TRABAJO DE GRADO

Opción Seminario-Diplomado

Implementación de un modelo de Outsourcing inteligente para la gestión de servicios TIC mediante GLPI

Corporación Universitaria Remington

Facultad de Ingenierías

Ingeniería de Sistemas

David Arturo Ruiz Chanchi

Jorge Mauricio Sepúlveda Castaño

Opción de Trabajo de grado Seminario-Diplomado

2026

Dedicatoria

Dedico este trabajo a mi familia, por su apoyo constante, paciencia y motivación durante mi proceso de formación académica. Su acompañamiento ha sido fundamental para mantener la disciplina, la responsabilidad y el compromiso necesarios para avanzar en mi desarrollo profesional.

También dedico este informe a todas las personas que, desde el ámbito académico y laboral, han contribuido a fortalecer mi interés por las tecnologías de la información, la gestión de servicios TIC y la mejora continua de los procesos organizacionales.

Agradecimientos

Agradezco a la Corporación Universitaria Remington por brindar los espacios académicos necesarios para fortalecer mis conocimientos en transformación digital, Outsourcing inteligente y gestión de servicios de tecnologías de la información.

De igual manera, agradezco al docente Jorge Mauricio Sepúlveda Castaño por la orientación brindada durante el seminario, por los lineamientos compartidos en las actividades desarrolladas y por la retroalimentación que permitió mejorar la construcción del presente informe técnico.

Finalmente, agradezco a mis compañeros de formación y a las personas que, desde su experiencia académica o profesional, aportaron ideas, ejemplos y reflexiones útiles para comprender la importancia de aplicar buenas prácticas en la tercerización de servicios TIC, la gestión de riesgos y la transferencia de conocimiento.

Tabla de contenido

Resumen

El presente informe técnico tiene como propósito analizar la aplicación del Outsourcing inteligente en tecnologías de la información mediante el diseño de un modelo de gestión para una Mesa de ayuda TIC apoyada en la plataforma GLPI. El trabajo parte de la necesidad de organizar la atención de incidentes y requerimientos tecnológicos en una institución universitaria, estableciendo procesos claros para el registro, clasificación, seguimiento, escalamiento y cierre de casos. A partir de este enfoque, se integran conceptos vistos en el seminario, como acuerdos de nivel de servicio, indicadores de desempeño, gestión de riesgos, seguridad de la información y transferencia de conocimiento. (GLPI Project, 2025)

El desarrollo del informe se fundamenta en dos componentes principales: la construcción de un acuerdo de nivel de servicio para mesa de ayuda TIC y la elaboración de una propuesta de Outsourcing orientada a la operación del servicio. Estos elementos permiten definir responsabilidades entre cliente y proveedor, tiempos de escalamiento, condiciones contractuales y mecanismos de control. Asimismo, se consideran riesgos asociados a la tercerización, tales como fuga de información, ransomware, fallas de proveedores y debilidades en la documentación operativa. (IBM, Types of Service Level Agreement (SLA) metrics, 2024)

Como resultado, se plantea un modelo técnico que busca mejorar la trazabilidad del soporte, fortalecer la continuidad operativa, facilitar la toma de decisiones mediante reportes y reducir la dependencia de conocimiento no documentado. El informe también resalta la importancia de aplicar controles de seguridad, cumplir la normativa de protección de datos personales y promover prácticas de mejora continua en servicios tercerizados. En este sentido, GLPI se presenta como una herramienta útil para centralizar la operación, mientras que el

ANS/SLA actúa como instrumento de control para evaluar el desempeño del proveedor. (National Institute of Standards and Technology, 2024)

Palabras clave: Outsourcing TIC, mesa de ayuda, GLPI, ANS/SLA, Gestión de riesgos.

