UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Modelo de gestión de incidentes de tecnologías de la información para la Universidad Nacional Pedro Ruiz Gallo

PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

Autores:

Bach. Marco Antonio Torres Ventura
Bach. Edgard Ivan Sánchez Niquén

Asesor:

Dr. Ing. Ernesto Kalo Celi Arévalo

Lambayeque, Perú

2026

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Modelo de gestión de incidentes de tecnologías de la información para la Universidad Nacional Pedro Ruiz Gallo

PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

APROBADO POR EL SIGUIENTE JURADO:

Dra. Ing. Pilar del Rosario Ríos Campos
Presidente

Dr. Ing. Jesús Bernardo Olavarria Paz
Secretario

Ing. Luis Alberto Llontop Cumpa
Vocal

Dr. Ing. Ernesto Kalo Celi Arévalo
Asesor

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

ACTA DE SUSTENTACIÓN N°013-2026-UI-FICSA

Siendo las 10:30 am horas del día 10 de agosto del 2026, se reunieron de manera presencial los miembros de jurado de la tesis titulada: **"MODELO DE GESTIÓN DE INCIDENTES DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO", con código N° IS_V_2025_011,** designado por **Resolución Decanal N° 373-2025-UNPRG-FICSA** con la finalidad de Evaluar y Calificar la sustentación de la tesis antes mencionada, conformado por los siguientes docentes:

DRA. ING. PILAR DEL ROSARIO RIOS CAMPOS	**PRESIDENTE**
DR. ING. JESUS BERNARDO OLAVARRIA PAZ	**SECRETARIO**
ING. LUIS ALBERTO LLONTOP CUMPA	**VOCAL**

Asesorado por DR. ING. ERNESTO KARLO CELI AREVALO.

El acto de sustentación fue autorizado por **OFICIO VIRTUAL N° 185-2026-UIFICSA**, la tesis fue presentada y sustentada por los Bachilleres: **MARCO ANTONIO TORRES VENTURA y EDGARD IVAN SANCHEZ NIQUEN,** tuvo una duración de 90 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
MARCO ANTONIO TORRES VENTURA	17	DIECISIETE	BUENO
EDGARD IVAN SANCHEZ NIQUEN	17	DIECISIETE	BUENO

Por lo que quedan **APTOS** para obtener el Título Profesional de **INGENIERO DE SISTEMAS** 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 12:00 m. Se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

DRA. ING. PILAR DEL ROSARIO RIOS CAMPOS
PRESIDENTE

DR. ING. JESUS BERNARDO OLAVARRIA PAZ
SECRETARIO

ING. LUIS ALBERTO LLONTOP CUMPA
VOCAL

Facultad de Ingeniería Sistemas y Arquitectura UNIDAD DE INVESTIGACIÓN DIRECTOR U.N.P.R.G.

JHFF/bcm

CONSTANCIA DE VERIFICACION DE ORIGINALIDAD

Yo **Ernesto Karlo Celi Arévalo** usuario revisor de Tesis [x] Trabajo de Suficiencia Profesional [ ] y/o Trabajo Académico [ ] Titulado: **Modelo de gestión de incidentes de tecnologías de la información para la Universidad Nacional Pedro Ruiz Gallo.**

Cuyo autor (es) son: **Marco Antonio Torres Ventura**; con DNI N° **72681013** y **Edgard Ivan Sánchez Niquén;** con DNI N° **46082353**; declaro que la evaluación realizada por el Programa informático, ha arrojado un porcentaje de similitud **8%,** verificables en el Resumen del Reporte automatizado de similitudes que se acompaña.

El suscrito (a) analizó reporte y concluyó que cada una de las coincidencias detectadas dentro del porcentaje de similitud permitido no constituyen plagio y que el documento cumple con la integridad científica y con las normas para el uso de citas y referencias establecidas en los protocolos respectivos,

Se cumple con adjuntar el Recibo Digital a efectos de la trazabilidad respectiva del proceso.

Lambayeque, 20 de Agosto del 2026

.....

Firma (Asesor)

Nombres y Apellidos: Ernesto Karlo Celi Arévalo

DNI 18068078

Adjunta:

Resumen de Reporte automatizado de similitudes
Recibo digital

Tesis Modelo de gestión de incidentes de tecnologías de la información para la Universidad Nacional Pedro Ruiz Gallo

ORIGINALITY REPORT

8%	8%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	hdl.handle.net Internet Source	2%
2	repositorio.uss.edu.pe Internet Source	<1%
3	repositorio.unprg.edu.pe Internet Source	<1%
4	repositoriotec.tec.ac.cr Internet Source	<1%
5	upc.aws.openrepository.com Internet Source	<1%
6	doi.org Internet Source	<1%
7	repositorio.ucv.edu.pe Internet Source	<1%
8	www.coursehero.com Internet Source	<1%
9	Submitted to Universidad Tecnológica Centroamericana UNITEC Student Paper	<1%
10	www.docstoc.com Internet Source	<1%
11	alicia.concytec.gob.pe Internet Source	<1%
12	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Student Paper	<1%
13	repositorio.puce.edu.ec Internet Source	<1%
14	bibdigital.epn.edu.ec Internet Source	<1%
	core.ac.uk	

Dr. Ernesto Karlo Celi Arévalo
DNI 18068078
ASESOR

Ing. Ernesto Karlo Celi Arévalo

DNI. 18068078

15	Student Paper	<1 %
16	repositorio.unitec.edu Internet Source	<1 %
17	repositorio.utelesup.edu.pe Internet Source	<1 %
18	Submitted to FUNIBER Student Paper	<1 %
19	repositorio.uti.edu.ec Internet Source	<1 %
20	Lanuza Bustamante, Narda Naomi. "Gestión de incidencias basadas en ITIL 4.0 para reducir tiempos en la dirección de tecnologías de información de una Universidad Privada", Universidad Nacional del Altiplano de Puno (Peru) Publication	<1 %
21	www.investigacionaplicadarevista.com Internet Source	<1 %
22	repositorio.unprg.edu.pe:8080 Internet Source	<1 %
23	www.estrategia.gobiernoenlinea.gov.co Internet Source	<1 %
24	core.ac.uk Internet Source	<1 %
25	repositorio.puce.edu.ec Internet Source	<1 %
26	Barba Vera, Ruth Genoveva. "Metodología basada en políticas de QoS en SDN para el control de amenazas internas y mejora del rendimiento en intranets académicas.", Pontificia Universidad Catolica del Peru (Peru) Publication	<1 %
27	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Student Paper	<1 %
28	oai.e-spacio.uned.es Internet Source	<1 %
29	Submitted to Universidad Cesar Vallejo Student Paper	<1 %
30	docplayer.es Internet Source	<1 %

Dr. Ernesto Karlo Celi Arévalo
DNI 18068078
ASESOR

Ing. Ernesto Karlo Celi Arévalo

DNI. 18068078

31	Submitted to Universidad Europea de Madrid Student Paper	<1%
32	www.parlamento-navarra.es Internet Source	<1%
33	www.researchgate.net Internet Source	<1%
34	repositorioinstitucional.buap.mx Internet Source	<1%
35	www.reicomunicar.journalgestar.org Internet Source	<1%
36	burjcdigital.urjc.es Internet Source	<1%
37	www.ilustrados.com Internet Source	<1%
38	www.przetargi.info Internet Source	<1%
39	fupvirtual.edu.co Internet Source	<1%
40	pdfcookie.com Internet Source	<1%
41	tesis.pucp.edu.pe Internet Source	<1%
42	journalingeniar.org Internet Source	<1%
43	Submitted to Universidad Nacional del Centro del Peru Student Paper	<1%

Exclude quotes	On	Exclude matches	< 15 words
Exclude bibliography	On		

Dr. Ernesto Karlo Celi Arévalo
DNI 18068078
ASESOR

Ing. Ernesto Karlo Celi Arévalo

DNI. 18068078

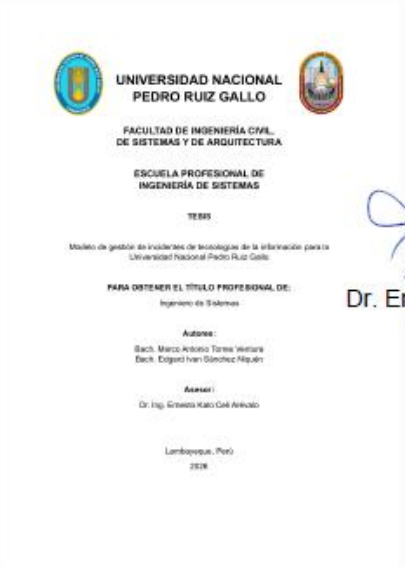
turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Marco Torres Ventura Y Edgard Sánchez Niquén
Assignment title:	Quick Submit
Submission title:	Tesis Modelo de gestión de incidentes de tecnologías de la inf...
File name:	Informe_de_tesis_Torres_Sanchez_Final.docx
File size:	874.58K
Page count:	117
Word count:	31,750
Character count:	186,109
Submission date:	20-Aug-2026 10:49AM (UTC-0500)
Submission ID:	3015165902



UNIVERSIDAD NACIONAL
PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL,
DE SISTEMAS Y DE ARQUITECTURA

ESCUELA PROFESIONAL DE
INGENIERÍA DE SISTEMAS

TESIS

Modelo de gestión de incidentes de tecnologías de la información para la Universidad Nacional Pedro Ruiz Gallo

PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

Autores:
Bach. Marco Antonio Torres Ventura
Bach. Edgard Ivan Sánchez Niquén

Asesor:
Dr. Ing. Ernesto Karlo Celi Arévalo

Lambayeque, Perú
2026

Dr. Ernesto Karlo Celi Arévalo
DNI 18068078
ASESOR

Ing. Ernesto Karlo Celi Arévalo

DNI. 18068078

DEDICATORIA

A quienes creyeron en mí incluso cuando yo dudé.
Gracias por acompañarme hasta el final.

Edgard Ivan Sánchez Niquén

A mis padres, cuya ausencia se transformó en una presencia constante que me impulsa a perseverar y no rendirme. Su amor trasciende el tiempo y siguen guiando mi camino.

Marco Antonio Torres Ventura

AGRADECIMIENTOS

Quiero expresar mi sincero agradecimiento a mi asesor de tesis, por su orientación, dedicación y valiosos aportes técnicos, los cuales fueron fundamentales para el desarrollo y culminación de este trabajo de investigación.

De manera especial, agradezco a mi familia por su apoyo incondicional, comprensión y constante motivación durante todo este proceso académico. Su confianza y aliento fueron esenciales para alcanzar este logro.

Edgard Ivan Sánchez Niquén

A la memoria de mis padres y a mis hermanos, por su constante apoyo, por ser un ejemplo de fortaleza y perseverancia, y por guiarme con sus palabras y acciones en el camino hacia mis metas.

A mi asesor, por su guía académica y valiosas observaciones, que me permitieron orientar adecuadamente el desarrollo del presente trabajo.

Marco Antonio Torres Ventura

RESUMEN

La presente investigación abordó el problema de la gestión inadecuada de los incidentes de tecnologías de la información (TI) en la Universidad Nacional Pedro Ruiz Gallo, caracterizada por la ausencia de procedimientos formales, falta de una mesa de ayuda estructurada, inexistencia de criterios estandarizados de clasificación y priorización, y una atención reactiva basada en comunicaciones informales. Esta situación genera impactos directos en procesos académicos y administrativos críticos, como la matrícula, el registro académico, la docencia virtual, la gestión de la investigación y los trámites institucionales, afectando la continuidad y calidad de los servicios digitales. La investigación se desarrolló bajo un enfoque cualitativo, con un tipo de investigación descriptiva–propositiva, ya que no se buscó implementar el modelo en la realidad, sino analizar la situación actual y proponer una solución estructurada. El método utilizado fue analítico–sintético, apoyado en técnicas como la revisión documental, entrevistas simuladas a personal técnico de la Oficina de Tecnologías de la Información y el análisis comparativo con las buenas prácticas del marco referencial ITIL 4, específicamente la práctica de Gestión de Incidentes. Como principales resultados, se identificaron brechas significativas en gobernanza de TI, infraestructura tecnológica, seguridad digital, roles y flujos de escalamiento, así como la ausencia de métricas e instrumentos de control. A partir de ello, se desarrolló una propuesta de modelo de gestión de incidentes basado en ITIL 4, que incluye el diseño de una mesa de ayuda como Punto Único de Contacto, reglas de categorización y priorización, flujos de trabajo estandarizados, integración con seguridad digital, generación de métricas e informes y mecanismos de mejora continua. El estudio concluye que el modelo propuesto constituye una alternativa viable y pertinente para fortalecer la gestión de los servicios de TI en la UNPRG.

Palabras clave: Gestión de incidentes de TI; ITIL 4; Mesa de ayuda; Servicios de tecnologías de la información; Gobierno digital.

ABSTRACT

This research addressed the problem of inadequate information technology (IT) incident management at the Universidad Nacional Pedro Ruiz Gallo, characterized by the absence of formal procedures, the lack of a structured service desk, non-standardized classification and prioritization criteria, and a reactive approach based on informal communications. This situation directly affects critical academic and administrative processes such as enrollment, academic records management, virtual teaching, research management, and institutional procedures, compromising service continuity and quality. The study was conducted using a qualitative approach, with a descriptive–propositional research design, as the objective was not to implement the model but to analyze the current situation and propose a structured solution. An analytical–synthetic method was applied, supported by document review, simulated interviews with technical staff from the IT Office, and a comparative analysis against ITIL 4 best practices, particularly the Incident Management practice. The main findings revealed significant gaps in IT governance, technological infrastructure, digital security, defined roles, escalation workflows, and the absence of metrics and control mechanisms. Based on these results, a proposed ITIL 4–based incident management model was developed, including a service desk as a Single Point of Contact, incident categorization and prioritization rules, standardized workflows, integration with digital security processes, metrics and reporting mechanisms, and continuous improvement practices. The study concludes that the proposed model represents a feasible and relevant alternative to strengthen IT service management at the university.

Keywords: IT incident management; ITIL 4; Service desk; Information technology services; Digital governance.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La continua dependencia de las organizaciones respecto a sus sistemas de información ha vuelto inevitable que, tarde o temprano, experimenten incidentes vinculados a la tecnología. A veces se trata de fallas pequeñas, casi rutinarias, y en otras ocasiones aparecen interrupciones más serias que pueden paralizar procesos completos. Cuando no existe una forma ordenada de enfrentar estos problemas, el impacto suele sentirse en la operación diaria: retrasos, malestar de los usuarios, pérdida de datos, o incluso decisiones tomadas a ciegas por no contar con información fiable en el momento oportuno. Tal como apunta la ISO/IEC 27035 sobre la gestión de incidentes, reaccionar sin un sistema formal deja a la organización “expuesta a disrupciones evitables y a la repetición de vulnerabilidades conocidas” (ISO, 2016).

Implementar un sistema de gestión de incidentes de TI significa algo más que abrir tickets y cerrarlos cuando parece que ya funcionan. Implica definir cómo se detectan, registran, atienden y comunican los incidentes; quién se responsabiliza de cada etapa; en qué momento se debe escalar la atención; y cómo se aprende de lo ocurrido para evitar que vuelva a suceder. Cuando este ciclo se vuelve parte de la cultura organizacional, las interrupciones ya no sorprenden tanto, pues se cuenta con un mecanismo que absorbe el golpe y reduce la afectación.

Para guiar la implementación, han surgido distintos marcos de referencia reconocidos a nivel internacional. Uno de los más utilizados es ITIL, particularmente en su proceso de Incident Management, que propone prácticas para restaurar la operación normal del servicio en el menor tiempo posible (Axelos, 2019). También se apoyan en normas como la ISO/IEC 20000, orientada a la gestión de servicios de TI, y en algunos casos en recomendaciones de NIST, sobre todo cuando el incidente involucra ciberseguridad. De uno u otro modo, estos marcos ofrecen puntos de partida que reducen la improvisación y ayudan a estandarizar cómo se trabaja internamente.

Las universidades, aunque a veces se las imagina alejadas de estas preocupaciones más “tecnológicas”, dependen profundamente de sus servicios informáticos. Matrículas en línea, aulas virtuales, bases de datos académicas, sistemas de investigación, repositorios institucionales, pagos, trámites administrativos: prácticamente todo se sostiene sobre plataformas que requieren estabilidad. En entornos donde conviven miles de usuarios con necesidades muy distintas, la probabilidad de que aparezcan

incidentes diariamente es bastante alta, y si no se gestionan adecuadamente, el efecto se acumula como una especie de desgaste silencioso.

En la Universidad Nacional Pedro Ruiz Gallo (UNPRG), esto se percibe con claridad. Es muy común que, en momentos críticos del semestre académico, una caída del sistema de información académico (SIA) retrase el proceso de matrícula, incidiendo directamente en el calendario de matrículas o en el inicio de las clases, obligado a reorganizar o recalendarizar un semestre académico completo; o que ciertos reportes administrativos no pudieron enviarse a tiempo porque el módulo correspondiente dejó de funcionar por un evento no controlado. Son episodios cotidianos, casi anecdóticos, pero que juntos muestran la necesidad de contar con una estructura más sólida para atender incidentes de TI. La universidad no solo debe responder, sino hacerlo con rapidez, trazabilidad y criterios claros que no dependan únicamente de la disponibilidad del personal técnico en turno.

Además, al tratarse de una institución pública con responsabilidad social, la UNPRG enfrenta un desafío adicional: garantizar continuidad en los servicios para miles de estudiantes de Lambayeque y de otras regiones que dependen del acceso digital para su formación. Esto convierte la gestión de incidentes en un asunto no solo técnico, sino también académico y social. Cuando un sistema falla durante una evaluación virtual, o cuando un investigador pierde acceso temporal a sus datos, el daño trasciende lo operativo y toca el proceso educativo en sí mismo.

Por ello, resulta relevante preguntarse qué tipo de modelo permitiría organizar esta actividad de un modo más consistente. No basta con soluciones rápidas ni con “apagar incendios”. Se necesita una estructura que mire hacia ITIL, como uno de los marcos más consolidados en servicios de TI, y lo adapte a la realidad universitaria, que no siempre es tan predecible como la de una empresa privada. En ese sentido, la investigación plantea la siguiente pregunta central: ***¿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 tecnologías de la información en la Universidad Nacional Pedro Ruiz Gallo?***

La formulación de esta pregunta deriva de una necesidad práctica: comprender cómo se gestionan actualmente los incidentes en los procesos académicos y administrativos, e identificar en qué puntos fallan o se quedan cortos. Solo con ese diagnóstico será posible diseñar una propuesta que responda a las condiciones reales de la institución.

Aquí surgen el objetivo general: ***Desarrollar una propuesta de modelo de gestión de incidentes de tecnologías de la información basado en las buenas prácticas del marco referencial ITIL como soporte a los servicios de tecnologías de la información en la Universidad Nacional Pedro Ruiz Gallo***. Para lograr este objetivo, se propuso los siguientes objetivos específicos: **(1)** ***analizar la forma en que hoy se atienden los incidentes, contrastándolos con las buenas prácticas de ITIL*****, y (2)** ***identificar problemas y debilidades en los procesos académicos y administrativos que brindan servicios relacionado con la gestión de incidentes*****.**

A partir de ese análisis, la investigación se orienta a proponer los componentes clave de una mesa de ayuda que cumpla un rol articulador. No se trata únicamente de un repositorio de tickets; se piensa como un nodo central donde convergen las solicitudes, se clasifican según criterios definidos y se distribuyen hacia los equipos correspondientes. Por ello, los objetivos siguientes incluyen (3) *diseñar los elementos funcionales y estructurales de esa mesa de ayuda*, (4) *definir reglas de categorización y priorización de los incidentes*, y (5) *establecer flujos de trabajo coherente con ITIL*.

Desde una perspectiva práctica, esta investigación aspira a generar un instrumento que ordene la atención de incidentes en la UNPRG, reduzca tiempos de respuesta y mejore la experiencia de estudiantes, docentes y personal administrativo. A nivel teórico, aporta al entendimiento de cómo ITIL puede adaptarse a un contexto universitario público peruano, que suele tener procesos más rígidos y recursos limitados. En términos de relevancia, responde a una necesidad institucional visible, mientras que su pertinencia recae en el hecho de que la universidad se encuentra en un proceso de modernización en el cual los servicios digitales ocupan un lugar cada vez más central.

En conjunto, estos elementos justifican la realización de la presente investigación y fundamentan su contribución: ofrecer un modelo claro, aplicable y validado que permita mejorar la forma en que la universidad enfrenta los incidentes tecnológicos que afectan su operación diaria.

DISEÑO TEÓRICO

1.1. Antecedentes

La investigación *"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"* parte de un problema muy concreto: los servicios de TI de la escuela sufrían tiempos de atención largos y un número apreciable de incidencias que quedaban sin resolver, lo que afectaba la eficacia global del servicio percibido por los usuarios internos. El objetivo general fue proponer e implementar un modelo de gestión de incidencias basado en ITIL para mejorar la eficacia del servicio, operacionalizando esta eficacia mediante métricas como el tiempo de resolución, el número de incidencias registradas y el número de incidencias resueltas. En términos teóricos, el trabajo combina la noción de eficacia de la norma ISO 9000 con la definición de gestión de incidentes de ITIL v3 y las guías de Van Bon sobre operación del servicio, incorporando subprocesos como registro, categorización, diagnóstico, resolución y cierre de incidentes. Metodológicamente se plantea como una investigación aplicada, apoyada en la definición de variables e indicadores, y en la prueba práctica del modelo durante un mes dentro de la organización, comparando el comportamiento de los indicadores antes y después de su uso. Los resultados muestran que la aplicación del modelo reduce el tiempo de resolución y disminuye el número de incidencias sin resolver, evidenciando un impacto positivo en la eficacia del servicio TI y aportando un esquema replicable de roles, métricas y flujo de trabajo para pequeñas unidades académicas que gestionan servicios tecnológicos.

El estudio *"Modelo de gestión de incidentes, aplicando ITIL v3.0 en un organismo del Estado peruano"* se desarrolla en la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), ente rector del Sistema Nacional de Informática. El diagnóstico inicial revela problemas de baja transparencia, demoras en la atención, falta de historial de incidencias, ausencia de acuerdos de nivel de servicio y una Mesa de Ayuda mal implementada, lo que se traduce en deficiente gestión de incidentes y de los servicios TI orientados a entidades públicas. Frente a ello, el objetivo central fue formular un nuevo modelo de gestión de incidentes basado en ITIL v3.0 que contribuya a restaurar rápidamente los servicios y a asegurar la continuidad de los procesos de negocio en la ONGEI. El marco teórico combina ITIL (particularmente la fase de Operación del Servicio y

el proceso de gestión de incidencias) con la norma ISO/IEC 20000 y el enfoque de sistemas de gestión de calidad de ISO 9001, estructurando subprocesos como registro, categorización, escalamiento, gestión de incidentes graves y emisión de informes. El estudio adopta un enfoque aplicado de diseño de modelo: realiza diagnóstico organizacional, mapea el sistema de gestión existente y luego propone un nuevo organigrama para TI, define roles, catálogos de servicio, flujos y lineamientos para la Mesa de Ayuda. Entre los principales aportes se tuvo la formalización del proceso, la creación de un único punto de contacto, la mejora esperada en tiempos de respuesta y satisfacción de usuarios, así como la generación de un modelo técnico y referencial replicable en otras entidades del sector público peruano (Loayza, 2015).

En la investigación *"Desarrollo de un modelo de gestión de incidentes basado en ITIL v3.0 para el área de Facilities Management de la empresa Tgestiona"*, el autor aborda la problemática de un área de Facilities que brinda servicios de soporte sin contar con procesos claramente definidos de gestión de incidentes, ni criterios homogéneos de categorización y priorización, lo que generaba respuestas poco consistentes y dificultades para controlar los tiempos de atención. El objetivo general fue desarrollar un modelo de gestión de incidentes apoyado en las buenas prácticas de ITIL v3.0, específicamente adaptado al contexto de Facilities Management. Teóricamente, la tesis se fundamenta en el marco de ITIL como referencia de gestión de servicios, enfatizando el proceso de gestión de incidencias, la noción de categorías y niveles de prioridad, y el uso de acuerdos de nivel de servicio como mecanismo para alinear expectativas entre negocio y TI. La investigación se estructura como un estudio aplicado de tipo propositivo, que parte del análisis de la situación actual y de antecedentes similares, para luego diseñar un modelo que integra flujo de trabajo, roles, matriz de categorización y esquemas de prioridad. De acuerdo con la síntesis citada por Ninaraqui, uno de los resultados clave del estudio es que el modelo ITIL permitió identificar de forma sistemática los tipos de categorías y niveles de priorización, facilitando que los responsables del control del sistema atiendan los incidentes de la "mejor forma posible" y reporten su cierre dentro de los plazos establecidos, contribuyendo así a una operación más predecible del servicio (Cáceres, 2019).

El estudio de posgrado *"Implementación de procesos ITIL de gestión de incidencias y problemas. Aplicación en una empresa de Desarrollo y*

Mantenimiento de Software" se sitúa en un contexto de creciente demanda de servicios TIC y de fuerte dependencia del negocio respecto de la disponibilidad de dichos servicios. El problema identificado es la falta de procesos formales y eficaces de gestión de incidencias y problemas en una empresa de desarrollo y mantenimiento de software, lo que se traduce en debilidades de calidad y tiempos de respuesta. El objetivo del estudio fue implementar y desplegar dos procesos de gestión TI: gestión de incidencias y gestión del problema, basados en el marco ITIL, apoyándose en herramientas ITSM del mercado. El fundamento teórico combina la literatura de ITSM, la biblioteca ITIL y el análisis comparativo de marcos y herramientas de gestión de servicios. Metodológicamente, el trabajo realiza primero un análisis detallado de los procesos actuales, identificando carencias; luego revisa los principales frameworks y herramientas ITSM; finalmente, define un nuevo proceso de gestión de incidencias y problemas y lo implementa en una herramienta seleccionada (como JIRA Atlassian). Los resultados obtenidos incluyen la corrección de limitaciones previas, la mejora de la organización de los servicios TI y una mayor madurez en la gestión de incidencias y problemas, constituyendo un aporte práctico al demostrar la implantación real de procesos ITIL en una empresa concreta (Zender, 2024).

