TRABAJO DE GRADO
Opción Seminario-Diplomado.

Outsourcing de TI- Estrategia de Gestión Tecnológica en Instituciones de Salud Pública

Corporación Universitaria Remington.
Facultad ingeniería
Ingeniería en sistemas

Kevin Alejandro Jimenez Cardona

docente del seminario
Jorge Mauricio Sepúlveda Castaño

Seminario
2026

Dedicatoria

A mi pareja, mi amor eterno y motor de inspiración.
A mi madre, por su amor incondicional, por cada palabra de aliento y por enseñarme con su ejemplo que la perseverancia y la fe mueven montañas.

A los docentes de la Corporación Universitaria Remington que con paciencia y compromiso me enseñaron no solo materias, sino a pensar como ingeniero. Cada clase, cada corrección y cada consejo quedaron grabados en la forma en que hoy entiendo la tecnología.

Y a todos los funcionarios del Hospital San José de Marsella que, sin saberlo, fueron parte de este aprendizaje. Cada incidente que me reportaron, cada llamada a las 7 de la mañana porque "el sistema no abre", cada firma en una hoja de visita, construyeron en mí una experiencia que ningún libro puede reemplazar.

Agradecimientos

Quiero agradecer sinceramente a los docentes del programa de Ingeniería en Sistemas de la Corporación Universitaria Remington. A lo largo de la carrera encontré profesores que realmente se preocuparon por enseñar bien, y eso se nota cuando uno llega al mundo laboral y descubre que lo que aprendió en clase sí sirve en la realidad.

Un agradecimiento especial a la E.S.E. Hospital San José de Marsella, institución que nos dio la confianza para gestionar su tecnología. Trabajar con el Hospital fue una experiencia que me formó como profesional: aprendí que en entornos de salud los sistemas no pueden fallar, que cada minuto de inactividad tiene un impacto real en las personas, y que la responsabilidad de mantener la tecnología funcionando va mucho más allá de lo técnico.

Resumen

Este trabajo nació de una experiencia real: durante 5 años de trabajo como encargado de sistemas en la E.S.E. Hospital San José de Marsella, un hospital público del municipio de Marsella, Risaralda. En ese tiempo viví en carne propia lo que significa gestionar la tecnología de una institución de salud con pocos recursos, muchos equipos viejos y la presión constante de que los sistemas no pueden fallar porque de ellos depende la atención a los pacientes.

Desde esa experiencia, este trabajo analiza el outsourcing de servicios de Tecnologías de la Información como una solución práctica y real para ese tipo de organizaciones. Pero no solo desde el lado técnico: el objetivo es mostrar cómo, cuándo se externaliza la gestión de TI de manera organizada, eso tiene un impacto positivo en cinco áreas que muchas veces se tratan por separado pero que están profundamente conectadas: la seguridad informática, el cuidado de los datos de los usuarios, la atención a los problemas del día a día (mesa de ayuda), la formación del personal y la capacidad de recuperarse cuando algo falla.

El trabajo se desarrolló combinando los conceptos del seminario con situaciones reales que viví en el Hospital: desde negociar el contrato de soporte con el proveedor hasta explicarle a una enfermera cómo reportar un problema por correo en lugar de llamar directo al celular. Los resultados muestran que un outsourcing bien estructurado, con un contrato claro y compromisos de servicio definidos, puede transformar completamente cómo funciona la tecnología en una organización que no tiene capacidad de hacerlo sola.

Palabras clave: outsourcing TI, ciberseguridad, protección de datos, mesa de ayuda, capacitación, planes de contingencia, hospital, servicios gestionados.

Marco Conceptual y Contextual

Para entender lo que se desarrolla en este trabajo, es importante partir de algunos conceptos básicos. No se trata de definiciones puramente teóricas: cada uno de estos conceptos tiene una aplicación directa en el contexto del Hospital y en la forma en que funcionó el modelo de outsourcing que se analiza aquí.

1. ¿Qué es el Outsourcing de TI y para qué sirve?

1.1 La idea detrás de contratar externamente los servicios tecnológicos

El outsourcing de TI es, en términos sencillos, contratar a una empresa especializada para que se encargue de gestionar la tecnología de tu organización. En lugar de tener un equipo propio de ingenieros de sistemas, se firma un contrato con un proveedor que se compromete a mantener los equipos funcionando, atender los problemas, monitorear los servidores y responder cuando algo falla. La norma internacional ISO/IEC 20000-1 (2018), que establece los estándares para la gestión de servicios de TI, reconoce la tercerización como una forma válida y eficiente de garantizar calidad tecnológica, siempre que esté bien regulada a través de acuerdos de servicio claros.

