



TRABAJO DE GRADO
Opción Seminario-Diplomado.

Automatización de procesos TI mediante outsourcing: beneficios y retos en la delegación de backups, recuperación ante desastres y mantenimiento preventivo

Corporación Universitaria Remington.

Facultad de Ingenierías
Ingeniería de Sistemas

DEYFA PALACIOS PALACIOS
RUBEN DARIO ASPRILLA PEREA
KAMIL STEVEN CUESTA CAICEDO

JORGE MAURICIO SEPÚLVEDA CASTAÑO

Opción de Trabajo de grado: Seminario de Grado
2026.

Dedicatoria

Dedicamos este trabajo a nuestras familias, por su apoyo, comprensión y confianza durante todo este proceso de formación. A las personas que estuvieron presentes en los momentos de mayor esfuerzo que, con sus palabras y acompañamiento, nos motivaron a seguir adelante y no desistir ante las dificultades.

También dedicamos este logro a todas las personas que, de una u otra manera, aportaron en nuestro crecimiento personal y profesional. Este trabajo representa no solo el resultado de un proceso académico, sino también la satisfacción de alcanzar una meta construida con dedicación, aprendizaje y perseverancia.

Agradecimientos

Inicialmente agradecemos a Dios por permitirnos llegar hasta esta etapa y brindarnos la fortaleza necesaria para afrontar cada reto durante el proceso académico. A nuestras familias, por su valioso apoyo, paciencia y acompañamiento constante, especialmente en aquellos momentos en los que fue necesario dedicar tiempo y esfuerzo para cumplir con las responsabilidades.

A la institución y a los docentes que hicieron parte de nuestra formación profesional, por compartir sus conocimientos y aportar herramientas que hoy nos permiten comprender y enfrentar diferentes situaciones del ámbito tecnológico y laboral. De manera especial, agradecemos a todas las personas que contribuyeron directa o indirectamente al desarrollo de este trabajo de grado, ya mediante sus orientaciones, experiencias o palabras de motivación, cada uno de sus aportes fueron de gran importancia para alcanzar este resultado y culminar satisfactoriamente esta etapa académica.

Tabla de Contenidos

Resumen.....	5
Marco conceptual y contextual	6
Outsourcing de tecnologías de la información.....	7
Automatización de procesos TI	8
Backup y recuperación de la información	8
Recuperación ante desastres	9
Mantenimiento preventivo	10
Continuidad del negocio	11
Proveedores especializados de servicios TI.....	11
Acuerdos de nivel de servicio (SLA).....	12
Seguridad de la información	13
Contexto del caso de estudio: Centro Veterinario Huellas S.A.S.....	14
Desarrollo e implementación del aprendizaje.....	16
3. Matriz de servicios tercerizados.....	17
Diagnóstico de la situación inicial	25
Propuesta de outsourcing	25
Conclusiones	29
Referencias.....	30
Apéndice	32

Resumen

La gestión de la infraestructura tecnológica en organizaciones pequeñas y medianas suele desarrollarse de manera reactiva. En muchos casos, se atiende un servidor cuando presenta una falla, se realiza una copia de seguridad de manera ocasional y no se dispone de un plan formal para responder ante un desastre informático. Este trabajo analiza cómo el outsourcing de procesos de TI, específicamente en las áreas de copias de seguridad, recuperación ante desastres y mantenimiento preventivo, puede transformar esta dinámica reactiva en una gestión planificada y sostenible en el tiempo.

Para ilustrar esta transformación, se desarrolla el caso de Centro Veterinario Huellas S.A.S., una clínica veterinaria ficticia que, como muchas empresas de su tamaño, dependía de un esquema informal de soporte técnico y no contaba con procedimientos documentados de respaldo ni de continuidad operativa. A partir de este caso, se presenta el diagnóstico inicial, el diseño de una propuesta de tercerización con un proveedor especializado, el proceso de implementación y los resultados obtenidos. Asimismo, se analizan los beneficios alcanzados, entre ellos una mayor continuidad del servicio, la reducción de los tiempos de inactividad y el acceso a conocimiento especializado. De igual manera, se consideran los retos asociados con la delegación de procesos críticos en un tercero, como la dependencia del proveedor, la gestión del cambio interno y la protección de la información sensible de clientes y pacientes.

El trabajo se fundamenta en literatura académica sobre outsourcing de sistemas de información y en referencias técnicas relacionadas con las buenas prácticas de respaldo y continuidad operativa. De esta manera, busca ofrecer una perspectiva aplicada y realista sobre las implicaciones de delegar estas actividades a un proveedor externo.

Palabras clave: Outsourcing de TI, automatización, backups, recuperación ante desastres y mantenimiento preventivo.

Marco conceptual y contextual

El trabajo aborda la automatización de procesos de tecnologías de la información mediante un modelo de outsourcing, tomando como caso de estudio académico al Centro Veterinario Huellas S.A.S. La propuesta parte de una situación frecuente en organizaciones pequeñas y medianas: la necesidad de mantener disponibles sus sistemas y proteger la información, pero sin contar necesariamente con un equipo interno especializado para atender de manera permanente todas las actividades relacionadas con tecnología. En una clínica veterinaria, la tecnología cumple un papel importante en actividades como el registro de los pacientes, la administración de las historias clínicas, la programación de citas, la facturación, el manejo de información de los propietarios y la comunicación con los clientes. Por esta razón, una falla en los equipos, la pérdida de información o una interrupción prolongada de los sistemas puede afectar tanto en las labores administrativas como la atención de los pacientes.