1. Marco conceptual y contextual

El marco conceptual y contextual del presente informe técnico reúne los conceptos necesarios para comprender la aplicación del Outsourcing inteligente en servicios de tecnologías de la información. En este apartado se abordan elementos como la tercerización de servicios TIC, la gestión de mesa de ayuda, los acuerdos de nivel de servicio, las métricas de desempeño, los riesgos informáticos y la transferencia de conocimiento. Estos conceptos permiten sustentar la propuesta desarrollada y relacionarla con un entorno institucional donde la atención tecnológica requiere organización, control y continuidad operativa.

1.1 Outsourcing inteligente en TI

El Outsourcing en tecnologías de la información consiste en delegar a un proveedor externo la prestación de determinados servicios tecnológicos, con el propósito de mejorar la eficiencia operativa, acceder a capacidades especializadas y permitir que la organización concentre sus recursos en actividades estratégicas. En un enfoque inteligente, la tercerización no se limita a contratar soporte técnico, sino que incorpora medición del desempeño, seguridad, gestión de riesgos, cumplimiento contractual y mejora continua.

Dentro de este modelo, el proveedor deja de ser únicamente un ejecutor operativo y pasa a desempeñar un rol de aliado estratégico, capaz de aportar herramientas, metodologías, reportes y conocimiento técnico para fortalecer la gestión tecnológica de la institución. Para lograrlo, es necesario establecer responsabilidades claras, canales de comunicación, acuerdos de servicio,

controles de acceso y mecanismos de seguimiento que permitan evaluar el cumplimiento de lo contratado. (IBM, What is an SLA?, 2024)

En el contexto de este informe, el Outsourcing inteligente se aplica a la gestión de una mesa de ayuda TIC mediante una plataforma de gestión de tickets como GLPI. Esta decisión permite centralizar los casos reportados por los usuarios, documentar la atención realizada, controlar tiempos de respuesta y generar información útil para la toma de decisiones. (GLPI Project, 2025)

1.2 Gestión de servicios TIC y soporte institucional

La gestión de servicios TIC comprende el conjunto de procesos, recursos y herramientas utilizados para atender las necesidades tecnológicas de una organización. Su propósito es garantizar que los servicios digitales funcionen de manera estable, que los usuarios reciban atención oportuna y que las áreas responsables puedan controlar la calidad, continuidad y eficiencia de la operación tecnológica.

En una institución universitaria, estos servicios pueden incluir soporte sobre plataformas académicas, correo institucional, conectividad, equipos de cómputo, aplicaciones administrativas, accesos de usuario y recursos tecnológicos usados en procesos académicos o administrativos. Por esta razón, es necesario contar con procedimientos formales que permitan registrar solicitudes, asignar responsables, documentar soluciones y generar reportes sobre el comportamiento del servicio.

El uso de una plataforma como GLPI permite organizar esta gestión mediante tickets, categorías, prioridades, responsables, niveles de servicio y seguimiento histórico de los casos atendidos. De esta manera, la institución puede reducir la atención informal, mejorar la trazabilidad

y contar con información verificable para auditorías, reportes de desempeño y acciones de mejora. (GLPI Project, 2025)

La gestión adecuada del soporte institucional también contribuye a la continuidad operativa, ya que permite identificar incidentes recurrentes, priorizar servicios críticos y establecer rutas de atención para situaciones que requieran intervención especializada. Esto resulta especialmente importante cuando el servicio es tercerizado, porque facilita el control sobre las responsabilidades del proveedor y evita que el conocimiento técnico quede disperso o sin documentación.

1.3 Acuerdos de nivel de servicio e Indicadores de desempeño

Los acuerdos de nivel de servicio, conocidos como ANS o SLA, son instrumentos que permiten definir las condiciones bajo las cuales se prestará un servicio entre un cliente y un proveedor. En ellos se establecen aspectos como alcance, responsabilidades, tiempos de respuesta, disponibilidad, métricas de cumplimiento, mecanismos de seguimiento y consecuencias ante posibles incumplimientos. (IBM, What is an SLA?, 2024)

En servicios TIC tercerizados, el ANS cumple una función de control porque convierte las expectativas del cliente en compromisos medibles. Esto evita que la evaluación del proveedor dependa únicamente de percepciones subjetivas y permite revisar el desempeño mediante datos concretos, como cantidad de casos atendidos, tiempos promedio de solución, porcentaje de cumplimiento, disponibilidad del servicio y satisfacción de los usuarios.