En el estudio *"Propuesta de implementación del proceso de Gestión de Incidentes, basado en ITIL para Inversiones TB S.A."* se desarrolla en una empresa costarricense donde el proceso de gestión de incidentes existía de forma informal, con brechas importantes en el registro, seguimiento y cierre de incidencias de TI. El problema central es la falta de un proceso estructurado que permita asegurar una atención oportuna y trazable, lo que repercute en la continuidad del servicio y en la percepción de los usuarios. El objetivo fue presentar una propuesta de implementación del proceso de gestión de incidentes basado en el marco ITIL para mejorar las operaciones de servicios TI de la organización. Para ello, el estudio se apoya teóricamente en ITIL como estándar de referencia, en los factores de éxito de la práctica de gestión de incidentes y en la literatura de ITSM; además analiza las capacidades del entorno Microsoft 365 y de herramientas líderes del mercado para digitalizar el proceso. Desde el punto de vista metodológico, se realiza un diagnóstico del estado actual mediante entrevistas, encuestas y observaciones pasivas, identificando brechas que luego se evalúan con los factores de éxito ITIL. La contribución principal es una propuesta estructurada que incluye política de gestión de incidentes,

lineamientos para la herramienta tecnológica y un diseño de proceso que, según el autor, permitirá mejorar la prestación de servicios TI y aumentar la eficiencia operativa de la empresa (Céspedes-Garbanzo, 2024).

La investigación *"Design and Implementation of an Automated IT Incident Management System for Small and Medium-Sized Enterprises"* se centra en el problema que viven muchas pymes: equipos de TI pequeños, poco tiempo para operar procesos formales y ausencia de herramientas adecuadas para gestionar los incidentes de forma sistemática. El objetivo declarado es encontrar y diseñar un sistema disponible que permita automatizar la mayor parte del proceso de gestión de incidentes, mejorando el tiempo de actividad y reduciendo costos. En el plano teórico, el trabajo revisa el proceso de gestión de incidentes según ITIL, discute sus actividades (detección y registro, clasificación, priorización, escalamiento, resolución y cierre) y las relaciona con prácticas contemporáneas de ITSM y acuerdos de nivel de servicio. Metodológicamente, combina una revisión de literatura y de soluciones SaaS (OpsGenie, PagerDuty, xMatters) con el diseño e implementación de una solución propia, basada en tecnologías como Drupal, Prometheus, Mattermost y PagerDuty para cubrir registro, monitoreo, comunicación, gestión de guardias y documentación postincidente. Aunque no se presenta como un experimento estadístico, el estudio muestra cómo la automatización de partes del proceso, alineada con los principios de ITIL, puede reducir el tiempo de resolución y mejorar la fiabilidad de los servicios digitales, proponiendo una arquitectura práctica para equipos pequeños que necesitan aplicar buenas prácticas de gestión de incidentes sin una infraestructura corporativa pesada (Hasan, 2021).

1.2. Fundamento teórico

1.2.1. Gestión de Servicios de TI (ITSM)

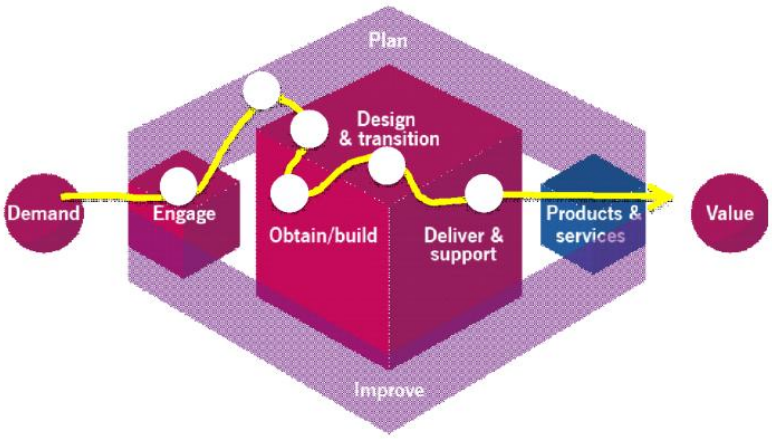
IT Service Management (ITSM) se define como un enfoque basado en procesos para diseñar, administrar y entregar servicios de TI que apoyen los objetivos del negocio, como lo señala Trinidad, et.al. (2021). Esta definición no se queda solo en la operación técnica; enfatiza que la razón de ser de ITSM es contribuir al logro de objetivos organizacionales, lo que lo convierte en un componente estratégico y no únicamente en una función de soporte.

El mismo estudio muestra que la adopción de marcos de referencia de ITSM (como ITIL, ISO/IEC 20000 o CMMI-SVC) permite mejorar la calidad del servicio,

la satisfacción del cliente y reducir costos en la provisión de servicios de TI, siempre que se implemente con buenas prácticas de gestión de procesos y factores humanos adecuados (motivación, compromiso, competencias del personal). ITSM actúa como un puente entre la operación diaria de TI y los indicadores de desempeño que importan al negocio: calidad percibida, continuidad del servicio, tiempo de respuesta, etc.

Desde una perspectiva más aplicada, Harjanto y Aji (2024) analizan ITSM a través una perspectiva de gestión de activos de TI (ITAM) en una empresa de ciberseguridad, mostrando que los activos tecnológicos existen para soportar servicios de negocio y que su gestión debe alinearse explícitamente con los objetivos empresariales. Su estudio cualitativo en una start-up del sector seguridad concluye que cuando se gobiernan los activos siguiendo ITIL 4 (y el Service Value Chain), mejora el control de costos, se reducen riesgos y se protege la reputación corporativa, porque la organización puede demostrar trazabilidad, cumplimiento y cuidado de los recursos tecnológicos críticos.

Figura 1. Etapas de la Cadena de Valor del Servicio (Service Value Chain-SVC) según ITIL 4

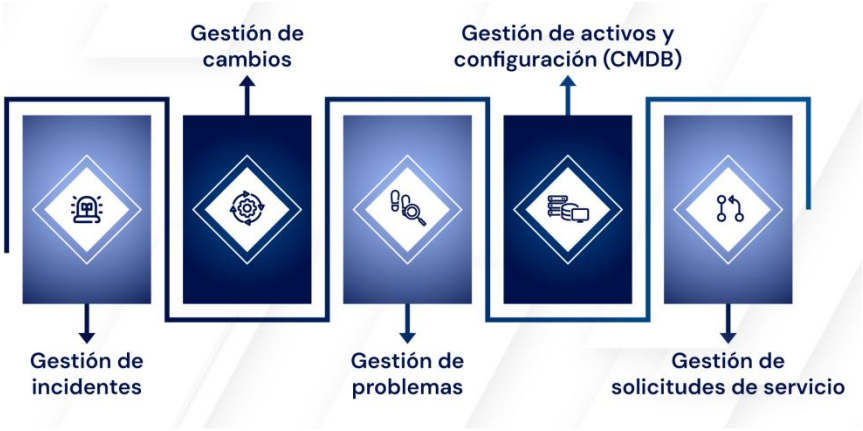


Nota: Obtenido de Harjanto y Aji (2024)

La articulación de ITSM con los procesos del negocio también se refleja en la forma en que ITIL 4 redefine el marco. Agutter (2020) explica que ITIL es el marco de buenas prácticas más difundido para ITSM y que su versión actual “ha evolucionado hacia un enfoque centrado en un sistema de valor que puede integrarse con otras prácticas de gestión”. En otra parte de la descripción del libro se indica que el modelo operativo digital de ITIL 4 ha sido diseñado para ayudar a los equipos de TI a crear, entregar y operar productos y servicios técnicos que se ajusten a la estrategia de negocio de la organización. Esto

refuerza la idea de que ITSM, entendido a través de ITIL 4, no es solo un catálogo de procesos, sino una forma de organizar y acoplar flujos de valor entre TI y las unidades de negocio.

Figura 2. Procesos de la Gestión de Servicios de TI (ITSM), según ITIL 4



Nota: Obtenido de Agutter (2020)

En el plano de la seguridad de la información, la literatura reciente subraya que ya no se puede tratar como un tema separado de la gestión de servicios. Sekti (2025) sostiene que “la seguridad de la información se ha convertido en una piedra angular de la gestión moderna de servicios de TI, impulsada por la creciente dependencia de la infraestructura digital”. El autor plantea cómo la confidencialidad, integridad y disponibilidad deben gestionarse dentro del ciclo de vida de los servicios de TI, integrando la gestión de riesgos, la respuesta a incidentes, el cumplimiento normativo y los controles de seguridad como parte del propio ITSM, no como un añadido posterior.

El mismo trabajo sobre *IT Service Information Security Management* plantea estrategias para salvaguardar los servicios incluyendo medidas de seguridad proactivas, evaluación de vulnerabilidades y planeamiento de respuesta a incidentes, todo ello alineado con objetivos organizacionales y requerimientos de cumplimiento. Esta visión encaja con lo que se suele esperar de un modelo de gestión de incidentes de TI en una universidad: no se trata solo de “arreglar fallas”, sino de proteger datos sensibles (académicos, administrativos, de investigación) y garantizar continuidad de operaciones críticas como matrícula, aulas virtuales o sistemas de biblioteca.

Por su parte, Harjanto y Aji (2024) muestran que una práctica específica de ITSM (IT Asset Management) basada en ITIL 4 contribuye tanto al desempeño financiero como a la ciberseguridad: una gestión rigurosa de activos ayuda a reducir vulnerabilidades, controlar el uso de licencias, asegurar que los equipos tengan versiones actualizadas y minimizar la exposición a incidentes que puedan afectar la imagen y la confianza en la organización. Aunque el estudio se centra en activos, el razonamiento es extrapolable a otros procesos de ITSM, incluyendo la gestión de incidentes, ya que todos comparten el mismo marco ITIL 4 y el mismo enfoque de alineamiento con el negocio.

Estas fuentes respaldan que ITSM puede entenderse como un enfoque de gestión de servicios de TI orientado a procesos, alineado con los objetivos del negocio, que integra prácticas de seguridad de la información y que, en la actualidad, se operacionaliza principalmente a través de marcos como ITIL 4.

1.2.2. ITIL 4 como marco de referencia para la gestión de servicios

En la edición de ITIL Foundation: ITIL 4 Edition, publicada en 2020, se presenta ITIL 4 como la evolución de las buenas prácticas de gestión de servicios y se introduce explícitamente el Service Value System (SVS) como modelo central. El SVS se considera como un sistema que integra principios guía, gobernanza, cadena de valor del servicio, prácticas de gestión y mejora continua para facilitar la creación de valor a partir de la demanda de las partes interesadas. Además, se indica que “el sistema de valor del servicio muestra cómo todos los componentes y actividades de la organización trabajan juntos para permitir la creación de valor” (Axelos, 2020). Esta definición delimita de forma clara los componentes conceptuales de la gestión de servicios: principios, procesos, prácticas, gobernanza, mejora continua.

Ferreira (2021) ofrece un planteamiento más aplicado, al explicar cómo ITIL 4 reorganiza la gestión de servicios de TIC en torno al SVS y a la Service Value Chain (SVC). En su artículo sobre la importancia del marco ITIL en la gestión de servicios de tecnologías de la información y comunicación, el autor resume que la versión ITIL 4 incorpora Service Value System, Service Value Chain, cuatro dimensiones de la gestión de servicios, principios guía y prácticas de ITIL como elementos clave del nuevo modelo. Además, señala que este marco proporciona una visión holística en la que el valor del servicio para clientes y partes interesadas se sitúa en el centro del esquema conceptual, lo cual facilita estudiar

la relación entre procesos de TI, madurez organizacional y resultados de negocio. Esto permite, por ejemplo, definir constructos como valor percibido del servicio, alineamiento TI-negocio o madurez de prácticas ITIL y relacionarlos con la implementación de incident management u otras prácticas específicas.

Por otro lado, Santosa y Mulyana (2023) muestran de forma explícita cómo ITIL 4 puede emplearse como marco de referencia conceptual en estudios de arquitectura y diseño de gestión de servicios. Su artículo *"The IT Services Management Architecture Design for Large and Medium-sized Companies based on ITIL 4 and TOGAF Framework"* desarrolla una arquitectura empresarial de gestión de servicios apoyada en las mejores prácticas de ITIL 4 y el marco TOGAF. Los autores indican que su investigación se centra en preparar un diseño de arquitectura empresarial en la gestión de servicios de TI, tomando como referencia las mejores prácticas de ITIL 4. De este modo, ITIL 4 no se usa solo como guía operativa, sino como modelo conceptual que estructura dominios de negocio, datos, aplicaciones y procesos, demostrando su utilidad para delimitar el alcance del sistema de gestión de servicios y derivar artefactos (catálogos de servicios, modelos de datos, diagramas de casos de uso) que luego pueden evaluarse empíricamente.

1.2.3. Práctica de Incident Management en ITIL 4

La gestión de incidentes es una de las prácticas operativas más críticas dentro del marco ITIL 4, pues constituye el mecanismo principal para restaurar la operación normal del servicio cuando ocurre una interrupción. En la guía oficial *ITIL 4 Practice Guide: Incident Management*, Axelos (2020) señala que 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". Esta definición subraya dos ideas clave: por un lado, que los incidentes son considerados eventos inevitables en la operación de servicios de TI; y por otro, que la respuesta a dichos incidentes debe ser organizada, sistemática y orientada a mantener la continuidad operativa. Para ITIL 4, el valor no se genera solo al diseñar servicios, sino al asegurar que estos continúen funcionando incluso ante fallas, por lo que Incident Management se convierte en un pilar del sistema de valor del servicio.

Un aspecto central de la práctica es su ciclo de vida, compuesto, según Axelos (2020), por actividades como detección, registro, clasificación, priorización,

diagnóstico, resolución y cierre del incidente. Estas actividades permiten que la organización mantenga trazabilidad y asegure que cada incidente reciba el nivel de atención adecuado. ITIL 4 también distingue entre incidentes regulares y *major incidents*, que son aquellos cuya interrupción afecta a un número significativo de usuarios o servicios críticos. La guía señala que, para estos casos, la organización debe prever roles especializados como el *major incident manager* y flujos de coordinación más estrictos (Axelos, 2020). Esta distinción es particularmente útil en instituciones universitarias, donde un incidente en el sistema de matrícula o en la plataforma de aulas virtuales puede considerarse mayor por su impacto institucional.

Dzemydienė, et.al. (2024) aportan una perspectiva aplicada que refuerza la estructura conceptual de ITIL 4. En su estudio sobre gestión de incidentes en instituciones educativas, las autoras destacan que los servicios TIC del sector académico deben operar sin interrupciones debido a su función en los procesos de enseñanza, investigación y administración. Ellas afirman que “la gestión de incidentes basada en ITIL 4 constituye una de las prácticas más importantes para garantizar la continuidad del trabajo de los sistemas interoperables de una institución educativa” (p. 286). El estudio propone un algoritmo que combina actividades de reconocimiento temprano de incidentes, reglas de clasificación y mecanismos de priorización orientados a asegurar que el personal técnico pueda distinguir rápidamente entre eventos informativos, incidentes comunes y situaciones críticas. Esta aproximación demuestra que ITIL 4 no solo es un modelo conceptual, sino un marco adaptativo que puede integrarse con sistemas de monitoreo, herramientas de soporte a la decisión y mesas de ayuda.

Otro aporte relevante del trabajo de Dzemydienė et al. (2024) es el énfasis en la automatización y el soporte algorítmico para la toma de decisiones. Las autoras argumentan que, en entornos con alta demanda operativa, la identificación manual de incidentes no es suficiente, por lo que recomiendan incorporar métodos inteligentes que permitan analizar patrones y predecir interrupciones potenciales. Esto coincide con la visión de Axelos (2020), que plantea que la eficacia de la práctica depende de combinar procesos definidos, equipos capacitados y herramientas tecnológicas que faciliten la ejecución de cada actividad del ciclo de vida del incidente.

Desde otra perspectiva, Nugroho y Fianty (2023) analizan la madurez de los procesos de help desk e incident management utilizando un modelo de autoevaluación basado en ITIL. Su estudio revela que muchas organizaciones carecen de documentación sistemática, niveles de servicio formalizados y mecanismos de integración entre incident management, problem management y la base de errores conocidos. Los autores señalan que estas brechas reducen la eficiencia de los servicios de TI y generan tiempos de respuesta inconsistentes. Entre sus conclusiones afirman que mejorar la gestión de incidentes aplicando las mejores prácticas de ITIL permite aumentar la integración de procesos, fortalecer el cumplimiento de SLA y elevar la satisfacción de los usuarios (Nugroho & Fianty, 2023). Aunque su análisis se desarrolla en el contexto de ITIL v3, los principios evaluados, como documentación, priorización, escalamiento, integración con “problem management”, siguen plenamente vigentes en ITIL 4, lo que facilita su traslado al diseño de modelos de gestión para organizaciones públicas como la UNPRG.

1.2.4. Elementos estructurales de Incident Management

En la guía oficial *ITIL®4 Practice Guide: Incident Management*, Axelos (2020) deja claro que la práctica no es solo una secuencia de pasos, sino un conjunto estructurado de componentes que se apoyan en las cuatro dimensiones de la gestión de servicios: (1) organización y personas, (2) información y tecnología, (3) socios y proveedores, y (4) flujos de valor y procesos. La guía afirma que la gestión de incidentes es “un elemento fundamental de la gestión de servicios” y que la restauración rápida del servicio es clave para la satisfacción del usuario, la credibilidad del proveedor y el valor creado en la relación de servicios (Axelos, 2020). Esta afirmación sitúa a Incident Management como una práctica estructural, que articula roles, procesos, herramientas y datos bajo un mismo propósito.

Uno de los aportes más claros de Axelos (2020) sobre los elementos estructurales es la tabla de entradas, actividades y salidas del proceso de gestión de incidentes. La guía indica que el proceso se alimenta de insumos como datos de monitoreo y eventos, consultas de usuarios, información de configuración, inventario de activos de TI, catálogo de servicios, acuerdos de nivel de servicio (SLA), políticas de continuidad y de seguridad, y registros de problemas o base de conocimiento. A partir de esas entradas, se ejecutan actividades nucleares, como: detección, registro, clasificación, diagnóstico y

resolución de incidentes, que culminan en salidas como el restablecimiento del servicio, la actualización de la base de conocimiento, la revisión del incidente y la retroalimentación para la mejora continua (Axelos, 2020). La estructura del proceso se define por un flujo claro de información que entra, se transforma mediante actividades estandarizadas y genera productos concretos (servicio restaurado, datos registrados, lecciones aprendidas).

La guía también detalla elementos estructurales específicos como los modelos de incidente, los incidentes mayores y las workarounds. Un “incident model” se describe como *“un enfoque repetible para la gestión de un tipo particular de incidente”* (Axelos, 2020). Esto implica que, para incidentes recurrentes, la organización debe contar con procedimientos predefinidos, plantillas de registro, pasos de diagnóstico y criterios de escalamiento ya establecidos. En el caso de los major incidents, el documento indica que se requiere un coordinador responsable (por ejemplo, un *major incident manager*), un equipo temporal dedicado, recursos específicos (como presupuesto para expertos externos) y un modelo de comunicación acordado con usuarios, clientes, reguladores y otros grupos de interés. Todo ello configura una estructura organizativa y procedimental que distingue de manera explícita la gestión “normal” de incidentes y la gestión de situaciones críticas.

Desde un enfoque aplicado, Dzemydienė, et.al. (2024) muestran cómo estos elementos estructurales se concretan en una institución educativa. En su propuesta de gestión de incidentes TIC basada en ITIL 4, las autoras señalan que, para resolver incidentes de la infraestructura tecnológica, es necesario definir pasos específicos, asignar personas responsables y elegir tecnologías de soporte siguiendo las recomendaciones de la metodología. Su enfoque describe un algoritmo de gestión de incidentes donde se integran la detección temprana, la clasificación, la priorización y el apoyo de un subsistema de soporte a la decisión capaz de diferenciar eventos informativos de incidentes reales. En este contexto, los elementos estructurales incluyen: reglas de clasificación, baremos de prioridad, matrices para decidir la ruta de atención, mecanismos de registro y, sobre todo, una asignación clara de responsabilidades.

Dzemydienė et al. (2024) subrayan que, en una institución educativa, la continuidad de las “cadenas TIC” exige que la práctica de gestión de incidentes se apoye en una estructura estable que combine roles, procesos y tecnología.

Por eso, su modelo incorpora tanto el Service Desk como las herramientas de monitoreo y los repositorios de conocimiento, de forma que los incidentes puedan ser detectados automáticamente, escalados según su criticidad y documentados para su posterior análisis. Esta articulación es muy similar a lo que ITIL 4 plantea en la guía de práctica: incident management contribuye a varias actividades de la Service Value Chain (engage, deliver & support, design & transition, improve, obtain/build) y se interconecta con otras prácticas como monitoring and event management, service configuration management y change enablement (Axelos, 2020).

Por su parte, Ramadhan (2024) refuerza esta visión estructural en un estudio sobre análisis de riesgos utilizando el marco ITIL V.4 en un sistema de biblioteca digital. En su investigación se indica que la práctica de incident management se descompone en siete etapas dentro del modelo ITIL 4 y que, a partir de estas, se diseñó un conjunto de procedimientos operativos estándar (SOP) para abordar incidentes y problemas en la plataforma INLISLite (Ramadhan, 2024). Además, el autor emplea un diagrama RACI para definir quién es responsable, quién es el dueño de la decisión, quién debe ser consultado y quién solo informado en cada etapa de la gestión de incidentes. Esta aproximación muestra que los elementos estructurales no se limitan al flujo de actividades, sino que incluyen también la matriz de roles, la documentación formal (SOP, formularios) y los mecanismos de evaluación de capacidad y madurez de la práctica.

El propio Ramadhan (2024) destaca que, al evaluar las capacidades del sistema con el marco ITIL 4, fue posible diseñar un SOP con formularios adicionales para varias actividades del proceso, lo que permitió mejorar la gestión de incidentes y problemas del sistema de biblioteca. Esto coincide con la noción de Practice Success Factors (PSF) descrita por Axelos (2020): componentes funcionales complejos que combinan actividades y recursos de las cuatro dimensiones de servicio y que, en el caso de Incident Management, incluyen “detectar incidentes temprano”, “resolver incidentes de forma rápida y eficiente” y “mejorar continuamente los enfoques de gestión de incidentes” (traducción propia). Así, los PSF se convierten en otro elemento estructural clave: agrupan procesos, personas, información y tecnología en bloques funcionales que deben estar presentes para que la práctica cumpla su propósito.

En base a lo descrito podemos identificar que los elementos estructurales de Incident Management en ITIL 4 abarcan:

a. un conjunto de entradas (datos de monitoreo, consultas de usuarios, información de configuración, SLAs, registros de problemas, base de conocimiento),
b. un flujo definido de actividades (detección, registro, clasificación, diagnóstico, resolución, cierre, revisión),
c. salidas bien identificadas (servicio restaurado, registros actualizados, lecciones aprendidas, indicadores),
d. una estructura organizacional con roles explícitos (service desk, equipos de apoyo, coordinador de incidentes mayores, responsables definidos vía RACI),
e. artefactos formales (modelos de incidente, SOP, formularios, políticas y planes de continuidad y seguridad),
f. factores de éxito que combinan procesos, personas y tecnología para asegurar detección temprana, resolución eficaz y mejora continua.

1.2.5. La mesa de ayuda como elemento habilitador clave

La mesa de ayuda (service desk) aparece como un elemento habilitador clave de toda la gestión de servicios de TI, y muy en particular de la gestión de incidentes. En la guía oficial de ITIL 4 Foundation se define que “el propósito de la práctica de service desk es capturar la demanda de resolución de incidentes y de solicitudes de servicio” (Axelos, 2020). Dicho de otro modo, la mesa de ayuda es la puerta de entrada formal a los servicios de TI: concentra las interacciones con los usuarios, registra lo que ocurre, coordina la respuesta con otros equipos y permite que la organización controle de forma unificada cómo se atienden los problemas que afectan a sus 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”, indicando que su propósito es funcionar como un puente de comunicación entre ambas partes. El autor explica que el service desk suele registrar y gestionar todos los incidentes, solicitudes de servicio y solicitudes de acceso, y además proporciona la interfaz para los demás procesos de operación del servicio. En esa perspectiva, la mesa de ayuda no es un simple “call center técnico”, sino un servicio visible de TI, el lugar donde la mayoría de usuarios tiene su primera

experiencia de soporte y donde se define buena parte de la percepción de calidad del servicio (Mahardika, 2022). Si esta función falla, el resto del modelo de gestión de incidentes queda cojo, porque no existe un punto confiable donde concentrar la demanda, priorizarla y canalizarla.

La misma investigación de Mahardika (2022) detalla que las tareas de una mesa de ayuda incluyen recibir y registrar incidentes, clasificarlos por prioridad y categoría, realizar el escalamiento cuando corresponde, buscar soluciones y mantener informados a los usuarios sobre el avance de la atención. Además, debe coordinarse con otros procesos ITIL (como gestión de problemas, de cambios o de accesos) y reportar a la gerencia el desempeño del servicio. El autor plantea que, sin una mesa de ayuda o help desk bien estructurado, la organización puede enfrentar ineficiencias significativas, precisamente porque se pierde trazabilidad y se dispersa la comunicación con los usuarios. Todo esto muestra que la mesa de ayuda es un habilitador organizacional: convierte las buenas prácticas en actividades concretas, con responsables, flujos de información y métricas observables.

