de la Escuela Profesional de Ingeniería de Minas de la Universidad Nacional de Moquegua* [Tesis, Universidad Continental].

Nugroho, A. F. J., & Fianty, M. I. (2023). Streamlining IT Help Desk and Incident Management: Harnessing the Power of the ITIL Framework for Enhanced Efficiency in IT Services. *Journal of Information Systems and Informatics, 5*(2), 683–695. https://doi.org/10.51519/journalisi.v5i2.496

Nurjanah, S., Istiyono, E., Widihastuti, W., Iqbal, M., & Kamal, S. (2023). *The application of Aiken's V method for evaluating the content validity of instruments that measure the implementation of formative assessments*. Journal of Research and Educational Research Evaluation, 12(2), 125–133.

Orozco, J. V., & Tovar, C. V. (2018). Incident management based on Information Technology Infrastructure Library (ITIL) for higher education institutions. *Espacios, 39*(10).

Palilingan, V. R., & Batmetan, J. R. (2018). Incident management in academic information system using ITIL framework. *IOP Conference Series: Materials Science and Engineering, 306*(1), 012110. https://doi.org/10.1088/1757-899X/306/1/012110

Pereira, R., de Vasconcelos, J. B., Rocha, Á., & Bianchi, I. S. (2021). Business process management heuristics in IT service management: A case study for incident management. *Computational and Mathematical Organization Theory, 27*(3), 264–301. https://doi.org/10.1007/s10588-021-09331-2

Pita Astengo, L. H. (2022). *Efecto de un service desk en la gestión de incidentes de tecnologías de información en la Universidad Nacional de la Amazonía Peruana, Iquitos - 2020* [Tesis de maestría, Universidad Nacional de la Amazonía Peruana]. Repositorio Institucional UNAP.

Ramadhan, S. (2024). Risk assessment analysis using ITIL V.4 framework on INLISLite. *International Journal of Computer Applications, 186*(42), 44–50.

Santosa, I., & Mulyana, R. (2023). The IT services management architecture design for large and medium-sized companies based on ITIL 4 and TOGAF framework. *JOIV: International Journal on Informatics Visualization, 7*(1), 30–36. https://doi.org/10.30630/joiv.7.1.1590

Sekti, B. A. (2025). IT service information security management. En *Cases on information systems service management* (pp. 61–94). https://doi.org/10.4018/979-8-3373-2352-7.ch003

Sembina, G., Mayandinova, K., Naizabayeva, L., & Sagnayeva, S. (2022). Development of reference incident management model. *Eastern-European Journal of Enterprise Technologies, 6*(2), 41–50. https://doi.org/10.15587/1729-4061.2022.266387

Trinidad, M., Orta, E., & Ruiz, M. (2021). Gamification in IT service management: A systematic mapping study. *Applied Sciences, 11*(8), 3384. https://doi.org/10.3390/app11083384

Zahrothul Ain, A. A., & Safitri, C. (2023). Enhancing ITIL Incident Management: Innovative Machine Learning Approaches for Efficient Incident Prioritization and Resolution. *Jurnal Teknik Informatika, 16*(2), 204–214. https://doi.org/10.15408/jti.v16i2.31439

Zender Minaya, J. J. (2024). *Implementación de procesos ITIL de gestión de incidencias y problemas. Aplicación en una empresa de Desarrollo y Mantenimiento de Software* [Trabajo fin de máster, Universidad Nacional de Educación a Distancia].

# ANEXOS

## Anexo 1. Guía de entrevista para el análisis de la gestión de incidentes de TI

**Unidad de análisis:**
Personal vinculado a las áreas de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (UNTRM) y la Universidad Nacional Intercultural Fabiola Salazar Leguía de Bagua (UNIFSLB)

**Propósito del instrumento:**
Recoger información detallada sobre la forma en que actualmente se gestionan los incidentes de tecnologías de la información en ambas universidades, identificando prácticas reales, limitaciones y diferencias frente a las recomendaciones del marco ITIL 4.

**Objetivo de la investigación:**
Diseñar un modelo de gestión de incidentes de tecnologías de la información, basado en las buenas prácticas de ITIL 4, que sirva como soporte para mejorar la operación de los servicios de TI en la UNTRM y la UNIFSLB.