Los indicadores de desempeño permiten verificar si la operación tecnológica está respondiendo de acuerdo con los niveles pactados. Entre los indicadores más relevantes se encuentran el tiempo de primera respuesta, el tiempo de resolución, la cantidad de casos escalados,

el porcentaje de incidentes solucionados, la reincidencia de fallas y el cumplimiento mensual del servicio. (IBM, Types of Service Level Agreement (SLA) metrics, 2024)

En el contexto del presente informe, los ANS/SLA y los indicadores se integran como herramientas para supervisar el Outsourcing de servicios TIC. Su aplicación permite generar reportes, detectar incumplimientos, justificar acciones de mejora y establecer una relación más transparente entre la institución y el proveedor. De esta manera, el servicio deja de administrarse únicamente de forma reactiva y pasa a gestionarse con criterios técnicos, medibles y orientados a resultados.

1.4 Riesgos informáticos en servicios tercerizados

Los servicios TIC tercerizados pueden aportar eficiencia y capacidad técnica, pero también introducen riesgos que deben ser gestionados desde el contrato, la operación y la supervisión continua. Cuando un proveedor externo participa en procesos tecnológicos de una organización, puede tener acceso a usuarios, sistemas, información sensible, infraestructura, credenciales o procedimientos internos. Por esta razón, la tercerización requiere controles claros de seguridad, trazabilidad y responsabilidad.

Entre los riesgos más relevantes se encuentran el ransomware, la fuga de información, los accesos no autorizados, la ingeniería social, la falta de actualización de sistemas, los errores de configuración y la afectación de la disponibilidad de los servicios, la reputación institucional, la continuidad académica o administrativa y la protección de los datos personales. (National Institute of Standards and Technology, 2024)

La ingeniería social representa un riesgo especial porque no siempre ataca directamente la tecnología, sino el comportamiento de los usuarios. Técnicas como phishing, baiting, tailgating o

uso inseguro de redes Wi-Fi pueden facilitar el robo de credenciales, la instalación de software malicioso o el acceso indebido a sistemas institucionales. Por ello, el modelo propuesto debe contemplar campañas de sensibilización, validación de identidad, uso de canales oficiales y reporte de actividades sospechosas.

En Colombia, la protección de datos personales es un componente obligatorio cuando el servicio tercerizado implica tratamiento de información de estudiantes, docentes, funcionarios o usuarios externos. Esto exige definir compromisos de confidencialidad, autorización de uso de datos, control de accesos, reporte de incidentes y manejo adecuado de la información durante toda la relación contractual. (Congreso de Colombia, 2012)

La gestión de riesgos también debe incluir medidas preventivas como respaldos actualizados, políticas de actualización, separación de funciones, revisión periódica de permisos, destrucción segura de activos tecnológicos y documentación de procedimientos críticos. Estas prácticas permiten disminuir el impacto de incidentes y facilitan que la organización conserve control sobre el servicio, incluso cuando parte de la operación se encuentra en manos de un tercero.

1.5 Contexto de aplicación del informe

El contexto de aplicación del presente informe se ubica en una institución universitaria que requiere fortalecer la gestión de sus servicios TIC mediante un modelo de Outsourcing orientado al soporte tecnológico, la atención de usuarios y el control operativo de incidentes y requerimientos. En este entorno, los servicios digitales cumplen un papel fundamental para el desarrollo de actividades académicas, administrativas y de comunicación institucional.