En el contexto de ITIL 4, esta función se vuelve aún más relevante. La guía de ITIL plantea que la práctica de service desk participa en todos los flujos de valor donde hay interacción entre el proveedor de servicios y los usuarios, asegurando que la comunicación sea efectiva y conveniente para ambas partes (Axelos, 2020). Al integrarse con la Service Value Chain, la mesa de ayuda contribuye directamente a actividades como engage y deliver & support, y se relaciona de forma estrecha con la práctica de incident management, porque es el mecanismo estándar para registrar los incidentes, darles seguimiento y verificar su cierre. En un modelo de gestión de incidentes para una universidad, esto significa que la mesa de ayuda será el nodo central por donde pasan las incidencias de aulas virtuales, matrículas, bibliotecas digitales y sistemas administrativos, permitiendo aplicar criterios consistentes de clasificación, priorización y escalamiento.

Dzemydienė, Turskienė y Šileikienė (2024) ilustran esta idea en el ámbito educativo. Al analizar la gestión de incidentes TIC en instituciones de enseñanza, muestran que la infraestructura tecnológica se ha vuelto tan compleja que “requiere un Service Desk centralizado y software que la gestione de forma eficiente y responda con rapidez a los incidentes” (p. 293). En su propuesta, la mesa de ayuda se concibe como el centro que integra información

proveniente de sistemas de gestión de aprendizaje (LMS), directorios, gestores documentales y otros servicios; a partir de esa información, coordina la respuesta a los incidentes y soporta la toma de decisiones. Sin ese punto centralizado, señalan las autoras, resulta difícil garantizar la continuidad de las "cadenas TIC" que sostienen los procesos académicos y administrativos.

Además, Dzemydienė et al. (2024) desarrollan un algoritmo de gestión de incidentes donde la mesa de ayuda actúa como punto neurálgico: recibe los eventos, ayuda a distinguir entre información rutinaria e incidentes reales, aplica reglas de clasificación y priorización, y canaliza cada caso hacia el equipo técnico pertinente. Este enfoque confirma que la mesa de ayuda es un habilitador técnico y de proceso: sin ella, el modelo de incident management quedaría fragmentado, con equipos atendiendo problemas de forma aislada, sin una vista global del estado de los servicios ni datos confiables para mejora continua.

1.2.6. Clasificación y priorización de incidentes

En ITIL 4, la clasificación y priorización de incidentes se entiende como un componente estructural de la práctica de Incident Management. En la ITIL 4 Incident Management Practice Guide, Axelos (2020) explica que, antes de priorizar, se debe evaluar el impacto y la urgencia del incidente, pero sustenta que "evaluar el impacto y la urgencia de un incidente [...] no es priorización; sin embargo, esta evaluación es útil para la priorización". Es decir, la clasificación (por tipo de servicio, categoría, subcategoría) y la evaluación de impacto y urgencia generan la información que después permite decidir el orden de atención cuando los recursos son limitados. La misma guía introduce la idea de que los incidentes deben gestionarse dentro de un backlog compartido y que la prioridad de cada uno se establece en función de su efecto en el negocio, los tiempos objetivo de resolución (definidos en los SLA) y la disponibilidad de recursos del equipo (Axelos, 2020).

Dzemydienė, et.al. (2024) plantean que en el contexto de instituciones educativas con infraestructuras TIC complejas se debe tener como objetivo "crear un algoritmo de gestión y resolución de incidentes que permita una gestión eficaz de incidentes de acuerdo con las prioridades establecidas" (p. 51). Las autoras proponen un método de priorización integrado en la toma de decisiones, donde los incidentes se clasifican primero por tipo de servicio e infraestructura

afectada (servidores, red, módulos de software, etc.) y luego se priorizan considerando la criticidad de la cadena de servicios involucrada y el nivel de interrupción para usuarios clave como docentes y estudiantes. En su modelo, la priorización no se limita a una matriz estática, sino que se apoya en reglas que diferencian entre eventos informativos, incidentes menores y fallas graves; esas reglas se implementan dentro de una herramienta de gestión (Spiceworks) que automatiza el registro, la clasificación y parte de la decisión sobre a qué grupo técnico se deriva cada caso.

Por otro lado, la literatura reciente explora cómo la clasificación y priorización pueden automatizarse para reducir errores humanos y acelerar la respuesta. Zahrothul Ain y Safitri (2023), señalan que uno de los problemas clásicos del manejo manual es que se generan tickets mal categorizados y con prioridades asignadas de forma inconsistente, lo que alarga los tiempos de resolución. Su propuesta busca “acelerar el proceso de toma de decisiones en la gestión de incidentes [...] implementando machine learning para determinar la categoría, el grupo y la prioridad”. Al combinar algoritmos supervisados y no supervisados, las autoras muestran que es posible predecir automáticamente el nivel de prioridad de un incidente a partir de la descripción textual y de algunos metadatos, ayudando al equipo de operaciones a saber con claridad “qué incidente debe resolverse primero” y alineando la priorización con las buenas prácticas de ITIL (Zahrothul Ain & Safitri, 2023).

1.2.7. Escalamiento funcional y jerárquico

El escalamiento se entiende como el mecanismo formal para “sacar” un incidente del ámbito del equipo que ya no puede resolverlo a tiempo o con los recursos disponibles, garantizando que se mantengan los niveles de servicio acordados. La guía de práctica de Gestión de Incidentes de ITIL 4 subraya que el propósito central de la práctica es “minimizar el impacto negativo de los incidentes restaurando la operación normal del servicio lo antes posible”, y para ello exige procesos claros de asignación, re-asignación y coordinación entre distintos niveles de soporte y de gestión (Axelos, 2020). En la práctica, esa restauración rápida rara vez se logra sin algún tipo de escalamiento estructurado.

El escalamiento funcional es el tipo más visible en los entornos de TI. Implica reasignar el incidente a otro grupo o nivel de soporte con competencias técnicas más adecuadas (por ejemplo, pasar de un Service Desk de primer nivel a un

segundo o tercer nivel especializado). El trabajo de Sembina et al. (2022) ilustra muy bien este enfoque: las autoras proponen un modelo de gestión de incidentes de tres niveles, basado explícitamente en las buenas prácticas de ITIL, donde los incidentes simples se resuelven en el primer nivel, los técnicamente complejos pasan al segundo y los que afectan a toda la infraestructura se tratan en un tercer nivel experto. Mediante modelado BPMN (AS-IS/TO-BE) y simulaciones en MATLAB, muestran que incorporar un esquema claro de escalamiento funcional mejora la proporción de incidentes resueltos dentro del SLA del ~77 % al 85 %, superando el umbral del 80 % que la propia biblioteca ITIL considera indicador de un proceso eficaz.

El escalamiento jerárquico, por su parte, no busca tanto "más pericia técnica" como "más capacidad de decisión". Se activa cuando el incidente amenaza con incumplir SLA críticos, impacta a procesos de negocio sensibles o requiere autorizaciones extraordinarias (por ejemplo, parar un sistema clave, comunicar a usuarios externos, activar planes de continuidad). Kanellopoulos (2024) muestra cómo los planes de respuesta a incidentes en la industria naviera definen con precisión los roles, los "protocolos de escalamiento jerárquico" y los canales de comunicación con la alta dirección como condición para lograr una detección, clasificación y remediación rápidas de los ciberincidentes. El autor enfatiza que, sin esa cadena de escalamiento hacia niveles superiores de mando, la organización se vuelve lenta para tomar decisiones estratégicas (por ejemplo, detener operaciones o notificar a autoridades), lo que aumenta la exposición al riesgo y prolonga la recuperación.

ITIL 4 integra ambos tipos de escalamiento dentro de la práctica de gestión de incidentes como parte de un diseño más amplio de "value streams" y flujos de trabajo. La guía de práctica insiste en que los incidentes deben recibir "una gestión y una asignación de recursos apropiadas según su tipo", lo que se traduce en rutas predefinidas de escalamiento funcional (entre líneas o grupos de soporte) y jerárquico (hacia la cadena de mando) para incidentes mayores o de alto impacto (Axelos, 2020). En este sentido, el trabajo de Sembina et al. (2022) puede leerse como una validación empírica de la lógica ITIL: al rediseñar la arquitectura de soporte y explicitar cuándo y cómo se escalan los incidentes, logran reducir tiempos de resolución y las pérdidas por indisponibilidad de sistemas, sin recurrir a costosas herramientas de automatización.

De forma complementaria, los estudios sobre ciberseguridad y respuesta a incidentes en infraestructuras críticas refuerzan la idea de que el escalamiento jerárquico no es un mero formalismo, sino un componente estructural de la resiliencia organizacional. Kanellopoulos (2024) argumenta que los planes de respuesta eficaces combinan tres elementos: asignación clara de roles, protocolos de escalamiento jerárquico y ejercicios periódicos de simulación, lo que permite a la organización reaccionar con rapidez y coherencia ante incidentes complejos. Esta misma lógica puede trasladarse a la operación de servicios de TI: el escalamiento funcional asegura que "el problema llegue a quien sabe resolverlo" y el escalamiento jerárquico garantiza que "la organización tome las decisiones difíciles a tiempo".

1.2.8. Métricas e indicadores

Las métricas y los indicadores aparecen como el "lenguaje" con el que se observa y gobierna el desempeño de los procesos, en especial cuando se trata de incidentes. Cadena et.al. (2020) desarrollan un mapeo sistemático sobre métricas e indicadores para la gestión de incidentes de seguridad de la información y muestran que, ante el aumento de amenazas y vulnerabilidades, "la identificación y uso de métricas e indicadores es un factor crucial" para gestionar estos incidentes y salvaguardar el capital intelectual de las organizaciones. En su estudio, clasifican indicadores relacionados con coste, calidad y servicio (tiempo) y los vinculan con estándares como ISO 27004 y NIST 800-55, lo que refuerza la idea de que medir no es solo cuestión de contar tickets, sino de evidenciar cuán eficaz y eficiente es el proceso de respuesta y resolución de incidentes en su conjunto.

En ese mismo trabajo, los autores recuerdan una frase muy repetida en el ámbito de la gestión de servicios: "What is not defined cannot be measured. What is not measured cannot be improved" que en castellano se traduce como "Lo que no está definido no puede medirse. Lo que no se mide no puede mejorarse". Trasladado a ITIL 4 e Incident Management, esto implica que, si la organización no define con claridad qué entiende por tiempos de respuesta, niveles de servicio, impacto o esfuerzo de recuperación, difícilmente podrá mejorar la estabilidad de los servicios de TI o justificar inversiones en capacidad, automatización o capacitación del personal. El aporte del estudio de Cadena et al. (2020) es la tipificación de métricas como: detección, respuesta, coste, resiliencia, y ofrece un conjunto de indicadores que pueden ser utilizados en

cuadros de mando para la gestión de incidentes en contextos como el universitario.

El trabajo de Najjarpour et.al. (2025) ofrece un ejemplo muy cercano a lo que se necesita en una universidad: diseñan un panel operacional para la unidad de TI de hospitales docentes, cuyo núcleo es un conjunto estandarizado de 124 indicadores clave de desempeño distribuidos en dominios como hardware, software, redes, sistema de información hospitalaria e informes. A lo largo del artículo, los autores explican que las métricas de desempeño de la unidad TI se definen a partir de “estándares globales como ITIL y COBIT 5”, y subrayan que el panel permite monitorizar en tiempo real la operación, generar reportes analíticos y soportar decisiones tácticas y estratégicas. Aunque el estudio se sitúa en el sector salud, muestra de forma muy concreta cómo traducir marcos de referencia como ITIL en indicadores cuantitativos que cubren desde tareas administrativas hasta incidentes de seguridad de red y disponibilidad de servicios críticos. Para una universidad, el mensaje de fondo es claro: un modelo de gestión de incidentes sin un sistema de métricas bien estructurado tiende a quedarse en buenas intenciones, mientras que un conjunto de KPIs alineado con ITIL 4 permite observar el comportamiento del proceso, comparar contra objetivos y justificar mejoras continuas.

1.3. Operacionalización de las variables de la investigación

1.3.1. Definición conceptual de las variables

Variable 1: Gestión actual de incidentes de TI en la UNPRG

Es el conjunto de prácticas, procedimientos, recursos y roles que la Universidad Nacional Pedro Ruiz Gallo utiliza actualmente para registrar, atender y resolver incidentes vinculados a los servicios de TI. Incluye la forma real en que se detectan los incidentes, quién los atiende, cómo se asignan prioridades y qué tan oportuno es el restablecimiento del servicio.

Variable 2: Modelo propuesto de gestión de incidentes basado en ITIL 4

Es el diseño estructurado de un sistema de gestión de incidentes alineado con las prácticas de ITIL 4, que incluye elementos funcionales (flujo de incidentes, clasificación, priorización, escalamiento, cierre), elementos estructurales (mesa

de ayuda, roles, herramientas, métricas) y lineamientos de operación que permitan mejorar la gestión de los servicios tecnológicos de la universidad.

1.3.2. Definición operativa de las variables

Variable 1: Gestión actual de incidentes de TI en la UNPRG

Se evalúa mediante la identificación narrativa de brechas, problemas y debilidades en los procesos actuales de gestión de incidentes, analizando documentos institucionales, entrevistas a personal clave y comparación con buenas prácticas de ITIL 4.

Variable 2: Modelo propuesto de gestión de incidentes basado en ITIL 4

Opera a través del diseño del modelo estructurado, la definición de sus componentes y la validación por juicio de expertos en términos de claridad, suficiencia, coherencia y relevancia.

Tabla 1. Operacionalización de las variables de la investigación

Variable	Dimensión	Indicadores	Escala de medición	Técnica de recopilación de información
Gestión actual de incidentes de TI en la UNPRG	Procedimientos existentes	Existencia de lineamientos documentados para gestión de incidentes	Nominal (sí/no)	Revisión documental
		Nivel de formalización del proceso (flujo, pasos, responsables)	Ordinal (bajo – medio – alto)	Revisión documental / Entrevista
	Roles y responsabilidades	Claridad en la asignación de roles	Ordinal	Entrevista a responsables
		Existencia de niveles de soporte	Nominal	Revisión documental
	Registro y seguimiento de incidentes	Mecanismos actuales de registro (manual, digital, informal)	Nominal	Revisión documental / Entrevista
		Trazabilidad de los incidentes (si existe historial, seguimiento)	Ordinal	Revisión documental
	Clasificación y priorización	Criterios formales de priorización	Nominal	Revisión documental
		Consistencia en la clasificación	Cualitativa categórica	Entrevista / Análisis narrativo
	Escalamiento funcional y jerárquico	Existencia de rutas de escalamiento	Nominal	Revisión documental
		Tiempo estimado para escalar incidentes importantes	Ordinal (rápido – medio – lento)	Entrevista
	Percepción del servicio	Satisfacción general de usuarios internos (personal TI) sobre el proceso actual	Categórica	Entrevista cualitativa
	Brechas con respecto a ITIL 4	Número de prácticas ITIL 4 ausentes o débiles	Escala ordinal	Análisis comparativo
Modelo propuesto de gestión de incidentes basado en ITIL 4	Elementos funcionales del modelo	Coherencia del flujo de atención de incidentes con ITIL 4	Ordinal (bajo – medio – alto)	Juicio de expertos
		Claridad de fases: registro, clasificación, priorización, escalamiento, resolución y cierre	Ordinal	Juicio de expertos
	Mesa de ayuda (Service Desk)	Nivel de articulación de la mesa con incident management	Ordinal	Juicio de expertos
		Definición de roles y responsabilidades de la mesa	Categórica	Juicio de expertos
	Clasificación y	Adecuación de la matriz de impacto/urgencia	Ordinal	Juicio de expertos

	priorización	Claridad de categorías de incidentes	Categórica	Juicio de expertos
	Escalamiento funcional y jerárquico	Claridad del flujo y criterios de escalamiento	Ordinal	Juicio de expertos
		Definición de niveles de soporte	Nominal	Revisión del modelo
	Métricas e indicadores del modelo	Tiempo Promedio de Reparación (Mean Time to Repair – MTTR), Resolución en el primer contacto (First Contact Resolution), re-apertura.	Ordinal	Juicio de expertos
		Coherencia entre métricas y objetivos del modelo	Ordinal	Juicio de expertos
	Relevancia, coherencia y suficiencia del modelo	Valoración global del modelo	Ordinal (insuficiente – suficiente – adecuada – muy adecuada)	Juicio de expertos
	Viabilidad y aplicabilidad	Percepción de aplicabilidad para la UNPRG	Categórica	Juicio de expertos

DISEÑO METODOLÓGICO

2.1. Enfoque y tipo de investigación

La presente investigación se desarrolló bajo un **enfoque cualitativo**, pues buscó comprender y describir la situación actual de la gestión de incidentes de TI en la Universidad Nacional Pedro Ruiz Gallo desde la perspectiva de los actores involucrados, así como analizar los documentos institucionales y compararlos con las prácticas propuestas por ITIL 4. Debido a que no se pretendió manipular variables ni ejecutar pruebas experimentales, el estudio adoptó un **diseño descriptivo–propositivo**, orientado a caracterizar el proceso existente y formular un modelo basado en referentes teóricos.

2.2. Método de la investigación

El método de investigación aplicado fue el **método analítico–documental**, complementado con el análisis comparativo. Este método permitió examinar el estado actual del proceso, identificar brechas y contrastarlas con las buenas prácticas definidas por ITIL 4 Incident Management. Asimismo, se empleó el método **experticio**, puesto que la validación del modelo propuesto se realizó mediante el juicio de expertos.

2.3. Población y muestra

La **población** estuvo constituida por el personal vinculado a los servicios de TI de la Oficina de Tecnologías de la Información de la Universidad Nacional Pedro Ruiz Gallo, tanto administrativos como técnicos. Sin embargo, dado el carácter cualitativo y propositivo de la investigación, se seleccionó una **muestra no probabilística por criterio**, integrada por personal clave relacionado directamente con la atención de incidentes de TI. Esta selección se justificó porque dichas personas poseían conocimiento específico sobre la operación del proceso y podían describir con precisión las prácticas actualmente empleadas.

Asimismo, la muestra incluyó a **especialistas externos**, quienes participaron como jueces para validar el modelo propuesto. La técnica de muestreo utilizada para su elección fue el **muestreo intencional**, seleccionando profesionales con

experiencia demostrada en ITIL 4, gestión de servicios de TI y gestión de la seguridad de la información.

2.4. Técnicas e instrumentos de recolección de información

Las técnicas aplicadas permitieron obtener datos cualitativos y documentales adecuados a la naturaleza descriptiva de la investigación. Todas ellas se utilizaron de manera complementaria para desarrollar el diagnóstico, el análisis situacional y la fundamentación del modelo propuesto.

2.4.1. Entrevista semiestructurada

Se empleó la entrevista semiestructurada como técnica principal para recopilar información sobre la forma en que se gestionaban los incidentes de TI en la universidad. Esta técnica permitió explorar de manera flexible las percepciones del personal de TI respecto al registro de incidentes, los criterios de clasificación y priorización, los niveles de soporte utilizados, los mecanismos de escalamiento y las dificultades que enfrentaban durante la resolución de incidencias.

El **instrumento** consistió en una guía compuesta por preguntas abiertas (Ver Anexo 1), organizadas alrededor de los componentes esenciales del proceso de gestión de incidentes. Las entrevistas se dirigieron a personal técnico y administrativo involucrado directamente en el soporte de TI, lo que permitió obtener información detallada sobre las prácticas reales y contrastarlas con los lineamientos de ITIL 4 en la UNPRG.

2.4.2. Revisión documental

A fin de evaluar el nivel de formalización del proceso existente, se aplicó una revisión documental en detalle. Esta técnica permitió examinar procedimientos institucionales, manuales de organización y funciones, lineamientos relacionados con los servicios tecnológicos, registros de incidentes, reportes, evidencias de soporte, catálogos de servicios y documentación de herramientas informáticas.

La guía de revisión documental diseñada (Ver Anexo 2) estuvo orientada a determinar si la universidad contaba con políticas y procedimientos formalizados para la gestión de incidentes, si existían roles claramente establecidos, si se

realizaba trazabilidad de los casos, si se manejaban criterios formales de priorización y si las herramientas tecnológicas permitían registrar y supervisar incidentes adecuadamente. Este análisis posibilitó identificar vacíos normativos y operativos que justificaron el desarrollo del modelo propuesto.

2.4.3. Matriz comparativa ITIL 4 vs situación actual

Se elaboró una matriz comparativa entre los elementos esenciales de ITIL 4 Incident Management y la situación real observada en la UNPRG (Ver Anexo 3). Esta matriz permitió evidenciar brechas relacionadas con el registro y categorización de incidentes, ausencia de criterios de priorización, insuficiencia de rutas de escalamiento, carencias en la estructura de mesa de ayuda, débil documentación de soluciones y falta de métricas para evaluar el proceso.

El uso de esta matriz constituyó un paso clave para estructurar la propuesta, ya que organizó de modo sistemático los aspectos que debían fortalecerse para alcanzar un modelo de gestión alineado con ITIL 4.

RESULTADOS DE LA INVESTIGACIÓN

3.1. Análisis diagnóstico de la gestión de incidentes actual

3.1.1. Revisión documental de normas, procesos, riesgos e infraestructura

La revisión de documentos relacionados a la gestión de incidentes de TI en la UNPRG, encontramos que el *Plan de Gobierno Digital 2024–2026* evidenció que la universidad enfrenta una demanda creciente de servicios digitales, acompañada de incidentes frecuentes vinculados a disponibilidad, seguridad y continuidad operativa. El documento muestra que la Oficina de Tecnologías de la Información (OTI) es responsable de mantener los sistemas institucionales, coordinar la seguridad de la información y proveer soporte a todas las unidades académicas y administrativas. Además, se indica que el nivel de madurez digital institucional era aún limitado, lo cual afectaba directamente la capacidad de gestionar incidentes de manera ordenada y predecible.

Por su parte, la *Resolución que aprueba el Mapa de Procesos UNPRG (2022)* permitió identificar que el proceso Gestión de Tecnologías de Información y Comunicación (P.S.2) constituye un proceso transversal esencial en el funcionamiento institucional, recibiendo como insumos incidentes tecnológicos provenientes de todas las áreas de la universidad.

De los informes anuales sobre seguridad de la información, se detectó la existencia de un conjunto significativo de amenazas y vulnerabilidades. Entre ellas, se identificaron fallas en la disponibilidad del Sistema de Información Académica (SIA), interrupciones de red por configuraciones incorrectas del firewall, uso de software desactualizado, fallas en conectividad, debilidades en sistemas de respaldo y riesgos derivados de contraseñas mal gestionadas. Estos riesgos demuestran que la gestión de incidentes está fuertemente ligada a la estabilidad de la infraestructura.

Asimismo, del análisis de la documentación sobre la infraestructura tecnológica de la UNPRG, se pudo reconstruir el diseño general de la Red Telemática institucional. Esta red cuenta con un *backbone* de fibra óptica, switches de núcleo y de borde, servidores destinados a bases de datos, dominio, web, correo, firewall,

IDS, sistemas de protección eléctrica y sala de servidores. Esta infraestructura, aunque diseñada originalmente para ser robusta, presentaba ya signos de obsolescencia y carencias de mantenimiento, especialmente en lo referente a climatización y continuidad eléctrica, elementos críticos para la continuidad académica y administrativa.

Tabla 2. Hallazgos de la revisión documental en relación a la gestión de incidentes de TI

Categoría de documento	**Aspectos a revisar**	**Hallazgos esperados (basados en documentos revisados)**
Procedimientos de TI	Procedimiento formal de gestión de incidentes Fases, roles y flujos	- En los documentos institucionales no aparece ningún procedimiento formal para gestionar incidentes. - No se describen fases, roles, flujo de atención, mecanismos de escalamiento o cierre. - La atención actual es reactiva y depende del criterio individual del técnico. - Existe una brecha total de formalización del proceso de gestión de incidentes de TI.
Manual de Organización y Funciones (MOF) / Plan de Gobierno Digital (PGD)	Roles relacionados con TI, soporte, servicio al usuario	- Se identifican funciones generales de planificación, soporte, administración de sistemas y seguridad, adscrita a la OTI (Plan de Gobierno Digital PDG 2024–2026). - Sin embargo, los roles no están asociados a actividades específicas de gestión de incidentes. - No existe diferenciación entre niveles de soporte (1, 2 o 3). - No se asignan responsabilidades claras para registro, clasificación o priorización de incidentes.
Reglamentos o lineamientos de sistemas	Criterios para atención de incidentes Tiempos, categorías, prioridades	- No existen lineamientos específicos para atención de incidentes. - No se identifican criterios de impacto/urgencia, ni categorías de incidentes. - No se mencionan tiempos de respuesta ni protocolos de escalamiento. - Los documentos solo describen objetivos generales de seguridad digital, pero no los traducen en lineamientos operativos ITIL.
Reportes de incidentes o evidencias operativas	Tipo de incidentes Frecuencia Tiempos de atención	- Los documentos revisados no incluyen un repositorio o registro formal de incidentes. - Solo se observan incidentes de manera indirecta como fallas del SIA, problemas de firewall, caídas de red, fallas de energía y vulnerabilidades de seguridad. - No existe trazabilidad, tiempos de respuesta ni evidencia de cierres formales.
Herramientas TI (documentación técnica, Red Telemática)	Uso de software de tickets Monitoreo Base de conocimiento	- No se menciona ninguna herramienta ITSM ni sistema de tickets. - El monitoreo de red y servidores es limitado y depende de funciones básicas de firewall/router. - No existe base de conocimiento. - Se evidencia infraestructura (switches, servidores, firewall, UPS), pero sin herramientas de soporte asociadas a la gestión de incidentes.