A partir de este contexto, el trabajo se concentra en tres procesos de TI que pueden ser delegados a un proveedor especializado: las copias de seguridad o backups, la recuperación ante desastres y el mantenimiento preventivo. La intención no es entregar completamente la gestión tecnológica de la clínica a un tercero, sino establecer un esquema en el que determinadas actividades sean administradas por un proveedor externo mientras la organización conserva la supervisión sobre sus recursos, información y necesidades.

Outsourcing de tecnologías de la información

El outsourcing de tecnologías de la información consiste en recurrir a proveedores externos para desarrollar determinadas funciones o servicios relacionados con los sistemas y recursos tecnológicos de una organización. Esta alternativa puede utilizarse para acceder a conocimientos especializados, mejorar la eficiencia de determinados procesos y disponer de capacidades que podrían ser difíciles de mantener internamente. La decisión de tercerizar un proceso de TI debe analizar tanto sus posibles beneficios como los riesgos que puede generar. La literatura sobre outsourcing de TI identifica como motivaciones frecuentes la búsqueda de beneficios financieros y el acceso a capacidades especializadas, pero también señala riesgos relacionados con la pérdida de control, la pérdida de conocimiento interno y la aparición de costos no previstos (Lacity et al., 2017). Por esta razón, la tercerización no debe entenderse simplemente como contratar una empresa externa, sino como una relación que necesita condiciones claras de operación, seguimiento y control. En el caso del Centro Veterinario Huellas S.A.S., el outsourcing se plantea como una alternativa para delegar actividades técnicas que requieren seguimiento constante. El proveedor podría encargarse de configurar y supervisar los backups, apoyar los procedimientos de recuperación ante incidentes y programar actividades de mantenimiento preventivo. La clínica, por su parte, mantendría la responsabilidad sobre la información que maneja y sobre la supervisión del servicio contratado.

El proceso general de outsourcing de TI se ilustra en la *Figura 1*, incluida en el Apéndice al final de este trabajo de grado.

Automatización de procesos TI

La automatización de procesos TI consiste en utilizar herramientas tecnológicas para ejecutar actividades de manera programada, reduciendo la dependencia de tareas manuales. Dentro de una organización, esto puede facilitar actividades que deben realizarse periódicamente, como copias de seguridad, comprobaciones del estado de los sistemas, generación de alertas y algunas labores de mantenimiento. En este caso de estudio, la automatización permitirá que determinadas tareas no dependan exclusivamente de que una persona recuerde ejecutarlas.

El flujo de automatización de procesos se ilustra en la *Figura 2*, incluida en el Apéndice al final de este trabajo de grado.

En los backups pueden programarse para realizarse de acuerdo con una frecuencia previamente establecida y generar alertas cuando se presente un error. De esta manera, el personal responsable puede concentrarse en revisar los resultados y actuar cuando sea necesario. La automatización, sin embargo, no elimina la necesidad de supervisión. Un proceso programado puede presentar errores, quedarse sin espacio de almacenamiento o ejecutarse de manera incorrecta. Por esta razón, la propuesta debe contemplar mecanismos de monitoreo y verificación que permitan confirmar que las tareas realmente están cumpliendo su propósito.

Backup y recuperación de la información

Los backups son copias de la información que se conservan para poder recuperarla cuando los datos originales se pierden, se dañan o dejan de estar disponibles. En una organización que depende de sus sistemas de información, contar con copias de

seguridad confiables constituye una medida importante para reducir el impacto de diferentes incidentes tecnológicos.

El National Institute of Standards and Technology (NIST) señala que las organizaciones deben establecer políticas que definan aspectos como la frecuencia, el alcance y la ubicación de las copias de seguridad, teniendo en cuenta la importancia de los datos y las necesidades de disponibilidad e integridad de la información (Swanson et al., 2010). Esto resulta especialmente relevante para una clínica veterinaria, donde la pérdida de información puede dificultar la consulta de antecedentes y el seguimiento de los servicios prestados a los pacientes. En el Centro Veterinario Huellas S.A.S. se plantea que el proceso de backup sea automatizado y administrado por el proveedor de outsourcing. El esquema deberá contemplar la programación de las copias, su almacenamiento, la generación de alertas y la realización periódica de pruebas de restauración. No sería suficiente con saber que existe una copia; también es necesario comprobar que dicha copia puede utilizarse cuando se necesite.

Recuperación ante desastres

La recuperación ante desastres comprende las acciones necesarias para restablecer los sistemas y servicios tecnológicos después de una interrupción grave. NIST plantea que la planificación de contingencias debe considerar aspectos como la identificación de prioridades, los controles preventivos, las estrategias de recuperación, las pruebas y el mantenimiento del plan (Swanson et al., 2010). En el contexto de una clínica veterinaria, una situación de este tipo podría presentarse por daños en un equipo, fallas del almacenamiento, errores humanos, problemas de software o un incidente que afecte la

infraestructura tecnológica. La gravedad dependerá de los sistemas afectados y del tiempo durante el cual permanezcan fuera de servicio. La propuesta de outsourcing busca que el Centro Veterinario Huellas S.A.S. tenga procedimientos previamente definidos para responder ante este tipo de situaciones. Esto implica identificar qué información y servicios deben recuperarse primero, dónde se encuentran las copias de seguridad, quién debe autorizar la recuperación y cuáles son los tiempos esperados para restablecer cada servicio. Esta planificación se relaciona directamente con la continuidad del negocio. La ISO 22301:2019 establece un marco para que las organizaciones puedan prepararse ante interrupciones, responder a ellas y recuperar sus actividades, fortaleciendo su capacidad de recuperación frente a diferentes situaciones (International Organization for Standardization [ISO], 2019).