**Cuestionario para entrevista semiestructurada (Guía de preguntas)**

a. ¿Cuáles son los incidentes más comunes que se presentan en los servicios de TI de la universidad? ¿En qué sistemas o servicios ocurren con mayor frecuencia?
b. Cuando ocurre un incidente, ¿cómo se detecta normalmente? ¿Siempre lo reporta el usuario o a veces el área de TI lo identifica antes?
c. En la práctica, ¿cómo se registran los incidentes? ¿Se utiliza algún formato, sistema o simplemente se comunican de manera directa?
d. ¿Existe algún repositorio o historial donde se almacenen los incidentes atendidos? ¿Se puede hacer seguimiento de casos anteriores?
e. ¿Hay un procedimiento formal que guíe la atención de incidentes o cada caso se maneja según la experiencia del personal?
f. ¿Existe un punto único de contacto para que los usuarios reporten incidentes (por ejemplo, mesa de ayuda)? Si no existe, ¿cómo llegan los reportes normalmente?
g. ¿Cómo se asignan los incidentes al personal responsable? ¿Se sigue algún criterio o depende de la disponibilidad del momento?
h. ¿Se utilizan categorías o tipos de incidentes (por ejemplo: red, software, hardware)? ¿Cómo se definen?
i. ¿Se priorizan los incidentes? En caso afirmativo, ¿qué criterios se consideran (impacto, urgencia, número de usuarios afectados, etc.)?
j. ¿Se han establecido niveles de soporte (primer nivel, segundo nivel, especialistas)? ¿Cómo se organiza la atención entre estos niveles?
k. Cuando un incidente no puede resolverse en el primer intento, ¿cómo se gestiona su derivación o escalamiento?

l. ¿En qué casos un incidente se considera crítico o urgente? ¿Se maneja de forma diferente a los demás?
m. ¿Qué herramientas utilizan actualmente para gestionar los incidentes (sistemas de tickets, correos, llamadas, aplicaciones, etc.)?
n. ¿Se cuenta con algún sistema de monitoreo que permita detectar fallas antes de que los usuarios las reporten?
o. Cuando se resuelve un incidente, ¿la solución queda documentada para futuras consultas? ¿Existe alguna base de conocimiento?
p. ¿Cómo se realiza el cierre de un incidente? ¿Se valida con el usuario si el problema fue resuelto?
q. ¿Se miden tiempos de atención o resolución de incidentes? ¿Se generan reportes o indicadores?
r. ¿Existe coordinación con otras áreas, por ejemplo seguridad de la información, cuando el incidente lo requiere?
s. Desde su experiencia, ¿cuáles son las principales limitaciones o problemas en la forma actual de gestionar los incidentes?
t. Finalmente, ¿qué aspectos considera que deberían implementarse o mejorarse para lograr una gestión de incidentes más eficiente en la universidad?

**Anexo 2. Instrumento para el análisis de documentación institucional**

**Unidad de análisis:**

Documentos institucionales de las áreas de Tecnologías de la Información de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (UNTRM) y la Universidad Nacional Intercultural Fabiola Salazar Leguía de Bagua (UNIFSLB), tales como reglamentos, manuales, planes, directivas y evidencias operativas vinculadas a la gestión de servicios de TI.

**Finalidad del instrumento:**

Examinar el grado de estructuración y formalización de la gestión de incidentes de TI en ambas universidades, así como su nivel de correspondencia con las prácticas recomendadas por ITIL 4.

**Objetivo de la investigación:**

Diseñar un modelo de gestión de incidentes de tecnologías de la información basado en ITIL 4 que contribuya a mejorar la operación de los servicios tecnológicos en la UNTRM y la UNIFSLB.

**Criterios del análisis documental**

| Categoría de análisis | Elementos a examinar | Evidencias a identificar |
|---|---|---|
| Procesos y procedimientos de TI | Existencia de documentos que regulen la atención de incidentes de TI. Definición de etapas, responsables y flujo de atención. | Determinar el nivel de formalización del proceso y posibles vacíos en su estructura. |
| Estructura organizacional (ROF/MOF) | Funciones asignadas al área de TI, soporte técnico y atención al usuario. Distribución de responsabilidades. | Evaluar el grado de claridad en la asignación de funciones relacionadas con la gestión de incidentes. |
| Normativa y lineamientos de TI | Presencia de criterios para la atención de incidentes (clasificación, prioridad, tiempos de respuesta). | Identificar si existen lineamientos operativos y su correspondencia con buenas prácticas como ITIL 4. |
| Registros y evidencias operativas | Documentación de incidentes: tipo, frecuencia, tiempos de atención, resolución. | Analizar la existencia de trazabilidad, patrones recurrentes y debilidades en el registro de incidentes. |
| Infraestructura y herramientas de soporte TI | Uso de sistemas de tickets, herramientas de monitoreo, repositorios de conocimiento. | Identificar el nivel de soporte tecnológico disponible para la gestión de incidentes. |