3.1.2. Descripción de la gestión de incidentes a partir de las entrevistas con responsables de la OTI

Se realizaron dos entrevistas tomando como base el cuestionario del Anexo 1. La primera al responsable de la red la gestión de la infraestructura tecnológica de la UNPRG (backbone, firewall, red inalámbrica, sala de servidores) y la segunda, a la responsable de la gestión y puesta en producción de las aplicaciones académicas administrativas (SIA, Aula Virtual, Turnitin, Selgestiun) y administrativas (SIAF, tesorería, contabilidad y planillas).

Con relación a la primera entrevista relacionada a la gestión de incidentes desde la perspectiva de la gestión de la infraestructura tecnológica, se obtuvieron las siguientes observaciones:

1. Incidentes más frecuentes en los servicios de TI

   El responsable explicó que los incidentes más frecuentes estaban relacionados con la disponibilidad de la red y con fallas en los equipos del backbone. Mencionó que, por ejemplo, la pérdida de conectividad en ciertas facultades era común debido a segmentos de fibra que ya habían superado su vida útil y a switches que operaban por encima de su capacidad recomendada. A eso se sumaban incidentes generados por configuraciones heredadas del firewall, las cuales producían bloqueos inesperados o aperturas excesivas que comprometían tanto la seguridad como la continuidad del servicio. Señaló también que existían problemas serios por variaciones de voltaje, que, aunque eran mitigadas parcialmente por UPS antiguos, seguían afectando los servidores y equipos críticos instalados en la sala de máquinas.

2. Procedimiento formal para registrar y atender incidentes

   Comentó que no existe un procedimiento formal documentado ni aprobado por la universidad. En la práctica, cada técnico de red atendía los incidentes según experiencia personal. Algunos mantenían cuadernos o archivos propios donde anotaban lo que ocurría, pero no existía un registro unificado ni un flujo de atención oficial. Gran parte de los incidentes llegaba mediante llamadas telefónicas, mensajes de WhatsApp o visitas directas a la oficina, sin que quedara trazabilidad de lo reportado. Esto generaba, según su apreciación, una

gestión reactiva y fragmentada, sin oportunidades claras para analizar tendencias.

3. Asignación de los incidentes a los responsables de su atención

   Explicó que la asignación dependía de quién recibiera el aviso. Si la llamada la atendía un técnico de redes, este mismo asumía el caso, aun cuando fuera un tema relacionado con servidores o seguridad. En ocasiones, el responsable derivaba el incidente a otro especialista, pero de manera informal, sin un canal establecido. También mencionó que, al no existir un punto único de contacto, muchos usuarios llamaban directamente a la persona que recordaban que les ayudó la última vez, lo que creaba una distribución desigual de la carga de trabajo y, en algunos casos, retrasos innecesarios.

4. Criterios utilizados para la clasificación y priorización de incidentes de TI

   Indicó que no existían criterios formales, aunque de manera intuitiva se priorizaban los incidentes que afectaban servicios académicos críticos como matrícula o acceso al SIA. Sin embargo, reconocía que esta priorización dependía de la percepción del técnico y no de un marco definido. A veces un problema menor recibía más atención que uno mayor simplemente porque el usuario afectado insistía más o porque el incidente causaba molestias visibles, aunque no tuviera un impacto real en los procesos.

5. Existencia de una mesa de ayuda o punto único de contacto con los usuarios

   Fue directo en señalar que la universidad no cuenta con una mesa de ayuda oficial, ni física ni digital. Lo más cercano era un correo electrónico institucional al que pocos usuarios escribían. La mayoría recurría al contacto personal: llamadas, mensajes o incluso visitas a la OTI. Explicó que eso se traducía en una gestión dispersa y difícil de controlar, ya que un incidente podía quedar sin atención si el técnico receptor olvidaba anotarlo o si no estaba presente el día que el evento ocurría.

6. Niveles de soporte definidos

   Expresó que tampoco existían niveles formales de soporte. Reconoció que existía una “dinámica natural” en la que los técnicos con más experiencia

resolvían los incidentes más complejos, pero esto se daba por costumbre, no por diseño. No había un nivel 1, nivel 2 o nivel 3 como en modelos ITIL; tampoco existía un responsable designado para incidentes mayores.

7. Manejo del escalamiento funcional y/o jerárquico

   Describió que el escalamiento funcional ocurría solo cuando el técnico que recibía el incidente sabía que no podía resolverlo. Entonces “buscaba al compañero que manejara ese tema”. En cuanto al escalamiento jerárquico, dijo que este casi no existía salvo cuando el incidente afectaba un servicio crítico y algún decano o director presionaba a la alta dirección. En esas situaciones, la autoridad universitaria exigía atención inmediata, pero sin un protocolo claro.

8. Herramientas que se usan para registrar, monitorear o resolver incidentes

   Mencionó que no existía un software especializado. El monitoreo de tráfico y disponibilidad se realizaba mediante herramientas básicas del firewall y del router, pero no había paneles consolidados ni alertas automáticas. Los registros de incidentes estaban dispersos en hojas de cálculo personales, correos electrónicos y mensajes instantáneos.

9. Dificultades o limitaciones que identifica en el proceso actual

   Enumeró varias limitaciones: la ausencia de una mesa de ayuda, la falta de registro unificado, infraestructura obsoleta, equipos que operaban en ambientes sin climatización adecuada, fallas eléctricas frecuentas y la inexistencia de políticas operativas. También remarcó que la universidad había sufrido intentos de intrusión por parte de actores maliciosos, lo cual demostraba la necesidad de controles más rigurosos y una gestión de incidentes estructurada.

10. Consideraciones para mejorar la gestión de incidentes en la UNPRG

    Consideraba fundamental implementar un sistema de registro de incidentes, establecer una mesa de ayuda, definir niveles de soporte y flujos de escalamiento, actualizar la infraestructura crítica y mejorar la climatización y respaldo energético. Reconoció que sin estas mejoras, cualquier intento por implementar ITIL quedaría incompleto.

En relación a la segunda entrevista relacionada a la gestión de incidentes desde la perspectiva de la gestión de las aplicaciones, se obtuvieron las siguientes observaciones:

1. Tipos de incidentes más frecuentes en los servicios de TI

   Explicó que los incidentes más recurrentes eran las caídas del SIA durante periodos de alta demanda, especialmente matrícula y cierre de notas. También mencionó problemas de acceso y lentitud en el Aula Virtual, fallas en la integración de Turnitin, y errores en el registro de tesis en Selgestiun debido a bases de datos inconsistentes. Se sumaban incidentes provocados por credenciales incorrectas, cargas masivas de estudiantes o interrupciones en la red que impedían que los servicios funcionaran adecuadamente.

2. Procedimiento formal para registrar y atender incidentes

   Indicó que no existía tal procedimiento. Los usuarios reportaban problemas “al técnico que conocían” por teléfono o mensajería instantánea. En algunos casos se registraban correos electrónicos, pero no existía un repositorio unificado ni trazabilidad. Subrayó que esto afectaba especialmente al SIA, ya que muchos incidentes no quedaban registrados y, por lo tanto, no se analizaban de forma retrospectiva.

3. Asignación de los incidentes a los responsables de su atención

   Señaló que la asignación dependía de quién estuviera disponible. Si el asunto era del SIA, por ejemplo, usualmente lo atendía ella; si era un problema de la base de datos o un módulo especializado, se derivaba al técnico que lo había desarrollado o mantenido. No había un sistema que asignara automáticamente casos ni mecanismos formales para distribuir el trabajo.

4. Criterios utilizados para la clasificación y priorización de incidentes de TI

   Reconoció que no existían criterios formales, pero que en la práctica se priorizaban los incidentes que afectaban procesos institucionales como matrícula o emisión de actas. A veces se basaban en la urgencia expresada por el usuario, lo que generaba inequidades: incidentes críticos pasaban

desapercibidos mientras que problemas menores recibían atención inmediata por presión externa.

5. Existencia de una mesa de ayuda o punto único de contacto con los usuarios
   Afirmó que no existe mesa de ayuda. Los usuarios se comunicaban con la OTI por distintos canales y cada uno atendía “por su lado”. Consideraba que esta dispersión generaba duplicidad de esfuerzos y pérdida de información.

6. Niveles de soporte definidos
   Explicó que tampoco se contaba con niveles de soporte formalizados. Ella misma terminaba atendiendo incidentes que en un modelo ideal serían de tercer nivel, mientras que incidentes simples seguían ocupando tiempo que podría delegarse a un primer nivel inexistente.

7. Manejo del escalamiento funcional y/o jerárquico
   El escalamiento, según explicó, era totalmente informal. Si el incidente superaba su capacidad, buscaba a otro técnico; si el incidente afectaba un proceso crítico, informaba directamente al jefe de la OTI. No existían criterios ni tiempos definidos para determinar cuándo escalar un caso.

8. Herramientas que se usan para registrar, monitorear o resolver incidentes
   Mencionó que el SIA tenía logs básicos, pero no estaban diseñados para la gestión de incidentes. El Aula Virtual tenía informes de fallos, pero no se analizaban de manera sistemática. Turnitin y Selgestiun dependían de plataformas externas o de registros mínimos. No existía un sistema ITSM, lo cual dificultaba el análisis de tendencias y la mejora continua.

9. Dificultades o limitaciones que identifica en el proceso actual
   Explicó que la principal limitación era la fragmentación del soporte: cada sistema tenía su propio “modo de atención” informal. A esto se sumaban la falta de documentación, la ausencia de un equipo exclusivamente dedicado al desarrollo y mantenimiento del SIA, deficiencias en la infraestructura de red y fallas recurrentes de energía que afectaban la disponibilidad de los servicios.

10. Consideraciones para mejorar la gestión de incidentes en la UNPRG

Indicó que era indispensable contar con una mesa de ayuda, un sistema de registro centralizado, roles definidos, una matriz de clasificación y priorización y un sistema de escalamiento claro. También consideraba urgente reforzar la infraestructura, especialmente los servidores que alojan el SIA y los sistemas del Aula Virtual, y mejorar la seguridad para evitar ataques a bases de datos académicas.

El análisis cruzado permitió identificar coincidencias, divergencias y patrones que caracterizan la gestión actual de incidentes de TI en la UNPRG, a partir de las percepciones del responsable de la red telemática y la responsable de aplicaciones.

a. Coincidencias entre ambas entrevistas

Ambos coinciden en que la universidad opera bajo un modelo reactivo, sin un procedimiento formal para registrar, clasificar o tratar los incidentes. La ausencia de una mesa de ayuda es señalada como la raíz de múltiples problemas: dispersión de canales, dependencia de contactos personales, pérdida de información y duplicidad de esfuerzos. Esta falta de un punto único de contacto afecta tanto a incidentes de infraestructura como a incidentes en aplicaciones críticas como el SIA o el Aula Virtual.

En cuanto a la asignación de incidentes, los dos responsables describen un sistema totalmente informal, basado en disponibilidad inmediata del técnico. Se confirma que no existen niveles de soporte, ni roles definidos, ni flujos de escalamiento. Ambos consideran que la asignación de incidentes recae en quien “sabe más del tema”, lo cual demuestra un modelo centrado en personas, no en procesos.

Otro punto coincidente es la frecuencia de incidentes críticos, especialmente caídas del SIA y fallas de red. Ambos reconocen que parte del problema deriva de la infraestructura obsoleta, carencias de climatización y fallas eléctricas. La responsable de aplicaciones enfatiza la sobrecarga del SIA en

temporada de matrícula, mientras que el responsable de red destaca problemas del firewall y del cableado estructurado.

Los dos entrevistados manifiestan preocupación por los intentos de intrusión y el riesgo que representan para las bases de datos académicas. Esta coincidencia revela una debilidad estructural en la seguridad informática, vinculada a contraseñas débiles, falta de monitoreo y ausencia de un SGSI.

b. Diferencias observadas entre ambas entrevistas

- El responsable de red atribuye los incidentes principalmente a fallas de infraestructura, mientras que la responsable de aplicaciones pone énfasis en las limitaciones del software, cargas de usuarios, inconsistencias en bases de datos y problemas de integración.

- Para el responsable de red, el mayor riesgo es la caída de conectividad; para la responsable de aplicaciones, la caída del SIA es el problema más crítico, por su impacto directo en los procesos académicos.

- La responsable de aplicaciones percibe mayor presión institucional debido a los incidentes, ya que los usuarios finales la contactan de manera directa y constante; el responsable de red experimenta mayor carga técnica que administrativa.

- Estas diferencias complementan la visión del problema: la infraestructura y las aplicaciones fallan simultáneamente porque no existe un sistema formal que articule ambos mundos.

c. Patrones comunes

Del cruce de ambas entrevistas emergen tres patrones transversales:

- Fragmentación total del proceso de atención de incidentes. No hay integración de la gestión de incidentes entre redes, servidores, seguridad y aplicaciones.
- Gestión dependiente del conocimiento individual. Lo que cada técnico sabe determina la rapidez y eficacia de la atención.

- Ausencia de registros y métricas. Todos los incidentes se pierden en conversaciones informales, haciendo imposible analizar tendencias o planificar mejoras.

3.2. Identificación de los problemas y debilidades en los procesos académicos y administrativos que brindan servicios relacionado con la gestión de incidentes

Los procesos académicos y administrativos de la UNPRG dependen fuertemente de los servicios de tecnologías de la información, como:

a. SIA, Aula Virtual, Servicio de registro de tesis y proyectos de investigación (Selgestiun), Servicio de verificación de duplicidad de documentos académicos y de investigación (Turnitin), Servicio de Biblioteca virtual, Servicio de Repositorio institucional de investigaciones, Correo institucional para el caso de los servicios académicos y;
b. SIAF, tesorería, contabilidad y planillas, para el caso de los servicios administrativos.

Tomando como base la Guía de revisión documental, según el Anexo 2, se realizó una revisión de los principales documentos físicos y digitales que cuenta la OTI, lo cual permitió identificar las debilidades estructurales y operativas que comprometen la continuidad, eficiencia y seguridad de estos procesos. Los resultados de este análisis se muestra a continuación:

a. Falta de un procedimiento formal para gestionar incidentes

La ausencia de un procedimiento institucional para registrar, clasificar, atender y cerrar incidentes provoca:

- Respuesta reactiva, sin capacidad de anticipación.
- Atención desordenada, basada en llamadas o mensajes informales.
- Pérdida de información, ya que no existe trazabilidad sobre incidentes repetitivos.
- Imposibilidad de medir desempeño, al no existir métricas ni reportes.

Esta debilidad impacta directamente procesos sensibles como matrícula, emisión de notas, trámites administrativos, servicios estudiantiles y actividades docentes, que dependen de plataformas digitales críticas.

b. Infraestructura tecnológica envejecida o insuficientemente mantenida

Los documentos técnicos revelan que la red telemática, incluyendo backbone, switches, firewall y servidores, presenta señales de obsolescencia y riesgos operacionales:

- Segmentos de fibra y equipos de red antiguos con fallas intermitentes.
- Configuraciones del firewall heredadas, permisivas o incorrectas.
- Servidores expuestos a sobrecalentamiento por fallas de climatización.
- UPS envejecidos e incapaces de sostener cargas críticas ante apagones.

Estas condiciones generan interrupciones de servicios esenciales como:

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

La degradación de infraestructura incrementa la probabilidad de interrupciones durante momentos de alta demanda, como matrícula, evaluaciones, cierre de notas o periodos de graduación.

c. Vulnerabilidades significativas de seguridad digital

El análisis de riesgos muestra múltiples amenazas:

- Contraseñas débiles y poca gestión de credenciales.
- Equipos con antivirus desactualizado.
- Configuraciones inseguras en firewall y servicios.

- Ausencia de un SGSI institucional.
- Intentos de intrusión hacia bases académicas.

Estas vulnerabilidades comprometen la integridad y confidencialidad de:

- Registros académicos (notas, matrículas, historiales).
- Tesis y proyectos registrados en Selgestiun.
- Evidencias de originalidad en Turnitin.
- Datos personales de estudiantes y docentes.

La pérdida o alteración de registros académicos representa uno de los riesgos institucionales más altos documentados.

d. Deficiencias en la continuidad operativa: energía y climatización

La sala de servidores presenta problemas recurrentes:

- Variaciones de voltaje y apagones que afectan continuidad.
- Sistemas de climatizaciones inestables o insuficientes en temporadas de calor.

Estas condiciones provocan:

- Reinicios no planificados de equipos críticos.
- Daños progresivos en hardware.
- Lentitud o caída de servicios alojados (SIA, correo, bases de datos).

Los procesos académicos dependen de que estas plataformas se mantengan operativas; sin embargo, actualmente la continuidad no está garantizada.

e. Ausencia de herramientas tecnológicas para el soporte y la gestión de incidentes

Los documentos revisados confirman que no existen:

- Sistemas de tickets.
- Plataforma de Mesa de Ayuda.
- Monitoreo centralizado de red y servidores.
- Base de conocimientos técnica.

El personal técnico carece de herramientas básicas para:

- Registrar incidentes.
- Identificar tendencias.
- Gestionar carga de trabajo.
- Establecer niveles de servicio.

La falta de herramientas conduce a una operación artesanal que limita la eficiencia institucional.

f. Procesos académicos críticos altamente vulnerables

Los procesos académicos identificados en el Mapa de Procesos, como: matrícula, registro académico, gestión docente, emisión de grados y títulos, dependen directamente de sistemas como el SIA. Los incidentes reportados muestran que:

- El SIA se cae bajo carga elevada.
- La red falla en momentos críticos del ciclo académico.
- Las bases de datos sufren inconsistencias por consultas mal diseñadas.

Estas debilidades generan:

- Retrasos en matrícula.
- Inconformidad estudiantil.
- Afectación a cronogramas institucionales.
- Sobrecarga del personal académico y administrativo.

g. Dependencia excesiva del conocimiento individual de los técnicos

Las entrevistas reflejan que:

- La asignación de incidentes depende de quién está disponible, no de habilidades.
- Los técnicos operan sin documentación ni procedimientos.
- Las respuestas varían según la experiencia personal y no según un flujo estandarizado.

Esto provoca las siguientes consecuencias:

- Inconsistencia en la calidad del servicio.

- Riesgo alto ante rotación de personal.
- Dificultad para mejorar procesos o documentar lecciones aprendidas.

h. Falta de roles y niveles de soporte formalmente definidos

La estructura actual no distingue entre:

- Soporte de primer nivel (atención inicial).
- Soporte especializado (nivel 2).
- Expertos o responsables por servicio (nivel 3).

Esta situación genera lo siguiente:

- Sobrecarga en personal especializado.
- Retrasos en resolución de incidentes.
- Dificultad para establecer métricas de eficiencia.

i. Escalamiento funcional y jerárquico inexistente o informal

El escalamiento solo ocurre cuando:

- El técnico reconoce que no puede resolver el incidente.
- Un decano o director presiona por solución.

Esto conlleva a tener las siguientes debilidades:

- Falta de criterios de severidad.
- Ausencia de tiempos máximos para escalar.
- Riesgo elevado en incidentes mayores o de seguridad.

j. Carencia de un sistema de monitoreo preventivo

La red telemática no cuenta con herramientas que permitan detectar:

- Caídas de switches.
- Sobrecalentamiento de servidores.
- Saturación de ancho de banda.
- Intentos de intrusión.

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

Tabla 3. Resultados del diagnóstico de la gestión de incidentes de TI en la UNPRG, por revisión documental

Categoría revisada	Aspectos a revisar	Hallazgos encontrados
Procedimientos de TI	¿Existe un procedimiento formal de gestión de incidentes? ¿Contiene fases, roles y flujos?	Se evidencia la **ausencia de un procedimiento institucional formal** para la gestión de incidentes de TI. No se identifican fases definidas (registro, clasificación, priorización, resolución y cierre), ni flujos estandarizados de atención. La gestión actual es reactiva, informal y dependiente de comunicaciones directas (llamadas, mensajes), lo que genera pérdida de trazabilidad, atención desordenada e imposibilidad de medir el desempeño del proceso.
Manual de Organización y Funciones (MOF)	Roles relacionados con TI, soporte, servicio al usuario	Los documentos revisados no definen **roles específicos asociados a la gestión de incidentes**, ni diferencian funciones de soporte de primer, segundo y tercer nivel. Las responsabilidades son genéricas y no están orientadas a la atención de incidentes, lo que provoca sobrecarga del personal especializado, dependencia del conocimiento individual y dificultades para establecer responsabilidades claras y métricas de eficiencia.
Reglamentos o lineamientos de sistemas	Criterios para atención de incidentes, tiempos, categorías	No se identifican reglamentos o lineamientos que establezcan **criterios formales de clasificación, priorización, severidad o tiempos de atención de incidentes**. La atención se realiza sin matrices de impacto y urgencia, sin tiempos máximos de respuesta ni criterios para declarar incidentes mayores, lo que evidencia una **brecha significativa respecto a las buenas prácticas de ITIL 4**.
Reportes de incidentes	Tipo de incidentes, frecuencia, tiempos de atención	No existen reportes formales de incidentes que permitan conocer su tipo, frecuencia, duración o reincidencia. La falta de registros históricos impide identificar patrones, analizar causas raíz y evaluar el impacto de los incidentes sobre procesos críticos como matrícula, emisión de notas, gestión administrativa y servicios estudiantiles. Se confirma una **carencia total de trazabilidad y control del desempeño**.
Herramientas TI (documentación técnica)	Uso de software de tickets, monitoreo, base de conocimiento	Se constata la **ausencia de herramientas tecnológicas de soporte** para la gestión de incidentes: no existen sistemas de tickets, plataforma de Mesa de Ayuda, monitoreo centralizado de red y servidores ni base de conocimientos institucional. Esta situación deriva en una operación artesanal, sin capacidad para identificar tendencias, gestionar carga de trabajo ni implementar monitoreo preventivo de infraestructura, seguridad y rendimiento.

3.3. Diseño de los elementos funcionales y estructurales de esa mesa de ayuda

3.3.1. Propósito del diseño de los elementos funcionales y estructurales de la mesa de ayuda

El diseño de los elementos funcionales y estructurales de una Mesa de Ayuda en la UNPRG tuvo como propósito establecer un mecanismo institucional, ordenado y eficiente para gestionar los incidentes de tecnologías de la información que afectan los procesos académicos y administrativos. Su finalidad central fue transformar la actual atención reactiva y dispersa en un proceso estandarizado, capaz de

garantizar trazabilidad, tiempos de respuesta predecibles y un soporte técnico coherente con las necesidades de la comunidad universitaria.

La Mesa de Ayuda busca convertirse en el punto único de contacto entre los usuarios y la OTI, permitiendo canalizar las solicitudes mediante procedimientos formales de registro, clasificación, priorización, asignación y resolución. Este componente funcional es crucial para reducir la dependencia del conocimiento individual de los técnicos, minimizar la pérdida de información y asegurar que cada incidente sea atendido de manera sistemática, independientemente del área o persona que lo reporte.

Desde una perspectiva estructural, su diseño pretende organizar roles, niveles de soporte y rutas de escalamiento, definiendo quién atiende qué tipo de incidentes, en qué orden y bajo qué criterios. Esto permite que los incidentes críticos, como caídas del SIA, interrupciones de red, fallas en servidores o ataques de seguridad, sean gestionados con la urgencia adecuada, evitando retrasos en procesos institucionales clave como matrícula, registro de notas, trámites administrativos o actividades docentes.

La Mesa de Ayuda se plantea como un componente esencial para fortalecer la gobernanza digital de la UNPRG, garantizando que la atención de incidentes se alinee con buenas prácticas como ITIL 4. Con ello, se crea la base para mejorar la continuidad operativa, elevar la calidad del servicio, generar métricas reales de desempeño y promover la mejora continua de los servicios tecnológicos universitarios

3.3.2. Identificación de las brechas existentes en relación a ITIL 4

En base a los resultados del análisis diagnóstico de la forma cómo la UNPRG gestiona los incidentes de TI, a continuación, se desarrolla una comparativa que identifica las brechas existentes de la situación actual en relación a las buenas prácticas de ITIL 4 para la gestión de incidentes.

