TRABAJO DE GRADO

Opción Seminario-Diplomado.

Outsourcing de Seguridad en Redes para una Empresa Proveedora de Servicios de Internet (ISP): Caso JYR Services

Yary Marcela Santiago Santiago

Roonal Flaminio Fonseca Chaparro

Jolman Alexis Cordoba Olmos.

Asesor

Jorge Mauricio Sepúlveda Castaño

Corporación Universitaria Remington.
Facultad de Ingenierías.
Ingeniería de Sistemas.
Seminario de Outsourcing en Tecnologías de la Información
2026.

Dedicatoria

A Dios y dedicado a nuestras familias, quienes han sido nuestro principal apoyo durante toda la carrera y brindarnos la sabiduría, el entusiasmo y la motivación necesaria. También a los docentes, ingenieros y a quienes trabajan en la sede Uniremington Yopal por compartir sus conocimientos y experiencia adquiridas que contribuyeron en nuestro aprendizaje y aquellas personas que creyeron en nosotros en este proceso de aprendizaje

Agradecimientos

Expresamos nuestro más grande agradecimiento a los ingenieros, docentes y personal administrativo Corporación Universitaria Remington Yopal por la entrega en nuestro proceso de formación como ingenieros de sistemas.

Al tutor del seminario de Outsourcing en TI, por orientar este proceso con rigor y pertinencia. Su vocación, exigencia y apoyo constante nos ha impulsado a mejorar nuestras habilidades y motivarnos a seguir avanzando con seguridad, responsabilidad y compromiso en el ámbito de sistemas.

A cada uno de ellos, gracias por compartir sus conocimientos y experiencias para seguir adelante y poder desarrollar el documento presente.

Tabla de contenido

Resumen

El presente trabajo de grado tiene como propósito analizar la viabilidad y las condiciones de implementación de un modelo de outsourcing para la gestión de la seguridad en redes en una empresa proveedora de servicios de internet (ISP), denominada JYR Services, creada como caso de estudio ficticio representativo del sector en Colombia.

Para el desarrollo del ejercicio se combinó la revisión de marcos de referencia como ITIL 4, ISO/IEC 20000-1 e ISO/IEC 27001:2022 con el análisis de la situación actual de JYR Services, identificando los procesos susceptibles de outsourcing, los riesgos asociados y los mecanismos de gobernanza necesarios para mantener el control estratégico sobre los servicios externalizados. Entre los hallazgos más relevantes se destaca que la externalización del centro de operaciones de seguridad (SOC), la gestión de vulnerabilidades y el monitoreo de red representa la alternativa más costo-efectiva para la empresa, siempre que se establezcan acuerdos de nivel de servicio (SLA) robustos y mecanismos de supervisión permanentes.

Los resultados confirman que el outsourcing en TI, aplicado correctamente al campo de la seguridad en redes, no implica pérdida de control organizacional, sino una redistribución estratégica de responsabilidades que permite al ISP enfocar sus recursos internos en la innovación y la calidad del servicio al cliente.

Palabras clave: outsourcing en TI, seguridad en redes, ISP, SOC, SLA, gobernanza TI.

Marco conceptual y contextual

En esta sección se presentan los fundamentos teóricos y el contexto organizacional que enmarcan el ejercicio académico. Se parte de los conceptos esenciales del outsourcing en TI, se revisan los marcos de referencia más relevantes para la gestión de servicios tecnológicos tercerizados y se describe el entorno de JYR Services como empresa objeto de estudio.

Outsourcing en tecnologías de la información

En el contexto de las empresas proveedoras de internet, el outsourcing consiste en delegar determinadas funciones tecnológicas a proveedores especializados con el propósito de mejorar la eficiencia operativa, acceder a conocimiento técnico especializado y optimizar los recursos de la organización. Más que una estrategia para disminuir costos representa una alternativa que permite a las empresas concentrarse en sus actividades principales mientras expertos externos asumen procesos que requieren altos niveles de especialización.

Para una empresa proveedora de servicios de internet como JYR Services, el outsourcing en seguridad de redes constituye una opción viable para fortalecer la protección de su infraestructura tecnológica sin asumir los elevados costos que implica mantener un equipo interno dedicado exclusivamente a la ciberseguridad. De esta manera, la organización conserva el control sobre las decisiones estratégicas mientras aprovecha la experiencia técnica del proveedor contratado.