**Anexo 3. Matriz de contraste entre ITIL 4 y la situación actual de la gestión de incidentes de TI**

**Finalidad de la matriz:**

Identificar y analizar las diferencias existentes entre las prácticas actuales de gestión de incidentes de tecnologías de la información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (UNTRM) y la Universidad Nacional Intercultural Fabiola Salazar Leguía de Bagua (UNIFSLB), frente a los elementos y lineamientos establecidos por ITIL 4 en la práctica de Incident Management.

**Objetivo de la investigación:**

Diseñar un modelo de gestión de incidentes de tecnologías de la información basado en ITIL 4 que contribuya a mejorar la operación de los servicios tecnológicos en la UNTRM y la UNIFSLB.

| Componente de ITIL 4 | Referencia conceptual en ITIL 4 | Situación observada en UNTRM y UNIFSLB | Nivel de brecha identificado |
|---|---|---|---|
| Registro de incidencias | Todo incidente debe ser capturado de forma estructurada en un sistema centralizado que permita su seguimiento. | | No implementado / Parcial / Informal |
| Punto de contacto único (Service Desk) | Se establece un punto centralizado que canaliza la comunicación con los usuarios y gestiona el ciclo de vida de los incidentes. | | Inexistente / Informal / Parcial |
| Categorización de incidentes | Se requiere una clasificación estructurada basada en categorías y subcategorías para facilitar su tratamiento. | | Ausente / Limitada / Adecuada |
| Priorización de incidentes | La atención debe organizarse según niveles de impacto y urgencia previamente definidos. | | Inexistente / Débil / Parcial |
| Estructura de niveles de soporte | Deben establecerse niveles de atención (primer, segundo y tercer nivel) con funciones claras. | | No definido / Parcial / Definido |

| | | | |
|---|---|---|---|
| Escalamiento técnico (funcional) | Los incidentes deben ser derivados a niveles especializados cuando superan la capacidad inicial de atención. | | Ausente / Poco estructurado / Definido |
| Escalamiento organizacional (jerárquico) | Deben definirse mecanismos para escalar incidentes críticos a niveles de decisión superiores. | | Inexistente / Incipiente / Formalizado |
| Gestión de la resolución | Las soluciones aplicadas deben ser documentadas para reutilización y aprendizaje organizacional. | | Ausente / Limitado / Implementado |
| Cierre de incidentes | El cierre debe ser formal, validado por el usuario y registrado adecuadamente. | | No implementado / Parcial / Formal |
| Monitoreo y gestión de alertas | Se recomienda el uso de herramientas para detección temprana de fallas e incidentes. | | Bajo / Parcial / Adecuado |
| Herramientas de gestión (ITSM) | Se deben utilizar plataformas que integren registro, seguimiento, priorización y reportes. | | Ausente / En implementación / Implementado |
| Indicadores de desempeño | Se deben definir métricas para evaluar tiempos, eficiencia y calidad del servicio. | | Inexistente / Parcial / Implementado |
| Definición de roles | Los roles y responsabilidades deben estar claramente establecidos y documentados. | | Difuso / Parcial / Claro |
| Formalización del proceso | El proceso debe estar documentado, aprobado y difundido en la organización. | | Ausente / Poco formalizado / Formalizado |
| Gestión de incidentes de seguridad | Debe existir articulación con la gestión de seguridad de la información y respuesta a incidentes. | | Inexistente / Limitado / Integrado |

## Anexo 4. Instrumento de validación del modelo de gestión de incidentes mediante evaluación experta

### Matriz de validación del modelo mediante juicio especializado

**Finalidad del instrumento**

El presente instrumento tiene como finalidad recopilar la valoración de especialistas en gestión de tecnologías de la información, gestión de servicios TI, ITIL 4 y seguridad de la información, respecto a la calidad técnica, consistencia metodológica y aplicabilidad del modelo de gestión de incidentes propuesto.