La institución cuenta con usuarios internos y externos que dependen de recursos tecnológicos como plataformas académicas, correo institucional, conectividad, equipos de

cómputo, aplicaciones administrativas, herramientas ofimáticas y servicios de autenticación. Cuando estos recursos presentan fallas o requieren ajustes, es necesario disponer de un proceso formal que permita atender las solicitudes de manera ordenada, priorizada y documentada.

El modelo propuesto toma como referencia el uso de GLPI como plataforma de gestión, debido a que permite administrar tickets, niveles de servicio, categorías, responsables y seguimiento de casos. En este informe, dicha herramienta se considera un eje operativo para mejorar la trazabilidad, conservar evidencia de atención y generar información útil para evaluar el desempeño del proveedor. (GLPI Project, 2026)

La aplicación del Outsourcing en este contexto debe realizarse bajo condiciones claras de alcance, seguridad, medición y transferencia de conocimiento. Por ello, el informe integra los aprendizajes obtenidos durante el seminario y los aplica en un modelo que combina acuerdos de nivel de servicio, gestión de riesgos, control de indicadores, protocolos de escalamiento, documentación técnica y buenas prácticas contractuales.

2. Desarrollo e implementación del aprendizaje

En esta sección se presenta la aplicación práctica de los conceptos trabajados durante el seminario, tomando como base el diseño de un modelo de Outsourcing para servicios TIC en una institución universitaria. El ejercicio integra la construcción de un Acuerdo de Nivel de Servicio, la definición de una propuesta de tercerización, la identificación de riesgos informáticos, la organización del soporte tecnológico y el uso de una plataforma de gestión para controlar la operación.

2.1 Metodología aplicada para el diseño del modelo

La metodología utilizada en el presente informe corresponde a un ejercicio técnico de tipo descriptivo y aplicado, basado en el análisis de los contenidos desarrollados durante el seminario, las actividades previas sobre ANS/SLA y propuesta de Outsourcing, y la revisión de fuentes técnicas relacionadas con gestión de servicios TIC, niveles de servicio, ciberseguridad y protección de datos. A partir de estos insumos se construyó un modelo orientado a una institución universitaria, tomando como caso de aplicación la gestión de servicios tecnológicos mediante una plataforma de tickets.

Para la construcción del modelo se siguieron cuatro pasos principales. En primer lugar, se identificaron las necesidades del contexto institucional, especialmente la atención de incidentes, requerimientos, usuarios y servicios tecnológicos críticos. En segundo lugar, se definieron los componentes operativos del servicio, incluyendo alcance, canales de atención, escalamiento, indicadores y responsabilidades. En tercer lugar, se elaboró una matriz de riesgos utilizando criterios de probabilidad e impacto en escala de 1 a 5, con el fin de priorizar amenazas asociadas al Outsourcing TIC. Finalmente, se plantearon resultados esperados y acciones de mejora relacionadas con trazabilidad, continuidad operativa, seguridad y transferencia de conocimiento.

2.2 Diseño del modelo de Outsourcing para servicios TIC

El modelo propuesto parte de la necesidad de contratar un proveedor externo que apoye la atención tecnológica institucional bajo condiciones claras de alcance, responsabilidad y seguimiento. Para ello, se plantea una estructura de servicio en la que el proveedor atiende incidentes, requerimientos y consultas relacionadas con recursos tecnológicos autorizados,

mientras la institución conserva la supervisión del contrato, la aprobación de cambios y la evaluación del desempeño.

La implementación del modelo requiere diferenciar tres elementos principales: el alcance operativo del servicio, los compromisos medibles del proveedor y los controles necesarios para reducir riesgos. El alcance define qué actividades serán atendidas; los compromisos permiten evaluar el cumplimiento mediante tiempos, disponibilidad e indicadores; y los controles establecen medidas de seguridad, confidencialidad, escalamiento y documentación.