Mantenimiento preventivo

El mantenimiento preventivo comprende las actividades realizadas de manera planificada para conservar los equipos y sistemas en condiciones adecuadas de funcionamiento y detectar posibles problemas antes de que se conviertan en fallas mayores. En la clínica, este proceso puede incluir la revisión periódica de computadores, servidores, dispositivos de almacenamiento, sistemas operativos, aplicaciones y elementos relacionados con la infraestructura tecnológica. También puede contemplar la revisión de espacio disponible, actualizaciones, registros de errores y condiciones básicas de funcionamiento. La participación de un proveedor especializado permitiría establecer un calendario de mantenimiento y llevar un registro de las actividades realizadas. Esto representa un cambio frente a una gestión basada únicamente en atender los problemas

cuando ya se han presentado. El propósito sería pasar hacia una gestión más preventiva, donde las revisiones se programen y los hallazgos puedan ser atendidos antes de generar una interrupción.

Continuidad del negocio

La continuidad del negocio se relaciona con la capacidad de una organización para prepararse, responder y recuperarse ante situaciones que puedan interrumpir sus actividades. La ISO 22301:2019 presenta la continuidad del negocio como un sistema de gestión orientado a proteger a las organizaciones frente a incidentes disruptivos y facilitar la recuperación de sus operaciones (ISO, 2019). Para el Centro Veterinario Huellas S.A.S., la continuidad tiene una relación directa con la disponibilidad de sus recursos tecnológicos. Si la información de los pacientes no está disponible, si el sistema de citas presenta una falla o si los equipos utilizados para las actividades administrativas dejan de funcionar, determinadas tareas pueden verse afectadas. Por esta razón, los backups, la recuperación ante desastres y el mantenimiento preventivo no deben verse como actividades aisladas. Los tres procesos forman parte de una estrategia que busca disminuir la posibilidad de interrupciones y mejorar la capacidad de respuesta cuando una falla llegue a presentarse.

Proveedores especializados de servicios TI

Los proveedores especializados de servicios TI son organizaciones externas que cuentan con personal, conocimientos y herramientas para prestar servicios relacionados con tecnología. En un modelo de outsourcing, estos proveedores pueden asumir determinadas responsabilidades previamente acordadas con la organización contratante.

planteamos que el proveedor seleccionado tenga experiencia en administración de infraestructura, respaldo de información, recuperación de servicios y mantenimiento preventivo. También deberá contar con mecanismos de monitoreo y atención de incidentes que permitan conocer el estado de los servicios contratados.

La selección del proveedor representa uno de los aspectos que debe analizarse con cuidado. El costo del servicio es solamente uno de los elementos que intervienen en la decisión. También deben revisarse la capacidad técnica, experiencia, seguridad de la información, tiempos de respuesta y condiciones contractuales. Estudios sobre outsourcing de TI han identificado precisamente la pérdida de control, la pérdida de conocimiento y los costos inesperados entre los riesgos que pueden aparecer cuando una organización terceriza servicios tecnológicos (Lacity et al., 2017). Por ello, el modelo propuesto para la clínica debe mantener mecanismos de supervisión y evaluación del proveedor.

Acuerdos de nivel de servicio (SLA)

Los acuerdos de nivel de servicio, conocidos como SLA (Service Level Agreement), permiten establecer las condiciones bajo las cuales un proveedor debe prestar un servicio. En una relación de outsourcing, estos acuerdos sirven para definir responsabilidades, niveles esperados de atención y mecanismos mediante los cuales se puede evaluar el cumplimiento. El SLA podría establecer aspectos como la frecuencia de los backups, los tiempos máximos de atención de incidentes, los tiempos esperados de recuperación, la frecuencia del mantenimiento preventivo y la entrega de informes sobre las actividades realizadas. La importancia de estos acuerdos también ha sido estudiada

dentro del outsourcing de TI. Goo et al. (2008) encontraron una relación positiva entre determinadas características de los SLA, el compromiso entre las partes y los resultados de la relación de outsourcing. Esto muestra que el acuerdo no debería limitarse a establecer un precio, sino que debe ayudar a organizar la relación entre la clínica y el proveedor.

Seguridad de la información

La seguridad de la información adquiere especial importancia cuando una organización permite que un proveedor externo tenga acceso a sistemas, infraestructura o información. La ISO/IEC 27001:2022 establece requisitos para implementar y mantener un sistema de gestión de seguridad de la información, con un enfoque basado en la gestión de los riesgos relacionados con la información (ISO, 2022). En el Centro Veterinario Huellas S.A.S. este aspecto debe ser tenido en cuenta desde la selección del proveedor. La información almacenada en los sistemas de la clínica puede incluir datos relacionados con los propietarios de los animales, historias clínicas veterinarias, facturación y registros administrativos. Por ello, el acceso del proveedor debe estar limitado a las funciones que realmente necesita desarrollar. También deben establecerse mecanismos para controlar las cuentas de acceso, proteger las copias de seguridad, registrar actividades relevantes y definir qué ocurre con la información cuando finaliza el contrato. De esta manera, la tercerización de los servicios TI puede aprovechar las capacidades del proveedor sin perder de vista la protección de la información de la organización.

Contexto del caso de estudio: Centro Veterinario Huellas S.A.S.

Para desarrollar la propuesta se utilizará Centro Veterinario Huellas S.A.S. como una organización ficticia creada exclusivamente para fines académicos. No se pretende presentar esta empresa como una entidad real ni atribuirle datos que no hayan sido comprobados. Los datos utilizados en las siguientes etapas del trabajo serán supuestos técnicos contruidos para representar una clínica veterinaria de tamaño pequeño o mediano. El Centro Veterinario. se plantea como una clínica dedicada a la atención de animales de compañía, principalmente perros y gatos. Dentro de sus actividades se encuentran la asignación de citas, consulta veterinaria, seguimiento de pacientes, registro de historias clínicas, facturación y comunicación con los propietarios. Para apoyar estas actividades, la clínica utiliza computadores, conexión a Internet, sistemas de información y almacenamiento digital de datos. El crecimiento de las actividades hace que la información tecnológica tenga cada vez mayor importancia para el funcionamiento de la clínica. Las historias de los pacientes, los datos de contacto de los propietarios, los registros de servicios y la información administrativa necesitan estar disponibles cuando el personal los requiera.

