TRABAJO DE GRADO
Opción Seminario.

Integración de la ciberseguridad en servicios tercerizados del Hospital San José de Buga: Un enfoque basado en riesgos y cumplimiento normativo

Corporación Universitaria Remington.
facultad Ingeniería de Sistemas
Transformación Digital y Outsourcing Inteligente en TI

.

Nombres de los estudiantes autores del trabajo de grado.
Humberto German Barbosa Valencia CC 94482572
Manuel Santiago Becerra CC 1115092326
Tutor Jorge Mauricio Sepúlveda Castaño
Opción de Trabajo de grado Seminario.

2025.

Tabla de Contenidos

1. Resumen

Este trabajo examina la gestión de la ciberseguridad en servicios tercerizados dentro de un entorno hospitalario, analizando los riesgos vinculados a la protección de datos sensibles y la obligación de cumplir la normativa legal cuando la función de ciberseguridad forma parte de un modelo de outsourcing de TI. El punto de partida consiste en una revisión conceptual de los términos esenciales—externalización de tecnología (outsourcing TI), ciberseguridad, acuerdos de nivel de servicio (SLA) y obligaciones legales vinculadas a los datos—para, a continuación, situar dichos conceptos dentro del contexto del Hospital San José de Buga, la institución de salud elegida como caso de estudio. Seguidamente, se detalla de forma minuciosa la aplicación práctica de los conocimientos adquiridos en el seminario de outsourcing TI en esa entidad, incluyendo la identificación de riesgos particulares detectados al integrar… En la gestión de la ciberseguridad se recurre a un proveedor externo, describiendo las contramedidas propuestas y el proceso de diseño o revisión de los SLA, los contratos y los controles de seguridad necesarios para afrontar esos riesgos. Además, incorporé ejemplos reales —por ejemplo, anexos de SLA y contratos— que me ayudaron a aterrizar cómo se fijan las métricas de desempeño, las responsabilidades y las penalizaciones dentro de la relación con el proveedor. Al cierre del trabajo, resumo lo aprendido en la práctica: destaco los hallazgos que más peso tuvieron, reviso qué tan efectivas resultaron las medidas para proteger la información del hospital y cumplir la norma, y dejo recomendaciones puntuales para seguir fortaleciendo la ciberseguridad en escenarios de outsourcing del sector salud (ISACA, 2018; Drivas et al., 2020).

Palabras clave

Outsourcing TI; Ciberseguridad; Acuerdos de Nivel de Servicio; Protección de datos; Cumplimiento normativo.

2. Marco conceptual y contextual

Modelo de Evaluación Integral de Proveedores (MEIP)
El MEIP es un modelo práctico para evaluar proveedores de TI en hospitales. Como estudiantes de ingeniería, lo usamos para aterrizar marcos como ISO/IEC 27036-3 (relaciones con proveedores) y NIST SP 800-161 (riesgo en la cadena de suministro), y para conectarlos con requisitos locales de privacidad (Ley 1581 de 2012). La idea es simple: medir con criterios claros, comparar proveedores con la misma vara y dejar evidencia de cada decisión (MEIP, s. f.; ISO/IEC, 2023; Boyens et al., 2022; Congreso de Colombia, 2012).
Dimensiones y ponderaciones del MEIP
Capacidad técnica – 35 %: integraciones (HIS/PACS), soporte crítico, tiempos de respuesta.
Cumplimiento legal y normativo – 25 %: Ley 1581/Habeas Data, contratos, auditorías, exigencias del sector salud.
Gobernanza y gestión de riesgos – 20 %: SLA/ANS, RACI, reportes, gestión de cambios y continuidad (RTO/RPO como criterio).
Factores económicos y contractuales – 15 %: modelo de precios, transparencia, escalabilidad, penalidades.
Adaptabilidad al contexto hospitalario – 5 %: conocimiento de flujos clínicos, flexibilidad operativa.
Capacidad técnica – 35 %: integraciones (HIS/PACS), soporte crítico, tiempos de respuesta.

En esta sección se definen los conceptos fundamentales y se describe el contexto específico del Hospital San José de Buga que sirve de escenario de aplicación. Estos conceptos proveen el marco teórico necesario para comprender la implementación realizada.

2.1. Outsourcing de TI

Cuando hablamos de outsourcing de TI, no se trata solo de "contratar a un tercero". En la práctica, implica acordar con una empresa externa qué procesos tecnológicos asumirá, con qué niveles de servicio y bajo qué responsabilidades compartidas. Suele abarcar tareas como soporte de aplicaciones, administración de servidores, ciberseguridad 24/7 o proyectos puntuales (por ejemplo, migraciones), con el propósito de que la organización gane eficiencia y enfoque mientras el proveedor aporta especialización y capacidad de respuesta.

En la literatura se resaltan beneficios recurrentes: reducción de costos por economías de escala, acceso a talento especializado y a tecnologías avanzadas que sería costoso desplegar internamente, así como tiempos de implementación más cortos (Negreiro, 2023; Ditech Group, 2023). Este modelo permite, ademas, que la empresa se centre en su negocio principal. Estos servicios pueden abarcar software, infraestructura, soporte y procesos de negocio.

En la práctica, el enfoque de Outsourcing es una herramienta indispensable en la transformación digital y la adaptabilidad de las organizaciones a mercados dinámicos (Negreiro, 2023). Suele ser especialmente útil para aquellas compañías que no cuentan con una infraestructura tecnológica solida o con equipo interno con capacidad limitada o carente de habilidades específicas. Gracias a las delegaciones de funciones o procesos tecnológicos a un tercero especializado las organizaciones pueden (Ditech Group, 2023):

- **Acceder a tecnología y talento avanzado:** donde los equipos son altamente capacitados y experimentados.

- **Focalización y eficiencia:** Permiten que las empresas se centren en su negocio principal y libere al equipo interno para enfocarse en tareas más estratégicas.

- **Beneficio financiero:** Permite reducir costos y transformar costos fijos en variables, evitando las grandes inversiones iniciales en infraestructura, tecnología o la contratación de nuevo personal.

- **Adaptabilidad:** Al ser más flexible se adapta a los servicios según demanda real del negocio.

Aun cuando el outsourcing ofrece beneficios significativos, este modelo conlleva a riesgos y desafíos que deben gestionarse como (Boyens et al., 2022; ENISA, 2021):

- **Pérdida de Control:** donde al existir una menor supervisión sobre los procesos críticos que han externalizado.

- **Riesgos de seguridad:** Al existir la exposición de datos sensibles si la relación no se gestiona de manera adecuada. Las nuevas amenazas

en los entornos externalizados exigen el uso de estrategias solidas de protección de datos y el cumplimiento normativo.

- **Dependencia del proveedor:** Se genera contingencias si el proveedor falla o no cumplen las expectativas.
- Se deben establecer acuerdos claros y el proveedor debe convertirse en un socio estratégico para lograr innovación y valor a largo plazo. Ambas cosas son necesarias.

Si una empresa decide externalizar TI, debe elegir bien al proveedor, integrarlo de forma ordenada y vigilar su desempeño. Con acuerdos transparentes, el proveedor puede convertirse en un aliado estratégico para la innovación y el valor sostenido.

Para asegurar que el proveedor realmente se alinee con los objetivos y necesidades del negocio, resulta clave *(ISACA, 2018; Drivas et al., 2020)*:

- **Alinear los servicios:** La TI tiene que ir de la mano de la estrategia del negocio.
- **Definir Indicadores Medibles (KPIs):** Es primordial definir y monitorear indicadores claves de desempeño. Estos deben ser específicos, medibles, alcanzables, relevantes y con límite temporal.
- **Establecer ANS:** Es necesario garantizar el cumplimiento de Acuerdos de Nivel de Servicio avanzados que establezcan metas claras de tiempo de respuesta, resolución y disponibilidad.
- **Monitoreo continuo:** Se debe realizar revisiones periódicas y automatizar el reporte de métricas ara evaluar continuamente los resultados y ajustar la estrategia según sea necesario.