Modelos de outsourcing aplicables a la seguridad en redes

Las organizaciones pueden adoptar diferentes modelos de outsourcing en función de sus necesidades operativas, presupuesto y nivel de control deseado sobre los servicios tecnológicos. En materia de seguridad en redes, estos modelos permiten distribuir responsabilidades entre el personal interno y proveedores especializados, facilitando la implementación de soluciones más robustas frente a las amenazas actuales. Para un ISP de

mediana escala como JYR Services, la selección del modelo adecuado depende del equilibrio entre el control estratégico y el apoyo técnico externo.

Modelos de Outsourcing de Seguridad

MSSP (Managed Security Service Provider): Corresponde a un proveedor especializado que se encarga de administrar de manera continua los servicios de seguridad informática de una organización. Además del monitoreo permanente, estos proveedores apoyan la detección, análisis y respuesta frente a incidentes, permitiendo que empresas como JYR Services fortalezcan su seguridad sin crear un equipo interno dedicado exclusivamente a esta función.

- Co-sourcing: Es un modelo de colaboración en el que la empresa y el proveedor externo comparten responsabilidades. Mientras el personal interno conserva el control de las decisiones estratégicas y de los procesos más sensibles, el proveedor aporta conocimiento técnico y recursos especializados para complementar la operación.
- SECaaS (Security as a Service): Consiste en ofrecer herramientas y soluciones de seguridad mediante servicios en la nube, generalmente bajo un esquema de suscripción. Este modelo permite acceder a tecnologías de protección actualizadas sin realizar inversiones elevadas en infraestructura propia.
- SOCaaS (Security Operations Center as a Service): Permite que una organización disponga de un centro de operaciones de seguridad administrado por un tercero. A través de este servicio se supervisan los eventos de seguridad, se identifican posibles amenazas y se coordina la respuesta a incidentes de manera continua.

Marcos de referencia para la gestión del outsourcing en ti

La implementación de un modelo de outsourcing requiere apoyarse en marcos de referencia reconocidos internacionalmente que orienten la gestión de los servicios, la administración de riesgos y el aseguramiento de la calidad. Estas buenas prácticas permiten establecer procesos claros entre la organización contratante y el proveedor, garantizando que la prestación del servicio contribuya al cumplimiento de los objetivos del negocio.

Los marcos y estándares principales incluyen:

- ITIL (Information Technology Infrastructure Library): Reúne un conjunto de buenas prácticas orientadas a organizar y mejorar la gestión de los servicios de tecnologías de la información. En una estrategia de outsourcing facilita la definición de procesos, la atención de incidentes y el seguimiento de los niveles de servicio acordados con el proveedor.
- COBIT (Control Objectives for Information and Related Technologies): Es un marco de gobierno y gestión de TI que ayuda a las organizaciones a mantener el control de sus procesos tecnológicos, administrar los riesgos y asegurar que los servicios contratados estén alineados con los objetivos institucionales.
- ISO/IEC 20000-1: Es una norma internacional enfocada en la gestión de servicios de tecnologías de la información. Su aplicación permite establecer procedimientos estandarizados para planificar, operar, evaluar y mejorar continuamente los servicios prestados por un proveedor.
- CMMI-SVC (Capability Maturity Model Integration for Services): Es un modelo utilizado para evaluar y fortalecer la capacidad de las organizaciones que prestan servicios. Su implementación favorece la mejora continua de los procesos y contribuye a ofrecer servicios más consistentes y de mayor calidad.

Fases clave en la gestión con proveedores

Gobernanza y estrategia: Antes de contratar un proveedor es necesario definir cuáles procesos pueden ser externalizados y cuáles deben permanecer bajo responsabilidad de la organización por su importancia para el negocio. Esta decisión permite mantener el control sobre las funciones estratégicas.

Gestión de acuerdos (SLA): Los acuerdos de nivel de servicio establecen los compromisos que debe cumplir el proveedor, incluyendo indicadores de desempeño, tiempos de respuesta y niveles mínimos de disponibilidad que servirán para evaluar la calidad del servicio.