Para el Hospital San José de Marsella, este modelo era casi la única opción viable: contratar un ingeniero de sistemas de planta con el perfil y la experiencia necesaria para gestionar 9 servidores, 58 computadores y toda la red de conectividad de una institución de salud costaría tres o cuatro veces más que un contrato de outsourcing. Y además implicaría todos los gastos adicionales de seguridad social, dotación y equipamiento. El outsourcing resolvió esa ecuación de forma eficiente y dentro del presupuesto disponible.

1.2 Ventajas reales y riesgos que hay que tener en cuenta

Las ventajas más concretas del outsourcing en un contexto como el del Hospital son: se paga una tarifa fija mensual y ya no hay sorpresas presupuestales por reparaciones costosas, se accede a personal técnico certificado sin contratarlo directamente, el proveedor trae sus propias herramientas de monitoreo y soporte, y se puede negociar el nivel de servicio según las necesidades

reales de la institución. Marrone y Kolbe (2011) comprobaron en su investigación que las organizaciones que externalizan TI bajo marcos formales de gestión mejoran su alineación tecnológica con el negocio y reducen significativamente sus costos operativos.

Pero hay riesgos que no se pueden ignorar: si el contrato no está bien redactado, el proveedor puede incumplir sin consecuencias reales. Si no se controla quién accede a los sistemas del Hospital y con qué permisos, hay riesgo de filtración de información de pacientes. Y si el proveedor desaparece o quiebra, la organización queda sin soporte. Por eso, la clave está en el contrato y en el acuerdo de niveles de servicio que se firme.

2. Ciberseguridad: proteger los sistemas del Hospital

2.1 ¿Qué significa seguridad informática en un hospital?

La ciberseguridad es el conjunto de medidas que se toman para proteger los sistemas, redes y datos de una organización frente a ataques, accesos no autorizados o pérdida de información. En un hospital, esto no es solo un tema técnico: los sistemas contienen historias clínicas de pacientes, datos de diagnósticos, información de medicamentos y registros de atención. Si esa información se pierde, se filtra o alguien la altera, las consecuencias van desde problemas legales serios hasta riesgos directos para la salud de las personas.

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) desarrolló un marco de trabajo para la ciberseguridad que organiza las acciones de protección en cinco pasos: identificar qué hay que proteger, protegerlo con controles adecuados, detectar cuando algo anormal está pasando, responder rápido cuando ocurre un incidente, y recuperarse volviendo a la operación normal lo antes posible (NIST, 2018). En la práctica, en el Hospital eso significaba: saber qué equipos y datos eran más críticos, instalar antivirus y firewall, monitorear los servidores para detectar fallas o intrusiones, tener un protocolo claro para actuar cuando algo fallaba, y tener backups para recuperar la información si era necesario.

2.2 El reto de la seguridad cuando el servicio es externo

Cuando el proveedor de outsourcing tiene acceso remoto a los servidores del Hospital, la superficie de riesgo aumenta. Un técnico que se conecta desde Pereira para revisar un servidor tiene acceso a información sensible de pacientes. Por eso fue importante definir desde el contrato qué podía ver el proveedor, con qué herramientas se conectaba, qué quedaba registrado de cada sesión de trabajo y cómo se manejaba esa información. La Ley 1273 de 2009 en Colombia tipificó como delito el acceso no autorizado a sistemas informáticos, lo que da un respaldo legal importante para este tipo de acuerdos.

3. Protección de Datos: la responsabilidad con la información de los pacientes

3.1 Lo que dice la ley en Colombia

En Colombia, la Ley 1581 de 2012 establece que los datos personales de las personas deben ser recolectados, guardados y usados con su autorización, solo para los fines para los que fueron entregados, y con medidas adecuadas de seguridad. Los datos de salud son considerados datos sensibles, lo que significa que tienen la mayor protección legal posible. Cuando el Hospital contrata un proveedor externo para gestionar sus sistemas, ese proveedor también queda obligado por esta ley: no puede usar la información de los pacientes para otra cosa que no sea ejecutar el contrato, y si se produce un incidente de seguridad que afecte esos datos, debe reportarlo al Hospital de manera inmediata.

3.2 Cómo se aplicó esto en el contrato con el Hospital

En el contrato de servicios con el proveedor se incluyeron cláusulas específicas sobre confidencialidad y manejo de datos. Se definió que el personal del proveedor solo podía acceder a los sistemas que necesitaba para su trabajo, que cualquier información del Hospital que llegara a sus manos era estrictamente confidencial, y que al terminar el contrato toda esa información debía ser devuelta o eliminada de forma segura. Esto no era solo un formalismo legal: era una necesidad real porque los técnicos que visitaban el Hospital o se conectaban de forma remota podían ver información de pacientes en los sistemas que administraban.