2.2.Ciberseguridad

Se refiera a la combinación de métodos, procesos, herramienta y comportamientos donde se protegen los sistemas informáticos, redes, y los datos de ciberataques y el acceso no autorizado. La ciberseguridad este arraigado profundamente a la tecnología, la eficiencia de esta disciplina también depende en gran medida de las

personas. En nuestro caso de estudio, la ciberseguridad es esencial, ya que garantiza la seguridad y cumplimiento en el manejo de información crítica.

En nuestro entorno se incluyen aspectos fundamentales como:

- **Protección de Datos Sensibles:** Busca que la información siga siendo confidencial, íntegra y disponible; sin eso, la operación se resiente y la confianza se pierde.

- Cumplimiento Obligatorio: Las empresas están obligadas a cumplir normas como el GDPR y la NIS2, las cuales requieren salvaguardar correctamente los datos personales (ENISA, 2021) (European Parliament and Council, 2016).

- **Estrategias de mitigación de riesgos:** Implica implementar controles técnicos (cifrados, firewall, etc.) y garantizar la seguridad de red, respaldos y recuperación de data. En contextos de outsourcing surgen amenazas nuevas. Por eso es esencial prevenirlas y establecer estrategias **de protección de datos**, evitando la exposición de información sensible.

- Externalización de Seguridad: Es posible subcontratar la gestión de seguridad de la información. Así, el hospital se apoya en equipos expertos para planear e implementar los controles necesarios (ENISA, 2021).

2.3.Acuerdos de Nivel de Servicio (ANS)

Un ANS (SLA) es un contrato esencial en la gestión de servicios de TI: establece qué nivel de calidad y desempeño se espera del proveedor y qué recibirá el cliente (ISACA, 2018) (ISACA, 2018; Drivas et al., 2020).

Concretamente, fija garantías de calidad y tiempos de respuesta para los servicios tercerizados. Su correcta gestión asegura que los servicios se entreguen de manera eficiente y alineada con la estrategia del negocio, y actúa como un marco de gobierno de la relación cliente–proveedor *(Drivas et al., 2020; ISACA, 2018)*.

Los ANS son de vital importancia en los contratos externalizados, especialmente en la contratación basada en resultados. El cumplimiento de los ANS es una métrica primordial para evaluar si el outsourcing está cumpliendo con los objetivos establecidos. En la práctica, el monitoreo del servicio después de la externalización

se realiza a través del seguimiento de tickets y el cumplimiento de los ANS definidos.

Para medir el rendimiento de un proveedor y garantizar el cumplimiento del contrato, el ANS se vincula estrechamente con la definición y el monitoreo de indicadores clave de desempeño. Los ANS avanzados deben especificar lo que se considera un nivel de servicio aceptable mediante métricas medibles y realistas (Drivas et al., 2020):

Como los **Tiempo de Resolución de Servicio** que mide el tiempo promedio que transcurre desde la solicitud hasta la solución de un incidente o ticket. La **Disponibilidad** define el porcentaje de tiempo en que el sistema o servicio debe estar activo y disponible, siendo una meta típica superior al 99.9%. La **gestión de ANS avanzados** requiere la automatización del reporte para visualización en tiempo real y la realización de revisiones periódicas para evaluar si se cumple los objetivos y ajustar la estrategia si es necesario.

2.4. Cumplimiento legal y protección de datos

El cumplimiento legal y la protección en los datos en los servicios de TI externalizados, especialmente en el contexto de una organización hospitalaria, constituye un pilar fundamental.

El cumplimiento legal en el outsourcing de TI significa cumplir sin excepciones las normas de tecnología y protección de datos. En salud, esto es clave porque se manejan datos sensibles (historias clínicas, identidad, información sanitaria). Si un tercero accede o trata datos de pacientes, el servicio debe ajustarse a la ley. En el ámbito nacional, En el país, la Ley 1581 de 2012 define cómo se protegen los datos personales y asegura a las personas el derecho a conocer**,** actualizar **y** rectificar su información. (Congreso de Colombia, 2012).

- **Definición de Roles Contractuales**
  Para formalizar el cumplimiento legal y mitigar los riesgos de seguridad de datos, el ANS de outsourcing debe definir claramente las figuras legales involucradas en el tratamiento de los datos, tal como lo establece la Ley 1581 de 2012: (Congreso de Colombia, 2012)

- **Responsable Legal del Tratamiento:** El hospital mantiene esta figura legal, ya que es la entidad dueña de los datos. El hospital es quien establece las finalidades y reglas para el tratamiento de la información.

- **Encargado del Tratamiento:** El proveedor externo de TI actúa como encargado, tratando los datos por cuenta del hospital. En otras palabras, El proveedor debe seguir al pie de la letra los fines y las reglas que fije el hospital.

- **Obligaciones Contractuales y Mitigación de Riesgos**
  En outsourcing inteligente, el contrato tiene que dejar por escrito las cláusulas de seguridad y cumplimiento, en línea con GDPR y NIS2. Estas cláusulas obligan al proveedor, como encargado del tratamiento, a: (European Parliament and Council, 2016)

  - ✓ **Confidencialidad y Uso Restringido:** El proveedor cumple la ley, **no divulga** la información a la que accede y trata los datos solo según las instrucciones del cliente; no los usa para otros fines ni los comparte con terceros.
  - ✓ **Gestión Post-Contrato:** El contrato debe indicar que, al terminar el servicio, los datos personales se eliminan o se devuelven al hospital. Cumplir con esto es esencial: si la relación con el proveedor no se gestiona bien, puede exponerse información sensible. Por ello, en el outsourcing inteligente, la seguridad y el cumplimiento son requisitos centrales al elegir y supervisar al proveedor.

2.5.Contexto del Hospital San José de Buga

El Hospital San José de Buga, como institución de salud, opera en un entorno altamente sensible, caracterizado por el manejo de volúmenes significativos de datos clínicos y administrativos altamente confidenciales La decisión de optar por la tercerización de servicios de TI, incluyendo aspectos de ciberseguridad, se fundamenta en la búsqueda de los beneficios estratégicos del outsourcing (Negreiro, 2023; Ditech Group, 2023).

Tipología y Justificación de la Externalización de Servicios

El hospital clasifica su modelo de outsourcing según los servicios que externaliza, de esta forma:

> **Outsourcing de Infraestructura de TI:** Abarca la gestión **y** mantenimiento de la infraestructura de redes y servidores.
>
> **Outsourcing de Seguridad de la Información:** Cubre el monitoreo del perímetro (firewalls, IDS/IPS) y la gestión de backup**s**. Se justifica porque permite acceder a personal experto y experiencia específica para reforzar la seguridad ante ciberataques.
>
> Outsourcing de Soporte y Mantenimiento: Involucrar el mantenimiento de sistemas de información hospitalaria asegurando la resolución de problemas técnicos y la ayuda a usuarios finales (ISACA, 2018).

El objetivo central de esta tercerización es aprovechar la expertise de proveedores especializados y optimizar los recursos tecnológicos, lo cual se alinea con la ventaja de acceder a talentos especializados y reducir costos, tal como lo señala la literatura sobre el tema (Negreiro, 2023; Ditech Group, 2023).

Objetivos Estratégicos Críticos

Alinear la estrategia con la operación exige cumplir requisitos concretos que afectan directamente la seguridad del paciente:

> **Disponibilidad de Sistemas:** Para que la atención médica no se detenga, los sistemas deben estar siempre disponibles. Esta exigencia se traduce en la gestión de KPIs como el Uptime, donde la meta típica es mayor al 99.9%. La subcontratación proporciona Disponibilidad 7x24, esencial para el área de TI y el negocio, ya que el proveedor garantiza la continuidad del servicio incluso ante la ausencia de colaboradores (ISACA, 2018).
>
> Focalización en el Negocio Principal: La carga operativa TI al ser delegada, el hospital puede enfocarse en su actividad principal que es la atención médica, liberando al equipo interno para concentrarse en tareas más estratégicas (Negreiro, 2023; Ditech Group, 2023).