En el escenario planteado, la clínica no cuenta con un departamento de TI amplio y permanente. Algunas tareas tecnológicas son realizadas por personal interno y otras dependen de soporte externo cuando se presenta un inconveniente. Esta situación puede generar una gestión principalmente reactiva, debido a que determinadas actividades de mantenimiento o respaldo pueden depender de la disponibilidad de una persona y no de un procedimiento automatizado y supervisado.

A partir de esta situación se propone implementar un modelo de outsourcing TI enfocado inicialmente en tres procesos: backup, recuperación ante desastres y mantenimiento preventivo. El proveedor especializado tendría la responsabilidad técnica de configurar, ejecutar y monitorear las actividades acordadas, mientras que la clínica conservaría la supervisión del servicio, la definición de sus necesidades y el control sobre la información. La propuesta busca que las actividades tecnológicas pasen de una dinámica basada principalmente en la atención de problemas hacia una gestión más organizada y preventiva. Los backups podrían ejecutarse automáticamente de acuerdo con una programación definida; el mantenimiento podría realizarse mediante un calendario periódico; y la recuperación ante desastres podría apoyarse en procedimientos previamente documentados y probados. El caso también permitirá analizar los posibles inconvenientes del modelo. Entre ellos se encuentran la dependencia del proveedor, la necesidad de proteger los accesos a los sistemas, los costos de contratación, el riesgo de pérdida de control sobre algunas actividades y la necesidad de comprobar permanentemente el cumplimiento de los niveles de servicio. Estos aspectos son relevantes porque la tercerización puede generar beneficios, pero también exige una adecuada gestión de la relación entre cliente y proveedor. De esta manera, Huellas S.A.S. funcionará como escenario académico para aplicar los conocimientos relacionados con outsourcing de TI, automatización, continuidad operativa, seguridad de la información y gestión de proveedores. El propósito será diseñar una propuesta que pueda responder a las necesidades tecnológicas de la clínica sin perder de vista que la tecnología debe estar al servicio de las actividades principales de la organización.

Desarrollo e implementación del aprendizaje

La propuesta de outsourcing para el Centro Veterinario Huellas S.A.S. se estructura a partir de un diagnóstico de la situación tecnológica y de la necesidad de transformar una gestión principalmente reactiva en un esquema preventivo, automatizado y medible. El modelo se concentra en cuatro servicios: copias de seguridad, recuperación ante desastres, mantenimiento preventivo y soporte técnico especializado. La clínica conserva la responsabilidad sobre sus procesos, información y decisiones de negocio, mientras el proveedor asume las actividades técnicas expresamente definidas.

La implementación inicia con un inventario de activos, servicios y datos. Posteriormente se determina la criticidad de cada servicio, se valoran los riesgos, se establecen los niveles de servicio y se configuran las actividades automatizadas. La operación queda respaldada por procedimientos documentados, evidencias de ejecución y un esquema de indicadores que permite revisar periódicamente el desempeño del proveedor. Este enfoque permite que el outsourcing sea controlable. La clínica no solamente contrata una capacidad técnica externa, sino que define qué debe hacerse, con qué frecuencia, en cuánto tiempo, quién es responsable, qué evidencia debe generarse y cómo se tratará un incumplimiento. La relación se administra mediante un SLA y se verifica mediante KPI.

3. Matriz de servicios tercerizados

Servicio	Actividades	Frecuencia	Entregables	Responsable proveedor	Responsable interno	Herramientas	Evidencia
Backups	Programar, ejecutar, monitorear, revisar errores y conservar copias	Diaria; revisión semanal; restauración mensual	Reporte de backup y restauración	Administrador TI/backup	Responsable interno designado	Software de backup, almacenamiento y monitoreo	Logs, alertas, reporte y acta de prueba
Recuperación ante desastres	Activar procedimiento, recuperar servicios, validar integridad y documentar	Prueba trimestral y cada incidente P1	Informe de recuperación	Especialista de continuidad	Gerencia/responsable interno	Procedimiento DR, backups, checklist	Ticket, acta, tiempos RTO/RPO y evidencia de restauración
Mantenimiento preventivo	Revisión de equipos, servidor, almacenamiento, actualizaciones, capacidad y errores	Mensual; revisión integral trimestral	Informe de mantenimiento	Técnico de infraestructura	Coordinador interno	Checklist, inventario y monitoreo remoto	Checklist, tickets y reporte
Soporte especializado	Recibir, clasificar, diagnosticar, solucionar y escalar incidentes	Según demanda y SLA	Ticket de servicio cerrado	Mesa de ayuda/especialista	Usuario/coordinador	Mesa de servicios, correo, teléfono y monitoreo	Ticket con horas de reporte, respuesta y cierre

Matriz de criticidad y prioridades

La matriz de criticidad permite establecer qué servicios requieren atención prioritaria. La clasificación se basa en el impacto sobre la atención de pacientes, la disponibilidad de información, la operación administrativa y la continuidad del servicio.