Monitoreo y control: La supervisión permanente del proveedor permite verificar el cumplimiento de los acuerdos establecidos, identificar oportunidades de mejora y asegurar que los servicios continúen respondiendo a las necesidades de la empresa.

Contexto de JYR services

JYR Services es una empresa ficticia creada para este ejercicio académico, cuyas características son representativas de un ISP de mediana escala en Colombia. Opera en una ciudad intermedia con una base de aproximadamente 18.000 suscriptores residenciales y 1.200 clientes empresariales. Su infraestructura combina tecnología FTTH (Fiber to the Home) en zonas urbanas con redes HFC (Hybrid Fiber-Coaxial) en zonas periféricas.

El área de TI de JYR Services cuenta con 12 profesionales, de los cuales ninguno tiene dedicación exclusiva a la ciberseguridad. Las funciones de seguridad se realizan de forma reactiva, sin procesos formales de gestión de incidentes ni de monitoreo continuo. La empresa no cuenta con un SOC propio ni ha implementado herramientas de correlación de eventos (SIEM). Esta situación la expone a riesgos significativos en un entorno donde los ataques a infraestructuras ISP han aumentado un 67% en Colombia durante 2023, según datos del CSIRT de ColCERT (2024).

Desarrollo e implementación del aprendizaje

En esta sección se presenta el análisis realizado sobre JYR Services y el diseño del modelo de outsourcing en seguridad de redes propuesto. El ejercicio se estructuró en cuatro fases: diagnóstico del estado actual, identificación de funciones de outsourcing, diseño del modelo de outsourcing y definición del esquema de gobernanza y control.

Metodología

La propuesta desarrollada corresponde a una metodología documental-propositiva basada en el análisis de un caso de estudio ficticio. Para su construcción se realizó la revisión de literatura especializada, estándares internacionales y buenas prácticas relacionadas con outsourcing en tecnologías de la información y seguridad en redes. Posteriormente, esta información fue aplicada al contexto de JYR Services con el propósito de diseñar un modelo de outsourcing ajustado a las necesidades de una empresa ISP de mediana escala.

Diagnóstico del estado actual: ¿qué se puede tercerizar?

El punto de partida del proceso de outsourcing es la identificación clara de qué funciones son candidatas a tercerización y cuáles deben permanecer bajo control interno. Para JYR Services se realizó un inventario de procesos de seguridad, clasificándolos según dos criterios: el nivel de especialización requerido y el grado de sensibilidad estratégica de cada función.

Como resultado de este análisis, se determinó que las funciones con mayor potencial de tercerización son el monitoreo continuo de la red (24/7), la gestión de vulnerabilidades y parches, la respuesta a incidentes de seguridad y las auditorías periódicas de cumplimiento. En contraste, funciones como la definición de la arquitectura de seguridad, la gestión de contraseñas y certificados de los equipos core y las relaciones con entes regulatorios deben mantenerse bajo gobierno interno, dado su carácter estratégico y su vinculación directa con la operación crítica del ISP.

Diseño del modelo de outsourcing selectivo

Estructura del Modelo Propuesto

Para JYR Services se recomienda un modelo de outsourcing selectivo con elementos de co-sourcing, que externalice las siguientes funciones de seguridad a un proveedor externo certificado en ISO/IEC 27001 e ISO/IEC 20000-1: Centro de Operaciones de Seguridad (SOC) gestionado con monitoreo 24/7/365, gestión de vulnerabilidades y análisis periódico de riesgos, respuesta a incidentes de niveles 1 y 2, y mantenimiento y actualización de firmas en sistemas IPS y firewall.

Las funciones que permanecen bajo gobierno interno incluyen la definición de políticas de seguridad, la gestión de identidades y accesos privilegiados (PAM), la coordinación con ColCERT ante incidentes de alto impacto y la supervisión del cumplimiento del SLA por parte del proveedor. Este balance garantiza que JYR Services no pierda el control estratégico de su postura de seguridad mientras accede a capacidades operativas de primer nivel.