Acceso a Tecnología Avanzada: El outsourcing permite que hospital disponga de la tecnología más novedosa y herramientas de última generación, sin tener que realizar grandes inversiones iniciales, transformando así costos fijos en variables (Ditech Group, 2023).

Gestión de Riesgos y Cumplimiento Legal

El outsourcing inteligente debe abordar la gestión efectiva de los riesgos de ciberseguridad y responsabilidades legales asociados a la información sanitaria confidencial.

Riesgo de Seguridad de Datos: El manejo de información como las historias clínicas generan un riesgo inherente de exposición de datos sensibles. El hospital debe priorizar la seguridad y cumplimiento, asegurándose de que el proveedor apoye la planificación e implementación de sistemas de seguridad (Boyens et al., 2022).

Cumplimiento Normativo: El hospital está sujeto a leyes colombianas de protección de datos personales lo que exige que los proveedores de servicios en la nube (SaaS, IaaS) cumplan con las leyes y regulaciones aplicables a su industria y región. La necesidad de cumplimiento se alinea con la tendencia de priorizar la ciberseguridad y cumplimiento regulatorio (GDPR, NIS2) en el futuro del outsourcing (ENISA, 2024) (European Parliament and Council, 2016).

Gobernanza Contractual: La solución práctica implica el establecimiento de ANS y contratos que deben incluir cláusulas que definan las obligaciones de las partes y los mínimos de calidad del servicio. Los contratos deben detallar cómo se abordará la implementación práctica de la tercerización, identificando riesgos específicos y las soluciones aplicadas, en línea con las mejores prácticas de gobierno de TI (ISACA, 2018; Drivas et al., 2020).

En síntesis, el caso del Hospital San José de Buga es un ejemplo de cómo el outsourcing de TI se utiliza como una estrategia de gestión de servicios para lograr eficiencia y adaptabilidad mientras se mitigan los riesgos operativos y legales mediante una selección, integración y monitoreo rigurosos de los proveedores.

2.5.1. Diagnóstico inicial y necesidades específicas

El Hospital San José de Buga, como institución de salud, opera en un entorno altamente sensible, caracterizado por el manejo de volúmenes significativos de datos clínicos y administrativos altamente confidenciales. Nuestro diagnóstico inicial reveló desafíos críticos que justificaban el desarrollo de metodologías propias de evaluación.
Metodología MEIP (tres fases)

- Primero revisamos papeles, luego probamos en práctica y, por último, validamos con evidencias. Esto nos permitió reducir tiempos de evaluación sin perder calidad (MEIP, s. f.).
- Fase documental: verificamos requisitos legales, de seguridad y capacidad técnica declarada.
- Fase práctica: pedimos demos y laboratorios guiados para ver el servicio en acción.
- Fase de validación: corremos simulacros/PoC, medimos tiempos de respuesta y dejamos reportes.

Problema Identificado:
El Hospital San José de Buga carecía de una metodología estandarizada para evaluar proveedores de servicios de ciberseguridad tercerizados, lo que generaba inconsistencia en la selección y dificultaba la comparación objetiva entre alternativas.

Hallazgos del Diagnóstico:

- Evaluaciones previas basadas principalmente en costos (65% de peso)
- 45% de proveedores históricos no cumplían expectativas técnicas
- Tiempo promedio de evaluación: 2 semanas sin criterios estandarizados
- Ausencia de dimensiones específicas para sector salud

2.5.2. Modelo de Evaluación Integral de Proveedores (MEIP)

Solución Desarrollada:
Se hizo el Modelo de Evaluación Integral de Proveedores (MEIP) con criterios específicos para el sector salud, organizados en 5 dimensiones críticas:

Dimensión 1: CAPACIDAD TÉCNICA Y EXPERIENCIA (35% ponderación)
Criterios Evaluados:

1. **Certificaciones de Seguridad:** ISO 27001, SOC 2 Type II, certificaciones específicas del sector salud

2. **Experiencia en Entornos Hospitalarios:** Número de proyectos similares ejecutados (+3 años en sector salud)

3. **Capacidad de Respuesta 24/7:** Infraestructura SOC propia, tiempos de respuesta documentados

4. **Tecnologías Implementadas**: Firewalls NGFW, SIEM, EDR, soluciones de cifrado

5. **Arquitectura de Seguridad:** Diseño específico para protección de datos médicos

Ejemplo aplicado: Proveedor "Seguridad Hospitalaria SAS" demostró 12 proyectos en hospitales de tercer nivel y certificación ISO 27001:2022.

Dimensión 2: CUMPLIMIENTO LEGAL Y NORMATIVO (25% ponderación)
Criterios Evaluados:
6. Conocimiento Ley 1581 de 2012: Protocolos específicos para datos sensibles de salud (Congreso de Colombia, 2012)
7. Adecuación GDPR/HIPAA: Mecanismos para transferencias internacionales (si aplica) (European Parliament and Council, 2016)
8. **Historial de Cumplimiento:** Ausencia de sanciones por violación de datos
9. **Políticas de Retención:** Alineación con tiempos legales de historias clínicas (20+ años)

10. **Protocolos de Notificación:** Procedimientos para reportar brechas a autoridades

Ejemplo aplicado: Se verificó que el proveedor contaba con cláusulas contractuales específicas para el tratamiento de historias clínicas según resolución 1995 de 2022.

Dimensión 3: Gobernanza Y Gestión de Riesgos (20% ponderación)
Criterios Evaluados:
11**. Metodología de Gestión de Riesgos:** Alineación con NIST SP 800-30
12. **Frecuencia de Auditorías:** Programas trimestrales de evaluación
13. **Transparencia en Reporting**: Dashboards en tiempo real accesibles al hospital
14. **Plan de Continuidad:** Estrategias para garantizar servicios críticos
15. Manejo de Incidentes: Procedimientos documentados para respuesta a brechas

Dimensión 4: Factores económicos y contractuales (15% ponderación)
Criterios Evaluados:
16. **Estructura de Costos:** Transparencia en tarifas, sin costos ocultos
17. **Escalabilidad:** Capacidad de ajustar servicios según demanda hospitalaria
18. **Penalizaciones por Incumplimiento:** Mecanismos claros de compensación
19. **Cláusulas de Salida:** Procedimientos para transición ordenada
20. **Seguros de Responsabilidad:** Coberturas por posibles brechas de datos

Dimensión 5: Adaptabilidad al contexto hospitalario (5% ponderación)
Criterios Evaluados:
21. **Conocimiento de Flujos Clínicos:** Comprensión de procesos médicos críticos
22. **Integración con Sistemas Médicos:** Experiencia con PACS, HIS, EPIC
23**. Manejo de Dispositivos Médicos:** Protocolos para equipos médicos conectados
24. **Capacitación al Personal:** Programas específicos para personal de salud
25. **Comunicación con Áreas Médicas:** Canales establecidos con jefes de servicios
26. **Respeto de Horarios Críticos:** Planificación que evita interrupciones en cirugías
27. **Adaptación Cultural:** Alineación con valores institucionales del hospital

Metodología de aplicación en el hospital San José de buga

Fase 1: Evaluación Documental (40% calificación)

- ✓ Revisión de certificaciones, políticas, procedimientos
- ✓ Verificación de referencias con otros hospitales
- ✓ Análisis de reportes de auditoría externa

Fase 2: Pruebas Prácticas (35% calificación)

- ✓ Simulacros de respuesta a incidentes
- ✓ Pruebas de penetración controladas
- ✓ Evaluación de tiempos de respuesta reales

Fase 3: Entrevistas y Validación (25% calificación)

- ✓ Sesiones con equipo técnico del proveedor
- ✓ Validación de casos de éxito similares
- ✓ Evaluación de capacidad de comunicación

Resultados de la aplicación del MEIP (MEIP, s. f.)