Prioridad	Criterio	Ejemplo	Cobertura	Primera respuesta	RPO	RTO
P1 – Crítica	La interrupción afecta directamente la operación y puede generar pérdida de información o imposibilidad de prestar el servicio.	Fallo del sistema principal, pérdida de información clínica crítica o indisponibilidad de servicios esenciales.	24 x 7	≤ 15 minutos	≤ 4 horas	≤ 4 horas
P2 – Alta	La interrupción afecta de manera importante la operación, pero existen alternativas temporales para continuar las actividades.	Fallas en aplicaciones de gestión, problemas de conectividad o servicios que afectan procesos importantes.	06:00–22:00	≤ 30 minutos	≤ 24 horas	≤ 8 horas

P3 – Media	La incidencia genera afectación parcial y puede ser gestionada sin comprometer de manera inmediata la continuidad de la operación.	Mantenimiento correctivo, errores menores de aplicaciones o problemas en equipos no críticos.	Horario laboral	≤ 4 horas hábiles	≤ 24 horas	≤ 2 días hábiles
P4 – Baja	La incidencia tiene un impacto reducido y puede ser atendida mediante la programación de actividades de soporte.	Solicitudes de configuración, consultas técnicas o ajustes menores.	Horario laboral	≤ 1 día hábil	No aplica	≤ 5 días hábiles

Matriz de riesgos

Para el ejercicio se utiliza una escala de probabilidad e impacto de 1 a 5. El nivel de riesgo se obtiene multiplicando probabilidad por impacto. La valoración deberá actualizarse cuando cambien los activos, servicios, amenazas o controles.

Riesgo	Causa	Prob .	Impact o	Nivel	Control / tratamiento	Responsabl e
Falla de backups	Error de configuración, almacenamiento lleno o tarea detenida.	3	5	15 - Alto	Monitoreo, alertas, revisión y restauración mensual.	Proveedor
No poder restaurar	Copia corrupta o procedimiento no probado.	2	5	10 - Alto	Pruebas mensuales/trimestrales y procedimiento DR.	Proveedor + clínica
Indisponibilidad del proveedor	Falta de personal o incumplimiento.	3	4	12 - Alto	SLA, escalamiento y proveedor alternativo.	Gerencia
Acceso no autorizado	Credenciales compartidas o privilegios excesivos.	2	5	10 - Alto	Mínimo privilegio, cuentas nominativas, MFA si está disponible y logs.	Proveedor + clínica
Mantenimiento mal ejecutado	Cambio sin pruebas o sin ventana autorizada.	2	4	8 - Medio	Checklist, ventana de mantenimiento, backup previo y reversión.	Proveedor
Pérdida de conocimiento interno	Dependencia excesiva del tercero.	3	3	9 - Medio	Documentación y transferencia de conocimiento.	Proveedor + clínica
Pérdida de conectividad	Falla de Internet.	3	4	12 - Alto	Canal alternativo y contingencia.	Clínica + proveedor
Incumplimiento del SLA	Falta de seguimiento.	2	4	8 - Medio	KPI, comité de servicio y plan de mejora.	Gerencia + proveedo

Acuerdo de Nivel de Servicio (SLA)

El Acuerdo de Nivel de Servicio formaliza las condiciones bajo las cuales el proveedor prestará el servicio. En este caso, el SLA debe integrarse al contrato o funcionar como anexo operativo del contrato. Su finalidad es evitar que expresiones

como “atención oportuna”, “backup periódico” o “mantenimiento preventivo” queden sujetas a interpretaciones.

Elemento	Condición propuesta
Objeto	Prestación de backups, recuperación ante desastres, mantenimiento preventivo y soporte especializado.
Horario	P1: 24 x 7. P2: 06:00–22:00. P3 y P4: horario laboral.
Canales	Mesa de servicios/ticket, correo institucional y teléfono para P1/P2.
Clasificación	El proveedor clasifica el incidente y la clínica puede solicitar revisión de la prioridad.
Primera respuesta	P1 ≤15 min; P2 ≤30 min; P3 ≤4 h hábiles; P4 ≤1 día hábil.
Solución	P1 ≤4 h; P2 ≤8 h; P3 ≤2 días hábiles; P4 ≤5 días hábiles, salvo dependencia justificada de terceros.
Backups	Ejecución automatizada diaria; frecuencia superior para información crítica cuando el RPO lo requiera; alertas ante errores.
Restauración	Prueba mensual de restauración y simulacro trimestral de recuperación ante desastre.
RPO	Hasta 4 h para información crítica y hasta 24 h para información estándar.
RTO	Hasta 4 h para servicios críticos (P1), hasta 8 h para servicios de alta prioridad (P2), hasta 2 días hábiles para servicios de prioridad media (P3) y hasta 5 días hábiles para solicitudes de prioridad baja (P4).
Mantenimiento	Mensual para componentes críticos y revisión integral trimestral, con ventana autorizada.
Informes	Informe mensual con backups, restauraciones, incidentes, mantenimiento, disponibilidad y KPI.
Escalamiento	N1 mesa de ayuda; N2 especialista; N3 líder técnico; N4 responsable de clínica y dirección del proveedor.
Seguridad	Cuentas nominativas, mínimo privilegio, protección de credenciales, registro de actividades y control de información al terminar contrato.
Incumplimientos	Registro de desviación, causa, acción correctiva, responsable y fecha de cierre; reiteraciones activan revisión contractual.
Revisión	Revisión operativa mensual y revisión formal trimestral del SLA.

Ruta de escalamiento

Nivel	Responsable	Activación	Acción	Escalamiento
N1	Mesa de ayuda	Todo ticket	Registrar, clasificar y resolver	Inmediato si requiere especialidad
N2	Especialista TI	No resuelto en N1	Diagnóstico y solución técnica	P1: 15 min; P2: 30 min
N3	Líder técnico	Falla compleja o riesgo de superar RTO	Coordinar recursos y recuperación	Antes del 50% del tiempo objetivo
N4	Clínica + dirección proveedor	Incidente mayor o incumplimiento inminente	Decidir contingencia, comunicación y mejora	Antes del vencimiento del objetivo

Matriz de KPI

Los KPI convierten el control del outsourcing y la automatización en un proceso verificable. Las metas propuestas son académicas y deben ajustarse después de obtener una línea base real.