**Propósito de la investigación**

Diseñar un modelo de gestión de incidentes de tecnologías de la información fundamentado en las buenas prácticas de ITIL 4, orientado a fortalecer la operación, continuidad y calidad de los servicios tecnológicos en el contexto universitario.

**Datos del evaluador experto**

Nombre completo:
Formación académica:
Área de especialización:
Experiencia en gestión de TI / ITIL /Seguridad de la información (años):
Organización de procedencia:

**Indicaciones para la evaluación**

Se solicita revisar cada componente del modelo propuesto y valorar los criterios presentados utilizando la escala definida. Asimismo, se recomienda incluir observaciones que contribuyan a mejorar la propuesta.

**Escala de valoración:**

| Valor | Interpretación |
|---|---|
| 1 | Muy deficiente |
| 2 | Deficiente |
| 3 | Aceptable |
| 4 | Bueno |
| 5 | Excelente |

**Instrumento de valoración del modelo de gestión de incidentes**

| Dimensión de evaluación | Definición del criterio | Aspectos específicos a evaluar | Puntuación (1–5) | Observaciones del experto |
|---|---|---|---|---|
| **Cobertura del modelo** | El modelo contempla los componentes necesarios para gestionar incidentes conforme a buenas prácticas | ¿Incluye actividades clave como registro, categorización, priorización, escalamiento, resolución y cierre? | | |
| | | ¿Incorpora elementos organizativos como mesa de ayuda, roles, niveles de soporte y métricas? | | |
| | | ¿Integra los componentes mínimos para garantizar la operatividad del proceso? | | |
| **Comprensibilidad** | El modelo es claro en su estructura, definiciones y representación de procesos | ¿Los flujos de trabajo son fáciles de interpretar? | | |
| | | ¿Los roles y responsabilidades están definidos de manera precisa? | | |
| | | ¿La documentación del modelo es clara y accesible? | | |
| **Consistencia interna** | Los elementos del modelo mantienen coherencia entre sí y con el enfoque ITIL 4 | ¿El modelo refleja adecuadamente las prácticas de ITIL 4? | | |
| | | ¿Existe relación lógica entre componentes estructurales y operativos? | | |
| | | ¿La priorización se basa correctamente en criterios de impacto y urgencia? | | |
| **Pertinencia institucional** | El modelo responde al contexto y necesidades de la organización universitaria | ¿El modelo aborda problemas reales identificados en el diagnóstico? | | |
| | | ¿Es viable su implementación en el entorno institucional? | | |
| | | ¿Se adapta a las capacidades actuales de la organización? | | |

## Anexo 5. Definición de perfiles funcionales para los niveles de atención en la gestión de incidentes de TI

A continuación, se describen los perfiles propuestos para cada nivel de atención dentro del proceso de gestión de incidentes. Estos perfiles han sido diseñados considerando las capacidades técnicas, operativas y organizativas requeridas para asegurar una atención eficiente y alineada con buenas prácticas de ITSM.

### Perfil funcional – Nivel 1: Analista de Atención Inicial de Incidentes

**a. Ubicación organizacional:**

Oficina de Tecnologías de la Información (OTI)

**b. Objetivo del rol:**

Brindar atención inicial a los usuarios, registrar y categorizar incidentes a través del Punto Único de Contacto, realizar diagnósticos básicos, resolver incidencias de baja complejidad y asegurar la trazabilidad del proceso.

**c. Responsabilidades principales:**

- Registrar todos los incidentes en la plataforma ITSM.
- Clasificar y priorizar los incidentes conforme a los criterios definidos.
- Resolver incidentes simples mediante el uso de la base de conocimientos.
- Mantener comunicación continua con los usuarios.
- Escalar los casos que superen su capacidad técnica al siguiente nivel.
- Documentar soluciones recurrentes para fortalecer el conocimiento institucional.

**d. Capacidades requeridas:**

- Conocimientos generales en tecnologías de información.
- Manejo de sistemas de tickets o herramientas ITSM.
- Habilidades comunicativas y orientación al usuario.
- Capacidad de trabajo bajo presión en periodos críticos.
- Orden y rigurosidad en el registro de información.

### Perfil funcional – Nivel 2: Especialista en Plataformas e Infraestructura Tecnológica

**a. Ubicación organizacional:**

Oficina de Tecnologías de la Información (OTI)

**b. Objetivo del rol:**

Atender incidentes de mayor complejidad técnica, garantizando la estabilidad de los servicios críticos institucionales como sistemas académicos, plataformas virtuales, redes y servidores.