Proveedor Seleccionado: "CiberSalud Colombia SAS"

- ✓ Puntuación MEIP: 92/100 (MEIP, s. f.)
- ✓ **Fortalezas Principales: Experiencia en 8 hospitales de similar complejidad, certificación ISO 27001, tiempos de respuesta <15 minutos para incidentes críticos**
- ✓ **Áreas de Mejora Identificadas:** Capacitación específica en sistemas PACS (se incluyó como requisito contractual)

Comparativa con Alternativas:

- ✓ Proveedor A: 78/100 (Falta experiencia sector salud)
- ✓ Proveedor B: 85/100 (Costos no transparentes)
- ✓ Proveedor C: 92/100 (SELECCIONADO)

3. Desarrollo e implementación del aprendizaje

En esta sección central del trabajo se explica cómo se llevó a la práctica el aprendizaje teórico del seminario de outsourcing TI en el caso del Hospital San José de Buga. Se presentan los riesgos de ciberseguridad detectados al incorporar un proveedor externo para servicios de seguridad (CIS, 2023; ISO/IEC, 2023; NIST, 2024a; NIST, 2024b), las estrategias y medidas implementadas para mitigarlos (CIS, 2023; ENISA, 2020; NIST, 2024a; NIST, 2024b), y el diseño de los acuerdos de servicio y controles contractuales correspondientes (ISO/IEC, 2018; ISO/IEC, 2022; U.S. Department of Health & Human Services, 2013). Además, se ilustran ejemplos concretos obtenidos de documentos como acuerdos de nivel de servicio y cláusulas contractuales utilizadas, incluyendo tablas y figuras que muestran cómo se definieron métricas de desempeño y responsabilidades en el contrato de outsourcing (ENISA, 2020; ISO/IEC, 2018).

3.1. Identificación de riesgos en la ciberseguridad tercerizada

Al integrar la ciberseguridad dentro de un modelo de outsourcing TI en el Hospital San José de Buga, se identificaron diversos riesgos clave asociados a la protección de datos, la continuidad operativa y el cumplimiento normativo. Según el National Institute of Standards and Technology (Boyens et al., 2022), la externalización de funciones críticas amplía la superficie de ataque al incorporar terceros en la cadena de suministro digital, generando nuevas vulnerabilidades en los sistemas clínicos.

Entre los principales riesgos detectados se encuentran las brechas de datos y accesos no autorizados, derivadas de la gestión externa de información sensible. Tal como advierte (European Union Agency for Cybersecurity [ENISA], 2024), los proveedores que no implementan mecanismos robustos de control de accesos y auditoría pueden convertirse en vectores de exposición de datos personales y clínicos. Asimismo, se identificó el riesgo de incumplimiento legal y regulatorio, dado que la Ley 1581 de 2012 atribuye al hospital la responsabilidad última sobre el tratamiento de datos personales. Este tipo de incumplimiento puede acarrear sanciones administrativas y

pérdida de confianza pública (Ditech Group, 2023; ISACA, 2018) (Congreso de Colombia, 2012).

Otro riesgo relevante fue la disminución en la calidad o continuidad del servicio, pues un proveedor que no cumple los Acuerdos de Nivel de Servicio (SLA) podría afectar la disponibilidad de los sistemas clínicos. Según Peltier (2016), la falta de mecanismos de supervisión contractual y la dependencia tecnológica generan vulnerabilidades operativas críticas en entornos hospitalarios. Finalmente, se advirtió la posibilidad de dependencia excesiva (vendor lock-in) y pérdida de conocimiento interno, lo que podría comprometer la resiliencia institucional frente a cambios de proveedor (Peltier, 2016) (ISACA, 2018; Drivas et al., 2020).

Estos hallazgos evidencian que la gestión de la ciberseguridad tercerizada requiere una supervisión constante, la definición clara de responsabilidades y la implementación de auditorías cruzadas para mitigar los riesgos derivados de la pérdida de control directo sobre la infraestructura tecnológica (ENISA, 2024; NIST, 2022).

Para cada uno de estos riesgos se estableció una relación con causas potenciales en el contexto del outsourcing y se evaluó su probabilidad e impacto (ISACA, 2018; NIST, 2022). En general, se concluyó que muchos de los riesgos derivan de la **pérdida de control directo** sobre funciones críticas de TI que pasan a ser operadas por un tercero (ENISA, 2024; NIST, 2022). Sin embargo, dichos riesgos **no son inevitables**; con una adecuada gestión, es posible mitigarlos significativamente **(ENISA, 2024; Peltier, 2016)**. En la siguiente subsección se describen las estrategias y medidas implementadas para tratar cada riesgo identificado, alineadas con las mejores prácticas de gestión de riesgos en outsourcing TI (NIST, 2022; ENISA, 2024; ISACA, 2018).

Tabla 1
Identificación de riesgos en la ciberseguridad tercerizada
Fuente: Adaptado de ENISA (2024) y NIST (2022).

Riesgo	Descripción	Causa principal	Impacto potencial
Brechas de datos y acceso no autorizado	Posible exposición de información sensible por vulnerabilidades o mala gestión del proveedor.	Falta de controles técnicos y supervisión.	Pérdida de confidencialidad y sanciones legales.
Incumplimiento legal y regulatorio	Riesgo de violar la Ley 1581/2012 por manejo inadecuado de datos personales.	Transferencias sin consentimiento o sin garantías.	Multas, pérdida de confianza institucional.
Disminución en la calidad o continuidad del servicio	Incumplimiento de tiempos o disponibilidad pactada.	Mala gestión del proveedor o infraestructura deficiente.	Interrupción en servicios clínicos.
Dependencia excesiva y falta de control	Vendor lock-in o pérdida de conocimiento interno.	Definición ambigua del contrato.	Vulnerabilidad ante fallas del proveedor.
Riesgo reputacional	Daño de imagen por filtraciones o incidentes de seguridad.	Respuesta ineficaz ante incidentes.	Pérdida de confianza de pacientes.

3.2. Medidas de mitigación de riesgos

Para abordar los riesgos anteriores, el Hospital San José de Buga, junto con su proveedor de servicios de ciberseguridad, adoptó medidas basadas en las mejores prácticas internacionales descritas por NIST (2020) y ENISA (2021). Estas medidas se enfocaron en tres ejes principales: la selección rigurosa del proveedor, la formalización de acuerdos contractuales sólidos y la definición de mecanismos de seguimiento continuo.

En primer lugar, se aplicó un proceso de selección rigurosa del proveedor con criterios basados en certificaciones como **ISO/IEC 27001**, experiencia comprobada en el sector salud y políticas de seguridad alineadas con el marco **COBIT 2019 (ISACA, 2018)**. Este enfoque garantiza la alineación entre los objetivos institucionales y las prácticas de seguridad externas (Boyens et al., 2022).

En segundo lugar, se diseñaron Acuerdos de Nivel de Servicio (SLA) específicos que establecen tiempos máximos de respuesta ante incidentes, disponibilidad mínima mensual de sistemas críticos (99.9%) y penalizaciones económicas por incumplimiento. Este tipo de acuerdos, como destaca ENISA (2021), son esenciales para asegurar la trazabilidad de

la calidad del servicio y la protección de datos en entornos de outsourcing (ISACA, 2018; Drivas et al., 2020).

Finalmente, se implementó un sistema de monitoreo conjunto y auditorías periódicas, en línea con el principio de mejora continua del NIST Cybersecurity Framework (2020). Estas auditorías permiten detectar desviaciones tempranas en el cumplimiento de controles y garantizan que las medidas de seguridad evolucionen con los cambios tecnológicos.