Desde la perspectiva del seminario, este diseño permite comprender que el Outsourcing en TI no debe limitarse a delegar tareas técnicas, sino que debe gestionarse mediante acuerdos formales, canales definidos, seguimiento periódico y transferencia de conocimiento. De esta manera, la institución puede aprovechar capacidades externas sin perder control sobre la calidad del servicio ni sobre la información relacionada con su operación tecnológica. (IBM, What is an SLA?, 2024)

En el caso aplicado, la plataforma GLPI funciona como apoyo para organizar la atención, asignar responsables y generar reportes. Su uso permite que el modelo propuesto tenga trazabilidad y que la revisión del servicio se base en datos registrados, no únicamente en percepciones o comunicaciones informales. (GLPI Project, 2025)

2.3 Implementación del ANS/SLA como mecanismo de control

La implementación del ANS/SLA dentro del modelo propuesto permite transformar las condiciones del servicio en compromisos verificables entre la institución y el proveedor. Este instrumento define qué se espera del servicio, cómo se medirá su cumplimiento y qué acciones podrán aplicarse cuando los niveles pactados no sean alcanzados. (IBM, What is an SLA?, 2024)

Para el caso aplicado, el ANS/SLA se utiliza como base para establecer tiempos de primera respuesta, tiempos de solución, disponibilidad esperada, clasificación de prioridades, responsabilidades de atención y mecanismos de seguimiento. Estos elementos permiten que la evaluación del proveedor no dependa únicamente de opiniones, sino de datos registrados durante la operación del servicio.

El control del servicio se apoya en indicadores como cumplimiento mensual del ANS, cantidad de casos solucionados, porcentaje de tickets vencidos, nivel de satisfacción del usuario, reincidencia de incidentes y resolución en primer contacto. La revisión periódica de estos indicadores facilita la identificación de fallas, la toma de decisiones y la aplicación de planes de mejora. (IBM, Types of Service Level Agreement (SLA) metrics, 2024)

Además de medir el desempeño, el ANS/SLA permite delimitar responsabilidades. La institución debe definir los servicios incluidos, suministrar la información necesaria y aprobar cambios cuando corresponda; por su parte, el proveedor debe atender los casos dentro de los tiempos establecidos, documentar las acciones realizadas, escalar oportunamente y presentar reportes de gestión.

De esta manera, el ANS/SLA se convierte en un mecanismo de gobierno del servicio, ya que permite controlar la calidad de la atención, revisar el cumplimiento contractual y mantener una relación más transparente entre las partes. Su implementación fortalece el modelo de Outsourcing porque vincula la operación diaria con criterios técnicos, medibles y sujetos a mejora continua.

2.4 Gestión de incidentes, requerimientos y escalamiento mediante GLPI

En el modelo propuesto, GLPI se utiliza como herramienta de apoyo para organizar la operación del servicio, permitiendo que los incidentes y requerimientos sean gestionados mediante tickets. Esto facilita que cada solicitud cuente con un registro formal, una categoría, una prioridad, un responsable asignado y un historial de acciones realizadas durante su atención. (GLPI Project, 2025)

La gestión de incidentes se orienta a restaurar el funcionamiento normal de los servicios tecnológicos cuando se presentan fallas, interrupciones o degradaciones. En este caso, la plataforma permite identificar el servicio afectado, clasificar el nivel de urgencia, registrar evidencias y controlar los tiempos de respuesta definidos en el ANS/SLA. Esto permite priorizar situaciones críticas, como fallas de conectividad, bloqueos de acceso, interrupciones en plataformas académicas o problemas que afecten a varios usuarios.

Por otra parte, los requerimientos corresponden a solicitudes que no representan una falla, pero que son necesarias para el desarrollo de las actividades institucionales. Entre ellos se encuentran creación o modificación de usuarios, instalación de software autorizado, configuración básica de equipos, asignación de permisos y orientación sobre herramientas tecnológicas. Al registrarlos en GLPI, la institución puede dar seguimiento al estado de cada solicitud y conservar evidencia del servicio prestado.