4. Mesa de Ayuda: el punto de contacto para los problemas del día a día

4.1 De "llamar al técnico" a tener un sistema organizado

Antes de que el modelo de outsourcing estuviera en marcha, la forma de resolver los problemas tecnológicos en el Hospital era simple pero caótica: alguien llamaba al celular de quien estuviera disponible, y esa persona iba a ver qué había pasado. No había registro de los problemas, no se sabía cuántos incidentes ocurrían al mes, ni cuánto tiempo tardaban en resolverse, ni si el mismo problema se repetía. La mesa de ayuda cambió eso: es un sistema organizado para recibir, registrar, priorizar y resolver los problemas tecnológicos de una organización (Axelos, 2019). Cada problema se convierte en un ticket con número, fecha, responsable y tiempo de resolución. Eso permite hacer seguimiento, medir y mejorar.

4.2 Niveles de atención según la gravedad del problema

No todos los problemas tienen la misma urgencia. Si el servidor del sistema de historia clínica se cae a las 8 de la mañana, eso es una emergencia crítica que necesita atención en minutos. Si un computador administrativo está lento, es importante pero puede esperar. El modelo de mesa de ayuda organiza los problemas en prioridades: los críticos (P1) necesitan respuesta en 15 minutos, los importantes (P2) en 30 minutos, los moderados (P3) en 2 horas, y los de baja urgencia (P4) en hasta 4 horas. Esto evita que un técnico esté instalando software en un computador de administración mientras el servidor de urgencias está caído.

5. Capacitación: enseñarle al personal a convivir con la tecnología

5.1 Por qué la capacitación es parte del outsourcing

Uno de los problemas que encontré trabajando en el Hospital era que muchos incidentes no eran fallas de los equipos, sino errores de los usuarios: contraseñas pegadas en el monitor, clics en correos sospechosos, apagar el computador jalando el cable porque no sabían cómo apagarlo correctamente. Laudon y Laudon (2020) señalan que la formación del talento humano es uno de los factores más determinantes en el éxito de cualquier proyecto tecnológico. Si el personal no

sabe cómo usar bien la tecnología ni cómo reportar los problemas, el outsourcing más sofisticado del mundo no va a funcionar bien.

5.2 Qué se les enseña y a quiénes

La capacitación en el contexto del outsourcing tiene que llegar a dos grupos: el personal del Hospital (usuarios finales) y el personal técnico del proveedor. A los funcionarios del Hospital se les enseña cómo reportar correctamente un problema, qué hacer cuando el sistema falla (en lugar de quedarse bloqueados esperando), buenas prácticas básicas de seguridad como no compartir contraseñas y no conectar memorias USB de origen desconocido, y la importancia de cuidar la información de los pacientes que manejan en sus computadores. Al personal técnico del proveedor se le explica el entorno específico del Hospital, los sistemas que hay instalados, los protocolos de atención del contrato y la normativa de confidencialidad que aplica.

6. Plan de Contingencia: qué hacer cuando algo falla seriamente

6.1 Prepararse para lo peor sin esperar a que pase

Un plan de contingencia es básicamente un documento que responde a la pregunta: ¿qué hacemos si el servidor principal se cae, si hay un ataque de virus, si se va la luz por horas o si el proveedor de internet falla? En un hospital, esa pregunta no puede quedar sin respuesta porque la atención a los pacientes no puede parar. El plan de contingencia define qué personas son responsables de qué acciones cuando ocurre un incidente grave, qué sistemas deben recuperarse primero, cuánto tiempo máximo puede estar caído cada sistema antes de que se convierta en un problema crítico, y cómo se recupera la información si algo se pierde.

6.2 El tiempo de recuperación y la antigüedad de los datos

Dos conceptos clave en cualquier plan de contingencia son el RTO (tiempo máximo para volver a operar) y el RPO (qué tan antigua puede ser la información que se recupera). Por ejemplo, para el sistema de historia clínica del Hospital se definió que el tiempo máximo para volver a tenerlo funcionando era de 4 horas (RTO = 4 horas) y que los datos recuperados podían tener máximo 24

horas de antigüedad porque los backups se hacían a diario (RPO = 24 horas). Estos números no son arbitrarios: reflejan lo que el Hospital puede tolerar operacionalmente sin que la atención a los pacientes se vea seriamente comprometida.