KPI	Fórmula	Meta	Periodicidad	Fuente	Responsable
Backups exitosos	(Backups exitosos / backups programados) $\times$ 100	≥ 95 %	Semanal / mensual	Logs de backup	Proveedor
Restauraciones exitosas	(Pruebas exitosas / pruebas realizadas) $\times$ 100	100%	Mensual	Actas y logs	Proveedor + clínica
Mantenimiento cumplido	(Mantenimientos a tiempo / programados) $\times$ 100	≥ 90 %	Mensual	Calendario / tickets	Proveedor
Disponibilidad crítica	((Tiempo total – indisponibilidad no programada) / tiempo total) $\times$ 100	≥ 98 %	Mensual	Monitoreo	Proveedor
Primera respuesta SLA	(Incidentes dentro del tiempo / incidentes totales) $\times$ 100	≥ 90 %	Mensual	Mesa de servicios	Proveedor
Recuperación SLA	(Recuperaciones dentro del objetivo / recuperaciones totales) $\times$ 100	≥ 90 %	Mensual	Tickets + DR	Proveedor
Incidentes recurrentes	Número de incidentes repetidos por causa	≤ 5 % del total	Mensual	Mesa de servicios	Proveedor + clínica
Satisfacción de usuarios	(Valoraciones favorables / respuestas válidas) $\times$ 100	≥ 90 %	Mensual / trimestral	Encuesta	Clínica
Informes entregados a tiempo	(Informes entregados / informes programados) $\times$ 100	100%	Mensual	Repositorio documental	Proveedor

Las metas establecidas para los KPI tienen carácter preliminar, debido a que el caso corresponde a un escenario académico. Durante las primeras semanas de operación se deberá recopilar información real sobre disponibilidad, tiempos de respuesta, cumplimiento de backups, restauraciones y mantenimiento. Estos datos permitirán establecer una línea base y determinar si las metas propuestas son técnicamente alcanzables antes de incorporarlas como compromisos definitivos dentro del SLA.

Evidencias de cumplimiento

Cada servicio debe dejar evidencia trazable. Para backups se conservarán logs de ejecución, alertas y reportes. Para restauraciones se conservarán actas de prueba y resultados. Para mantenimiento se conservarán checklists, tickets e informes. Para incidentes se conservarán los tickets con prioridad, hora de reporte, hora de primera respuesta, acciones realizadas, escalamiento y cierre. Para el SLA se conservará el informe mensual de cumplimiento. Para los KPI se conservarán los datos de origen y el cálculo efectuado. La evidencia debe permitir responder cinco preguntas: qué actividad se realizó, cuándo se realizó, quién la ejecutó, cuál fue el resultado y si se cumplió el nivel acordado. Si una actividad no puede demostrarse mediante evidencia, no debe considerarse plenamente verificable.

Plan de implementación

Fase	Actividades	Duración	Entregable	Criterio de aceptación
1. Preparación	Inventario, responsables, criticidad, riesgos y línea base.	Semana 1	Inventario + matrices	Servicios críticos identificados.
2. Diseño	SLA, políticas de backup, RPO/RTO, DR y mantenimiento.	Semanas 2–3	SLA + procedimientos	Aprobación clínica/proveedor.
3. Configuración	Automatización, monitoreo, alertas y mesa de servicios.	Semanas 4–5	Servicios configurados	Pruebas satisfactorias.
4. Pruebas	Restauración, incidente P1, escalamiento y evidencias.	Semana 6	Actas de pruebas	RTO/RPO y escalamiento validados.
5. Operación controlada	Backups, mantenimiento, tickets y KPI.	Semanas 7–10	Informe de servicio	KPI calculados.
6. Mejora continua	Revisión de SLA, riesgos y acciones correctivas.	Trimestral	Plan de mejora	Acciones cerradas.

Diagnóstico de la situación inicial

Antes de plantear la solución, se realizó un diagnóstico académico de las principales condiciones relacionadas con la gestión de tecnología de la clínica. Los datos presentados en esta sección corresponden a un escenario construido para desarrollar el ejercicio y no representan información obtenida de una empresa real. El diagnóstico inicial de la gestión de servicios TI se presenta en la *Tabla 1*, incluida en el Apéndice al final de este trabajo de grado. La situación anterior muestra que el principal inconveniente no está necesariamente relacionado con la falta de equipos o sistemas, sino con la manera en que se administran. Una organización puede disponer de recursos tecnológicos adecuados y, aun así, estar expuesta a pérdidas de información o interrupciones si no cuenta con mecanismos de prevención y recuperación.

Propuesta de outsourcing

Del diagnóstico se plantea contratar un proveedor externo especializado para asumir algunas actividades técnicas. La intención es que la clínica conserve el control de sus procesos principales y de la información que utiliza, mientras el proveedor se encargue de aquellas tareas que requieren conocimientos especializados y seguimiento constante. Entre los servicios que se propone tercerizar se encuentran el mantenimiento preventivo, las copias de seguridad, el soporte técnico especializado y la recuperación ante posibles incidentes. Esta decisión permite establecer responsabilidades concretas y evitar que la solución de los problemas dependa exclusivamente de la disponibilidad o conocimiento del personal interno. El outsourcing tampoco significa entregar completamente la gestión tecnológica a un tercero. La clínica debe conservar la

capacidad de supervisar el servicio, definir sus necesidades y verificar que el proveedor cumpla con las condiciones acordadas. Para ello, se propone establecer un acuerdo de nivel de servicio o SLA, donde se especifiquen los tiempos de atención, actividades incluidas, responsabilidades y mecanismos de seguimiento.