El escalamiento se aplica cuando un caso no puede ser resuelto en el primer nivel de soporte y requiere la intervención de un área especializada. En estos casos, el ticket debe conservar el diagnóstico inicial, las acciones ejecutadas, la prioridad asignada y la información necesaria para que el siguiente nivel continúe la atención sin reprocesos. (GLPI Project, 2026)

La aplicación de GLPI en este proceso permite reducir la informalidad en la atención, mejorar la comunicación con los usuarios y generar reportes útiles para analizar el comportamiento del servicio. Con esta información, la institución puede identificar fallas recurrentes, revisar cargas de trabajo, evaluar el cumplimiento del proveedor y tomar decisiones orientadas a la mejora continua.

2.5 Matriz de riesgos para el servicio tercerizado

La evaluación de riesgos permite identificar situaciones que podrían afectar la continuidad, seguridad y calidad del servicio tercerizado. Para este informe se propone una matriz básica basada en probabilidad e impacto, utilizando una escala de 1 a 5, donde 1 representa un nivel bajo y 5 un nivel alto. Esta valoración facilita priorizar los riesgos más críticos y definir controles preventivos o correctivos para la operación del servicio. (National Institute of Standards and Technology, 2024)

Tabla 1. Matriz de riesgos del servicio de Outsourcing TIC

Riesgo identificado	**Causa probable**	**Impacto**	**Probabilidad**	**Nivel de riesgo**	**Control recomendado**
Fuga de información	Accesos no controlados, manejo inadecuado de datos o ausencia de confidencialidad contractual.	5	3	15	Firmar acuerdos de confidencialidad, controlar permisos y registrar acciones del proveedor.

Ransomware o Malware	Correos maliciosos, descargas inseguras, equipos sin actualización o falta de cultura de seguridad.	5	3	15	Mantener respaldos actualizados, antivirus, actualizaciones y capacitación a usuarios.
Ingeniería social	Suplantación de identidad, Phishing, llamadas falsas o solicitudes no verificadas.	4	4	16	Validar identidad, usar canales oficiales y capacitar sobre correos sospechosos.
Incumplimiento del ANS/SLA	Falta de seguimiento, recursos insuficientes o mala clasificación de prioridades.	4	3	12	Revisar indicadores mensuales, aplicar planes de mejora, ajustar prioridades y definir sanciones contractuales cuando corresponda.
Pérdida de conocimiento técnico	Rotación del personal del proveedor o	4	3	12	Crear base de conocimiento, documentar procedimientos

	ausencia de documentación.				y realizar transferencia periódica.
Fallas en la continuidad del servicio	Dependencia de un solo proveedor, ausencia de contingencia o interrupciones no previstas.	5	2	10	Definir plan de continuidad, contactos de escalamiento y protocolos de recuperación.
Uso de software no autorizado	Instalaciones sin aprobación o falta de control sobre licencias.	3	3	9	Gestionar inventario, restringir permisos y validar solicitudes antes de ejecutar cambios.
Tratamiento inadecuado de datos personales	Desconocimiento normativo o falta de políticas de manejo de información.	5	2	10	Aplicar controles de protección de datos, confidencialidad y cumplimiento de la ley 1581.

El resultado de la matriz muestra que los riesgos más relevantes para el servicio tercerizado se relacionan con seguridad de la información, ingeniería social, pérdida de datos y cumplimiento

de los niveles de servicio. Estos riesgos deben ser controlados desde el inicio del contrato, mediante cláusulas claras, políticas internas, reportes periódicos, capacitación y supervisión continua.