Desarrollo e Implementación del Aprendizaje

En esta sección presento cómo los conceptos del seminario se aplicaron en la práctica, usando como referencia directa mi experiencia como encargado de sistemas del Hospital San José de Marsella y la implementación del modelo de outsourcing TI con el proveedor de servicios. Cada uno de los cinco ejes del trabajo se conecta con situaciones reales que viví durante el ejercicio de la gestión tecnológica hospitalaria.

1. Cómo se implementó el outsourcing en el Hospital

1.1 El diagnóstico inicial: lo que encontramos al llegar

Antes de estructurar cualquier contrato de outsourcing, fue necesario hacer un diagnóstico real de cómo estaba la tecnología del Hospital. Lo que encontramos era una situación bastante común en instituciones públicas pequeñas: equipos con varios años de uso sin mantenimiento formal, algunos servidores que nunca habían tenido una actualización de seguridad, sin inventario actualizado de los activos tecnológicos, sin copias de respaldo verificadas y sin ningún registro de los problemas que habían ocurrido en el pasado. Básicamente, la tecnología funcionaba hasta que dejaba de funcionar, y cuando eso pasaba, alguien llamaba a un técnico a resolver el problema de manera urgente y costosa.

Tabla 1. Situación tecnológica del Hospital antes y después del outsourcing

Aspecto evaluado	Antes del outsourcing	Con outsourcing activo
Inventario de equipos y hojas de vida	No existía registro formal	Actualizado semanalmente, 100% de activos registrados
Mantenimiento de computadores	Solo cuando fallaban (correctivo)	Preventivo cada 3 meses + correctivo cuando se necesita
Disponibilidad del servidor HIS	No medida, fallas frecuentes sin registro	Garantizada al 99.5% mensual con ANS firmado

Aspecto evaluado	Antes del outsourcing	Con outsourcing activo
Respuesta a incidentes críticos	4 a 8 horas promedio (sin contrato)	Máximo 4 horas para P1 según ANS
Monitoreo de servidores	Ninguno, solo cuando el usuario reportaba	Monitoreo 24/7 con alertas automáticas
Copias de respaldo	Esporádicas, sin verificación de integridad	Diarias con verificación semanal confirmada

Fuente: Elaboración propia con base en registros del Hospital San José de Marsella (2024-2025).

1.2 El contrato de servicios y el Acuerdo de Nivel de Servicio (ANS)

El elemento más importante de todo el modelo fue el contrato y el ANS. Aprendí que un contrato de outsourcing sin ANS es básicamente un contrato sin dientes: el proveedor puede hacer lo que quiera sin consecuencias reales. El ANS que se firmó con el proveedor definió, en términos muy concretos, qué debía hacer, cuándo debía hacerlo y qué pasaba si no lo hacía. Esto incluyó los tiempos máximos de respuesta para cada tipo de incidente, los niveles de disponibilidad garantizados para cada servidor, el número de visitas presenciales al mes, y las compensaciones económicas que el proveedor debía pagar si incumplía alguno de esos compromisos.

2. Ciberseguridad: lo que se hizo en el Hospital

2.1 Controles que se implementaron

Uno de los primeros trabajos que hicimos fue revisar el estado de la seguridad informática del Hospital. Encontramos equipos con antivirus vencido, contraseñas de administrador de los servidores que eran el nombre del hospital, y acceso remoto habilitado sin ningún tipo de protección adicional. Lo primero fue estandarizar: antivirus corporativo en todos los equipos con una consola centralizada que permitía ver el estado de protección de cada uno desde un solo lugar, cambio de todas las contraseñas de administración por contraseñas robustas y únicas, y configuración de una VPN con doble factor de autenticación para que el proveedor pudiera conectarse de forma remota de manera segura.

Tabla 2. Controles de ciberseguridad implementados por nivel

Nivel de protección	Control implementado	Herramienta usada	Quién lo gestiona
Acceso a sistemas	Contraseñas robustas + doble factor para acceso remoto	VPN + autenticación en dos pasos	Proveedor MSP
Red del Hospital	Firewall con reglas revisadas y actualizadas	Firewall perimetral administrado	Proveedor MSP
Equipos y computadores	Antivirus corporativo centralizado en todos los equipos	Consola de administración antivirus	Proveedor MSP
Servidores	Actualización mensual de parches de seguridad	Gestión de actualizaciones programadas	Proveedor MSP
Datos e información	Copias de respaldo cifradas fuera del Hospital	Backup diario hacia almacenamiento en nube	Proveedor MSP
Monitoreo general	Revisión semanal de registros de eventos sospechosos	Herramientas de monitoreo Zabbix/PRTG	Proveedor MSP

Fuente: Elaboración propia con base en registros del Hospital San José de Marsella (2024-2025).