**c. Responsabilidades principales:**

- Gestionar incidentes derivados desde el primer nivel.
- Ejecutar diagnósticos técnicos avanzados y análisis de causa raíz.
- Resolver problemas relacionados con infraestructura, aplicaciones y seguridad.
- Documentar soluciones técnicas especializadas.
- Identificar oportunidades de mejora y vulnerabilidades.
- Coordinar con el nivel experto en casos que excedan su alcance.

**d. Capacidades requeridas:**

- Dominio técnico en redes, servidores, bases de datos o aplicaciones.
- Capacidad analítica para resolución de problemas complejos.
- Uso de herramientas de monitoreo y diagnóstico.
- Trabajo colaborativo interdisciplinario.
- Enfoque en mejora continua.

**Perfil funcional – Nivel 3: Especialista externo o experto en soluciones críticas**

**a. Ubicación organizacional:**

Articulación entre la OTI y proveedores especializados.

**b. Objetivo del rol:**

Intervenir en incidentes de alta criticidad o naturaleza estructural que requieren conocimientos altamente especializados o soporte de proveedores externos.

**c. Responsabilidades principales:**

- Atender incidentes críticos relacionados con sistemas centrales, seguridad o infraestructura avanzada.
- Implementar soluciones definitivas, parches o correcciones estructurales.
- Participar en la gestión de incidentes mayores.

- Coordinar con la alta dirección y responsables del proceso.
- Documentar soluciones estratégicas orientadas a la prevención.

**d. Capacidades requeridas:**

- Conocimiento experto en áreas técnicas específicas.
- Capacidad de resolución en escenarios de alto riesgo.
- Dominio de estándares de seguridad y continuidad.
- Habilidades de coordinación y liderazgo técnico.
- Pensamiento estratégico.

## Anexo 6. Cálculo de los coeficientes de validación y concordancia de las valoraciones de los expertos

### 1. Cálculo del coeficiente V de Aiken

#### 1.1. Fórmula y datos de partida

$$V = \frac{\sum s}{n(c-1)}$$

Donde:

- n (Número de expertos): 4
- c (Número de categorías de la escala): 5
- vm (Valor mínimo de la escala): 1
- ce: Es la calificación dada por el experto.
- s = ce − vm: Es el ajuste de las puntuaciones para que comiencen desde 0.

La escala empleada fue:

1 = Muy deficiente

2 = Deficiente

3 = Aceptable

4 = Bueno

5 = Excelente

#### 1.2. Promedios globales obtenidos con la tabla ajustada

Los promedios globales del modelo fueron:

| Criterio | Promedio global |
|---|---|
| Cobertura del modelo | 4.73 |
| Comprensibilidad | 4.72 |
| Consistencia interna | 4.64 |
| Pertinencia institucional | 4.58 |

#### 1.3. Sustitución en la fórmula

Dado que:

$$n(c-1) = 4(5-1) = 16$$

y utilizando promedios:

$$\mathrm{V}=\frac{\bar{x}-1}{4}$$

a. Cobertura del modelo

$$V=\frac{4.73-1}{4}=\frac{3.73}{4}=0.9325\approx 0.93$$

b. Comprensibilidad

$$V=\frac{4.72-1}{4}=\frac{3.72}{4}=0.93$$

c. Consistencia interna

$$V=\frac{4.64-1}{4}=\frac{3.64}{4}=0.91$$

d. Pertinencia institucional

$$V=\frac{4.58-1}{4}=\frac{3.58}{4}=0.895\approx 0.90$$

**2. Cálculo del coeficiente W de Kendall**

**2.1. Datos de partida**

Para este cálculo se consideraron:

- Número de expertos (m): 4
- Número de componentes evaluados (n): 11

Los 11 componentes fueron:

1. Registro de incidentes
2. Clasificación y categorización
3. Priorización
4. Resolución

5. Escalamiento
6. Cierre formal
7. Mesa de Ayuda (PUC)
8. Roles y niveles de soporte
9. Métricas e indicadores
10. Base de conocimientos
11. Uso de la base de conocimientos

La escala utilizada: 1=Muy deficiente, 5 = Excelente

**2.2. Fórmula del coeficiente W de Kendall**

Como existen empates en las valoraciones (muchos 4 y 5 repetidos), se utilizó la fórmula corregida:

$$W = \frac{12S}{m^2\,(n^3 - n) - m\sum T}$$

Donde:

W: coeficiente de concordancia de Kendall

S: suma de las desviaciones cuadráticas de los rangos totales

m: número de expertos

n: número de componentes evaluados

∑T: corrección por empates

**2.2. Procedimiento para el cálculo**

Primero, las puntuaciones de cada experto fueron convertidas en rangos. Como el valor 5 representa mayor valoración, se le asignó el mejor rango. Cuando existieron empates, se usó el rango promedio.