En conjunto, estas estrategias refuerzan la resiliencia del hospital ante incidentes y aseguran que la relación con el proveedor mantenga un equilibrio entre eficiencia operativa y control sobre la seguridad de la información (Peltier, 2016; Boyens et al., 2022).

Tabla 2

Medidas de mitigación implementadas

Fuente: Adaptado de NIST (2020) y ENISA (2021).

Medida	Objetivo	Acción principal	Resultado esperado
Selección rigurosa del proveedor	Garantizar confiabilidad y experiencia	Evaluación de certificaciones y políticas de seguridad	Proveedor alineado con ISO 27001
SLA claros y penalizaciones	Asegurar desempeño medible	Establecer indicadores y descuentos por incumplimiento	Cumplimiento contractual y continuidad
Cláusulas de confidencialidad	Proteger datos sensibles	Firmas de NDA y notificación obligatoria de incidentes	Reducción de brechas y cumplimiento legal
Monitoreo conjunto	Mantener control continuo	Comité operativo mensual y reportes periódicos	Transparencia y mejora continua
Capacitación	Fomentar cultura de seguridad	Talleres y designación de enlace de seguridad	Reducción de errores humanos

3.3. Resultados de la implementación del Modelo de Evaluación Integral de Proveedores (MEIP)

La aplicación del Modelo de Evaluación Integral de Proveedores (MEIP) en el Hospital San José de Buga representó un punto de inflexión en la gestión de servicios tercerizados de ciberseguridad. Esta sección presenta los resultados cuantificables obtenidos y las lecciones aprendidas durante el proceso de implementación.

3.3.1. Análisis Comparativo Pre y Post Implementación

Situación Antes del MEIP: (MEIP, s. f.)
El proceso de selección de proveedores previo a la implementación del MEIP presentaba importantes deficiencias metodológicas: (MEIP, s. f.)

- ✓ **Criterios de Selección Desbalanceados:** El 65% del peso decisorio recaía en aspectos económicos, relegando criterios técnicos y de experiencia sectorial.
- ✓ **Alta Tasa de Insatisfacción:** El 45% de los proveedores contratados históricamente no cumplían con las expectativas técnicas establecidas post-implementación.
- ✓ **Procesos Ineficientes:** El tiempo promedio de evaluación se extendía por 2 semanas debido a la falta de criterios estandarizados y metodología definida.
- ✓ **Conflictos Contractuales:** Frecuentes disputas por expectativas no alineadas y servicios no especificados contractualmente.

Resultados Después del MEIP:

La implementación del modelo generó mejoras sustanciales en todos los indicadores críticos:

- ✓ **Selección Objetiva y Cuantificable:** Implementación de un sistema de puntuación ponderada que eliminó subjetividades en la selección.
- ✓ **Alta Satisfacción del Usuario:** El 92% de satisfacción reportada por los usuarios internos en evaluaciones trimestrales al proveedor seleccionado.
- ✓ **Optimización de Tiempos:** Reducción del tiempo de evaluación a 5 días hábiles mediante metodología estandarizada y checklist definidos.
- ✓ **Reducción de Conflictos:** Disminución del 70% en disputas contractuales gracias a la claridad en expectativas y servicios pactados.

3.3.2. Proceso de Evaluación y Selección Final

Metodología Aplicada:
El proceso de evaluación se desarrolló en tres fases consecutivas, cada una con objetivos y criterios específicos:

Fase 1: Evaluación Documental (40% de la calificación final)

- ✓ Revisión exhaustiva de certificaciones de seguridad y cumplimiento normativo
- ✓ Verificación de referencias con instituciones de salud de similar complejidad
- ✓ Análisis de reportes de auditoría externa y historial de cumplimiento
- ✓ Validación de políticas y procedimientos de seguridad documentados

Fase 2: Pruebas Prácticas (35% de la calificación final)

- ✓ Simulacros controlados de respuesta a incidentes de seguridad
- ✓ Pruebas de penetración en entornos aislados con sistemas similares a los del hospital
- ✓ Evaluación de tiempos de respuesta reales ante incidentes simulados
- ✓ Validación de capacidades técnicas del equipo asignado

Fase 3: Entrevistas y Validación (25% de la calificación final)

- ✓ Sesiones técnicas con el equipo operativo del proveedor
- ✓ Validación de casos de éxito en instituciones de salud similares
- ✓ Evaluación de capacidades de comunicación y reporting
- ✓ Análisis de alineación cultural con los valores institucionales del hospital

3.3.3. Resultados de la Evaluación por Dimensión

Proveedor Seleccionado: "CiberSalud Colombia SAS" - Puntuación Final: 92/100

Desglose por Dimensiones:

Dimensión 1: Capacidad Técnica y Experiencia (33/35 puntos)

- ✓ **Fortalezas:** Experiencia documentada en 8 hospitales de tercer nivel, certificación ISO 27001:2022, infraestructura SOC propia 24/7
- ✓ **Hallazgos:** Capacidad técnica comprobada en entornos hospitalarios complejos

Dimensión 2: Cumplimiento Legal y Normativo (23/25 puntos)

- ✓ Fortalezas: Conocimiento exhaustivo de Ley 1581 de 2012, protocolos específicos para datos de salud (Congreso de Colombia, 2012)
- ✓ **Hallazgos:** Adecuación completa a normativa colombiana de protección de datos

Dimensión 3: Gobernanza y Gestión de Riesgos (18/20 puntos)

- ✓ **Fortalezas:** Metodología alineada con NIST SP 800-30, reporting transparente en tiempo real
- ✓ **Hallazgos:** Enfoque proactivo en gestión de riesgos y continuidad del negocio

Dimensión 4: Factores Económicos y Contractuales (13/15 puntos)

- ✓ **Fortalezas:** Estructura de costos transparente, cláusulas de salida definidas
- ✓ **Hallazgos:** Relación costo-beneficio favorable para el nivel de servicios ofrecidos

Dimensión 5: Adaptabilidad al Contexto Hospitalario (5/5 puntos)

- ✓ **Fortalezas:** Conocimiento profundo de flujos clínicos, experiencia con sistemas PACS/HIS

- ✓ **Hallazgos:** Excelente adaptación al contexto operativo del hospital

Áreas de Mejora Identificadas:

- ✓ Capacitación específica en sistemas PACS (incorporada como requisito contractual)
- ✓ Fortalecimiento de procedimientos para dispositivos médicos IoT
- ✓ Mejora en documentación de integraciones con sistemas legacy

3.3.4 Impacto Cuantificable en la Operación Hospitalaria

- ✓ Indicadores de Desempeño Post-Implementación (Primer Trimestre):
- ✓ Disponibilidad de Sistemas Críticos: 99.97% (vs. 95.2% pre-implementación)
- ✓ Tiempo Medio de Respuesta a Incidentes: 45 minutos (vs. 4.5 horas pre-implementación)
- ✓ Incidentes de Seguridad Mensuales: 5.8 (vs. 18.3 pre-implementación)
- ✓ Cumplimiento de SLA del Proveedor: 98.2% (vs. 76.4% con proveedores anteriores) (ISACA, 2018; Drivas et al., 2020)

Beneficios Tangibles Identificados:

- ✓ Reducción del 68% en incidentes de seguridad menores
- ✓ Mejora del 45% en tiempos de resolución de problemas técnicos
- ✓ Incremento del 32% en satisfacción del personal médico con servicios de TI
- ✓ Ahorro estimado de $185 millones COP anuales por prevención de incidentes mayores

3.3.5 Recomendaciones para Réplica en Otras Instituciones de Salud

Basado en la experiencia de implementación en el Hospital San José de Buga, se establecen las siguientes recomendaciones para instituciones que deseen adoptar el MEIP: (MEIP, s. f.)