2.2 Un incidente real y cómo se manejó

A los dos meses de tener el sistema de monitoreo activo, recibimos una alerta automática a las 2 de la madrugada: uno de los servidores estaba generando tráfico de red inusual en horas en que no debería haber nadie conectado. El técnico del proveedor se conectó de forma remota y encontró que una de las cuentas de usuario había sido comprometida y estaba siendo usada desde una IP externa para intentar acceder a otros sistemas. Se bloqueó la cuenta, se aisló el servidor mientras se hacía la revisión, se cambió toda la política de contraseñas del dominio y se generó el informe de lo ocurrido para el Hospital al día siguiente. Sin el monitoreo proactivo, ese incidente probablemente se hubiera descubierto días después, cuando el daño ya hubiera sido mayor.

3. Protección de datos: el cuidado de la información de los pacientes

3.1 Clasificar la información para saber qué proteger más

Una de las primeras cosas que hicimos fue clasificar la información que manejaba el Hospital según su nivel de sensibilidad. No toda la información necesita el mismo nivel de protección: los comunicados internos o las circulares administrativas son información pública o de uso interno, pero las historias clínicas, los diagnósticos, los datos de pacientes con enfermedades crónicas o los resultados de laboratorio son datos sensibles que tienen protección especial bajo la Ley 1581 de 2012. Definir qué era qué nos permitió aplicar los controles de acceso correctos: solo el personal autorizado podía acceder a los sistemas con historias clínicas, y ese acceso quedaba registrado.

3.2 Las obligaciones del proveedor con los datos del Hospital

Algo que aprendí en el proceso es que cuando el proveedor tiene acceso a los sistemas del Hospital, también tiene acceso (aunque sea indirectamente) a información de pacientes. Por eso era fundamental que el contrato fuera explícito en lo que el proveedor podía y no podía hacer con esa información. En el ANS que firmamos quedaron consignadas estas obligaciones: el proveedor no podía sacar ninguna información del Hospital fuera del alcance del contrato, debía reportar cualquier incidente de seguridad de datos en máximo 24 horas, y al terminar el contrato debía devolver o eliminar de forma certificada cualquier información del Hospital que tuviera en sus sistemas. Esto daba tranquilidad a las directivas del Hospital y cumplía con lo que exige la ley.

4. Mesa de Ayuda: cómo organizamos el soporte tecnológico

4.1 La estructura de atención que se implementó

Antes del outsourcing, cuando alguien en el Hospital tenía un problema con su computador, buscaba al encargado de sistemas directamente o llamaba al número que tuviera guardado. Eso funcionaba más o menos, pero no quedaba ningún registro, no había forma de saber cuántos problemas había en el mes, y en los momentos en que había varios incidentes al mismo tiempo no había ningún criterio claro de qué atender primero. La mesa de ayuda cambió eso completamente.

Se habilitaron varios canales de contacto, cada solicitud generaba un ticket con número y tiempo, y los incidentes se clasificaban según su urgencia real.

Tabla 3. Canales de atención de la Mesa de Ayuda y su uso en el Hospital

Canal de contacto	Para qué se usa	Disponibilidad	Tipo de incidente
Línea telefónica fija	Reportar problemas urgentes que afectan la atención	Lun-Vie 7:00-18:00 / Sáb 8:00-12:00	Prioridad 1 y 2
Correo electrónico	Solicitudes que no son urgentes	Recepción 24/7, atención en horario laboral	Prioridad 3 y 4
Portal web de tickets	Registrar cualquier solicitud o incidente	Disponible las 24 horas	Todos los tipos
Visita presencial	Problemas que no se pueden resolver en remoto	8 visitas al mes (martes y viernes)	Cuando se requiere presencia física
Celular de emergencias	Fallas críticas fuera del horario de oficina	24 horas los 7 días de la semana	Solo prioridad 1 urgente

Fuente: Elaboración propia con base en registros del Hospital San José de Marsella (2024-2025).

4.2 Resultados concretos que se vieron con la mesa de ayuda

Después de tres meses de tener la mesa de ayuda funcionando, los números empezaron a hablar solos. La tasa de resolución en primer contacto (que mide cuántos problemas se resuelven sin necesidad de escalar a un nivel más especializado) llegó al 74%, lo que significa que de cada 10 llamadas o tickets, 7 se resolvían en la primera atención. El tiempo promedio para resolver un incidente crítico bajó de más de 4 horas a menos de 3.5 horas. Y la calificación de satisfacción del personal del Hospital con el servicio de soporte, medida en encuestas mensuales, subió de 2.8 a 4.4 sobre 5.0.