Criterios de Selección del Proveedor

La selección del proveedor de servicios de seguridad gestionados (MSSP, Managed Security Service Provider) debe responder a criterios técnicos, financieros y de cumplimiento normativo. Entre los criterios técnicos más relevantes se encuentran la certificación del proveedor en ISO/IEC 27001, la disponibilidad de un SOC con personal certificado CISSP o CEH, la experiencia comprobada en clientes del sector telecomunicaciones y la capacidad de integrar sus herramientas con la infraestructura existente del ISP mediante APIs y conectores estándar.

Desde la perspectiva financiera, el modelo de outsourcing debe contemplar un análisis de costo-beneficio que compare el costo total de propiedad (TCO) de una solución interna versus la contratación externa. Para JYR Services, el costo estimado de implementar un SOC interno de tres analistas 24/7 supera los COP 420 millones anuales, mientras que la contratación de un MSSP de nivel medio en el mercado colombiano oscila entre COP 120 y 180 millones anuales, incluyendo el servicio de SIEM gestionado, según cotizaciones de referencia del mercado local.

Definición del sla y kpis del servicio

El acuerdo de nivel de servicio es el instrumento contractual que formaliza las obligaciones del proveedor externo y los estándares mínimos de calidad que debe garantizar. Para el servicio de SOC gestionado de JYR Services se definieron los siguientes parámetros en el SLA: disponibilidad del servicio de monitoreo no inferior al 99.5% mensual, tiempo máximo de detección y notificación de incidentes críticos de 15 minutos, tiempo máximo de respuesta inicial a incidentes críticos de 30 minutos, tiempo máximo de resolución de incidentes de severidad media de 4 horas, y entrega mensual de informe ejecutivo de seguridad con análisis de tendencias y recomendaciones.

Los indicadores clave de rendimiento (KPI) que se utilizarán para evaluar el cumplimiento del SLA son el tiempo medio de detección (MTTD), el tiempo medio de respuesta (MTTR), la tasa de falsos positivos del SIEM, el porcentaje de incidentes escalados correctamente y el índice de satisfacción del equipo interno de TI con el servicio. Estos KPIs serán revisados mensualmente en comités de seguimiento entre TechNet S.A.S. y el proveedor.

Esquema de gobernanza del outsourcing

Uno de los riesgos más frecuentes en los procesos de outsourcing en TI es la pérdida de visibilidad y control sobre los servicios tercerizados, lo que puede derivar en dependencia del proveedor, degradación de la calidad del servicio o incumplimiento de obligaciones regulatorias. Para mitigar estos riesgos, se diseñó un esquema de gobernanza estructurado en tres niveles.

El nivel estratégico involucra a la dirección de JYR Services y al representante comercial del proveedor, con reuniones trimestrales para revisar la alineación del servicio con los objetivos del negocio, evaluar la continuidad del contrato y actualizar el alcance del SLA según la evolución de la infraestructura y el perfil de riesgo del ISP.

El nivel táctico incluye al jefe de TI de JYR Services y al gerente de cuenta del proveedor, con reuniones mensuales enfocadas en la revisión de KPIs, el análisis de incidentes relevantes del período y la planificación de mejoras operativas. En este nivel también se gestiona la transferencia de conocimiento para fortalecer gradualmente las capacidades internas del equipo de TI.

El nivel operativo contempla la interacción diaria entre el equipo de red de JYR Services y los analistas del SOC del proveedor, mediante una plataforma de ticketing compartida (ITSM) y canales de comunicación en tiempo real para la coordinación de respuesta a incidentes. Este nivel garantiza la continuidad operativa y la trazabilidad de todas las acciones tomadas sobre la infraestructura del ISP.

Riesgos del outsourcing y estrategias de mitigación

Todo proceso de tercerización conlleva riesgos inherentes que deben ser identificados, valorados y gestionados de forma proactiva. Para el caso de JYR Services se identificaron los riesgos más relevantes y se propusieron estrategias de mitigación alineadas con las mejores prácticas de la industria.

Tabla 1. Riesgos del outsourcing de seguridad en redes y estrategias de mitigación.