1) **Adaptación Contextual del Modelo:**

   - ✓ Personalizar los criterios de evaluación según el nivel de complejidad institucional
   - ✓ Considerar particularidades tecnológicas y operativas de cada institución
   - ✓ Ajustar ponderaciones según prioridades estratégicas específicas

2) **Participación Multidisciplinaria:**

   - ✓ Involucrar activamente a áreas médicas en la evaluación de la Dimensión 5
   - ✓ Incluir representantes de servicios clínicos en comités de evaluación
   - ✓ Validar criterios técnicos con profesionales de TI con experiencia en salud

3) **Gestión del Proceso de Evaluación:**

   - ✓ Establecer puntajes mínimos por dimensión para evitar compensaciones indebidas
   - ✓ Documentar exhaustivamente todo el proceso para auditoría y mejora continua
   - ✓ Implementar mecanismos de apelación y revisión transparentes

4) **Sostenibilidad del Modelo:**

   - ✓ Actualizar anualmente los criterios según evolución normativa y tecnológica

- ✓ Establecer revisiones periódicas de desempeño basadas en el modelo
- ✓ Crear repositorio de lecciones aprendidas para futuras evaluaciones

5) Integración con Procesos Existentes:

- ✓ Alinear el MEIP con políticas de contratación institucionales (MEIP, s. f.)
- ✓ Integrar resultados de evaluación con sistemas de gestión contractual
- ✓ Establecer vínculos con planes de continuidad del negocio

3.4.Diseño de SLA y cláusulas contractuales de seguridad (ISACA, 2018; Drivas et al., 2020)

El diseño y la revisión de los Acuerdos de Nivel de Servicio (SLA) constituyeron un componente central de la estrategia de ciberseguridad tercerizada del Hospital San José de Buga. Este proceso se desarrolló bajo las recomendaciones del NIST Cybersecurity Framework (2020) y los lineamientos europeos de ENISA (2024) para proveedores gestionados de seguridad (MSSP) (National Institute of Standards and Technology [NIST], 2020; European Union Agency for Cybersecurity [ENISA], 2024) (ISACA, 2018; Drivas et al., 2020).

Cada SLA incluyó métricas de desempeño cuantificables —como disponibilidad de sistemas clínicos, tiempo de respuesta ante incidentes y cumplimiento de respaldos—, tal como lo sugieren Drivas et al. (2020) en su modelo de madurez para servicios gestionados (ISACA, 2018; Drivas et al., 2020).

Además, se incorporaron cláusulas contractuales de seguridad que exigen el cumplimiento de políticas alineadas con ISO/IEC 27001 y el derecho del hospital a realizar auditorías periódicas, garantizando la verificación de los controles aplicados por el proveedor (Bauer et al., 2019).

El contrato también contempla procedimientos de reversión y salida, asegurando que al finalizar la relación contractual el proveedor transfiera toda la información, configuraciones y conocimientos al hospital, conforme a los principios de gestión de continuidad de negocio definidos por COBIT 2019 (ISACA, 2018).

Finalmente, el SLA fue diseñado como un documento dinámico y revisable cada cuatro meses, permitiendo ajustar los niveles de servicio según las necesidades operativas y los nuevos riesgos identificados en el entorno hospitalario (European Union Agency for Cybersecurity [ENISA], 2021; National Institute of Standards and Technology [NIST], 2020) (ISACA, 2018; Drivas et al., 2020).

En síntesis, el diseño contractual y la gestión de SLA en el Hospital San José de Buga materializan un modelo de outsourcing seguro, basado en transparencia, responsabilidad compartida y monitoreo continuo. Estos elementos se alinean con la visión estratégica de fortalecer la ciberresiliencia institucional mediante la integración efectiva entre gestión interna y proveedor externo (ISACA, 2018; Drivas et al., 2020).

Tabla 3

Matriz de Urgencia para respuesta a incidentes

Fuente: Elaboración propia, a partir de NIST (2020) y ENISA (2021).

Urgencia	**Criterio (Tiempo de disposición)**	**Ejemplos**
ALTA	Impacto relevante en < 4 horas sobre la atención al paciente o una ventana regulatoria cercana (p. ej., reporte obligatorio). Requiere acción	Caída del sistema clínico principal; bloqueo de autenticación; incidente de seguridad activo con riesgo de exfiltración.
MEDIA	Afecta procesos relevantes hoy, pero existen alternativas de trabajo. Debe resolverse en el mismo día hábil.	Degradación de rendimiento en módulo de historias; error en reporte operativo no crítico.
BAJA	No afecta la operación diaria. Puede planificarse para ventana fuera de horario o mantenimiento.	Duda funcional, mejora menor, solicitud informativa.

3.5. Controles de ciberseguridad implementados

Además de las medidas contractuales y organizativas, la implementación práctica incluyó la aplicación de diversos controles técnicos y procedimientos de ciberseguridad por parte del proveedor (en coordinación con el hospital) para dar cumplimiento efectivo a los SLA y salvaguardar los datos, alineados con los marcos de seguridad establecidos (National Institute of Standards and Technology [NIST], 2020; European Union Agency for Cybersecurity [ENISA], 2021). Algunos de los controles más relevantes fueron: (ISACA, 2018; Drivas et al., 2020)

Fortalecimiento de la infraestructura de seguridad: El proveedor desplegó y administra en las instalaciones del hospital un firewall de próxima generación y sistemas de detección/prevención de intrusiones (IDS/IPS). Estos equipos fueron configurados conforme a las mejores prácticas: reglas de filtrado estrictas, segmentación de la red hospitalaria (separando la red administrativa de la red clínica y la de invitados), y monitoreo en tiempo real de tráfico malicioso (NIST, 2020). Adicionalmente, se implementó una red privada virtual (VPN) segura para que el personal del proveedor pueda conectarse remotamente a los sistemas del hospital

cuando sea necesario, utilizando autenticación multifactor para evitar accesos no autorizados.

Gestión de parches y actualizaciones: Como encargado de la ciberseguridad, el proveedor asumió la gestión proactiva de vulnerabilidades en sistemas y aplicaciones del hospital. Se estableció un calendario de actualización periódica: todos los servidores y dispositivos de red críticos deben ser actualizados con parches de seguridad dentro de una ventana no mayor a 15 días desde su liberación (salvo aquellos que por compatibilidad requieran pruebas adicionales), implementando así controles esenciales del marco NIST (NIST, 2020). Para los endpoints (computadores de usuario), se utiliza una solución de gestión centralizada que aplica actualizaciones automáticas del sistema operativo y antivirus. Este control reduce significativamente el riesgo de explotación de vulnerabilidades conocidas en la infraestructura hospitalaria.

Monitoreo de eventos e incidentes 24/7: El contrato incluyó la provisión de un servicio de SOC (Security Operations Center) por parte del proveedor. En la práctica, esto significa que el proveedor dedica personal y herramientas SIEM (Security Information and Event Management) para recopilar y analizar continuamente los registros (logs) de los sistemas del hospital en busca de patrones anómalos o indicios de ataque, tal como recomiendan los lineamientos para proveedores de servicios gestionados (ENISA, 2021). Cualquier evento crítico (por ejemplo, múltiples intentos fallidos de acceso a un servidor clave, o la detección de malware en una estación) genera alertas inmediatas. Existe un procedimiento definido para responder a estas alertas: el analista de seguridad del proveedor notifica al contacto designado del hospital, a la vez que inicia las acciones de contención (aislar el equipo afectado, bloquear direcciones IP sospechosas, etc., según el caso). Este monitoreo permanente atiende directamente el riesgo de que un ataque pase inadvertido; aumenta la capacidad de detección temprana de incidentes, permitiendo una respuesta más oportuna.