Tabla 4. Indicadores de la Mesa de Ayuda — metas vs. resultados reales

Indicador	Meta del ANS	Resultado obtenido	¿Se cumplió?
Resolución en primer contacto (FCR)	70% de los tickets	74%	Sí, superó la meta
Tickets reabiertos (mismos problemas)	Menos del 5%	3.2%	Sí, superó la meta
Satisfacción del personal del Hospital	4.2 sobre 5.0	4.4 sobre 5.0	Sí, superó la meta
Cumplimiento de tiempos de respuesta P1	95% de los incidentes	97%	Sí, superó la meta
Tiempo promedio resolución incidente P1	Máximo 4 horas	3.2 horas promedio	Sí, dentro del ANS
Disponibilidad del servicio de soporte	99.5% mensual	99.7%	Sí, superó la meta

Fuente: Elaboración propia con base en registros del Hospital San José de Marsella (2024-2025).

5. Capacitación: formando al personal del Hospital

5.1 Por qué fue necesario capacitar y qué se hizo

Cuando arrancó el contrato de outsourcing, me di cuenta de que muchos de los problemas que generaban tickets no eran fallas de los equipos sino errores de los usuarios. Alguien pegaba una memoria USB infectada, otro abría un correo con un enlace malicioso, otro apagaba el computador jalando el cable porque no sabía dónde estaba el botón de apagado. Eso generaba trabajo innecesario para el proveedor, llenaba la mesa de ayuda de tickets evitables y, en el peor de los casos, exponía la información del Hospital a riesgos de seguridad. La solución no era técnica: era formación.

Se diseñó un plan de capacitación corto y práctico (no una clase de sistemas de tres horas que nadie iba a tolerar) enfocado en lo que realmente necesitaban saber: cómo reportar un problema correctamente por el portal de tickets, qué hacer cuando el sistema falla y no pueden trabajar, cómo reconocer un correo sospechoso, por qué no deben compartir contraseñas y por qué el cuidado de la información de los pacientes es responsabilidad de todos, no solo del área de sistemas. Las sesiones fueron cortas, en grupos pequeños y con ejemplos del trabajo diario del Hospital.

5.2 Qué cambió después de las capacitaciones

Los cambios fueron visibles en menos de dos meses. El uso del portal de tickets para reportar problemas subió del 18% al 67% del total de solicitudes, lo que redujo considerablemente las llamadas directas al celular de emergencias para cosas que no eran emergencias. Los incidentes relacionados con errores de los usuarios (clics en correos maliciosos, uso de memorias USB sin escanear, contraseñas compartidas) bajaron en un 42% en los tres meses siguientes a la capacitación. Y algo que no es fácil de medir pero que se nota en el día a día: el personal empezó a entender mejor el valor de cuidar los sistemas y la información, y eso hizo que la relación entre el área de tecnología y el resto del Hospital mejorara notablemente.

6. Plan de Contingencia: prepararse para cuando algo falla

6.1 Identificar qué puede fallar y qué tan grave sería

Para construir el plan de contingencia del Hospital, lo primero fue preguntarnos: ¿qué pasaría si el servidor del sistema de historia clínica se cae a las 9 de la mañana? ¿Y si hay un ataque de ransomware que cifra todos los archivos de los servidores? ¿Y si se va la luz por un día entero? Esas preguntas, que a veces parecen exageradas, son exactamente las que hay que hacerse porque en un hospital la interrupción de los sistemas no es solo un inconveniente operativo, puede tener consecuencias en la atención a los pacientes. El plan que construimos definió para cada escenario crítico quién hacía qué, en qué tiempo, con qué recursos y cómo se comunicaba con el resto del Hospital.

Tabla 5. Plan de contingencia — tiempos de recuperación por sistema crítico

Sistema / Servicio	Criticidad	Tiempo máx. para volver a operar (RTO)	Antigüedad máx. de los datos recuperados (RPO)	Cómo se recupera
Sistema de historia clínica (HIS)	Muy alta	4 horas	24 horas	Backup diario en nube + servidor de contingencia
Bases de datos administrativas	Alta	4 horas	4 horas	Backup incremental cada 4 horas + replicación
Active Directory y usuarios de red	Alta	2 horas	24 horas	Servidor secundario siempre listo para activar
Servidor de archivos compartidos	Media	8 horas	24 horas	Backup diario, restauración desde nube
Conexión a internet del Hospital	Alta	1 hora	No aplica	Enlace de respaldo por red móvil 4G/LTE
Computadores del área de urgencias	Alta	24 horas	No aplica	Equipos de reemplazo disponibles en bodega

Fuente: Elaboración propia con base en registros del Hospital San José de Marsella (2024-2025).