Riesgo	Probabilidad	Impacto	Estrategia de Mitigación
Dependencia excesiva del proveedor	Alta	Alto	Cláusulas de exit management y transferencia de conocimiento en el contrato
Exposición de información sensible de la infraestructura	Media	Muy alto	NDA estricto, acceso por VPN con MFA y registros de auditoría de accesos
Incumplimiento del SLA	Media	Alto	Penalizaciones contractuales y comités mensuales de seguimiento de KPIs
Continuidad del proveedor (quiebra o cambio)	Baja	Alto	Cláusula de escrow de datos y plan de transición en el contrato

Riesgo	Probabilidad	Impacto	Estrategia de Mitigación
Falta de alineación cultural y operativa	Media	Medio	Sesiones de onboarding, documentación de procesos y reuniones tácticas mensuales
Incumplimiento normativo (Ley 1581, CRC)	Baja	Muy alto	Auditorías de cumplimiento anuales y certificación ISO 27001 exigida al proveedor

Tabla 2. Comparativo costo-beneficio: SOC interno vs. outsourcing MSSP para JYR Services.

Ítem	SOC Interno	Outsourcing MSSP
Personal (3 analistas 24/7)	COP $360M/año	Incluido en contrato
Licencias SIEM y herramientas	COP $45M/año	Incluido en contrato
Capacitación y certificaciones	COP $18M/año	A cargo del proveedor
Infraestructura de monitoreo	COP $25M/año	A cargo del proveedor
Tiempo de implementación inicial	6-9 meses	4-6 semanas
Costo total estimado anual	COP $448M	COP $120M - $180M
Cobertura horaria	24/7 con rotación	24/7/365 garantizado

Ítem	SOC Interno	Outsourcing MSSP
Nivel de especialización disponible	Básico-Medio	Alto (CISSP, CEH)

Al comparar el escenario actual de JYR Services con el modelo de outsourcing propuesto, se evidencia una mejora significativa en la capacidad de respuesta frente a incidentes de seguridad. Mientras la situación inicial presenta limitaciones derivadas de la ausencia de un centro de operaciones de seguridad, monitoreo continuo y herramientas especializadas, el modelo propuesto incorpora procesos permanentes de vigilancia, respuesta y análisis que fortalecen la protección de la infraestructura tecnológica.

Desde el punto de vista económico, la contratación de un proveedor especializado permite reducir los costos asociados a la implementación y operación de un SOC interno, manteniendo al mismo tiempo un alto nivel de disponibilidad y especialización técnica. Esto favorece la continuidad del servicio, mejora la gestión de riesgos y permite que la empresa concentre sus recursos internos en actividades estratégicas para el negocio.

Conclusiones

El análisis realizado permitió establecer que un modelo de outsourcing selectivo constituye una alternativa viable para fortalecer la seguridad en redes de una empresa ISP como JYR Services, ya que facilita el acceso a personal especializado y tecnologías avanzadas sin asumir los costos de una operación completamente interna.

El éxito del modelo depende de la adecuada selección del proveedor, la definición de acuerdos de nivel de servicio claros y el seguimiento permanente mediante indicadores de desempeño que permitan garantizar el cumplimiento de los objetivos establecidos.

La aplicación de marcos de referencia como ITIL 4, ISO/IEC 20000-1 e ISO/IEC 27001 proporciona una base sólida para la gestión, supervisión y mejora continua de los servicios tercerizados, fortaleciendo la gobernanza de TI.

Aunque el outsourcing ofrece importantes beneficios operativos y financieros, también implica riesgos relacionados con la dependencia del proveedor y la protección de la información. Estos riesgos pueden mitigarse mediante estrategias de co-sourcing, transferencia de conocimiento y adecuados mecanismos de control.

Como limitación, este trabajo se desarrolló a partir de un caso de estudio ficticio, por lo que futuras investigaciones podrían validar la propuesta mediante su aplicación en empresas reales del sector de telecomunicaciones y evaluar sus resultados mediante indicadores operativos y financieros.

Referencias bibliografía

Think Us. (2026).s ¿Qué es el outsourcing? - Thinkus

Impulso Tecnológico. (s. f.). Outsourcing IT para empresas: guía para decidir. Outsourcing IT para empresas: guía para decidir

Icorp. (s. f.). Gestión de servicios de TI y marcos de referencia. Gestión de servicios de TI y marcos de referencia

AXELOS. (2019). ITIL Foundation: ITIL 4 Edition. TSO.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

International Organization for Standardization. (2018). ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements. ISO