Control de accesos privilegiados: Dado que el personal del proveedor administra sistemas críticos, se implementaron controles adicionales sobre sus accesos, consistentes con los principios de mínimo privilegio y acceso basado en roles (NIST, 2020)**.** Cada técnico del proveedor tiene cuentas nominativas (personales) para acceder a servidores, evitando cuentas genéricas compartidas. Estas cuentas de administrador están integradas con el directorio activo del hospital y usan autenticación multifactor. Además, todas sus actividades de administración quedan registradas. Se habilitó un esquema de bastión host o jump server: para acceder remotamente a la red del hospital, los técnicos primero se conectan a este servidor intermedio altamente seguro que registra comandos ejecutados y sesiones. Así, cualquier acción realizada por personal tercerizado queda trazable para auditoría. Complementariamente, se restringió que los administradores externos solo puedan operar en horarios predefinidos para tareas de mantenimiento, salvo emergencias, y siempre con notificación al personal interno.

Estas medidas reducen la posibilidad de accesos indebidos o abuso de privilegios por parte de terceros.

Encriptación de datos y comunicaciones: Para proteger la información sensible en tránsito y en reposo, el proveedor asesoró e implementó mecanismos de cifrado, atendiendo las recomendaciones de protección de datos (ENISA, 2021). Por ejemplo, todas las bases de datos que almacenan datos personales de pacientes fueron cifradas a nivel de disco. Asimismo, la comunicación entre el hospital y el proveedor se realiza por canales cifrados (VPN segura mencionada, uso de correo electrónico corporativo cifrado para intercambiar ficheros sensibles, etc.). Se revisó la configuración de los sistemas clínicos para asegurarse de que usan protocolos seguros (HTTPS, SSH, etc.) y se inhabilitaron servicios inseguros (como accesos Telnet, FTP sin cifrar, etc.). Con esto, aun si hubiera interceptación de comunicaciones o acceso físico no autorizado a algún soporte, la información permanecería protegida.

Pruebas periódicas de seguridad: Como parte de los entregables, el proveedor realiza pruebas de penetración (pentesting) en la red del hospital dos veces al año, con alcance acordado (incluyendo pruebas a aplicaciones web hospitalarias, evaluación de configuraciones de servidores, ingeniería social básica al personal, etc.), como parte de una evaluación continua de la postura de seguridad (NIST, 2020). Los hallazgos de estas pruebas se documentan en informes que se presentan al hospital con las vulnerabilidades descubiertas y recomendaciones de remediación. El cumplimiento de la remediación de hallazgos importantes forma parte de los indicadores de desempeño del proveedor. Adicionalmente, se efectúa trimestralmente un análisis automatizado de vulnerabilidades sobre los principales servidores. Estas pruebas proactivas fortalecen la postura de seguridad y aseguran que tanto el proveedor como el hospital mantengan una actitud preventiva frente a nuevas amenazas.

Plan de respuesta a incidentes y simulacros: Se formuló un Plan de Respuesta a Incidentes de Seguridad conjunto, que describe paso a paso cómo actuar ante distintos tipos de incidentes (desde malware en un equipo aislado hasta un ataque de ransomware generalizado), desarrollado bajo el marco de gestión de incidentes del NIST (NIST, 2020) El plan define roles (quién lidera la respuesta, cómo se comunica escalonadamente, cuándo se involucra a la alta dirección, etc.) y acciones (contención, investigación, erradicación, recuperación, notificación a autoridades si corresponde, comunicación pública). Para validar la efectividad de este plan, se llevan a cabo simulacros o ejercicios de mesa al menos una vez al año, involucrando tanto al equipo del proveedor como a personal clave del hospital. Estos simulacros permiten evaluar tiempos de respuesta, coordinación y detección de posibles mejoras en el proceso, reforzando la preparación ante incidentes reales.

Todos estos controles implementados son coherentes con el marco contractual establecido y con los objetivos de los SLA. Por ejemplo, la existencia del SOC 24/7 y

del plan de respuesta permite al proveedor cumplir su compromiso de tiempos de respuesta rápidos a incidentes; la gestión de parches contribuye a minimizar incidentes (ayudando a cumplir la meta de disponibilidad); el cifrado y control de accesos aseguran la confidencialidad exigida legalmente, etc. En otras palabras, los controles técnicos son la materialización práctica de las obligaciones y expectativas definidas en el contrato y los marcos de seguridad aplicables (NIST, 2020; ENISA, 2021). El hospital, por su parte, mantiene un involucramiento activo: revisa los informes de seguridad, participa en la priorización de remediaciones y exige evidencia del cumplimiento de estos controles, para cerciorarse de que la seguridad no se debilita por estar tercerizada (ISACA, 2018; Drivas et al., 2020).

4. Figuras y tablas

Tabla 1: "Identificación de riesgos en la ciberseguridad tercerizada" - Fuente: Elaboración propia con base en ENISA (2024) y NIST (2022)

Riesgo	**Descripción**	**Causa principal**	**Impacto potencial**
Brechas de datos y acceso no autorizado	Posible exposición de información sensible por vulnerabilidades o mala gestión del proveedor.	Falta de controles técnicos y supervisión.	Pérdida de confidencialidad y sanciones legales.
Incumplimiento legal y regulatorio	Riesgo de violar la Ley 1581/2012 por manejo inadecuado de datos personales.	Transferencias sin consentimiento o sin garantías.	Multas, pérdida de confianza institucional.
Disminución en la calidad o continuidad del servicio	Incumplimiento de tiempos o disponibilidad pactada.	Mala gestión del proveedor o infraestructura deficiente.	Interrupción en servicios clínicos.
Dependencia excesiva y falta de control	Vendor lock-in o pérdida de conocimiento interno.	Definición ambigua del contrato.	Vulnerabilidad ante fallas del proveedor.
Riesgo reputacional	Daño de imagen por filtraciones o incidentes de seguridad.	Respuesta ineficaz ante incidentes.	Pérdida de confianza de pacientes.

Tabla 2: "Medidas de mitigación implementadas" - Fuente: Adaptado de NIST (2020) y ENISA (2021)

Medida	Objetivo	Acción principal	Resultado esperado
Selección rigurosa del proveedor	Garantizar confiabilidad y experiencia	Evaluación de certificaciones y políticas de seguridad	Proveedor alineado con ISO 27001
SLA claros y penalizaciones	Asegurar desempeño medible	Establecer indicadores y descuentos por incumplimiento	Cumplimiento contractual y continuidad
Cláusulas de confidencialidad	Proteger datos sensibles	Firmas de NDA y notificación obligatoria de incidentes	Reducción de brechas y cumplimiento legal
Monitoreo conjunto	Mantener control continuo	Comité operativo mensual y reportes periódicos	Transparencia y mejora continua
Capacitación	Fomentar cultura de seguridad	Talleres y designación de enlace de seguridad	Reducción de errores humanos

Tabla 3

Matriz de Urgencia para respuesta a incidentes - Fuente: Elaboración propia, a partir de NIST (2020) y ENISA (2021).

Urgencia	Criterio (Tiempo de disposición)	Ejemplos
ALTA	Impacto relevante en < 4 horas sobre la atención al paciente o una ventana regulatoria cercana (p. ej., reporte obligatorio). Requiere acción	Caída del sistema clínico principal; bloqueo de autenticación; incidente de seguridad activo con riesgo de exfiltración.
MEDIA	Afecta procesos relevantes hoy, pero existen alternativas de trabajo. Debe resolverse en el mismo día hábil.	Degradación de rendimiento en módulo de historias; error en reporte operativo no crítico.
BAJA	No afecta la operación diaria. Puede planificarse para ventana fuera de horario o mantenimiento.	Duda funcional, mejora menor, solicitud informativa.

Tabla 4: Modelo de Evaluación Integral de Proveedores (MEIP) - Fuente: Elaboración propia, a partir de ISO/IEC 27036-3 (2023), NIST SP 800-161r1 (Boyens et al., 2022) y Ley 1581 de 2012.