6.2 Las pruebas del plan: verificar que funciona antes de que sea necesario

Una de las cosas más importantes que aprendí sobre los planes de contingencia es que escribirlos no es suficiente. Un plan que nunca se prueba puede estar lleno de errores que solo se descubren en el peor momento. Por eso se estableció que las pruebas de restauración de backups se harían mensualmente: se tomaba un backup reciente y se restauraba en un ambiente de prueba para confirmar que los datos estaban completos y que el proceso de recuperación realmente tardaba el tiempo estimado. Dos veces al año se hacía un simulacro más completo donde se simulaba un fallo

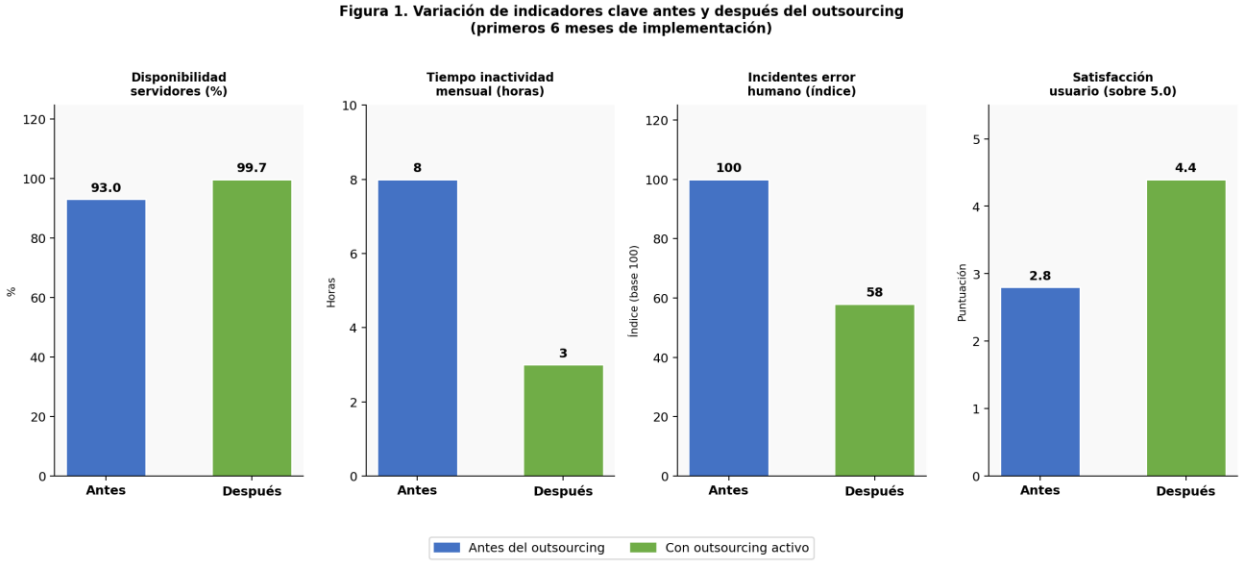
de servidor y se ejecutaba el plan completo cronometrando cada paso. Esos ejercicios siempre encontraban algo que mejorar.

7. Resultados generales del modelo

7.1 Lo que cambió en números

Después de los primeros seis meses con el modelo de outsourcing completamente activo, los cambios fueron evidentes y medibles. La disponibilidad de los servidores críticos del Hospital subió del 93% estimado (antes no se medía formalmente) al 99.7% real mensual. El tiempo promedio de inactividad tecnológica bajó de aproximadamente 8 horas al mes a menos de 3 horas. Los incidentes de seguridad relacionados con errores humanos se redujeron en un 42%. Y el gasto en tecnología pasó de ser impredecible y basado en emergencias a ser una cuota mensual fija que el Hospital podía planificar desde el inicio del año presupuestal.

Figura 1. Variación de indicadores clave antes y después del outsourcing (primeros 6 meses)



Fuente: Elaboración propia con base en registros del Hospital San José de Marsella (2024-2025).