Tabla 4. Comparación de la gestión de incidentes actual en la UNPRG en relación a las buenas prácticas de ITIL para la gestión de incidentes

Elemento del proceso (ITIL 4)	Buenas prácticas de ITIL 4	Situación actual en la UNPRG	Brecha identificada
Registro de incidentes	Todos los incidentes deben ser registrados de manera estructurada y en un repositorio centralizado.	No existe un registro formal ni único. Los incidentes se comunican por llamadas, mensajes o visitas presenciales. No hay trazabilidad.	**Brecha crítica:** ausencia total de sistema de registro y trazabilidad.
Punto único de contacto (Mesa de Ayuda)	ITIL exige un *Single Point of Contact* para recepción, registro y seguimiento de incidentes.	No existe mesa de ayuda. Cada usuario contacta directamente a técnicos de red o aplicaciones.	**Brecha estructural:** inexistencia de un PUC institucional.
Clasificación de incidentes	Debe existir una taxonomía formal basada en tipo, categoría y subcategoría.	No existen categorías establecidas; los técnicos clasifican según experiencia personal.	**Brecha metodológica:** ausencia de clasificación estandarizada.
Priorización de incidentes	La priorización debe basarse en matrices de impacto y urgencia predefinidas.	Priorización intuitiva basada en presión del usuario o criterio personal.	**Brecha operativa:** no existe matriz de priorización.
Asignación de incidentes	La asignación debe seguir roles y niveles de soporte definidos.	La asignación depende de quién recibe el aviso; no existe reparto formal ni automatizado.	**Brecha organizativa:** asignación reactiva y no documentada.
Niveles de soporte (1°, 2°, 3°)	ITIL define niveles de soporte claros y roles asociado a cada nivel.	No existen niveles formalizados; los técnicos atienden según disponibilidad.	**Brecha de diseño:** inexistencia de niveles de soporte.
Escalamiento funcional	Debe existir un procedimiento formal de escalamiento técnico según especialidad.	Escalamiento informal: se busca al técnico “que sabe más”.	**Brecha funcional:** escalamiento no estructurado.
Escalamiento jerárquico	Debe existir ruta jerárquica para incidentes de alto impacto (Major Incidents).	Ocurre solo por presión de alguna autoridad. No hay criterios para declarar incidente mayor.	**Brecha de gobernanza:** no existe gestión de incidentes mayores.
Resolución de incidentes	Debe documentarse la solución para retroalimentar la base de conocimiento.	La resolución depende de la experiencia del técnico. No se documentan soluciones.	**Brecha de conocimiento:** no existe repositorio de soluciones.
Cierre de incidentes	ITIL exige confirmación del usuario y cierre formal con registro del resultado.	No existe fase formal de cierre. No se valida satisfacción ni funcionalidad.	**Brecha de ciclo de vida:** ausencia de control de cierre.
Monitoreo y alertas	Deben existir herramientas proactivas de monitoreo y alertas tempranas.	No existen herramientas de monitoreo centralizado; el equipo identifica fallas solo cuando el usuario reporta.	**Brecha tecnológica:** monitoreo reactivo y limitado.
Herramientas ITSM	ITIL recomienda herramientas ITSM para registrar, priorizar, monitorear y reportar.	No existe software de tickets, dashboards ni métricas.	**Brecha tecnológica severa:** ausencia de plataforma ITSM.
Métricas (MTTR, re-apertura, backlog)	ITIL establece indicadores clave para evaluar eficiencia del proceso.	No existen métricas ni análisis histórico.	**Brecha analítica:** imposibilidad de medir desempeño.
Roles y responsabilidades	Roles deben definirse claramente en el MOF y en el procedimiento.	No están definidos formalmente ni vinculados a incident management.	**Brecha organizacional:** roles no alineados al proceso ITIL.
Documentación del proceso	Debe existir documentación del proceso, flujos, roles y protocolos.	No existe procedimiento documentado ni manual de incident management.	**Brecha documental:** inexistencia de procedimiento formal.
Gestión de incidentes de seguridad	ITIL sugiere coordinación con Security Management y SGSI.	Se manejan de forma aislada, sin integración con gestión de incidentes TI.	**Brecha transversal:** falta de integración TI–Seguridad.

El análisis comparativo entre la situación actual de la gestión de incidentes en la UNPRG y las buenas prácticas de ITIL 4 permitió identificar tres brechas estructurales que explican de manera integral las dificultades recurrentes en la operación de los servicios tecnológicos y su impacto directo en los procesos

académicos y administrativos. Estas brechas no actúan de forma aislada; por el contrario, se refuerzan mutuamente, generando un entorno propenso a fallas, interrupciones y sobrecarga operativa.

a. Brecha de gobernanza TI

La primera brecha se relaciona con la ausencia de un marco de gobernanza que regule formalmente la gestión de incidentes. La universidad no cuenta con un procedimiento institucional que establezca cómo deben registrarse, clasificarse, priorizarse, asignarse, escalarse, resolverse y cerrarse los incidentes tecnológicos. Esta falta de estructura ocasiona:

- Trazabilidad prácticamente nula, ya que no existe un repositorio único que permita conocer el historial de incidentes o identificar patrones de recurrencia.
- Prioridad fluctuante, dependiente de la percepción y criterio del técnico o del nivel de presión ejercido por el usuario afectado.
- Escalamiento improvisado, donde los incidentes solo se elevan jerárquicamente cuando generan presión institucional, no cuando el impacto lo amerita.
- Imposibilidad de evaluar el desempeño, dado que no se definen indicadores, tiempos objetivos ni mecanismos de retroalimentación.

La gobernanza débil deja a la institución sin capacidad para planificar preventivamente, responder estratégicamente ni tomar decisiones basadas en evidencia.

b. Brecha tecnológica

La segunda brecha emerge de la falta de herramientas tecnológicas adecuadas para apoyar la gestión de incidentes. La UNPRG no dispone de un sistema ITSM, software de tickets, plataforma de monitoreo centralizado ni base de conocimiento. Esta carencia genera:

- Ausencia de registro sistemático, lo cual impide documentar incidentes desde su inicio hasta su cierre.

- Monitoreo reactivo, donde el equipo técnico solo detecta fallas cuando el usuario las reporta.
- Falta de analítica, ya que no existen métricas que permitan determinar frecuencia, impacto, tiempos de resolución o cumplimiento de niveles de servicio.
- Dependencia del esfuerzo manual, lo que incrementa la posibilidad de errores y de pérdidas de información.

Al no contar con herramientas tecnológicas mínimas, la universidad enfrenta serias limitaciones para mantener la continuidad operativa de servicios esenciales, como el SIA, el Aula Virtual, Turnitin o Selgestiun, especialmente en momentos de alta demanda.

c. Brecha organizativa

La tercera brecha se refiere a la falta de claridad en la estructura interna relacionada con la atención de incidentes. Aunque el PGD y la normativa interna definen funciones generales de la OTI, no existen roles específicamente asignados al proceso de gestión de incidentes de TI, tales como agentes de mesa de ayuda, especialistas por nivel de soporte o responsables de incidentes mayores. Esta brecha se refleja en:

- Roles ambiguos o superpuestos, donde cualquier técnico atiende cualquier incidente, sin criterios definidos.
- Niveles de soporte inexistentes, lo que genera sobrecarga en personal especializado que debe resolver tanto problemas simples como complejos.
- Escalamiento funcional y jerárquico informal, sin rutas establecidas ni tiempos para escalar.
- Ausencia de responsabilidades formalizadas, lo cual impide asignar cuentas claras de desempeño o definir tiempos objetivo de resolución.

Esta desorganización provoca dependencia del conocimiento individual de cada técnico, lo que incrementa la vulnerabilidad ante rotación, indisponibilidad o sobrecarga del personal.

3.3.3. Identificación de los elementos funcionales y estructurales de la mesa de ayuda

A continuación, se desarrolla la propuesta integral de elementos funcionales y estructurales de una Mesa de Ayuda (Service Desk) diseñada específicamente para superar las debilidades diagnosticadas en la gestión de incidentes de TI de la UNPRG y alinearse con las buenas prácticas de ITIL 4.

La propuesta se estructura en la siguiente tabla que distingue los componentes estructurales (lo que la Mesa de Ayuda debe ser) y componentes funcionales (lo que la Mesa de Ayuda debe hacer o realizar).

Tabla 5. Propuesta de elementos estructurales y funcionales de la mesa de ayuda

Tipo de componente	Elemento propuesto	Descripción detallada alineada a ITIL 4
Estructural	Punto Único de Contacto (PUC)	La Mesa de Ayuda se constituye como el único canal oficial para recibir incidentes y solicitudes de TI. Centraliza reportes provenientes de estudiantes, docentes y personal administrativo. Reduce la dispersión actual y permite trazabilidad completa del incidente.
Estructural	Roles definidos (Nivel 1, Nivel 2, Nivel 3)	Se establecen roles específicos para atención de incidentes: Nivel 1: Agentes de soporte que registran, clasifican y resuelven incidentes básicos. Nivel 2: Especialistas en redes, servidores, bases de datos y aplicaciones. Nivel 3: Expertos, desarrolladores o proveedores externos para incidentes complejos.
Estructural	Responsable del proceso de gestión de incidentes	Encargado de supervisar cumplimiento de procedimientos, coordinar escalamiento, analizar tendencias y emitir informes. Alinea la operación con ITIL 4 y con el PGD institucional.
Estructural	Herramienta ITSM / Sistema de Tickets	Plataforma tecnológica que permite registrar, clasificar, priorizar, asignar, escalar, resolver y cerrar incidentes de forma estandarizada. Debe permitir generar métricas críticas (MTTR, backlog, % SLA cumplidos).
Estructural	Base de conocimientos (Knowledge Base)	Repositorio institucional con artículos, guías rápidas, soluciones documentadas y FAQs. Permite mejorar la eficiencia, reducir tiempos de atención y promover la autogestión.
Estructural	Flujos de escalamiento formal	Diseño estructurado de rutas para escalamiento funcional (según especialidad técnica) y escalamiento jerárquico (para incidentes mayores). Garantiza que incidentes críticos reciban atención inmediata.
Funcional	Registro estandarizado del incidente	Cada incidente se registra con campos estandarizados: fecha/hora, usuario, servicio afectado, categoría, severidad, síntomas, tiempo de respuesta, solución aplicada. Asegura trazabilidad y análisis histórico.
Funcional	Clasificación según taxonomía formal	Los incidentes se clasifican según categorías ITIL: hardware, software, red, seguridad, aplicaciones, acceso, impresión, servicios académicos, etc. Permite análisis por tendencia y asignación correcta.
Funcional	Priorización basada en impacto y urgencia	Uso de una matriz de priorización institucional. Ejemplo: caída del SIA = impacto alto, urgencia alta → prioridad 1. Esto elimina decisiones arbitrarias y asegura coherencia operativa.
Funcional	Asignación automática	El sistema ITSM asigna incidentes según categoría, carga de

	o semiautomática	trabajo y nivel de soporte. Reduce tiempos de recepción y mejora la eficiencia del personal técnico.
Funcional	Resolución documentada y estandarizada	Cada solución debe documentarse para alimentar la base de conocimientos y permitir replicabilidad. Evita variabilidad entre técnicos y reduce recurrencia de incidentes.
Funcional	Escalamiento oportuno	Si el incidente no puede resolverse en cierto tiempo o pertenece a un área especializada, el sistema ejecuta escalamiento automático hacia el nivel superior —funcional o jerárquico—.
Funcional	Cierre formal del incidente	El incidente se cierra solo después de verificar con el usuario la conformidad del servicio restablecido. ITIL exige esta validación final para garantizar continuidad.
Funcional	Generación de métricas e informes periódicos	Indicadores como MTTR, tasa de reabiertos, tiempo promedio de atención, volumen mensual por categoría y cumplimiento de SLAs permiten evaluar desempeño y apoyar la toma de decisiones estratégicas de la OTI.
Funcional	Comunicación proactiva con usuarios	En incidentes mayores, la Mesa de Ayuda notifica oportunamente a la comunidad universitaria sobre el estado del servicio. Mejora la transparencia y reduce incertidumbre.

3.3.4. Diseño de los elementos estructurales de la mesa de ayuda

A continuación, se describe el diseño de cada uno de los componentes estructurales propuestos:

a. Punto Único de Contacto (PUC)

Objetivo del PUC

El propósito del PUC es convertirse en el único canal institucional autorizado para recibir incidentes y solicitudes tecnológicas, reemplazando el modelo fragmentado actual donde estudiantes, docentes y trabajadores contactan directamente a técnicos individuales.

Este punto único permitirá:

- Organizar el soporte TI en torno a los procesos críticos de la universidad.
- Asegurar la continuidad del SIA, Aula Virtual, Turnitin y Selgestiun y el funcionamiento continuo y correcto de la infraestructura tecnológica.
- Reducir la dependencia del conocimiento personal de técnicos.
- Establecer un orden institucional para registrar, clasificar, priorizar y resolver incidentes.
- Proveer información para la toma de decisiones en la gestión universitaria.

Descripción de la organización del PUC

El PUC propuesto tendría la siguiente organización:

Tabla 6. Descripción de la organización del Punto Único de Contacto

Elemento estructural	Descripción específica
Ubicación orgánica del PUC	Se integra como unidad operativa dentro de la OTI, alineada con el PGD 2024–2026, con dependencia directa del Jefe de la OTI. Su creación formal deberá constar en resolución rectoral o directiva interna.
Equipo del PUC	**Agentes de primer nivel** asignados según facultades/dependencias administrativas o macroprocesos (por ejemplo: Área Académica, Área Administrativa, Servicios Generales). **Coordinador del PUC**, responsable de supervisar tiempos de atención y escalamiento. **Responsable del Proceso de Incidentes**, encargado de indicadores, informes y mejora continua.
Puntos de atención integrados	Plataforma digital, extensión telefónica institucional, módulo presencial en la OTI (para usuarios sin acceso digital). Este último es clave en la cultura administrativa de la UNPRG.
Sistema ITSM recomendado	Software institucional que permita gestionar incidentes de SIA, Aula Virtual, Turnitin, Selgestiun, Red Telemática y servicios de infraestructura. Debe permitir interoperar con los registros de riesgo digital del PGD.
Base institucional de conocimientos	Repositorio con procedimientos, soluciones documentadas, manuales del SIA, instructivos del Aula Virtual, guías de Turnitin y protocolos de redes. Debe actualizarse mensualmente.
Infraestructura de apoyo	Estación de trabajo exclusiva, pantallas de monitoreo de red, sistema de tickets, registro de llamadas y acceso a herramientas de diagnóstico rápido de red y servicios.

Descripción de la funcionalidad del PUC

El PUC debe desarrollar funciones específicas en la gestión de incidentes. Estas funciones se identifican y describen en la siguiente tabla:

Tabla 7. Descripción de la funcionalidad del Punto Único de Contacto

Elemento funcional	Descripción de la funcionalidad
Recepción y registro estandarizado de incidentes	Los incidentes se registran mediante un procedimiento formal estandarizado para todo tipo de incidente que afecte servicios académicos o administrativos
Clasificación de los incidentes	Las categorías sugeridas incluyen: - 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 (Selgestiun) - Servicio de Biblioteca virtual - Servicio de Repositorio institucional de investigaciones - Plataforma de correo institucional - Sistemas de gestión administrativa (SIAF, tesorería, contabilidad y planillas) - Red Telemática (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
Priorización de los incidentes	Se aplicará una matriz impacto × urgencia, adaptada al calendario académico: - Ej. Periodos de matrícula y cierre de notas → prioridad alta por defecto. - Ej. Caída del Aula Virtual durante exámenes → incidente mayor.
Asignación	El sistema ITSM distribuye automáticamente incidentes según la clasificación, evitando la carga excesiva sobre técnicos específicos.
Escalamiento funcional y jerárquico	El escalonamiento se activa automáticamente cuando sucede un incidente al nivel de soporte correspondiente.
Comunicación institucional	El PUC enviará comunicados oficiales (correo/red interna) ante incidentes mayores
Cierre con validación del usuario	El cierre será obligatorio solo tras confirmación del usuario, especialmente en procesos críticos.
Métricas estratégicas	Se medirán indicadores específicos, como MTTR, FCR, Tasa de reabiertos, fallos en periodos críticos

Flujo operativo del PUC

El flujo operativo del PUC tendrá la siguiente secuencia de actividades:

1. Usuario reporta incidente por canal oficial (web, correo, teléfono o módulo).
2. PUC registra el ticket con los campos específicos del servicio afectado.
3. Se determina si el incidente está relacionado con servicios académicos críticos.
4. Se clasifica y prioriza usando matriz adaptada al calendario universitario.
5. El ticket se asigna al nivel de soporte adecuado.
6. Nivel 1 intenta First Contact Resolution para incidentes simples:
    - Restablecer acceso al Aula Virtual
    - Problemas de credenciales del SIA
    - Consultas operativas básicas
7. Escalamiento automático para problemas como:
    - Caída total del SIA
    - Incidentes de red telemática que afecten facultades completas
    - Problemas en servidores críticos o firewall
8. Se actualiza al usuario durante todo el proceso.
9. Se resuelve el incidente y se documenta.
10. Se cierra el ticket con validación del usuario y registro final.

b. Roles y funciones por Nivel de Soporte

Los roles y funciones propuestas para la gestión de incidentes de TI se describen a continuación, según el nivel. Los perfiles de puesto para cada nivel se describen en el Anexo 4.

Nivel 1 – Técnico de Atención Inicial de Incidentes

Rol principal

Atención inicial y resolución de incidentes comunes mediante procedimientos ya documentados.

Funciones del Nivel 1

- Recibir todos los incidentes a través del Punto Único de Contacto.
- Registrar la información en el sistema ITSM de forma completa y estandarizada.
- Clasificar el incidente según taxonomía institucional (SIA, red, seguridad, Aula Virtual, etc.).
- Determinar la prioridad usando la matriz impacto × urgencia.
- Intentar First Contact Resolution (FCR) siguiendo guías y base de conocimiento.
- Escalar incidentes no resueltos o fuera de su alcance al Nivel 2.
- Mantener comunicación con el usuario sobre el estado del ticket.
- Contribuir a la base de conocimiento reportando soluciones recurrentes.

Personal que podría asumir este rol

Técnicos de soporte de la OTI con competencias básicas en hardware, software y procedimientos del SIA y Aula Virtual.

Nivel 2 – Especialista en Infraestructura y Servicios Digitales

Rol principal

Atender incidentes que requieren conocimiento técnico específico.

Funciones del Nivel 2

- Resolver incidentes relacionados con infraestructura, redes, servidores y bases de datos.
- Atender incidentes del SIA, Aula Virtual, Turnitin y Selgestiun que requieren análisis técnico.
- Analizar causas raíz en incidentes recurrentes.
- Proponer mejoras técnicas y correctivas.
- Documentar soluciones complejas en la base de conocimiento.
- Escalar incidentes al Nivel 3 cuando requieren intervención experta o proveedor externo.

Personal de las áreas que podría asumir este rol

- Redes y comunicaciones.
- Servidores y virtualización.
- Seguridad informática.
- Administradores de bases de datos.
- Administradores de aplicaciones (SIA, Moodle, Selgestiun).

Nivel 3 – Experto en soluciones tecnológicas críticas (proveedores)

Rol principal

Resolver incidentes complejos o estructurales que exceden las capacidades internas.

Funciones del Nivel 3

- Atender incidentes críticos del SIA que involucren errores de programación o integridad de datos.
- Resolver problemas de seguridad avanzada como intentos de hackeo o intrusión.
- Realizar intervenciones de alto riesgo en servidores, firewall o sistemas sensibles.
- Coordinar con proveedores de software o hardware para soporte de garantía.
- Validar correcciones definitivas y actualizaciones de versiones.
- Documentar soluciones estratégicas para prevenir recurrencia.

Personal que podría asumir este rol

- Desarrolladores de sistemas: SIA, Selgestiun, otros.
- Proveedores de Turnitin y Moodle.
- Fabricantes de hardware o firewall.
- Consultores externos especializados.

Competencias por nivel de soporte

La siguiente matriz identifica las competencias técnicas, operativas y actitudinales requeridas en cada nivel de soporte.

Tabla 8. Matriz de competencias para la gestión de incidentes en la UNPRG

Competencia	Nivel 1 Técnico de Atención Inicial	Nivel 2 Especialistas Infraestructura	Nivel 3 Expertos / Proveedores
Conocimiento general de TI	Conocimiento básico sobre hardware, software, red y sistemas institucionales (SIA, Aula Virtual, correo).	Conocimiento avanzado en áreas específicas: redes, servidores, bases de datos, aplicaciones.	Dominio profundo de tecnologías críticas: firewall, programación del SIA, ciberseguridad avanzada, infraestructura de misión crítica.
Diagnóstico inicial de incidentes	Capacidad para identificar síntomas y registrar información clara y completa.	Capacidad para ejecutar diagnósticos técnicos y aislar causas raíz.	Capacidad para analizar incidentes estructurales o complejos con herramientas avanzadas.
Uso de herramientas ITSM	Registrar, clasificar y priorizar tickets.	Actualizar estados, adjuntar diagnóstico, documentar soluciones.	Documentar soluciones estructurales y realizar análisis de tendencias.
Gestión de clientes	Comunicación clara y empática con usuarios; manejo de situaciones de estrés en periodos críticos (matrícula, exámenes).	Comunicación técnica con otros especialistas; coordinación con equipos de trabajo.	Comunicación estratégica con alta dirección y proveedores externos.
Resolución de incidentes	Capacidad para resolver problemas simples (accesos, contraseñas, configuraciones básicas).	Capacidad para resolver problemas de nivel intermedio y alto (red, bases de datos, aplicaciones).	Capacidad para aplicar correcciones definitivas, actualizaciones, parches y rediseño de soluciones.
Conocimiento de procesos	Comprender el flujo básico de incident management.	Comprender el proceso completo e integrar análisis técnico.	Dominio del ciclo completo basado en ITIL 4 y estándares de seguridad.
Uso de base de conocimientos	Consultar y aplicar guías y artículos.	Actualizar y crear nuevos artículos.	Validar contenido técnico especializado.
Escalamiento	Identificar cuando el incidente debe escalarse.	Realizar escalamiento funcional oportuno.	Ejecutar escalamiento jerárquico en incidentes mayores.
Habilidades blandas	Empatía, comunicación, escucha activa, paciencia.	Colaboración, pensamiento crítico, análisis estructurado.	Liderazgo técnico, negociación, toma de decisiones bajo presión.

Matriz RACI del Proceso de gestión de incidentes

La matriz RACI propuesta se basa en actividades clave del proceso ITIL 4 y los roles definidos para los tres niveles de soporte. Para la asignación de las fucniomes RACI se debe tener en cuenta la siguiente leyenda:

- **R (Responsible):** Ejecuta la actividad.

- **A (Accountable):** Responsable que se cumpla la actividad.
- **C (Consulted):** Consultado para decisiones técnicas.
- **I (Informed):** Debe ser informado del avance o resultado.

Tabla 9. Tabla RACI para la gestión de incidentes en la UNPRG

Actividad del proceso	Nivel 1 Técnico de Atención Inicial	Nivel 2 Especialistas Infraestructura	Nivel 3 Expertos / Proveedores	Responsable del proceso de incidentes	Usuarios de las unidades académicas y administrativas
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
Priorización (impacto × urgencia)	R	C	I	A	I
Intento de 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 funcional	R	A	I	C	I
Escalamiento jerárquico (incidentes mayores)	A	C	C	R	I
Comunicación con usuarios	R	I	I	A	C
Documentación en base de conocimiento	R	R	C	A	I
Validación del cierre	R	C	I	A	R / Usuario afectado
Generación de métricas (MTTR, FCR)	I	I	I	R / A	I
Mejora continua del proceso	C	C	C	A / R	I

De la tabla RACI propuesta se resumen lo siguiente:

- El **Nivel 1** asume la mayor parte de las tareas operativas, asegurando rapidez y orden.
- El **Nivel 2** sostiene la operación especializada, evitando sobrecarga y dispersión.
- El **Nivel 3** interviene solo cuando el incidente supera los recursos internos.
- El **Responsable del proceso** garantiza cumplimiento normativo, calidad, métricas y mejora continua.

Los usuarios de las unidades académicas y administrativas participan validando el cierre del proceso y reportando adecuada y oportunamente los incidentes.

c. Responsable del proceso de gestión de incidentes

Un elemento clave en la organización del proceso de gestión de incidentes es el responsable de su gestión. A continuación, se describe la propuesta:

Nombre institucional específico del rol

Coordinador Institucional de Gestión de Incidentes de TI (CIGI-TI)

Perfil de puesto

- **Puesto:** Coordinador Institucional de Gestión de Incidentes de TI (CIGI-TI)
- **Dependencia:** Oficina de Tecnologías de la Información (OTI)
- **Reporta a:** Jefatura de la OTI
- **Coordina con:** Mesa de Ayuda (PUC), Especialistas Nivel 2, Consultores Nivel 3, Seguridad Digital, Unidades Académicas y Administrativas

Propósito del puesto

Asegurar la operación efectiva, controlada y alineada a ITIL 4 del proceso de Gestión de Incidentes de TI, garantizando continuidad de servicios críticos (SIA, Aula Virtual, Red Telemática, Turnitin, Selgestiun) y el cumplimiento del Plan de Gobierno Digital institucional.

Funciones principales

- Supervisar el cumplimiento del procedimiento de Gestión de Incidentes en todo su ciclo de vida.
- Coordinar el escalamiento funcional y jerárquico, incluyendo incidentes mayores.
- Validar la correcta clasificación, priorización y cierre de incidentes.
- Analizar métricas (MTTR, FCR, backlog, reincidencia) e identificar tendencias.

- Emitir informes periódicos a la Jefatura OTI.
- Proponer mejoras continuas al proceso y a la Mesa de Ayuda.
- Asegurar la alineación con ITIL 4, seguridad digital y el PGD 2024–2026.
- Coordinar con seguridad digital ante incidentes de ciberseguridad.

Competencias requeridas

- Conocimiento sólido de ITIL 4 (Incident Management).
- Gestión de procesos y análisis de indicadores.
- Comunicación institucional y coordinación transversal.
- Pensamiento analítico y mejora continua.
- Conocimiento del entorno universitario y del PGD.