Por ejemplo, en el criterio Cobertura del modelo, el Experto 1 asignó siete valores de 5 y cuatro valores de 4. Entonces:

Para los siete valores de 5:

$$\frac{1 + 2 + 3 + 4 + 5 + 6 + 7}{7} = 4$$

Para los cuatro valores de 4:

$$\frac{8 + 9 + 10 + 11}{4} = 9.5$$

Así se construyeron los rangos para cada experto.

**Paso 1: Calcular del puntaje promedio por componente y por experto**

Para calcular el W de Kendall global, primero se obtuvo el promedio de los cuatro criterios para cada componente en cada experto.

| Componente | Experto 1 | Experto 2 | Experto 3 | Experto 4 |
|---|---|---|---|---|
| Registro de incidentes | 4.50 | 4.75 | 4.50 | 4.50 |
| Clasificación y categorización | 4.00 | 4.00 | 4.50 | 4.25 |
| Priorización | 4.75 | 5.00 | 4.75 | 4.75 |
| Resolución | 5.00 | 5.00 | 5.00 | 5.00 |
| Escalamiento | 5.00 | 5.00 | 5.00 | 5.00 |
| Cierre formal | 4.25 | 4.25 | 4.00 | 4.25 |
| Mesa de Ayuda (PUC) | 5.00 | 5.00 | 5.00 | 5.00 |
| Roles y niveles de soporte | 5.00 | 5.00 | 5.00 | 5.00 |
| Métricas e indicadores | 4.00 | 4.00 | 4.00 | 4.00 |
| Base de conocimientos | 5.00 | 5.00 | 5.00 | 5.00 |
| Uso de la base de conocimientos | 5.00 | 5.00 | 5.00 | 5.00 |

**Paso 2: Transformar los promedios en rangos**

Se ordenaron los valores de cada experto, asignando:

- Rango más bajo al valor más alto
- Rangos promedio cuando hubo empates

Ejemplo con el Experto 1

Los valores del Experto 1 fueron:

- 5.00 en 6 componentes
- 4.75 en 1 componente
- 4.50 en 1 componente
- 4.25 en 1 componente
- 4.00 en 2 componentes

Entonces:

Los seis valores 5.00 ocupan las posiciones 1 a 6:

$$\frac{1+2+3+4+5+6}{6} = 3.5$$

El valor **4.75** ocupa la posición 7 → rango 7

El valor **4.50** ocupa la posición 8 → rango 8

El valor **4.25** ocupa la posición 9 → rango 9

Los dos valores **4.00** ocupan las posiciones 10 y 11:

$$\frac{10+11}{2} = 10.5$$

Ese mismo procedimiento se realizó para los cuatro expertos.

Tabla de rangos obtenidos

| Componente | Rango E1 | Rango E2 | Rango E3 | Rango E4 | Suma de rangos |
|---|---|---|---|---|---|
| Registro de incidentes | 4.0 | 5.5 | 9.5 | 10.0 | 29.0 |
| Clasificación y categorización | 9.5 | 5.5 | 9.5 | 10.0 | 34.5 |
| Priorización | 4.0 | 5.5 | 4.0 | 4.5 | 18.0 |
| Resolución | 4.0 | 5.5 | 4.0 | 4.5 | 18.0 |
| Escalamiento | 4.0 | 5.5 | 4.0 | 4.5 | 18.0 |
| Cierre formal | 9.5 | 5.5 | 9.5 | 10.0 | 34.5 |
| Mesa de Ayuda (PUC) | 4.0 | 5.5 | 4.0 | 4.5 | 18.0 |
| Roles y niveles de soporte | 9.5 | 5.5 | 4.0 | 4.5 | 23.5 |
| Métricas e indicadores | 9.5 | 11.0 | 4.0 | 4.5 | 29.0 |
| Base de conocimientos | 4.0 | 5.5 | 4.0 | 4.5 | 18.0 |
| Uso de la base de conocimientos | 4.0 | 5.5 | 9.5 | 4.5 | 23.5 |