La matriz también permite evidenciar que la gestión del Outsourcing no debe centrarse únicamente en la atención técnica, sino en la protección integral del servicio. Por esta razón, los controles recomendados combinan medidas contractuales, operativas y preventivas, buscando que la institución conserve visibilidad sobre el proveedor y pueda responder oportunamente ante incidentes. (Congreso de Colombia, 2012)

2.6 Transferencia de conocimiento y mejora continua

La transferencia de conocimiento es un componente fundamental dentro del modelo de Outsourcing propuesto, debido a que permite conservar la información técnica generada durante la prestación del servicio y evitar que la operación dependa exclusivamente del proveedor o de personas específicas. En servicios TIC tercerizados, documentar procedimientos, soluciones frecuentes, configuraciones, responsables y rutas de escalamiento contribuye a mantener la continuidad operativa ante cambios de personal, rotación del equipo técnico o finalización del contrato.

Para el caso aplicado, se propone la construcción de una base de conocimiento asociada a la gestión del servicio, en la cual se registren guías de atención, soluciones recurrentes, recomendaciones de seguridad, procedimientos de soporte, preguntas frecuentes, evidencias técnicas y lecciones aprendidas. Esta base permitirá agilizar la atención de casos similares, reducir reprocesos y facilitar la capacitación de nuevos integrantes del equipo de soporte.

La mejora continua se apoyará en la revisión de los indicadores definidos en el ANS/SLA, los reportes generados por la plataforma de gestión, las encuestas de satisfacción, los incidentes recurrentes y los casos escalados. Con esta información, la institución y el proveedor podrán identificar oportunidades de ajuste en los procedimientos, fortalecer controles, actualizar documentación y priorizar acciones correctivas. (IBM, Types of Service Level Agreement (SLA) metrics, 2024)

También se recomienda realizar sesiones periódicas de transferencia de conocimiento entre el proveedor y el equipo interno de la institución. Estas sesiones pueden incluir revisión de casos críticos, explicación de procedimientos, socialización de cambios, actualización de protocolos y entrega de documentación técnica. De esta manera, la institución conserva mayor control sobre su operación tecnológica y reduce el riesgo de pérdida de conocimiento al finalizar la relación contractual.

La aplicación de este enfoque permite que el Outsourcing no se limite a resolver incidentes, sino que aporte aprendizaje organizacional. Así, cada caso atendido, cada reporte generado y cada ajuste realizado se convierte en una fuente de información útil para mejorar la calidad del servicio, fortalecer la seguridad operativa y apoyar la toma de decisiones institucionales.

2.7 Resultados esperados del modelo propuesto

Con la aplicación del modelo de Outsourcing propuesto se espera mejorar la organización del soporte tecnológico institucional, especialmente en la forma como se reciben, atienden y evalúan las solicitudes de los usuarios. Al contar con procesos definidos, responsables claros y mecanismos de seguimiento, la institución podrá reducir la atención informal y obtener una visión más precisa sobre el comportamiento de sus servicios TIC.

Uno de los principales resultados esperados es el fortalecimiento de la continuidad operativa. Al establecer prioridades, rutas de escalamiento y tiempos de atención, los servicios críticos podrán recibir una respuesta más oportuna y controlada. Esto permitirá disminuir el impacto de fallas tecnológicas sobre actividades académicas, administrativas y de comunicación institucional.

También se espera mejorar la toma de decisiones a partir de información confiable. Los reportes de gestión, indicadores de desempeño y registros históricos permitirán identificar fallas recurrentes, cargas de trabajo, niveles de cumplimiento, necesidades de capacitación y oportunidades de mejora. De esta manera, el área tecnológica podrá pasar de una gestión reactiva a una gestión más preventiva y planificada. (IBM, Types of Service Level Agreement (SLA) metrics, 2024)

En materia de seguridad, el modelo busca reducir riesgos asociados a accesos no autorizados, pérdida de información, solicitudes no verificadas y ausencia de documentación. La incorporación de controles básicos, compromisos de confidencialidad y procedimientos de atención contribuirá a proteger los recursos tecnológicos y los datos tratados durante la prestación del servicio. (National Institute of Standards and Technology, 2024)

Finalmente, el modelo permitirá fortalecer la relación entre la institución y el proveedor, debido a que establece reglas claras para la operación, la medición del desempeño, la comunicación y la transferencia de conocimiento. Esto favorece una tercerización más controlada, transparente y alineada con las necesidades reales de la organización.