Ubicación en el organigrama funcional

Rectorado / Alta Dirección

↳ Jefatura de la OTI

↳ **Coordinador Institucional de Gestión de Incidentes de TI (CIGI-TI)**

↳ Técnico de Atención Inicial – PUC (Nivel 1)

Especialistas en Infraestructura y Servicios Digitales (Nivel 2)

Consultores Expertos / Proveedores (Nivel 3)

Procedimiento de reporte y seguimiento del CIGI-TI

El procedimiento que debe seguir el CIGI-TI para asegurar el control, seguimiento y mejora del proceso de Gestión de Incidentes mediante reportes periódicos, análisis de métricas y acciones correctivas, es el siguiente:

Tabla 10. Diagrama SIPOC del Proceso de seguimiento y control de la Gestión de Incidentes

S – Proveedores (Suppliers)	I – Entradas (Inputs)	P – Proceso (Process)	O – Salidas (Outputs)	C – Clientes (Customers)
- Mesa de Ayuda (PUC – Nivel 1) - Especialistas Técnicos (Nivel 2) - Consultores Expertos / Proveedores (Nivel 3) - Sistema ITSM - Área de Seguridad Digital	- Tickets del sistema ITSM (abiertos y cerrados) - Registros de escalamiento funcional y jerárquico - Métricas operativas (MTTR, FCR, SLA) - Reportes de incidentes de seguridad	**1.** Consolidar información semanal de tickets y escalamiento. **2.** Analizar métricas mensuales para identificar tendencias, servicios críticos y reincidencias. **3.** Revisar incidentes mayores, validando causas raíz, tiempos de atención y comunicaciones realizadas. **4.** Elaborar informes ejecutivos mensuales y trimestrales para la Jefatura de la OTI y autoridades cuando corresponda. **5.** Definir planes de acciones correctivas (técnicas, procedimentales o de capacitación). **6.** Dar seguimiento a la implementación de acciones aprobadas. **7.** Retroalimentar a la Mesa de Ayuda, actualizando procedimientos y base de conocimientos.	- Informes de desempeño del proceso de incidentes - Indicadores consolidados de gestión (MTTR, FCR, SLA) - Recomendaciones de mejora continua - Procedimientos y base de conocimientos actualizados - Evidencias para el cumplimiento del PGD	- Jefatura de la OTI - Autoridades universitarias (cuando aplique) - Mesa de Ayuda (PUC) - Equipos técnicos Nivel 2 y 3 - Comunidad universitaria

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 UNPRG. 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 (Selgestiun)
- Servicio de Biblioteca virtual
- Servicio de Repositorio institucional de investigaciones
- Plataforma de correo institucional
- Sistemas de gestión administrativa (SIAF, tesorería, contabilidad y planillas)
- Red Telemática (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

Para cada servicio se debe tener almacenado el siguiente conocimiento:

Tabla 11. Definición de los tipos de artículos de la Base de Conocimientos

Tipo de artículo	Definición	Ejemplos
FAQs (bajo impacto)	Conjunto de preguntas y respuestas breves orientadas a resolver dudas frecuentes y de bajo impacto operativo. Están dirigidas principalmente a los usuarios finales (estudiantes, docentes y personal administrativo) y permiten la autogestión de incidentes simples, reduciendo la carga del Nivel 1 y evitando la generación innecesaria de tickets.	- ¿Por qué no puedo ver mis notas en el SIA? - ¿Qué hago si el Aula Virtual no carga? - ¿Por qué Turnitin no muestra el porcentaje de similitud? - ¿Cuándo se habilita el sistema de matrícula? - ¿A quién debo contactar si no tengo acceso a la red Wi-Fi?
Guías rápidas (para la autogestión)	Documentos concisos que describen, paso a paso, acciones que el usuario puede realizar por sí mismo para resolver problemas comunes sin intervención técnica directa. Su objetivo es empoderar al usuario, acelerar la solución de incidentes simples y mejorar la experiencia de uso de los servicios digitales institucionales.	- Cómo recuperar acceso al Aula Virtual - Cómo restablecer la contraseña institucional - Cómo verificar si un curso está activo en Moodle - Cómo cargar una tarea correctamente en Turnitin - Cómo acceder al SIA fuera del campus
Artículos de solución (para incidentes recurrentes)	Documentación técnica que describe la resolución validada de incidentes que se presentan de manera repetitiva. Incluyen síntomas, causa conocida y solución paso a paso, y están orientados al personal de soporte técnico para asegurar una atención consistente y reducir el tiempo promedio de resolución (MTTR).	- Solución a caída intermitente del SIA en matrícula - Corrección de error de acceso al módulo de notas del SIA - Restablecimiento de conexión Wi-Fi en una Facultad - Resolución de lentitud en el Aula Virtual durante evaluaciones - Solución a error de sincronización entre Moodle y Turnitin
Checklists técnicos (para el diagnóstico)	Listas estructuradas de verificación utilizadas por el personal técnico para realizar diagnósticos sistemáticos y ordenados. Permiten identificar rápidamente la causa de un incidente, evitar omisiones en el análisis y estandarizar la atención técnica, especialmente en incidentes de infraestructura, red y servidores.	- Checklist de revisión de red por facultad - Checklist de verificación de servicios del SIA - Checklist de revisión de servidores antes de matrícula - Checklist de seguridad básica en firewall - Checklist de climatización de la sala de servidores
Procedimientos (para incidentes críticos)	Documentos formales que describen de manera detallada y secuencial las acciones a seguir ante incidentes críticos o de alto impacto institucional. Incluyen responsabilidades, flujos de escalamiento y controles, y son de cumplimiento obligatorio para garantizar la continuidad de los servicios académicos y administrativos.	- Procedimiento para registro de tesis en Selgestiun - Procedimiento de atención de incidentes del SIA - Procedimiento para creación de usuarios institucionales. - Procedimiento de respaldo de bases de datos académicas - Procedimiento de escalamiento de incidentes mayores
Alertas técnicas (prevención)	Comunicaciones preventivas que informan sobre situaciones de riesgo, alta demanda, mantenimientos programados o amenazas potenciales. Su finalidad es anticipar incidentes, reducir su impacto y preparar a los usuarios y al personal técnico ante escenarios críticos, fortaleciendo la continuidad operativa y la seguridad.	- Alta demanda del SIA – recomendaciones - Mantenimiento programado del Aula Virtual - Interrupción temporal del servicio de red por trabajos eléctricos - Alerta de intentos de acceso no autorizado al SIA - Recomendaciones ante fallas eléctricas en la sala de servidores

Así mismo, para cada categoría de servicio se propone como información inicial, el siguiente conocimiento:

Tabla 12. Conocimientos iniciales propuestos por categoría de servicio

Incidente	Servicio afectado	Tipo de incidente	Síntomas observados	Causa conocida	Solución paso a paso	Nivel de soporte aplicable	Tiempo estimado de resolución
Caída del SIA en periodo de matrícula	Sistema de Información Académica (SIA)	Disponibilidad	No permite acceso, errores de carga, sesiones cerradas	Sobrecarga del servidor	N1: validar alcance y registrar. N2: revisar servicios y recursos. N3: optimizar o ampliar capacidad.	N1 → N2 → N3	30 min – 4 h
Lentitud del Aula Virtual en evaluaciones	Aula Virtual – Moodle	Rendimiento / Funcionalidad	Lentitud, errores al subir tareas	Alta concurrencia y plugins	N1: validar usuario/navegador. N2: revisar servicios y plugins.	N1 → N2	30 min – 2 h
Informe de similitud no generado	Turnitin	Integración / Servicio externo	Informe pendiente o no visible	Indisponibilidad del proveedor	N1: validar envío. N2: revisar integración. N3: coordinar con proveedor.	N1 → N2 → N3	1 – 24 h
Error en registro de tesis	Selgestiun	Aplicación	No guarda información, errores de validación	Datos incompletos o error de sistema	N1: validar datos. N2: revisar aplicación. N3: corrección por desarrollador.	N1 → N2 → N3	30 min – 2 h
Acceso denegado a Biblioteca virtual	Biblioteca virtual	Acceso	No permite ingreso a recursos	Problemas de autenticación	N1: validar credenciales. N2: revisar autenticación.	N1 → N2	15 – 60 min
Repositorio institucional no disponible	Repositorio institucional	Disponibilidad	No carga documentos	Falla de servidor o almacenamiento	N1: registrar incidente. N2: revisar servicios y almacenamiento.	N1 → N2	30 min – 3 h
Correo institucional no envía/recibe	Plataforma de correo	Acceso	Mensajes rebotados o sin envío	Bloqueo o falla del servicio	N1: validar cuenta. N2: revisar servicio de correo.	N1 → N2	15 – 90 min
Interrupción de sistemas administrativos	Sistemas administrativos	Disponibilidad	Procesos detenidos	Caída de servidor o red	N1: registrar y comunicar. N2: revisar infraestructura. N3: soporte especializado.	N1 → N2 → N3	1 – 6 h
Caída de red en facultad	Red Telemática	Conectividad	Sin acceso a red/Internet	Falla eléctrica o equipo de red	N1: validar alcance. N2: revisar switches/enlaces. N3: proveedor.	N1 → N2 → N3	1 – 6 h
Bloqueo de cuenta por seguridad	Seguridad en red	Seguridad	Usuario sin acceso	Intentos fallidos / alerta	N1: verificar identidad. N2: desbloqueo y análisis.	N1 → N2	15 – 90 min
Servidor físico no responde	Servidores físicos	Infraestructura	Servicios caídos	Falla de hardware o sobrecalentamiento	N2: revisar hardware. N3:	N2 → N3	2 – 8 h

					reemplazo/proveedor.		
Servicio en la nube indisponible	Servidores en la nube	Servicio de terceros	Aplicación no accesible	Falla del proveedor	N2: validar estado. N3: coordinar con proveedor.	N2 → N3	Variable (según proveedor)
Sobrecalentamiento en sala de servidores	Energía y climatización	Continuidad operativa	Alertas de temperatura	Falla de aire acondicionado	N2: revisar climatización. N3: proveedor especializado.	N2 → N3	2 – 8 h
Equipo de laboratorio no enciende	Equipos de laboratorio	Hardware	Equipo inoperativo	Falla eléctrica o hardware	N1: verificación básica. N2: mantenimiento correctivo.	N1 → N2	1 – 4 h
Equipo de cómputo con SO dañado	Equipos terminales (laboratorios)	Hardware / Software	No inicia sistema	Error de software	N1: validación. N2: reinstalación.	N1 → N2	1 – 3 h
Equipo administrativo lento	Equipos terminales (administrativos)	Hardware / Software	Bajo rendimiento	Software desactualizado	N1: limpieza y validación. N2: optimización.	N1 → N2	30 min – 2 h
Software académico no inicia	Software académico	Aplicación	Error de licencia o ejecución	Licencia vencida	N1: validar licencia. N2: reinstalar/activar.	N1 → N2	30 min – 2 h
Error en software de ofimática	Software de ofimática	Aplicación	Fallas en Word/Excel	Configuración dañada	N1: guía rápida. N2: reinstalación.	N1 → N2	15 – 60 min

Tabla 13. Tipos de artículos iniciales de la Base de Conocimientos por categoría de servicio

Categoría de servicio	Tipo de incidente	FAQs (bajo impacto)	Guías rápidas (autogestión)	Artículos de solución (recurrentes)	Checklists técnicos (diagnóstico)	Procedimientos (críticos)	Alertas técnicas (prevención)
Sistema de Información Académica (SIA)	Disponibilidad	¿Por qué no puedo ingresar al SIA?	Cómo verificar acceso al SIA en matrícula	Recuperación del SIA ante caída total	Checklist de verificación de servicios SIA	Procedimiento de contingencia en matrícula	Alerta por alta demanda en matrícula
Sistema de Información Académica (SIA)	Rendimiento	¿Por qué el SIA está lento?	Recomendaciones para usar el SIA en horas pico	Optimización de rendimiento del SIA	Checklist de consumo de recursos	Procedimiento de ajuste de capacidad	Alerta de saturación del sistema
Aula Virtual – Moodle	Acceso	¿Por qué no veo mis cursos?	Cómo ingresar correctamente al Aula Virtual	Solución a fallas de acceso masivo	Checklist de sincronización SIA–Moodle	Procedimiento de restauración de acceso	Alerta en periodos de evaluación
Aula Virtual – Moodle	Funcionalidad	¿Por qué no puedo subir tareas?	Cómo enviar tareas correctamente	Solución a errores en evaluaciones	Checklist de plugins y servicios Moodle	Procedimiento ante fallas en evaluaciones	Alerta previa a exámenes virtuales
Turnitin	Integración / Servicio externo	¿Por qué no aparece mi similitud?	Cómo verificar envío correcto	Solución a fallas de integración Moodle–Turnitin	Checklist de estado del servicio externo	Procedimiento de coordinación con proveedor	Alerta por indisponibilidad del proveedor
Selgestiun	Aplicación	¿Por qué no se registra mi tesis?	Cómo registrar correctamente una tesis	Corrección de errores de validación	Checklist de formularios y BD	Procedimiento de soporte a registros académicos	Alerta en periodos de titulación
Biblioteca virtual	Acceso	¿Por qué no accedo a recursos digitales?	Cómo acceder remotamente a la biblioteca	Solución a bloqueos de acceso	Checklist de autenticación institucional	Procedimiento de restablecimiento de acceso	Alerta por vencimiento de licencias
Repositorio institucional	Disponibilidad	¿Por qué no carga el repositorio?	Cómo verificar disponibilidad del repositorio	Restauración del servicio del repositorio	Checklist de servidor y almacenamiento	Procedimiento de recuperación del repositorio	Alerta por mantenimiento programado
Correo institucional	Acceso	¿Por qué no puedo enviar correos?	Cómo configurar el correo institucional	Recuperación de cuentas bloqueadas	Checklist de servicios de correo	Procedimiento ante caída del correo	Alerta por intentos de intrusión
Sistemas administrativos	Disponibilidad	¿Por qué no ingresa el sistema?	Recomendaciones ante caídas temporales	Solución a interrupciones administrativas	Checklist de servicios administrativos	Procedimiento de continuidad administrativa	Alerta en cierre contable o planillas
Red Telemática	Conectividad	¿Por qué no tengo Internet?	Cómo verificar conexión local	Solución a caídas de red por facultad	Checklist de switches y enlaces	Procedimiento de recuperación de red	Alerta por fallas eléctricas
Seguridad en red	Seguridad	¿Por qué se bloqueó mi cuenta?	Cómo cambiar credenciales seguras	Respuesta a incidentes de seguridad	Checklist de eventos de seguridad	Procedimiento de gestión de incidentes de seguridad	Alerta de amenazas activas
Servidores físicos	Infraestructura	¿Por qué el sistema no responde?	Acciones básicas ante lentitud	Solución a fallas de hardware	Checklist de hardware y recursos	Procedimiento de recuperación de servidores	Alerta por sobrecalentamiento
Servidores en la nube	Servicio de terceros	¿El servicio externo está caído?	Cómo verificar estado del proveedor	Gestión de indisponibilidad en la nube	Checklist de SLA con proveedor	Procedimiento de escalamiento externo	Alerta por fallas del proveedor

Energía y climatización	Continuidad operativa	¿Por qué se apagaron los sistemas?	Recomendaciones ante cortes eléctricos	Solución a fallas de climatización	Checklist de UPS y aire acondicionado	Procedimiento de emergencia de sala de servidores	Alerta por altas temperaturas
Equipos de laboratorio	Hardware	¿Por qué no enciende el equipo?	Cómo verificar conexión y encendido	Reparación de equipos de laboratorio	Checklist de hardware de laboratorio	Procedimiento de mantenimiento correctivo	Alerta por fallas recurrentes
Equipos terminales (laboratorios)	Hardware / Software	¿Por qué no funciona el software?	Cómo reiniciar y validar equipo	Reinstalación de sistema o software	Checklist de sistema operativo	Procedimiento de reinstalación estándar	Alerta por fallas masivas
Equipos terminales (administrativos)	Hardware / Software	¿Por qué mi equipo está lento?	Recomendaciones básicas de uso	Solución a fallas administrativas	Checklist de validación de equipo	Procedimiento de soporte administrativo	Alerta por obsolescencia
Software académico	Aplicación	¿Por qué no abre el software?	Cómo ejecutar correctamente el software	Solución a errores de licencia	Checklist de instalación y licencia	Procedimiento de soporte especializado	Alerta por vencimiento de licencias
Software de ofimática	Aplicación	¿Por qué falla Word o Excel?	Guía rápida de solución básica	Solución a errores recurrentes	Checklist de configuración ofimática	Procedimiento de reinstalación	Alerta por actualizaciones críticas

e. Flujos de escalamiento

El escalamiento propuesto es un escalonamiento funcional por tipo de incidente, que consiste en transferir la atención de un incidente desde el nivel inicial de soporte hacia un nivel técnico especializado, cuando el problema excede las capacidades, herramientas o conocimientos del personal de primer nivel.

Como está descrito en la fundamentación teórica, este tipo de escalamiento se basa en la especialización técnica requerida para resolver el incidente, y se activa cuando el incidente tiene las siguientes condiciones:

- No puede resolverse en el primer contacto.
- Requiere conocimientos avanzados o acceso privilegiado.
- Involucra componentes críticos de infraestructura o aplicaciones.

En este esquema, el escalamiento ocurre horizontalmente entre equipos técnicos (Nivel 1 → Nivel 2 → Nivel 3), manteniendo la trazabilidad del incidente y sin perder la responsabilidad sobre su seguimiento. Adicionalmente, la decisión de escalar se fundamenta en la categoría de servicio.

Propuesta de escalonamiento funcional

Cada tipo de incidente requiere conocimientos y herramientas distintas, por lo que debe ser atendido por el equipo más idóneo desde el punto de vista técnico.

Para cada categoría de servicio es escalonamiento funcional por tipo de incidente se muestra a continuación:

Tabla 14. Escalamiento funcional por categoría de servicio y tipo de incidente

Tipo de incidente	Servicio afectado	Nivel inicial	Escalamiento funcional (Nivel 2 – Especialidad técnica)	Escalamiento avanzado (Nivel 3)
Disponibilidad	Sistema de Información Académica (SIA)	Nivel 1 – Técnico de Atención Inicial de Incidentes (PUC)	Especialista en Aplicaciones Académicas y Servidores	Experto en Soluciones Tecnológicas Críticas (Desarrollador / Proveedor del SIA)
Rendimiento	Sistema de Información Académica (SIA)	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Servidores y Bases de Datos	Experto en Soluciones Tecnológicas Críticas (Arquitectura de sistemas)
Acceso	Aula Virtual – Moodle	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Plataforma Educativa Moodle	Experto en Soluciones Tecnológicas Críticas (Proveedor / Experto Moodle)

Tipo de incidente	Servicio afectado	Nivel inicial	Escalamiento funcional (Nivel 2 – Especialidad técnica)	Escalamiento avanzado (Nivel 3)
Funcionalidad	Aula Virtual – Moodle	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Aplicaciones Educativas	Experto en Soluciones Tecnológicas Críticas
Integración / Servicio externo	Turnitin	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Integración Moodle–Turnitin	Experto en Soluciones Tecnológicas Críticas (Proveedor Turnitin)
Aplicación	Selgestiun	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Aplicaciones Institucionales	Experto en Soluciones Tecnológicas Críticas (Desarrollador Selgestiun)
Acceso	Biblioteca virtual	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Autenticación y Accesos	Experto en Soluciones Tecnológicas Críticas (Proveedor de bases de datos)
Disponibilidad	Repositorio institucional	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Servidores y Almacenamiento	Experto en Soluciones Tecnológicas Críticas
Acceso	Correo institucional	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Servicios de Correo y Autenticación	Experto en Soluciones Tecnológicas Críticas (Proveedor de correo)
Disponibilidad	Sistemas administrativos	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Aplicaciones Administrativas y Servidores	Experto en Soluciones Tecnológicas Críticas (Proveedor / Especialista externo)
Conectividad	Red Telemática	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Redes y Comunicaciones	Experto en Soluciones Tecnológicas Críticas (Proveedor de telecomunicaciones)
Seguridad	Seguridad en red	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Seguridad Digital	Experto en Soluciones Tecnológicas Críticas (Consultor en Ciberseguridad)
Infraestructura	Servidores físicos	Nivel 2 – Especialista en Infraestructura y Servicios Digitales	Especialista en Infraestructura (Hardware y SO)	Experto en Soluciones Tecnológicas Críticas (Fabricante / Proveedor de hardware)
Servicio de terceros	Servidores en la nube	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Gestión de Servicios Cloud	Experto en Soluciones Tecnológicas Críticas (Proveedor cloud)
Continuidad operativa	Energía y climatización	Nivel 2 – Especialista en Infraestructura y Servicios Digitales	Especialista en Infraestructura Crítica	Experto en Soluciones Tecnológicas Críticas (Proveedor eléctrico / climatización)
Hardware	Equipos de laboratorio	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Soporte Técnico de Equipos	Experto en Soluciones Tecnológicas Críticas (Proveedor de hardware)
Hardware / Software	Equipos terminales (laboratorios)	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Sistemas Operativos y Software	Experto en Soluciones Tecnológicas Críticas
Hardware / Software	Equipos terminales (administrativos)	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Soporte TI Administrativo	Experto en Soluciones Tecnológicas Críticas
Aplicación	Software académico	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Software Académico	Experto en Soluciones Tecnológicas Críticas (Proveedor / Licenciante)
Aplicación	Software de ofimática	Nivel 1 – Técnico de Atención Inicial de Incidentes	Especialista en Soporte de Software de Ofimática	Experto en Soluciones Tecnológicas Críticas

En la tabla se formaliza el escalamiento funcional por especialidad técnica, asegurando que cada incidente sea derivado, desde el primer momento, al equipo con mayor capacidad de resolución, evitando decisiones improvisadas basadas en disponibilidad personal.

Criterios para la declaración de incidentes mayores

Es importante contar con criterios para la declaración de incidentes mayores porque estos permiten identificar oportunamente aquellos eventos que, por su alto impacto y urgencia, ponen en riesgo la continuidad de los procesos académicos y administrativos de la UNPRG. La definición previa de estos criterios evita decisiones improvisadas, reduce la dependencia del juicio individual y garantiza que los incidentes críticos, como caídas del SIA en matrícula, fallas de red a nivel institucional o incidentes de seguridad digital, activen de inmediato mecanismos formales de escalamiento, coordinación y comunicación. Asimismo, los criterios para incidentes mayores facilitan la asignación prioritaria de recursos técnicos, la intervención de especialistas o proveedores externos y la notificación a niveles directivos cuando corresponda, contribuyendo a minimizar el impacto institucional, reducir el MTTR y fortalecer la gobernanza de los servicios de TI conforme a las buenas prácticas de ITIL 4.

A continuación se proponen los criterios para declarar un incidente mayor:

Tabla 15. Criterios para declarar incidentes mayores

Criterio	Descripción	Condición de Incidente Mayor
Impacto académico	Afectación a matrícula, evaluaciones, notas o titulación	Interrupción total o prolongada
Impacto administrativo	Afectación a procesos clave institucionales	Paralización de procesos críticos
Cantidad de usuarios afectados	Número de estudiantes, docentes o administrativos	Más del 30% de usuarios
Duración del incidente	Tiempo sin solución	Mayor a 2 horas en servicios críticos
Seguridad de la información	Riesgo de acceso no autorizado o pérdida de datos	Confirmación o sospecha fundada
Infraestructura crítica	Energía, climatización, servidores	Fallas que comprometen continuidad
Reincidencia	Incidente repetitivo en corto periodo	Más de 3 veces en un mes
Visibilidad institucional	Riesgo reputacional o mediático	Alta exposición pública

La regla práctica para la declaratoria de un incidente mayor es: Si dos o más criterios se cumplen simultáneamente, el incidente debe ser declarado Incidente Mayor por el CIGI-TI.

Flujo del escalamiento propuesto

A continuación, se propone el flujo específico de escalamiento funcional y jerárquico.

1. **Inicio**
   Usuario reporta incidente al Punto Único de Contacto (PUC).
2. **Registro del incidente**
   El Analista de Soporte de Primer Nivel registra el ticket en el sistema ITSM.
3. **Clasificación y priorización**
   Se determina tipo, impacto y urgencia.
4. **¿Puede resolverse en Nivel 1?**
   - **Sí:** Resolver, validar con usuario y cerrar.
   - **No:** Escalar funcionalmente a Nivel 2.
5. **Atención por Nivel 2**
   El especialista técnico analiza y aplica solución.
6. **¿Requiere conocimiento experto o proveedor?**
   - **Sí:** Escalar a Nivel 3.
   - **No:** Continuar resolución.
7. **Evaluación de criticidad**
   El CIGI-TI evalúa si se cumplen criterios de incidente mayor.
8. **¿Es Incidente Mayor?**
   - **Sí:** Activar escalamiento jerárquico, notificar Jefatura OTI y autoridades.
   - **No:** Continuar flujo normal.
9. **Resolución del incidente**
   Se restablece el servicio.
10. **Validación con usuario**
    Confirmación de solución.
11. **Cierre del ticket**
    Registro de métricas (MTTR, FCR) y documentación.
12. **Fin del proceso**

3.3.5. Diseño de los elementos funcionales de la mesa de ayuda

a. Registro estandarizado del incidente

Objetivo del registro estandarizado del incidente

El registro estandarizado del incidente tiene como propósito establecer un mecanismo estandarizado, consistente y obligatorio para la captura de información relacionada con los incidentes de TI que afectan los servicios académicos y administrativos de la UNPRG. Este registro permite documentar

de manera estructurada cada evento reportado, asegurando que la información mínima necesaria esté disponible desde el primer contacto hasta el cierre definitivo del incidente.

Esto contribuye a reducir la informalidad en la atención de incidentes, evita la pérdida de información asociada a comunicaciones verbales o no documentadas y fortalece la gobernanza de los servicios de TI, alineándose con las buenas prácticas de ITIL 4 y con los objetivos del Plan de Gobierno Digital

Así mismo, constituye la base de la trazabilidad del proceso, ya que posibilita el seguimiento cronológico de las acciones realizadas, la identificación de responsables y la evaluación objetiva de los tiempos de atención y resolución. Asimismo, permite generar un histórico confiable de incidentes, indispensable para el análisis de tendencias, la detección de reincidencias y la toma de decisiones orientadas a la mejora continua.

Procedimiento para el registro estandarizado del incidente

El procedimiento de registro estandarizado del incidente se ejecuta como parte del proceso de gestión de incidentes y se desarrolla de la siguiente manera:

1. **Recepción del incidente**

   El incidente es reportado por el usuario a través del Punto Único de Contacto (PUC), utilizando los canales habilitados (plataforma ITSM, correo institucional, teléfono o atención presencial).
2. **Validación inicial de la información.**

   El Técnico de Atención Inicial de Incidentes de Primer Nivel verifica que la información proporcionada por el usuario sea suficiente para identificar el incidente, solicitando aclaraciones cuando sea necesario.
3. **Registro del incidente en el sistema ITSM.**

   El incidente se registra obligatoriamente en el sistema ITSM, utilizando los campos estandarizados definidos por la institución. No se inicia ninguna acción de atención sin el correspondiente registro.
4. **Clasificación y categorización**

El analista asigna el servicio afectado, la categoría del incidente y su nivel de severidad, considerando el impacto y la urgencia sobre los procesos académicos y administrativos.