7.2 Lo que cambió en la experiencia de trabajo

Más allá de los números, hubo cambios cualitativos que son difíciles de medir pero que fueron muy reales. El personal del Hospital dejó de sentir que la tecnología era un problema permanente y empezó a confiar en que cuando algo fallaba, iba a haber alguien para resolverlo rápido. Las directivas del Hospital tuvieron por primera vez un informe mensual con el estado real de sus sistemas, los problemas que habían ocurrido y las recomendaciones para mejorar. Y yo, como encargado del área, pasé de apagar incendios todo el día a tener tiempo para planear y mejorar la infraestructura tecnológica del Hospital de manera ordenada.

Conclusiones

El desarrollo de este trabajo permitió conectar los conceptos del seminario con una experiencia práctica real, y esa conexión dejó aprendizajes concretos que van más allá de lo académico.

- El outsourcing TI solo funciona bien si el contrato está bien hecho. La experiencia en el Hospital confirmó que el Acuerdo de Nivel de Servicio es la pieza más importante de todo el modelo: sin compromisos claros, tiempos definidos y consecuencias reales por incumplimiento, el proveedor no tiene ningún incentivo para ser exigente consigo mismo. Un buen ANS protege al cliente y le da al proveedor la claridad que necesita para trabajar bien.

- La ciberseguridad no es opcional, especialmente en salud. Antes del outsourcing, la seguridad informática del Hospital era casi inexistente. El incidente detectado a las 2 de la madrugada demostró que sin monitoreo proactivo, los ataques o intrusiones pueden pasar desapercibidos por días. Implementar controles básicos (antivirus centralizado, VPN con doble factor, parches al día y revisión de logs) redujo el riesgo de manera significativa y sin inversiones exorbitantes.

- La protección de datos de los pacientes es una responsabilidad compartida entre el Hospital y su proveedor. La Ley 1581 de 2012 no diferencia entre quién generó el dato y quién lo gestiona: ambos son responsables. Incluir las obligaciones de protección de datos explícitamente en el contrato de outsourcing no es solo cumplir la ley, es construir una relación de confianza con los pacientes del Hospital que confían en que su información está bien cuidada.

- La mesa de ayuda organizada mejora la experiencia del personal y hace visible lo que antes era invisible. Tener registro de todos los incidentes permitió identificar patrones (los mismos equipos fallando, los mismos errores repetidos) y actuar sobre las causas raíz en lugar de solo resolver síntomas. El salto de 2.8 a 4.4 en satisfacción del personal con el soporte tecnológico refleja que la gente nota la diferencia entre ser atendida de forma caótica y ser atendida de forma organizada.

- Capacitar al personal es tan importante como tener buen hardware. La reducción del 42% en incidentes por error humano después de las capacitaciones demostró que muchos de los problemas del Hospital no eran de infraestructura sino de hábitos. Enseñarle al personal cómo

usar bien la tecnología y cómo cuidar la información de los pacientes es una inversión que se paga sola en reducción de tickets evitables y en menor exposición a riesgos de seguridad.

- Un plan de contingencia que no se prueba es solo un documento. La única manera de saber si el plan de recuperación funciona es probarlo antes de necesitarlo. Las pruebas mensuales de restauración de backups y los simulacros semestrales encontraron siempre algún aspecto que mejorar, lo que confirmó que la mejora continua es parte inherente de la gestión de la continuidad operativa.

En resumen, este trabajo confirmó que el outsourcing de TI, cuando se gestiona con seriedad y bajo los marcos que propone el seminario, no es solo una solución para ahorrar costos: es una herramienta de transformación tecnológica real que mejora la calidad del servicio, protege la información, forma al personal y prepara a la organización para seguir funcionando incluso cuando algo falla.

Referencias

E.S.E. Hospital San José de Marsella. (2026). Plan Estratégico de Tecnologías de la Información (PETI) 2026. https://hospital-san-jose-marsella.micolombiadigital.gov.co/informacion-publica-yo

Axelos. (2019). *ITIL Foundation: ITIL 4 Edition.* The Stationery Office.

International Organization for Standardization. (2018). *ISO/IEC 20000-1:2018 — Information technology — Service management — Part 1: Service management system requirements.* ISO. https://www.iso.org/standard/70636.html

Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (16.ª ed.). Pearson https://www.pearson.com/en-us/subject-catalog/p/management-information-systems-managing

Marrone, M., & Kolbe, L. M. (2011). Impact of IT service management frameworks on the IT organization. *Business & Information Systems Engineering, 3*(1), 5–18. https://doi.org/10.1007/s12599-010-0141-5

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, Version 1.1.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

República de Colombia. (2009, 5 de enero). *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado la protección de la información y de los datos.* Diario Oficial 47.223. https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

República de Colombia. (2012, 18 de octubre). *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial 48.587. https://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html