La distribución de responsabilidades entre la clínica y el proveedor se presenta en *la Tabla 2*, incluida en el Apéndice al final de este trabajo de grado.

Esta distribución busca evitar confusiones sobre quién debe realizar cada actividad. La clínica mantiene la responsabilidad sobre su operación y sobre la información que maneja, mientras el proveedor aporta la capacidad técnica necesaria para mantener los servicios tecnológicos.

Implementación de la propuesta

Comienza con una revisión general de los equipos, sistemas y servicios utilizados por la clínica. En esta etapa se identifican los recursos más importantes, las posibles fallas y la información que debe tener prioridad dentro de las copias de seguridad. Después se establece un cronograma de mantenimiento preventivo. Esto representa un cambio frente al escenario inicial, ya que las revisiones dejan de depender exclusivamente de la aparición de una falla. El proveedor tendría que realizar las actividades programadas y entregar reportes que permitan conocer el estado de los equipos y las acciones realizadas.

Otro componente importante corresponde a los respaldos. Se propone establecer una periodicidad definida de acuerdo con la importancia de la información. NIST recomienda que las organizaciones establezcan políticas sobre la frecuencia, alcance y ubicación de las copias de seguridad, considerando la importancia de los datos y la

frecuencia con la que estos cambian (Swanson et al., 2010). Para el caso de la clínica, esto significa que la información más crítica debe contar con una protección más frecuente y con mecanismos que permitan recuperar los datos cuando sea necesario.

También elabora un procedimiento de recuperación ante desastres. En este documento se deben definir los sistemas prioritarios, las personas responsables, los pasos para recuperar la información y la manera de comprobar que el proceso haya funcionado correctamente. La planificación de contingencia permite que la recuperación de los servicios no dependa de decisiones improvisadas cuando ocurre una emergencia (Swanson et al., 2010).

Indicadores de seguimiento

Para evaluar la efectividad del modelo de outsourcing no basta con registrar que las actividades fueron programadas. La clínica y el proveedor deben medir el cumplimiento real mediante indicadores con fórmula, meta, periodicidad, fuente y responsable. Los KPI establecidos permiten evaluar la ejecución exitosa de los backups, la capacidad real de restaurar la información, el cumplimiento del mantenimiento preventivo, la disponibilidad de los servicios críticos, los tiempos de atención y recuperación, la recurrencia de incidentes, la satisfacción de los usuarios y la entrega oportuna de informes.

La lectura de los indicadores debe realizarse mensualmente. Cuando un KPI se encuentre por debajo de la meta, el proveedor deberá registrar la desviación, identificar la causa, proponer una acción correctiva, establecer un responsable y fijar una fecha de cierre. Las desviaciones repetitivas deben ser analizadas en la revisión trimestral del SLA

para determinar si es necesario modificar procedimientos, recursos, capacidades o condiciones contractuales.

Resultados esperados de la implementación

Con la implementación de la propuesta se espera que la clínica evolucione desde una gestión tecnológica reactiva hacia un modelo preventivo y controlado. El cambio no se limita a programar backups o realizar mantenimiento, sino que incorpora prioridades, responsabilidades, niveles de servicio, controles de riesgo, evidencias e indicadores. De esta manera, la organización podrá conocer si las actividades se están ejecutando de acuerdo con lo previsto y si los resultados cumplen las metas establecidas.

En el escenario académico, la mejora esperada se refleja en una mayor regularidad de los respaldos, una mayor capacidad para comprobar su restauración, un mantenimiento programado, mayor disponibilidad de los servicios críticos y una atención de incidentes sometida a tiempos definidos. Estos resultados deberán comprobarse mediante los KPI y no solamente mediante una apreciación cualitativa.

Conclusiones

El desarrollo de la propuesta evidencia que el outsourcing de TI puede constituir una alternativa para fortalecer la gestión tecnológica de una organización pequeña cuando se delimitan claramente los servicios, las responsabilidades y los mecanismos de control. En el caso académico del Centro Veterinario Huellas S.A.S., la tercerización de backups, recuperación ante desastres, mantenimiento preventivo y soporte especializado permite estructurar una gestión orientada a la prevención y a la continuidad de los servicios.

La principal mejora incorporada mediante esta corrección consiste en transformar los elementos conceptuales en instrumentos técnicos verificables. La matriz de servicios define actividades, frecuencias, entregables, responsables, herramientas y evidencias; la matriz de criticidad establece prioridades y tiempos de atención; la matriz de riesgos identifica amenazas, niveles y controles; el SLA formaliza las condiciones de prestación del servicio; y los KPI permiten medir objetivamente el desempeño del proveedor y la efectividad de la automatización. El modelo propuesto también reconoce que la tercerización no elimina la responsabilidad de la organización contratante. La clínica debe conservar la supervisión, definir sus necesidades, autorizar decisiones relevantes y revisar periódicamente los resultados. Por ello, la relación con el proveedor debe gestionarse mediante evidencias, indicadores, reuniones de seguimiento y planes de mejora. Bajo este enfoque, el outsourcing deja de ser una simple delegación de tareas y se convierte en un mecanismo de apoyo para la continuidad, la recuperación y el control de los servicios tecnológicos.