**Paso 3: Calcular la media de rangos**

$$\bar{R} = \frac{m(n+1)}{2}$$

$$\bar{R} = \frac{4(11+1)}{2}$$

**Paso 4: Calcular S**

$$S = \sum R_i - \bar{R}$$

$$S = 451$$

**Paso 5: Corrección por empates**

La corrección de empates fue:

$$\sum T = 2310$$

Sustituyendo:

$$W = \frac{12(451)}{4^2(11^3 - 11) - 4(2310)}$$

$$W = 0.46$$

Resultados por criterio

| Criterio evaluado | W de Kendall | Interpretación |
|---|---|---|
| Cobertura del modelo | 0.46 | Concordancia moderada |
| Comprensibilidad | 0.68 | Concordancia alta |
| Consistencia interna | 0.55 | Concordancia moderada |
| Pertinencia institucional | 0.67 | Concordancia alta |

Escala de interpretación

| Valor de W | Nivel de concordancia |
|---|---|
| 0.00 – 0.20 | Muy baja |
| 0.21 – 0.40 | Baja |
| 0.41 – 0.60 | Moderada |
| 0.61 – 0.80 | Alta |
| 0.81 – 1.00 | Muy alta |

Por tanto, el coeficiente W de Kendall indica que los expertos coincidieron ampliamente en sus valoraciones sobre los componentes del modelo.

## Anexo 7. Lineamientos normativos para la gestión de incidentes de TI

### 3. Objetivo normativo

El presente documento establece el marco organizativo, operativo y normativo para la gestión de incidentes de tecnologías de la información, con el propósito de asegurar la continuidad, calidad y seguridad de los servicios digitales que soportan los procesos académicos y administrativos, en alineación con ITIL 4 y las políticas de gobierno digital institucional.

### 4. Marco regulatorio de referencia

- Ley Universitaria N.° 30220.
- Lineamientos de Transformación Digital del Estado Peruano (SEGDI – PCM).
- Plan de Gobierno Digital institucional vigente.
- Documentos de gestión organizacional (mapa de procesos, normativas internas).
- ITIL 4 – Práctica de gestión de incidentes.

### 3. Alcance de aplicación

El cumplimiento de esta directiva es obligatorio para:

- La Oficina de Tecnologías de la Información (OTI).
- Estudiantes, docentes y personal administrativo.
- Proveedores externos vinculados a servicios tecnológicos institucionales.

### 4. Conceptos clave

- **Incidente:** Evento no planificado que interrumpe o degrada un servicio de TI.
- **Mesa de ayuda:** Unidad encargada de gestionar incidentes y solicitudes.
- **Punto Único de Contacto (PUC):** Canal centralizado de interacción con los usuarios.
- **Incidente mayor:** Evento de alto impacto que afecta procesos críticos.
- **ITSM:** Enfoque de gestión de servicios de TI orientado a la generación de valor.

### 5. Estructura de roles y responsabilidades

- **Coordinador del proceso de incidentes:** Supervisa la ejecución, analiza indicadores y coordina escalamientos.
- **Nivel 1 – Atención inicial:** Registra, clasifica y resuelve incidentes básicos.

- **Nivel 2 – Especialistas:** Atienden incidentes técnicos especializados.
- **Nivel 3 – Expertos:** Intervienen en incidentes críticos o estructurales.

## 6. Flujo general del proceso de incidentes

El proceso comprende las siguientes etapas:

1. Registro del incidente a través del PUC.
2. Clasificación según taxonomía definida.
3. Priorización basada en impacto y urgencia.
4. Asignación al nivel correspondiente.
5. Resolución del incidente.
6. Escalamiento cuando sea necesario.
7. Cierre formal con validación del usuario.

## 7. Seguimiento y evaluación del proceso

El desempeño del proceso será evaluado mediante indicadores clave como:

- Tiempo promedio de resolución (MTTR).
- Resolución en primer contacto (FCR).
- Distribución de incidentes por servicio.
- Índice de reincidencia.

Los resultados serán reportados de manera periódica para apoyar la toma de decisiones y la mejora continua.

## 8. Disposiciones finales

La Oficina de Tecnologías de la Información es responsable de la implementación, difusión y actualización del presente marco. Su aplicación es obligatoria a partir de su aprobación formal.