Conclusiones

La aplicación del Outsourcing inteligente en servicios TIC permite comprender que la tercerización no debe limitarse únicamente a delegar funciones técnicas, sino que requiere una estructura formal de gestión, seguimiento y control. En el caso desarrollado, la propuesta permitió integrar alcance del servicio, responsabilidades, indicadores, seguridad operativa y transferencia de conocimiento, elementos necesarios para que la institución conserve visibilidad sobre la operación tecnológica.

El diseño del ANS/SLA demostró ser una herramienta fundamental para establecer compromisos medibles entre la institución y el proveedor. Al definir tiempos de respuesta, disponibilidad, prioridades, métricas y mecanismos de seguimiento, el servicio puede evaluarse con base en datos concretos y no solamente en percepciones de los usuarios. Esto fortalece la transparencia contractual y facilita la toma de decisiones frente al desempeño del proveedor.

El uso de una plataforma de gestión como GLPI aporta valor al modelo propuesto porque permite organizar solicitudes, conservar evidencia, asignar responsables y generar reportes sobre el comportamiento del servicio. Esta trazabilidad favorece la mejora continua, reduce la informalidad en la atención y permite identificar fallas recurrentes o necesidades de ajuste en los procesos tecnológicos. (GLPI Project, 2025)

La identificación de riesgos informáticos evidenció que todo servicio tercerizado debe contemplar medidas de seguridad desde el inicio de la relación contractual. Riesgos como fuga de información, ingeniería social, ransomware, accesos no autorizados o pérdida de conocimiento técnico pueden afectar la continuidad institucional si no se gestionan con controles adecuados,

documentación, capacitación y responsabilidades claras. (National Institute of Standards and Technology, 2024)

Finalmente, el desarrollo del informe permitió evidenciar la importancia de la transferencia de conocimiento en proyectos de Outsourcing TIC. Documentar procedimientos, construir bases de conocimiento, revisar indicadores y realizar sesiones de seguimiento ayuda a que la institución no dependa totalmente del proveedor y pueda mantener continuidad en sus servicios, incluso ante cambios de personal, finalización del contrato o migración hacia otro modelo de operación.

Como reflexión final, el modelo propuesto representa una base técnica viable para ordenar la tercerización de servicios TIC, pero su éxito dependerá de la madurez institucional para sostener procesos documentados, revisar indicadores y exigir cumplimiento al proveedor. La herramienta tecnológica por sí sola no garantiza una buena gestión; se requiere compromiso organizacional, cultura de registro, capacitación continua y revisión periódica del servicio. En futuras mejoras, el modelo podría complementarse con auditorías internas, encuestas de satisfacción más detalladas, tableros de control y simulaciones de incidentes de seguridad.

Referencias

- Atlassian. (2025). *What is a service-level objective? SLO vs. SLA vs. SLI*. Atlassian. https://www.atlassian.com/incident-management/kpis/sla-vs-slo-vs-sli
- GLPI Project. (2025). *Service levels*. GLPI Help Center. https://help.glpi-project.org/documentation/modules/configuration/service_levels
- GLPI Project. (2026). *Setting up service levels (SLA)*. GLPI Help Center. https://help.glpi-project.org/tutorials/helpdesk/service_levels
- IBM. (2024). *Types of Service Level Agreement (SLA) metrics*. IBM Think. https://www.ibm.com/think/topics/sla-metrics
- IBM. (2024). *What is an SLA (service-level agreement)?* IBM Think. https://www.ibm.com/think/topics/service-level-agreement
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- Congreso de Colombia. (2012). Ley 1581 de 2012. Gestor Normativo - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981