Referencias

- AXELOS. (2019). *ITIL foundation: ITIL 4 edition*. TSO (The Stationery Office).
- Davenport, T. H., & Short, J. E. (1990). The new industrial engineering: Information technology and business process redesign. *Sloan Management Review*, 31(4), 11–27.
- Gilley, K. M., & Rasheed, A. (2000). Making more by doing less: An analysis of outsourcing and its effects on firm performance. *Journal of Management*, 26(4), 763–790. <https://doi.org/10.1177/014920630002600408>
- Goo, J., Kishore, R., Rao, H. R., & Nam, K. (2008). The role of service level agreements in relational management of information technology outsourcing: An empirical study. *MIS Quarterly*, 32(1), 119–145. <https://doi.org/10.2307/25148833>
- International Organization for Standardization. (2019). *Security and resilience—Business continuity management systems—Requirements (ISO 22301:2019)*. ISO.
- International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022)*. ISO.
- Lacity, M. C., Willcocks, L. P., & Craig, A. (2017). *Robotic process automation at Telefónica O2*. The Outsourcing Unit Working Research Paper Series.
- Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems* (NIST Special Publication 800-34 Rev. 1). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-34r1>

Vial, G. (2019). Understanding digital transformation: A review and a research agenda.

The Journal of Strategic Information Systems, 28(2), 118–144.

<https://doi.org/10.1016/j.jsis.2019.01.003>

Apéndice

A continuación, se presentan las tablas y figuras referenciadas a lo largo de este trabajo.



Figura 1. Proceso general de outsourcing de TI



Figura 2. Flujo de automatización de procesos

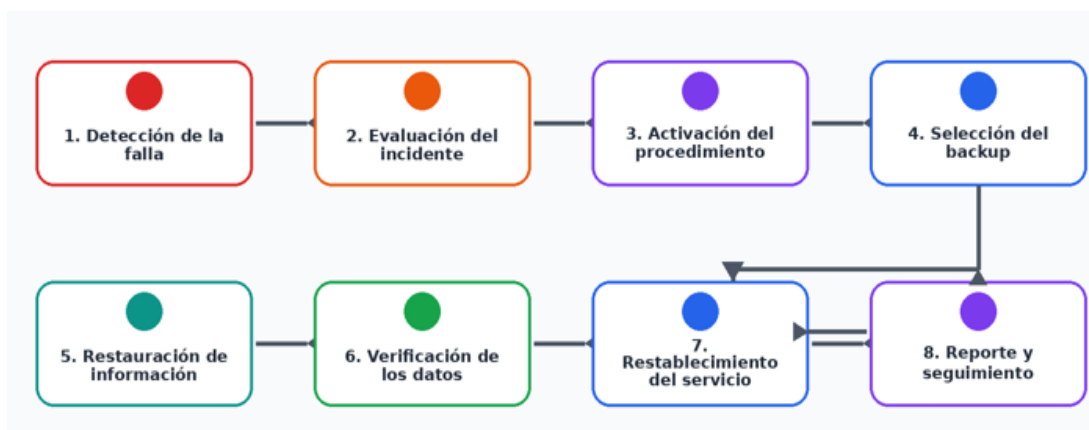


Figura 3. Aplicación del aprendizaje en el contexto empresarial

Tabla 1. Diagnóstico inicial de la gestión de servicios TI

Aspecto evaluado	Situación identificada
Mantenimiento de equipos	Se realiza principalmente cuando aparece una falla
Copias de seguridad	No existe una programación formal para todos los datos
Recuperación de información	No se cuenta con un procedimiento documentado
Soporte técnico	Se solicita cuando ocurre algún inconveniente
Supervisión de equipos	Se realiza de forma ocasional
Personal especializado	No existe un área interna dedicada exclusivamente a TI
Gestión de incidentes	Los problemas se atienden de acuerdo con su urgencia
Documentación	Los procedimientos técnicos se encuentran poco formalizados

Tabla 2. Distribución de responsabilidades

Actividad	Responsabilidad de la clínica	Responsabilidad del proveedor TI
Gestión de historias clínicas	Administrar y utilizar la información	Brindar soporte técnico
Administración de usuarios	Solicitar y autorizar accesos	Configurar técnicamente las cuentas
Copias de seguridad	Validar la importancia de la información	Ejecutar y supervisar los respaldos
Mantenimiento preventivo	Coordinar disponibilidad de equipos	Realizar las revisiones programadas
Recuperación ante fallas	Autorizar la recuperación	Ejecutar el procedimiento técnico
Soporte tecnológico	Reportar inconvenientes	Diagnosticar y solucionar incidentes
Monitoreo	Revisar los informes	Realizar seguimiento técnico
Seguridad	Establecer necesidades internas	Aplicar controles técnicos acordados

Tabla 3. Línea base académica y metas preliminares de los indicadores de gestión

TI

Indicador	Situación inicial	Meta
Cumplimiento de copias de seguridad	60%	95%
Mantenimiento preventivo realizado	50%	90%
Incidentes atendidos dentro del tiempo acordado	65%	90%
Disponibilidad de servicios tecnológicos	90%	98%
Procedimientos TI documentados	30%	90%
Recuperaciones de respaldo verificadas	40%	100%

Tabla 4. Comparación de la gestión antes y después de la propuesta

Aspecto	Situación inicial	Situación propuesta
Mantenimiento	Se realiza principalmente ante fallas	Se programa de manera preventiva
Copias de seguridad	Sin periodicidad definida	Programadas y supervisadas
Recuperación	Sin procedimiento formal	Plan de recuperación documentado
Soporte	Se solicita cuando surge un problema	Atención bajo condiciones establecidas
Seguimiento	Principalmente manual	Mediante indicadores
Especialización	Recursos internos limitados	Apoyo de personal especializado
Documentación	Parcial	Procedimientos definidos
Continuidad	Depende de la solución de cada incidente	Se apoya en prevención y recuperación