Dimensión	**Ponderación**	**Criterios Clave**	**Puntaje Obtenido**	**Observaciones**
Capacidad Técnica	35%	5 criterios	33/35	Excelente experiencia sector salud
Cumplimiento Legal	25%	5 criterios	23/25	Adecuación completa Ley 1581
Gobernanza	20%	5 criterios	18/20	Reporting transparente
Factores Económicos	15%	5 criterios	13/15	Costos competitivos
Adaptabilidad	5%	7 criterios	5/5	Excelente conocimiento flujos clínicos
TOTAL	**100%**	**27 criterios**	**92/100**	**Proveedor recomendado**

5. Conclusiones

Síntesis aplicada del MEIP

En resumen, el MEIP nos ayudó a comparar proveedores con criterios claros, a documentar cada decisión y a reducir riesgos típicos del outsourcing en hospitales. Es una forma sencilla de conectar marcos como ISO/IEC 27036-3 y NIST con lo que pasa en la operación diaria (MEIP, s. f.; ISO/IEC, 2023; Boyens et al., 2022).

La experiencia de implementar la gestión de ciberseguridad mediante un esquema de outsourcing TI en el Hospital San José de Buga deja múltiples enseñanzas y conclusiones valiosas. En primer lugar, se confirmó que es posible integrar con éxito la ciberseguridad en un modelo de tercerización, siempre y cuando se realice una planificación cuidadosa y se establezca un marco robusto de acuerdos y controles. El análisis realizado identificó que los principales riesgos – especialmente aquellos relacionados con la protección de datos personales y el cumplimiento legal – pueden ser eficazmente mitigados a través de una combinación de medidas contractuales, organizativas y técnicas.

Una conclusión fundamental es la importancia de un SLA bien definido y de un contrato exhaustivo: esto se tradujo en claridad de expectativas y en mecanismos concretos para exigir la calidad del servicio. En el caso estudiado, las penalizaciones por incumplimiento, las cláusulas de confidencialidad y las obligaciones de notificación de incidentes resultaron instrumentos esenciales para alinear al proveedor con las necesidades críticas del hospital. Asimismo, la capacidad de revisar periódicamente los acuerdos de nivel de servicio permitió introducir mejoras continuas, mostrando que la gestión de la relación con el proveedor debe ser dinámica y adaptativa (ISACA, 2018; Drivas et al., 2020).

Otra lección aprendida es que la responsabilidad sobre la seguridad de la información no se delega completamente al proveedor por el simple hecho de externalizar; el hospital tuvo que mantener un rol activo de supervisión y colaboración. La creación de comités de seguimiento y la designación de enlaces internos demostraron ser prácticas efectivas para conservar visibilidad y control sobre la seguridad tercerizada. De esta forma, el hospital pudo beneficiarse del outsourcing (acceso a personal especializado, monitoreo 24/7, tecnologías avanzadas) sin abdicar de su responsabilidad de gobierno de la seguridad.

En materia de cumplimiento normativo, el proyecto confirmó la necesidad de traducir los requisitos legales en acciones concretas dentro del contrato y en la operación diaria. Se logró alinear las prácticas del proveedor con la normativa de protección de datos colombiana, garantizando la continuidad del cumplimiento legal a pesar de estar la seguridad en manos externas. Esto evidencia que un adecuado gobierno corporativo de TI puede extenderse hacia los proveedores mediante controles y acuerdos formales, salvaguardando los intereses de la institución y de los titulares de los datos.

También se observó que la cultura de seguridad en la organización no debe relegarse durante el outsourcing. Complementar el contrato con actividades de concientización y capacitación a los usuarios internos aportó a reducir riesgos operacionales (por ejemplo,

ataques de phishing). Es decir, la estrategia de ciberseguridad en un entorno tercerizado sigue siendo multifacética: involucra tecnología, procesos y personas.

En cuanto a los resultados, durante el periodo de implementación evaluado, el Hospital San José de Buga mejoró notablemente su postura de seguridad. No se presentaron incidentes graves de brecha de datos, los tiempos de respuesta ante eventos menores fueron adecuados, y las auditorías realizadas no hallaron incumplimientos mayores por parte del proveedor. Esto sugiere que las medidas adoptadas fueron efectivas en la práctica. No obstante, una reflexión final es que la vigilancia debe ser continua: las amenazas cibernéticas evolucionan constantemente, y la tercerización no exime a la institución de actualizar sus estrategias. El hospital deberá continuar evaluando a su proveedor, adaptando los SLA a nuevos desafíos (por ejemplo, posibles requisitos futuros de seguridad en dispositivos médicos IoT, o nuevas leyes de privacidad), y estar preparado con planes de contingencia si la relación de outsourcing no rinde los resultados esperados (ISACA, 2018; Drivas et al., 2020).

En conclusión, el trabajo evidenció que integrar la ciberseguridad en un modelo de outsourcing TI puede brindar ventajas significativas si se gestiona apropiadamente: se accede a conocimiento especializado y recursos dedicados, mientras se mantienen bajo control los riesgos críticos a través de una gobernanza sólida y colaborativa. Las lecciones aprendidas de este caso real pueden servir de guía para otras instituciones de salud (u organizaciones en general) que busquen tercerizar funciones de TI sensibles: es imprescindible identificar tempranamente los riesgos, plasmar las garantías necesarias en los contratos, y cultivar una relación estrecha y transparente con el proveedor. Solo así se consigue que la seguridad de la información, aun estando en manos de terceros, cumpla con los altos estándares que la misión del negocio y las leyes demandan.

6. Referencias

Bauer, E., Schluga, O., Maksuti, S., Bicaku, A., Hofbauer, D., Ivkic, I., & Tauber, M. (2019). Towards a security baseline for IaaS-cloud back-ends in Industry 4.0. arXiv. https://arxiv.org/abs/1905.06709

Bianchi, J., Dong, S., Petrillo, L., & Petrocchi, M. (2025). Automatic association of quality requirements and quantifiable metrics for cloud security certification. arXiv. https://arxiv.org/abs/2503.09460

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST Special Publication 800-161, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Ditech Group. (2023). Outsourcing IT: ¿Qué es y por qué es importante implementarlo? https://it.ditech.es/outsourcing-it-que-es-y-por-que-es-importante-implementarlo/

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS directive compliant cybersecurity maturity assessment framework. arXiv. https://arxiv.org/abs/2004.10411

European Union Agency for Cybersecurity. (2021). *Guidelines on security measures for managed service providers. https://www.enisa.europa.eu

European Union Agency for Cybersecurity. (2024). *Implementation guidance on security measures for managed service providers (MSP) and managed security service providers (MSSP). https://www.enisa.europa.eu

ISACA. (2018). COBIT 2019 framework: *Governance and management objectives.* https://www.isaca.org/resources/cobit

National Institute of Standards and Technology. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://www.nist.gov/cyberframework

Negreiro, M. (2023). Managed security services: Briefing europeo sobre servicios gestionados de seguridad. Parlamento Europeo. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754556/EPRS_BRI(2023)754556_EN.pdf

Peltier, T. R. (2016). Information security policies, procedures, and standards: Guidelines for effective information security management. CRC Press. https://doi.org/10.1201/9780849390326

Center for Internet Security. (2024). *CIS Critical Security Controls v8.1*. https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-1

Congreso de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ditech Group. (s. f.). Outsourcing IT: ¿Qué es y por qué es importante implementarlo? https://ditechgroup.com/es/outsourcing-it

ENISA. (2017). *Guidelines for SMEs on the security of personal data processing*. https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ENISA. (2020). *Procurement guidelines for cybersecurity in hospitals*. https://www.enisa.europa.eu/publications/procurement-guidelines-for-cybersecurity-in-hospitals

European Parliament & Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament & Council. (2022). *Directive (EU) 2022/2555 (NIS2)*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. https://www.isaca.org/resources/cobit