5. **Asignación y control de tiempos**

   Se registra el tiempo de inicio del incidente y se asigna el responsable de atención, permitiendo el control del tiempo de respuesta y del tiempo total de resolución.

6. **Actualización del registro durante la atención**

   Cada acción relevante (escalamiento, diagnóstico, solución parcial o definitiva) se documenta en el registro del incidente, manteniendo la trazabilidad completa.

7. **Cierre del incidente**

   Una vez restablecido el servicio y validada la solución por el usuario, el incidente se cierra formalmente, registrando la solución aplicada y el tiempo total de atención.

Estructura del registro estandarizado del incidente

La estructura del registro estandarizado del incidente define los campos obligatorios que deben completarse para cada incidente registrado, el cual se muestra a continuación.

Tabla 16. Estructura del Registro estandarizado del incidente

Campo	Descripción
Fecha y hora de registro	Fecha y hora en que el incidente es registrado en el sistema ITSM.
Usuario reportante	Nombre, código o identificación del usuario que reporta el incidente.
Unidad / dependencia	Facultad, escuela, oficina administrativa u otra dependencia afectada.
Servicio afectado	Servicio de TI impactado (SIA, Aula Virtual, Red Telemática, Turnitin, Selgestiun, etc.).
Categoría del incidente	Tipo de incidente (acceso, disponibilidad, rendimiento, seguridad, infraestructura, otros).
Nivel de severidad	Clasificación del incidente según impacto y urgencia (bajo, medio, alto, crítico).
Síntomas observados	Descripción clara de lo que experimenta el usuario al momento del incidente.
Tiempo de respuesta	Tiempo transcurrido desde el registro hasta el inicio de la atención.
Responsable asignado	Nivel de soporte o especialista responsable de la atención del incidente.
Acciones realizadas	Detalle cronológico de las actividades ejecutadas durante la atención.
Solución aplicada	Descripción de la solución implementada para restablecer el servicio.
Fecha y hora de cierre	Momento en que el incidente se considera resuelto y cerrado.
Tiempo total de resolución	Tiempo total transcurrido desde el registro hasta el cierre del incidente.
Estado del incidente	Abierto, en atención, escalado, resuelto o cerrado.
Validación del usuario	Confirmación del usuario respecto a la resolución del incidente.

b. Clasificación de los incidentes

Objetivo de la clasificación de los incidentes

La clasificación de los incidentes según una taxonomía formal tiene como propósito establecer un lenguaje común, estructurado y consistente para identificar, categorizar y gestionar los incidentes de tecnologías de la información que afectan los servicios académicos y administrativos de la UNPRG.

Esta taxonomía permite que cada incidente sea identificado de manera uniforme desde su registro inicial, facilitando su asignación correcta al nivel de soporte correspondiente, la priorización adecuada según su impacto y urgencia, y la aplicación de flujos de escalamiento definidos. Asimismo, constituye un elemento clave para asegurar la trazabilidad del proceso, ya que permite consolidar información histórica confiable para el análisis de tendencias, la identificación de reincidencias y la toma de decisiones orientadas a la mejora continua.

Clasificación inicial de los incidentes

A continuación se propone la clasificación inicial de los incidentes de acuerdo a la categoría de los servicios contemplados en el sistema de gestión de incidentes para la UNPRG:

Tabla 17. Clasificación de incidentes según taxonomía formal – UNPRG

Categoría de servicio	Tipo de incidente	Descripción del incidente	Nivel de atención inicial	Escalamiento funcional esperado
Sistema de Información Académica (SIA)	Disponibilidad	El sistema no permite el acceso o presenta caídas totales durante matrícula o consultas académicas.	Nivel 1	Nivel 2 → Nivel 3
Sistema de Información Académica (SIA)	Rendimiento	Lentitud extrema en consultas, registro de notas o matrícula.	Nivel 1	Nivel 2
Aula Virtual – Moodle	Acceso	Usuarios no pueden ingresar a cursos o evaluaciones.	Nivel 1	Nivel 2
Aula Virtual – Moodle	Funcionalidad	Fallas en evaluaciones, carga de archivos o integración con Turnitin.	Nivel 1	Nivel 2 → Nivel 3
Turnitin	Integración / Servicio externo	No se genera el informe de similitud o queda en estado pendiente.	Nivel 1	Nivel 2 → Nivel 3
Selgestiun	Aplicación	Error al registrar tesis o proyectos de investigación.	Nivel 1	Nivel 2 → Nivel 3
Biblioteca virtual	Acceso	Usuarios no pueden acceder a bases de datos o recursos digitales.	Nivel 1	Nivel 2
Repositorio institucional de investigaciones	Disponibilidad	Indisponibilidad del repositorio o errores en la visualización de documentos.	Nivel 1	Nivel 2
Plataforma de correo institucional	Acceso	Usuarios no pueden enviar o recibir correos institucionales.	Nivel 1	Nivel 2
Sistemas de gestión administrativa (SIAF, tesorería, contabilidad, planillas)	Disponibilidad	Interrupción de procesos administrativos críticos.	Nivel 1	Nivel 2 → Nivel 3
Red Telemática (cableado, switches, antenas)	Conectividad	Caída parcial o total de red en facultades o áreas administrativas.	Nivel 1	Nivel 2 → Nivel 3
Seguridad en la red y las comunicaciones	Seguridad	Intentos de acceso no autorizado, alertas de intrusión o compromisos de cuentas de usuarios.	Nivel 1	Nivel 2 → Nivel 3
Servidores y almacenamiento – físicos	Infraestructura	Caída de servidores, fallas de hardware o saturación de recursos.	Nivel 2	Nivel 3
Servidores y almacenamiento en la nube	Servicio de terceros	Indisponibilidad o degradación de servicios alojados externamente.	Nivel 1	Nivel 2 → Nivel 3
Energía y climatización de sala de servidores	Continuidad operativa	Apagones, variaciones de voltaje o sobrecalentamiento.	Nivel 2	Nivel 3
Equipos de	Hardware	Equipos no operativos	Nivel 1	Nivel 2

Categoría de servicio	Tipo de incidente	Descripción del incidente	Nivel de atención inicial	Escalamiento funcional esperado
laboratorio		que afectan actividades académicas prácticas.		
Equipos terminales de laboratorios de cómputo	Hardware / Software	Fallas de sistema operativo, aplicaciones o periféricos.	Nivel 1	Nivel 2
Equipos terminales de áreas administrativas	Hardware / Software	Equipos no operativos que afectan trámites administrativos.	Nivel 1	Nivel 2
Software académico	Aplicación	Fallas en software especializado utilizado en cursos.	Nivel 1	Nivel 2
Software de ofimática	Aplicación	Errores en herramientas ofimáticas institucionales.	Nivel 1	Nivel 2

c. Priorización de los incidentes

Objetivo de la priorización de los incidentes

La priorización de los incidentes basada en impacto y urgencia tiene como propósito asegurar que los incidentes de tecnologías de la información sean atendidos en un orden coherente con su afectación real a los procesos académicos y administrativos de la UNPRG, y no únicamente por el orden de llegada o por presiones circunstanciales.

La priorización permite asignar los recursos técnicos disponibles de manera racional, garantizando que los incidentes que comprometen servicios críticos, como el Sistema de Información Académica, el Aula Virtual, la Red Telemática o la seguridad de la información, reciban atención inmediata. Asimismo, contribuye a reducir el riesgo institucional, mejorar la continuidad operativa y fortalecer la transparencia del proceso de gestión de incidentes.

Determinación del impacto de los incidentes

Determinar una escala de impacto es fundamental porque permite evaluar de manera objetiva el grado de afectación que un incidente de TI genera sobre los procesos académicos y administrativos de la UNPRG. El impacto mide la magnitud del daño operativo, académico o institucional, considerando factores como el número de usuarios afectados, la criticidad del servicio involucrado y la interrupción de actividades esenciales.

Sin una escala de impacto claramente definida, la atención de incidentes se basa en percepciones subjetivas o en la presión ejercida por los usuarios, lo que puede conducir a decisiones inadecuadas y a la asignación incorrecta de recursos técnicos. La escala de impacto permite homogeneizar los criterios de evaluación entre los distintos niveles de soporte, facilitando la comparación de incidentes y la generación de métricas confiables. Al clasificar los incidentes en niveles predefinidos, la institución puede analizar tendencias, identificar servicios con mayor nivel de afectación y orientar inversiones en infraestructura, seguridad o mejora de procesos. En este sentido, la escala de impacto se convierte en un instrumento clave para la toma de decisiones estratégicas y para la mejora continua de la gestión de servicios de TI.

A continuación se describe la escala para evaluar el impacto de los incidentes de TI:

Tabla 18. Escala para evaluar el impacto de los incidentes de TI – UNPRG

Nivel de impacto	Denominación	Significado
5	Crítico	Interrupción total de servicios institucionales críticos (SIA, matrícula, Aula Virtual, Red Telemática, seguridad digital) que afecta a gran parte de la comunidad universitaria o compromete la integridad de la información académica y administrativa.
4	Alto	Afectación significativa a procesos académicos o administrativos clave, como evaluaciones, emisión de notas, trámites administrativos o servicios de investigación, con impacto en múltiples unidades o facultades.
3	Medio	Interrupción parcial de un servicio que afecta a un grupo específico de usuarios (una facultad, área administrativa o laboratorio), sin paralizar completamente el proceso institucional.
2	Bajo	Incidente que afecta a un número reducido de usuarios o a funcionalidades no críticas, con alternativas temporales disponibles.
1	Mínimo	Incidente menor o consulta técnica que no afecta la continuidad del servicio ni los procesos académicos o administrativos.

Determinación de la urgencia de atención de los incidentes de TI

La escala para evaluar la urgencia es igualmente relevante, ya que permite establecer la rapidez con la que un incidente debe ser atendido, independientemente de su impacto inmediato. La urgencia está asociada al factor tiempo y a la probabilidad de que el incidente escale o genere consecuencias mayores si no se atiende oportunamente.

En la UNPRG, muchos incidentes pueden no tener un impacto crítico en el momento inicial, pero pueden volverse altamente disruptivos si no se resuelven a tiempo, especialmente durante periodos sensibles del calendario académico, como matrícula, evaluaciones parciales o cierre de notas. La tabla de urgencia permite anticipar estos escenarios y asignar prioridad a incidentes que, de prolongarse, podrían comprometer la continuidad de los servicios y la satisfacción de la comunidad universitaria.

Además, la definición de niveles de urgencia evita la atención improvisada y contribuye a una gestión más equitativa y transparente de los incidentes. A continuación, se describe la escala para evaluar la urgencia de atención de los incidentes de TI:

Tabla 19. Escala para evaluar la urgencia de atención del incidente de TI – UNPRG

Nivel de urgencia	Denominación	Significado
5	Inmediata	El incidente debe ser atendido de forma inmediata para evitar la paralización de procesos críticos o daños a la infraestructura, especialmente en periodos sensibles como matrícula, evaluaciones o cierre de notas.
4	Alta	Requiere atención prioritaria en corto plazo, ya que la demora puede escalar el impacto o afectar cronogramas académicos o administrativos.
3	Media	Puede ser atendido en el transcurso de la jornada laboral sin generar consecuencias graves para la operación institucional.
2	Baja	La atención puede programarse sin afectar la continuidad del servicio, manteniendo soluciones temporales.
1	Planificada	No requiere atención inmediata; puede resolverse en un periodo programado o como parte de mantenimiento regular.

Determinación de la priorización de los incidentes de TI

La prioridad del incidente se determina combinando el nivel de impacto y el nivel de urgencia, según la siguiente matriz:

Tabla 20. Escala para determinar la priorización de atención de los incidentes de TI – UNPRG

Impacto \ Urgencia	1 (Planificada)	2 (Baja)	3 (Media)	4 (Alta)	5 (Inmediata)
5 (Crítico)	Media	Alta	Alta	Crítica	Crítica
4 (Alto)	Media	Media	Alta	Alta	Crítica
3 (Medio)	Baja	Media	Media	Alta	Alta
2 (Bajo)	Baja	Baja	Media	Media	Alta
1 (Mínimo)	Baja	Baja	Baja	Media	Media

En la tabla de priorización de los incidentes de TI propuesta, se interpreta que:

- Los incidentes con prioridad **Crítica** activan atención inmediata y pueden derivar en escalamiento jerárquico.
- Los incidentes con prioridad **Alta** se atienden de forma prioritaria por el Nivel 2 – Especialista en Infraestructura y Servicios Digitales.
- Los incidentes con prioridad **Media o Baja** son gestionados por el Nivel 1 – Técnico de Atención Inicial de Incidentes, según disponibilidad y programación.

d. Asignación automática o semiautomática de los incidentes de TI

Objetivo de la asignación automática o semiautomática de los incidentes

La asignación automática o semiautomática de los incidentes tiene como propósito optimizar el tiempo de atención, reducir errores de derivación y asegurar que cada incidente sea atendido por el rol técnico más adecuado desde el inicio. Este mecanismo contribuye a disminuir el Tiempo promedio que se tarda en resolver un incidente (MTTR), incrementar la tasa de Resolución en el Primer Contacto (FCR) y fortalecer la trazabilidad del proceso de gestión de incidentes.

En el contexto de la UNPRG, donde coexisten múltiples servicios críticos (SIA, Aula Virtual, Red Telemática, seguridad, infraestructura y sistemas administrativos), la asignación manual basada en disponibilidad o conocimiento individual (criterio personal) generaría retrasos y variabilidad en la calidad del servicio. La asignación (semi)automática, sustentada en una taxonomía formal, matrices de impacto–urgencia y reglas de escalamiento, permite una atención objetiva, predecible y alineada con ITIL 4.

Procedimiento para la asignación

La asignación debe ejecutarse a través del sistema ITSM integrado al Punto Único de Contacto (PUC), combinando reglas automáticas con validaciones humanas cuando la criticidad lo requiera, bajo la siguiente secuencia operativa:

1. **Registro del incidente** por el Nivel 1 – Técnico de Atención Inicial de Incidentes, con campos estandarizados.

2. **Clasificación automática** por **servicio afectado** y **tipo de incidente** (según la taxonomía propuesta para la UNPRG).
3. **Cálculo de prioridad** mediante la **matriz Impacto × Urgencia**.
4. **Asignación automática** al **Nivel 1** cuando la prioridad lo permita, o **derivación automática** al Nivel 2 – Especialista en Infraestructura y Servicios Digitales según la especialidad.
5. **Validación semiautomática** por el Nivel 1 o el CIGI-TI en casos de prioridad Alta o Crítica.
6. **Escalamiento funcional** automático al **Nivel 3 – Experto en Soluciones Tecnológicas Críticas (proveedores)** cuando se cumplan reglas predefinidas (incidente mayor, dependencia de terceros).
7. **Reasignación controlada** si cambian impacto/urgencia o se detecta una categoría incorrecta.
8. **Registro de eventos de asignación** para trazabilidad y métricas.

Para la asignación se plantean las siguientes reglas:

Tabla 21. Reglas de asignación automática/semiautomática de incidentes de TI – UNPRG

Criterio	Condición	Asignación resultante	Tipo
Servicio afectado	SIA / Moodle / Selgestiun / Turnitin	Especialista por dominio (Aplicaciones)	Automática
Servicio afectado	Red Telemática / Servidores / Seguridad	Especialista en Infraestructura y Servicios Digitales	Automática
Prioridad	Baja o Media	Nivel 1 – Técnico de Atención Inicial de Incidentes	Automática
Prioridad	Alta	Nivel 2 – Especialista correspondiente	Semiautomática (validación N1)
Prioridad	Crítica	Nivel 2 + notificación CIGI-TI	Semiautomática (control)
Incidente mayor	≥ 2 criterios de incidente mayor	Activación Nivel 3 (proveedores)	Automática (regla)
Dependencia externa	Servicio de terceros (nube, Turnitin)	Nivel 3 – Proveedor	Automática
Reincidencia	≥ 3 veces/mes mismo servicio	Nivel 2 + alerta CIGI-TI	Semiautomática
Cambio de severidad	Aumento impacto/urgencia	Reasignación al nivel superior	Automática

e. Resolución documentada y estandarizada

Propósito de la resolución documentada y estandarizada

La resolución documentada y estandarizada tiene como propósito asegurar que todo incidente atendido deje evidencia técnica clara, reutilizable y verificable, evitando soluciones improvisadas, dependientes del conocimiento individual o difíciles de replicar. Este permite transformar cada incidente resuelto en conocimiento institucional, fortaleciendo la continuidad operativa y la mejora continua del proceso de gestión de incidentes.

En el contexto de la UNPRG, donde servicios críticos como el SIA, el Aula Virtual, la Red Telemática y los sistemas administrativos sostienen procesos académicos sensibles, documentar de manera uniforme la resolución de incidentes es clave para reducir reincidencias, disminuir el MTTR y aumentar el FCR.

Proceso propuesto de resolución documentada

1. **Ejecución de la solución**
   El nivel de soporte que resuelve el incidente (N1, N2 o N3) aplica la solución técnica conforme a procedimientos, checklists o experiencia especializada.
2. **Registro de la resolución en el sistema ITSM**
   La solución se documenta obligatoriamente en el ticket, utilizando campos estandarizados.
3. **Clasificación de la resolución**
   Se identifica si la solución corresponde a:
   - Incidente simple (FAQ o guía rápida)
   - Incidente recurrente (artículo de solución)
   - Incidente crítico (procedimiento formal).
4. **Validación técnica**
   - Resoluciones N1: validadas por N2 cuando sean nuevas o no documentadas.
   - Resoluciones N2/N3: validadas por el Responsable del Proceso de Gestión de Incidentes (CIGI-TI).
5. **Publicación en la Base de Conocimientos**
   Las resoluciones validadas se incorporan o actualizan como artículos de la Base de Conocimientos.

6. **Cierre del incidente**

   El incidente se cierra solo cuando:

   - El servicio ha sido restaurado.
   - La solución ha sido documentada.
   - El usuario confirma la conformidad (cuando aplique).

Estructura estandarizada de la resolución del incidente

Toda resolución debe registrarse utilizando la siguiente estructura mínima:

Tabla 22. Estructura estandarizada del registro de resolución de incidentes

Campo	Descripción
ID del incidente	Código único asignado al ticket para su identificación y trazabilidad.
Servicio afectado	Servicio impactado por el incidente (SIA, Aula Virtual, Red Telemática, Correo institucional, etc.).
Tipo de incidente	Clasificación del incidente según su naturaleza (disponibilidad, acceso, rendimiento, seguridad, entre otros).
Síntomas observados	Manifestación concreta del problema reportado por el usuario o detectado por monitoreo.
Causa raíz identificada	Origen del incidente identificado durante el análisis (técnica, operativa o externa), cuando aplique.
Acciones realizadas	Conjunto de pasos ejecutados por el personal de soporte para atender el incidente.
Solución final aplicada	Acción específica que permitió restablecer el servicio afectado.
Nivel de soporte	Nivel que resolvió el incidente: N1, N2 o N3.
Tiempo total de resolución	Tiempo transcurrido desde el registro hasta la solución del incidente; insumo para el cálculo del MTTR.
Estado final	Situación del incidente al cierre del ticket (Resuelto o Cerrado).
Referencia a KB	Código o enlace del artículo de la Base de Conocimientos generado o actualizado a partir del incidente.

f. Cierre formal del incidente

Propósito del cierre formal del incidente

El cierre formal del incidente constituye la última etapa del proceso de gestión de incidentes propuesto y tiene como propósito asegurar que el servicio afectado haya sido restablecido de manera efectiva, que la solución aplicada esté debidamente documentada y que exista conformidad por parte del usuario. Este cierre formal evita la reapertura innecesaria de incidentes, garantiza la trazabilidad del proceso y consolida el aprendizaje institucional a través de la Base de Conocimientos.

El cierre formal adquiere especial relevancia debido al impacto que los incidentes de TI tienen sobre procesos académicos críticos como matrícula,

evaluaciones, registro de notas, trámites administrativos y actividades de investigación. Un cierre no formalizado genera incertidumbre operativa, dificulta el análisis de métricas y debilita la gobernanza de los servicios de TI.

Condiciones obligatorias para el cierre del incidente

Un incidente podrá cerrarse formalmente únicamente cuando se cumplan todas las siguientes condiciones:

1. El servicio afectado ha sido restablecido y verificado.
2. La solución aplicada ha sido registrada en el sistema ITSM.
3. El nivel de soporte responsable ha documentado la causa y la solución.
4. El usuario ha confirmado la conformidad o se ha cumplido el tiempo de validación definido.
5. Se ha vinculado el incidente con un artículo de la Base de Conocimientos, si aplica.

Procedimiento propuesto de cierre formal

1. **Validación técnica de la solución**
   El nivel de soporte que resolvió el incidente verifica que el servicio opere correctamente y sin errores.
2. **Registro completo de la resolución**
   Se completa el formato estandarizado de resolución en el ticket, incluyendo tiempos, acciones y solución final.
3. **Confirmación del usuario**
   El usuario recibe una notificación de solución y dispone de un plazo definido para confirmar la conformidad.
4. **Actualización de la Base de Conocimientos**
   Si el incidente fue recurrente o relevante, se crea o actualiza el artículo correspondiente en la KB.
5. **Cierre del incidente en el sistema ITSM**
   El **Nivel 1 – Técnico de Atención Inicial de Incidentes** realiza el cierre formal, dejando evidencia documental.
6. **Seguimiento post-cierre (cuando aplique)**
   En incidentes críticos o mayores, el Responsable del Proceso de Gestión de Incidentes (CIGI-TI) revisa el cierre.

Roles involucrados en el cierre

- Nivel 1 – Técnico de Atención Inicial de Incidentes: ejecuta el cierre formal y comunica al usuario.
- Nivel 2 – Especialista en Infraestructura y Servicios Digitales: valida soluciones técnicas complejas.
- Nivel 3 – Experto en Soluciones Tecnológicas Críticas: certifica la resolución en incidentes mayores.
- Responsable del Proceso de Gestión de Incidentes (CIGI-TI): supervisa cierres críticos y métricas.

Criterios de reapertura del incidente

Un incidente puede ser reabierto porque el cierre formal no siempre garantiza que la solución aplicada haya sido efectiva, definitiva o sostenible en el tiempo, especialmente en entornos tecnológicos complejos como el de la UNPRG. La reapertura se justifica cuando el servicio afectado vuelve a presentar fallas dentro del periodo de validación, cuando el usuario confirma que el problema persiste o cuando se evidencia que la causa raíz no fue correctamente identificada ni tratada. Asimismo, un incidente puede reabrirse si durante una revisión posterior se detecta documentación incompleta, datos incorrectos en el registro o una solución aplicada de manera parcial.

Desde la perspectiva de ITIL 4, la reapertura es un mecanismo de control de calidad que protege la continuidad de los servicios académicos y administrativos, asegura la confiabilidad de las métricas (como MTTR y FCR) y evita que se consoliden cierres formales que no reflejan la realidad operativa del servicio.

Las condiciones que se proponen para que un incidente cerrado pueda reabrirse son:

1. El servicio vuelve a fallar dentro del periodo de validación.
2. El usuario reporta que la solución no fue efectiva.
3. Se detecta información incompleta o incorrecta en la documentación.

g. Generación de métricas e informes periódicos

La generación de métricas e informes periódicos tiene como propósito medir el desempeño real del proceso de gestión de incidentes propuesto, identificar tendencias, anticipar riesgos operativos y respaldar decisiones técnicas y de gestión. En una universidad pública como la UNPRG, donde los servicios digitales sostienen procesos críticos (matrícula, evaluación, registro académico, investigación y gestión administrativa), las métricas permiten pasar de una operación reactiva a una gestión basada en evidencia.

Las métricas que se proponen medir, son las siguientes:

Tabla 23. Métricas operativas

Indicador	Fórmula	Periodicidad	Responsable
MTTR por servicio y prioridad	Σ (Tiempo de resolución de incidentes) / Nº de incidentes resueltos (segmentado por servicio y prioridad)	Mensual	Responsable del Proceso de Gestión de Incidentes (CIGI-TI)
FCR del PUC	(Incidentes resueltos en primer contacto / Total de incidentes) × 100	Mensual	Nivel 1 – Técnico de Atención Inicial de Incidentes
Volumen de incidentes por categoría y tipo	Conteo de incidentes por categoría de servicio y tipo de incidente	Semanal / Mensual	CIGI-TI
Cumplimiento de SLA por prioridad	(Incidentes resueltos dentro del SLA / Total de incidentes) × 100	Mensual	Jefatura OTI / CIGI-TI
Reaperturas de incidentes	(Incidentes reabiertos / Incidentes cerrados) × 100 + análisis de causas	Mensual	CIGI-TI

Tabla 24. Métricas de calidad

Indicador	Fórmula	Periodicidad	Responsable
Satisfacción del usuario post-cierre	Promedio de puntuación de encuestas post-cierre	Mensual	Nivel 1 – Técnico de Atención Inicial de Incidentes
Incidentes recurrentes por servicio	Conteo de incidentes repetidos (≥ 2 o 3 veces en el periodo) por servicio	Mensual	CIGI-TI
Efectividad de la Base de Conocimientos (KB)	(Consultas a KB + Artículos creados/actualizados) por periodo	Mensual	Nivel 2 – Especialista en Infraestructura y Servicios Digitales

Tabla 25. Métricas de riesgos y continuidad

Indicador	Fórmula	Periodicidad	Responsable
Incidentes mayores	Conteo de incidentes mayores + duración total + impacto reportado	Trimestral	CIGI-TI / Jefatura OTI
Eventos de seguridad	Conteo de intentos/bloqueos + tiempo de contención promedio	Mensual / Trimestral	Especialista en Seguridad Digital
Disponibilidad de servicios críticos en periodos sensibles	(Tiempo total – Tiempo de indisponibilidad) / Tiempo total × 100	Trimestral	CIGI-TI

h. Comunicación proactiva con usuarios

La comunicación proactiva con los usuarios tiene como propósito anticipar impactos, reducir la incertidumbre y mejorar la percepción del servicio antes, durante y después de la ocurrencia de incidentes de TI. En la UNPRG, donde los servicios digitales sostienen actividades críticas (matrícula, evaluaciones, investigación y trámites administrativos), informar oportunamente es tan importante como resolver técnicamente el incidente.

El mecanismo de comunicación que se propone contempla los siguientes momentos:

1. **Prevención**
   Alertas por alta demanda (matrícula, evaluaciones), mantenimientos programados, riesgos identificados (energía, climatización).
2. **Detección del incidente**
   Aviso inmediato cuando un servicio crítico presenta indisponibilidad o degradación.
3. **Atención y seguimiento**
   Actualizaciones periódicas del estado del incidente, especialmente en incidentes mayores.
4. **Restablecimiento y cierre**
   Confirmación de la restauración del servicio y recomendaciones post-incidente.
5. **Aprendizaje**
   Difusión de buenas prácticas y guías de autogestión desde la Base de Conocimientos.

Los canales oficiales de comunicación serían:

1. Correo institucional (principal).
2. Avisos en SIA y Aula Virtual a través de banners informativos.
3. Portal institucional / Intranet para comunicar el estado de los servicios.
4. Mesa de Ayuda (PUC) a través de notificaciones automáticas del ITSM.

Los tipos de mensajes que aplicarías serían:

- Alertas técnicas preventivas previas a periodos críticos.
- Avisos de indisponibilidad cuando se inició un incidente.
- Actualizaciones de estado que informa sobre el progreso y tiempos estimados de solución.
- Avisos de restablecimiento cuando se cierra el incidente.
- Recomendaciones y guías con enlaces a la Base de Conocimientos.

DISCUSIÓN DE RESULTADOS

Los resultados obtenidos en el desarrollo de la presente tesis evidencian que la situación diagnosticada en la Universidad Nacional Pedro Ruiz Gallo (UNPRG) guarda una estrecha relación con los problemas identificados en investigaciones previas desarrolladas tanto en contextos universitarios como en entidades públicas y privadas. En particular, la ausencia de un proceso formal de gestión de incidentes, la dependencia del conocimiento individual del personal técnico y la inexistencia de herramientas ITSM coinciden con los hallazgos en estudios nacionales e internacionales que sirvieron como antecedentes de esta investigación.

Desde la perspectiva de la Gestión de Servicios de TI (ITSM), los resultados confirman que la gestión de incidentes no puede abordarse únicamente como una actividad operativa aislada, sino como un proceso transversal que debe alinearse con los objetivos institucionales. Tal como señalan Trinidad et al. (2021), ITSM constituye un enfoque basado en procesos orientado a apoyar los objetivos del negocio, lo que se refleja claramente en el contexto universitario, donde la indisponibilidad de servicios como el Sistema de Información Académica, el Aula Virtual o los sistemas administrativos impacta directamente en la matrícula, la evaluación académica y la gestión institucional.

La propuesta desarrollada en la tesis, centrada en un modelo de gestión de incidentes basado en ITIL 4, se sustenta teóricamente en el Service Value System (SVS) y en la práctica de Incident Management, lo que resulta coherente con los planteamientos de Axelos (2020) y Agutter (2020). Los resultados del diagnóstico muestran que la UNPRG carece de elementos estructurales básicos del SVS, tales como flujos de valor definidos, roles formalizados, métricas e integración con la mejora continua, situación que ya había sido identificada en estudios como el de Nugroho y Fianty (2023), donde la falta de documentación y de niveles de servicio formalizados limita la eficacia de la gestión de incidentes.

Al contrastar los resultados con antecedentes nacionales, se observa una fuerte similitud con investigaciones desarrolladas en universidades públicas peruanas, como el estudio realizado en la Universidad Nacional de Moquegua, donde se evidenció que la ausencia de un modelo ITIL provocaba tiempos elevados de resolución y una baja eficacia del

servicio. Al igual que en dicho estudio, la presente tesis demuestra que la formalización de procesos, roles y flujos constituye un factor crítico para mejorar el desempeño de los servicios de TI, aun cuando no se implemente inmediatamente el modelo propuesto.

En relación con la mesa de ayuda, los resultados obtenidos refuerzan su rol como elemento habilitador clave del proceso de gestión de incidentes. La inexistencia de un Punto Único de Contacto en la UNPRG reproduce las debilidades descritas por Mahardika (2022) y Dzemydienė et al. (2024), quienes señalan que sin un service desk centralizado se pierde trazabilidad, se fragmenta la atención y se deteriora la percepción del servicio. La propuesta de una Mesa de Ayuda estructurada, con niveles de soporte claramente definidos (N1, N2 y N3), responde directamente a estas brechas y se alinea con los modelos exitosos descritos en los antecedentes analizados.

Asimismo, los resultados relacionados con la clasificación, priorización y escalamiento de incidentes coinciden con la literatura reciente que enfatiza la necesidad de criterios formales basados en impacto y urgencia. Tal como indica Axelos (2020), la priorización adecuada es esencial para minimizar el impacto en el negocio, mientras que estudios aplicados en entornos educativos muestran que la ausencia de reglas claras genera atención desordenada y prolonga los tiempos de resolución. En este sentido, la matriz de impacto–urgencia propuesta en la tesis constituye una respuesta directa a las debilidades detectadas y se encuentra alineada con las buenas prácticas descritas por Dzemydienė et al. (2024).

Un aspecto relevante es la integración de la gestión de incidentes con la seguridad digital. Los resultados del análisis de riesgos evidencian vulnerabilidades significativas en la UNPRG, situación que concuerda con lo planteado por Sekti (2025), quien sostiene que la seguridad de la información se ha convertido en un componente inseparable de la gestión moderna de servicios de TI. La propuesta de integrar incident management con procesos de seguridad digital no solo responde a los hallazgos empíricos, sino que también se encuentra sólidamente respaldada por el marco teórico de ITIL 4 y por estudios recientes sobre ciberseguridad y continuidad operativa.

Finalmente, la incorporación de métricas e indicadores como MTTR, FCR, cumplimiento de SLA e incidentes mayores permite discutir los resultados desde una perspectiva de

mejora continua. Tal como señalan Cadena et al. (2020) y Najjarpour et al. (2025), lo que no se mide no puede mejorarse. En concordancia con estos planteamientos, la tesis demuestra que la UNPRG carece actualmente de información confiable para evaluar su desempeño en la gestión de incidentes, lo que refuerza la pertinencia de la propuesta de métricas como soporte a la toma de decisiones tácticas y estratégicas.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El análisis de la atención actual de incidentes evidenció que la gestión se realiza de manera reactiva, informal y poco estandarizada, basada principalmente en comunicaciones directas, llamadas o mensajes sin un registro estructurado. Al contrastar esta situación con las buenas prácticas de ITIL 4, se concluye que la UNPRG presenta brechas significativas en aspectos clave como el registro uniforme de incidentes, la priorización basada en impacto y urgencia, el escalamiento funcional y jerárquico, y la medición del desempeño. Estas brechas limitan la capacidad institucional para controlar, evaluar y mejorar de forma sistemática la atención de incidentes de TI.

2. La identificación de problemas y debilidades permitió concluir que los procesos académicos y administrativos de la UNPRG son altamente dependientes de servicios digitales críticos y, por tanto, vulnerables a fallas en la gestión de incidentes. Entre las principales debilidades se encuentran la ausencia de procedimientos formales, la infraestructura tecnológica con riesgos operativos, las vulnerabilidades de seguridad digital, la falta de herramientas de soporte y la dependencia del conocimiento individual del personal técnico. Estas condiciones generan impactos directos en actividades sensibles como matrícula, evaluación académica, registro de notas, gestión de investigación y trámites administrativos, afectando la eficiencia institucional y la percepción del servicio por parte de los usuarios.

3. El diseño de los elementos funcionales y estructurales de la mesa de ayuda permitió concluir que la implementación de un Punto Único de Contacto, con roles y niveles de soporte claramente definidos, constituye un componente esencial para ordenar y profesionalizar la atención de incidentes en la UNPRG. La propuesta de una mesa de ayuda estructurada, alineada con ITIL 4, facilita el registro, la clasificación, el seguimiento y el cierre formal de los incidentes, además de mejorar la comunicación con los usuarios. Asimismo, se concluye que la mesa de ayuda actúa como un habilitador clave para la generación de métricas, la gestión del conocimiento y la mejora continua del servicio.

4. La definición de reglas formales de categorización y priorización permitió concluir que la atención eficiente de incidentes requiere criterios claros y consistentes basados en el impacto y la urgencia. La ausencia de estas reglas en la situación actual genera atención desordenada y uso ineficiente de los recursos técnicos. Las propuestas de taxonomía de incidentes y la matriz de priorización desarrolladas en la investigación permiten establecer niveles de atención diferenciados, asegurar la asignación oportuna de recursos y reducir los tiempos de resolución, contribuyendo a la continuidad de los servicios críticos de la universidad.

5. El establecimiento de flujos de trabajo coherentes con ITIL permitió concluir que la formalización del proceso de gestión de incidentes es indispensable para garantizar la trazabilidad y el control del servicio. Los flujos propuestos, que abarcan desde el registro del incidente hasta su cierre formal, incorporan etapas de validación, escalamiento, documentación y retroalimentación que actualmente no se aplican de manera sistemática en la UNPRG. En consecuencia, se concluye que la adopción de flujos alineados con ITIL 4 fortalece la gobernanza de TI, mejora la coordinación entre áreas técnicas y proporciona una base sólida para la mejora continua del proceso.

6. La investigación permitió desarrollar una propuesta de modelo de gestión de incidentes de tecnologías de la información basado en las buenas prácticas del marco referencial ITIL, orientada a fortalecer el soporte de los servicios de TI en la Universidad Nacional Pedro Ruiz Gallo. El modelo propuesto responde de manera estructurada a las necesidades institucionales identificadas, integrando procesos, roles, flujos, métricas y mecanismos de comunicación que actualmente no se encuentran formalizados. Asimismo, la propuesta demuestra que la adopción de ITIL 4, aun en un enfoque descriptivo–propositivo, constituye una alternativa viable para mejorar la continuidad operativa, la trazabilidad y la calidad de los servicios digitales que sostienen los procesos académicos y administrativos de la universidad.

Recomendaciones

1. Desarrollar estudios de tipo aplicado o cuasi experimental que permitan implementar de manera piloto el modelo de gestión de incidentes basado en ITIL 4 en una o más unidades académicas o administrativas de la UNPRG. Este tipo de estudio permitiría medir empíricamente el impacto del modelo en indicadores como MTTR, FCR,

satisfacción del usuario y disponibilidad de servicios críticos, generando evidencia cuantitativa que complemente el enfoque descriptivo–propositivo de la presente investigación.

2. Ampliar el alcance de futuras investigaciones hacia la integración del proceso de gestión de incidentes con otras prácticas de ITIL 4, tales como la gestión de problemas, la gestión de cambios, la gestión de activos y la continuidad del servicio. Este enfoque permitiría analizar cómo la madurez de la gestión de incidentes propuesta influye en la reducción de incidentes recurrentes, en la estabilidad de la infraestructura tecnológica y en la mejora global de la gestión de servicios de TI en el contexto universitario.

3. Desarrollar estudios que analicen el impacto organizacional, cultural y de competencias del personal ante la adopción de un modelo de gestión de incidentes basado en ITIL. Este tipo de investigación permitiría identificar factores de resistencia al cambio, necesidades de capacitación y estrategias de gestión del cambio que faciliten la sostenibilidad del modelo en el tiempo, especialmente en instituciones públicas de educación superior como la UNPRG.

REFERENCIAS CONSULTADAS

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

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.

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

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].

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].

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

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

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. Cuestionario para entrevista semiestructurada

Unidad de análisis:
Dirigido a personal de la Oficina de Tecnologías de la Información (OTI) en la UNPRG

Propósito del cuestionario:
Recolectar información sobre cómo se gestionan actualmente los incidentes de TI en la UNPRG, identificando brechas con respecto a ITIL 4.

Objetivo de la investigación:
Desarrollar una propuesta de modelo de gestión de incidentes de tecnologías de la información basado en las buenas prácticas del marco referencial ITIL como soporte a los servicios de tecnologías de la información en la Universidad Nacional Pedro Ruiz Gallo

Cuestionario para entrevista semiestructurada (Guía de preguntas)

1. ¿Qué tipos de incidentes son los más frecuentes en los servicios de TI de la universidad?
2. ¿Existe actualmente un procedimiento formal para registrar y atender incidentes? Descríbalo.
3. ¿Cómo se asignan los incidentes a los responsables de su atención?
4. ¿Se aplican criterios de clasificación y priorización? ¿Cuáles?
5. ¿Existe una mesa de ayuda o punto único de contacto con los usuarios? ¿Cómo opera?
6. ¿Se cuenta con niveles de soporte definidos? Explique.
7. ¿Cómo se maneja el escalamiento funcional y/o jerárquico?
8. ¿Qué herramientas se usan para registrar, monitorear o resolver incidentes?
9. ¿Qué dificultades o limitaciones identifica en el proceso actual?
10. ¿Qué aspectos considera esenciales para mejorar la gestión de incidentes en la UNPRG?

Anexo 2. Guía de revisión documental

Unidad de análisis:
Para analizar reglamentos, manuales, lineamientos institucionales y evidencias de procesos relacionados a la gestión de incidentes de TI en la UNPRG

Propósito de la guía de revisión documental:
Identificar el nivel de formalización del proceso actual de gestión de incidentes de TI y su alineación con ITIL 4.

Objetivo de la investigación:
Desarrollar una propuesta de modelo de gestión de incidentes de tecnologías de la información basado en las buenas prácticas del marco referencial ITIL como soporte a los servicios de tecnologías de la información en la Universidad Nacional Pedro Ruiz Gallo

Criterios de revisión

Categoría revisada	Aspectos a revisar	Hallazgos esperados
Procedimientos de TI	¿Existe un procedimiento formal de gestión de incidentes? ¿Contiene fases, roles y flujos?	Identificación de brechas de formalización.
Manual de organización y funciones (MOF)	Roles relacionados con TI, soporte, servicio al usuario	Determinar claridad de funciones.
Reglamentos o lineamientos de sistemas	Criterios para atención de incidentes, tiempos, categorías	Evaluar consistencia con ITIL.
Reportes de incidentes	Tipo de incidentes, frecuencia, tiempos de atención	Hallar patrones y carencias en registro o trazabilidad.
Herramientas TI (documentación técnica)	Uso de software de tickets, monitoreo, base de conocimiento	Identificar el nivel de soporte tecnológico actual.

Anexo 3. Matriz comparativa ITIL 4 vs. Situación actual

Propósito de la matriz comparativa:
Determinar brechas entre las prácticas reales de la UNPRG y los componentes requeridos por ITIL 4 “Incident Management”.

Objetivo de la investigación:
Desarrollar una propuesta de modelo de gestión de incidentes de tecnologías de la información basado en las buenas prácticas del marco referencial ITIL como soporte a los servicios de tecnologías de la información en la Universidad Nacional Pedro Ruiz Gallo

Elemento de ITIL 4 Gestión de incidentes	Descripción según ITIL 4	Situación actual en la UNPRG	Brecha identificada
Registro de incidentes	Todos los incidentes deben ser registrados de manera estructurada y en un repositorio centralizado.	¿Se registra siempre? ¿Existen formatos?	Sí / No / Parcial
Punto único de contacto (Mesa de Ayuda)	Existe un *Single Point of Contact* para recepción, registro y seguimiento de incidentes.	¿Existe un único punto de contacto para la recepción, registro y seguimiento de incidentes?	Parcial / Informal / Sin procedimientos
Clasificación de incidentes	Debe existir una taxonomía formal basada en tipo, categoría y subcategoría.	¿Hay categorías formales?	Ausente / Incompleta / Adecuada
Priorización de incidentes	La priorización debe basarse en matrices de impacto y urgencia predefinidas.	¿Se usan criterios?	Brecha en criterios o matriz inexistente
Niveles de soporte (1°, 2°, 3°)	Deben estar definidos los niveles de soporte y los roles asociado a cada nivel, de manera clara	¿Están definidos los niveles de soporte y los roles asociado a cada nivel?	Sí / No / Parcial
Escalamiento funcional	Debe existir ruta jerárquica para incidentes de alto impacto (Major Incidents).	¿Hay niveles definidos?	Identificar y describir niveles o de roles
Escalamiento jerárquico	Debe documentarse la solución para retroalimentar la base de conocimiento.	¿Existe? ¿En qué casos?	Ausente / Poco formalizado / Formalizado
Resolución de incidentes	Debe documentarse la solución para retroalimentar la base de conocimiento.	¿Se documentan soluciones?	Ausente / Poco formalizado / Formalizado
Cierre de incidentes	ITIL exige confirmación del usuario y cierre formal con registro del resultado	¿Se realiza cierre formal?	Inexistente / Parcial / Es formal
Monitoreo y alertas	Deben existir herramientas proactivas de monitoreo y alertas tempranas.	¿Se utilizan herramientas para el monitoreo centralizado y gestión de alertas?	Sí / No / Parcial
Herramientas ITSM	ITIL recomienda	¿Se utilizan	Sí / No / Informal

	herramientas ITSM para registrar, priorizar, monitorear y reportar.	herramientas ITSM para registrar, priorizar, monitorear y reportar?	
Métricas	ITIL establece indicadores clave para evaluar eficiencia del proceso.	¿Se han establecido y se generan indicadores para evaluar la gestión de incidentes?	Sí / No / Informal
Roles y responsabilidades	Roles deben definirse claramente en el MOF y en el procedimiento.	¿Se ha definido los roles y responsabilidades del proceso de gestión de incidentes en la UNPRG?	Sí / No / Informal
Documentación del proceso	Debe existir documentación del proceso, flujos, roles y protocolos.	¿Existe un documento formal debidamente aprobado y comunicado sobre la gestión de incidentes de TI?	Ausente / Poco formalizado / Formalizado
Gestión de incidentes de seguridad	ITIL sugiere coordinación con Security Management y SGSI.	¿Se gestionan los incidentes de seguridad de la información? ¿La gestión de incidentes de seguridad de la información, están incorporados a la gestión de incidentes de TI?	Ausente / Poco formalizado / Formalizado

Anexo 4. Perfiles de puesto propuestos para cada nivel de asignación de los incidentes de TI

A continuación se presentan los perfiles sugeridos para cada nivel de asignación de los incidentes de TI. Estos perfiles se basan en las competencias requeridas para cada nivel dentro de la Mesa de Ayuda y el proceso de gestión de incidentes.

Perfil de puesto para Nivel 1: Técnico de Atención Inicial de Incidentes

a. **Dependencia orgánica:**
   Oficina de Tecnologías de la Información (OTI)

b. Propósito del puesto:
   Brindar atención inicial a los usuarios, registrar y clasificar incidentes en el PUC, realizar diagnóstico básico, resolver incidentes frecuentes y garantizar la trazabilidad del proceso.

c. Funciones principales:
- Registrar todos los incidentes en el sistema ITSM.
- Aplicar clasificación y priorización según criterios institucionales.
- Intentar resolución inmediata (FCR) siguiendo la base de conocimientos.
- Mantener comunicación activa con los usuarios.
- Derivar incidentes complejos al Nivel 2.
- Documentar soluciones comunes para fortalecer la base de conocimientos.

d. Competencias requeridas:
- Conocimientos básicos en TI: hardware, software, sistemas institucionales.
- Manejo de sistemas de tickets.
- Comunicación clara y trato amable con estudiantes, docentes y administrativos.
- Capacidad para trabajar bajo presión en periodos críticos (matrícula, cierre de notas).
- Orden, claridad documental y orientación al usuario.

Perfil de puesto para Nivel 2: Especialista en Infraestructura y Servicios Digitales

a. Dependencia orgánica:

Oficina de Tecnologías de la Información (OTI)

b. Propósito del puesto:

Atender incidentes que requieren conocimiento técnico especializado y asegurar el funcionamiento estable de servicios críticos como SIA, Aula Virtual, Turnitin, Selgestiun, Sistemas de gestión administrativa (SIAF, tesorería, contabilidad y planillas), Red Telemática y servidores institucionales.

c. Funciones principales:

- Atender incidentes escalados desde Nivel 1.
- Realizar diagnósticos técnicos y análisis de raíces causales.
- Gestionar incidentes complejos relacionados con infraestructura, seguridad o aplicaciones.
- Documentar soluciones técnicas avanzadas en la base de conocimientos.
- Identificar mejoras y vulnerabilidades recurrentes.
- Coordinar con el Nivel 3 para incidentes fuera del alcance técnico interno.

d. Competencias requeridas:

- Conocimiento avanzado en redes, servidores, bases de datos o aplicaciones.
- Capacidad para resolver problemas de alta complejidad.
- Manejo de herramientas de monitoreo, logs, diagnósticos avanzados.
- Habilidad para trabajar colaborativamente con especialistas de otras áreas.
- Orientación a análisis y mejora continua.

Perfil de puesto para Nivel 3: Experto en soluciones tecnológicas críticas (proveedores)

a. Dependencia orgánica:

Coordinación con la OTI y proveedores autorizados.

b. Propósito del puesto:

Resolver incidentes mayores, estructurales o críticos que superan la capacidad del Nivel 2, incluyendo problemas de seguridad, integridad de datos, desarrollo o configuración avanzada.

c. Funciones principales:

- Brindar soporte especializado en incidentes críticos del SIA, redes, firewall, seguridad o aplicaciones.
- Implementar soluciones definitivas, aplicar parches o corregir errores de software.
- Atender incidentes mayores declarados por la institución.
- Coordinar con alta dirección y responsables de procesos.
- Documentar soluciones estratégicas para prevenir recurrencias.

d. Competencias requeridas:

- Dominio profundo del área técnica (p. ej., seguridad, programación del SIA, arquitectura de red).
- Capacidad para resolver incidentes de alto riesgo.
- Conocimiento de estándares de seguridad y continuidad operativa.
- Habilidad para coordinar con directivos y proveedores.
- Liderazgo técnico y pensamiento estratégico.

Anexo 5. Directiva para la Gestión de Incidentes de Tecnologías de la Información en la Universidad Nacional Pedro Ruiz Gallo

1. FINALIDAD

La presente Directiva tiene por finalidad establecer el marco normativo, organizativo y operativo para la **Gestión de Incidentes de Tecnologías de la Información** en la Universidad Nacional Pedro Ruiz Gallo, con el objetivo de garantizar la continuidad, calidad y seguridad de los servicios tecnológicos que soportan los procesos académicos y administrativos, en concordancia con las buenas prácticas del marco ITIL 4 y los lineamientos del Plan de Gobierno Digital institucional.

2. BASE LEGAL

- Ley Universitaria N.° 30220.
- Lineamientos de Gobierno y Transformación Digital del Estado Peruano (SEGDI – PCM).
- Plan de Gobierno Digital de la UNPRG 2024–2026.
- Resolución que aprueba el Mapa de Procesos de la UNPRG (2022).
- ITIL 4 – Practice: Incident Management.

3. ÁMBITO DE APLICACIÓN

La presente Directiva es de cumplimiento obligatorio para:

- La Oficina de Tecnologías de la Información (OTI).
- Estudiantes, docentes y personal administrativo de la UNPRG.
- Proveedores externos que brinden soporte a servicios tecnológicos institucionales.

4. DEFINICIONES

Incidente: Interrupción no planificada o reducción de la calidad de un servicio de TI.

Mesa de Ayuda: Unidad operativa encargada de la atención de incidentes y solicitudes.

Punto Único de Contacto (PUC): Canal institucional exclusivo para el registro y seguimiento de incidentes.

Incidente Mayor: Incidente de alto impacto que afecta procesos académicos o administrativos críticos.

ITSM: Gestión de Servicios de Tecnologías de la Información.

5. ROLES Y RESPONSABILIDADES

5.1. Coordinador Institucional de Gestión de Incidentes de TI (CIGI-TI)

Responsable de supervisar el proceso, coordinar escalamiento, analizar métricas y emitir informes.

5.2. Técnico de Atención Inicial de Incidentes – PUC (Nivel 1)

Encargado del registro, clasificación, priorización y resolución inicial de incidentes.

5.3. Especialista en Infraestructura y Servicios Digitales (Nivel 2)

Responsable de resolver incidentes técnicos especializados.

5.4. Consultor experto en soluciones tecnológicas críticas (Nivel 3)

Interviene en incidentes complejos o estructurales.

6. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

El proceso de gestión de incidentes comprende las siguientes fases:

1. **Registro del incidente** a través del PUC.
2. **Clasificación** según taxonomía institucional.
3. **Priorización** basada en impacto y urgencia.
4. **Asignación** al nivel de soporte correspondiente.
5. **Resolución** del incidente.
6. **Escalamiento funcional o jerárquico**, de ser necesario.
7. **Cierre formal** con validación del usuario.

7. MÉTRICAS Y SEGUIMIENTO

El proceso será evaluado mediante indicadores como:

a. MTTR (Tiempo Promedio de Resolución).
b. FCR (First Contact Resolution).
c. Volumen de incidentes por servicio.
d. Tasa de reincidencia.

Los informes serán emitidos de forma mensual y trimestral.

8. DISPOSICIONES FINALES

La OTI es responsable de la difusión, actualización y cumplimiento de la presente Directiva.

La Directiva entra en vigencia a partir del día siguiente de su aprobación.