TRABAJO DE GRADO

Recomendaciones Para La Selección Y Auditorias De Proveedores De Outsourcing TI

Ciberseguridad en Entornos de Outsourcing: Retos Actuales y Estrategias de Protección

Corporación Universitaria Remington.

Nombre de la facultad: Facultad de Ingenierías

Nombre del programa académico: Ingeniería de Sistemas

Presentado por:

ANDRY YURLEY MELGAREJO GOMEZ

Docente: Jorge Mario Sepúlveda.

Seminario - Outsourcing

2025.

Tabla de contenido

RESUMEN

Este trabajo enfoca la necesidad de implementar procesos de selección y de auditoría a los proveedores de Outsourcing TI, es una práctica empresarial dentro del entorno actual, que ofrece ventajas tanto como la reducción de costos y el acceso a tecnologías avanzadas, disminuye significativamente la exposición a riesgos tecnológicos, de seguridad y de incumplimiento normativo, tanto a nivel global como local.

Debido a la necesidad de las empresas de tercerización de servicios se vuelto indispensable establecer criterios técnicos y metodológicos rigurosos y sólidos para garantizar la seguridad de la información, la calidad del servicio y la continuidad operativa.

Las auditorías de selección de proveedores es una herramienta proactiva que trasciende del cumplimiento contractual a otros elementos claves como la capacidad técnica y la experiencia comprobada del proveedor para diseñar y mantener soluciones, la seguridad y confidencialidad de la información, el cumplimiento legal y regulatorio para mitigar riesgos de sanciones y la reputación, referencias de desempeño para evaluar la trayectoria y la ética del proveedor.

Este trabajo detalla una metodología para las auditorías periódicas de proveedores, estructurada en etapas: planificación, ejecución y enfoque, evaluación de riesgos, Seguimiento y reportes y la creación de un Plan de Acción Correctiva (PAC) estructurado para eliminar las causas de las no conformidades detectadas cuyo seguimiento es esencial para asegurar la efectividad de las medidas adoptadas, mitigando los riesgos y fortaleciendo la gobernanza sobre terceros que manejan activos.

Palabras clave

(Outsourcing TI, Selección de proveedores, Planificación y Ejecución de Auditorias Gestión de Riesgos, Ciberseguridad, NIST, ISO/IEC 27001, Plan de Acción Correctiva)

1. Marco conceptual

1.1. Outsourcing de Servicios TI

La tercerización o outsourcing de servicios es un plan para empresas que incluye Encontrar a otros para llevar a cabo trabajos y tareas ordinarias para crear más dinero.

El outsourcing informático trata de reducir los costos, mejorar los funcionamientos en trabajo, usar recursos especiales. Y deja que un grupo se concentre en sus mejores habilidades (Gartner, 2025).

El outsourcing de TI es cuando se dan partes de servicios tecnológicos a una organización externa. No te confundas, esto ayuda a mejorar la eficiencia y tener acceso a expertos. La práctica se hace para bajar costos del trabajo. En esto hay cosas como hacer programas, ayuda en tecnología, manejar la infraestructura, proteger de cyberataques. También incluye moverse a la nube, y la gestión de proyectos completos (Quibit 2025).

1.2. Selección de Proveedores de Outsourcing Ti

Consiste en un proceso sistemático de evaluación, comparación y contratación de empresas que ofrecen servicios TI, considerando factores como la experiencia, trayectoria y casos de éxitos.

1.3. Marcos Normativos y Regulatorios

La gestión de riesgos en entornos de outsourcing se apoya en marcos normativos internacionales que definen requisitos específicos de seguridad de la información y control de terceros. Entre los más relevantes destacan:

- **ISO/IEC 27001:2022:** proporciona un enfoque sistemático para el establecimiento de Sistemas de Gestión de Seguridad de la Información (SGSI), incluyendo controles específicos para la gestión de relaciones con proveedores y la seguridad en acuerdos de outsourcing (Akker, 2025). La norma establece controles detallados en su Anexo

A.15 para abordar la seguridad en las relaciones con proveedores, incluyendo políticas específicas de seguridad, direccionamiento de la seguridad en acuerdos contractuales y gestión de la cadena de suministro de TIC (Administrador, 2025).

- **ITIL (Biblioteca de Infraestructura de Tecnología de la Información):** es un conjunto de prácticas para la gestión de servicios de TI, La guía ITIL ha sido elaborada para abarcar toda la infraestructura, desarrollo y operaciones de TI y gestionarla hacia la mejora de la calidad del servicio. (Global Suite 2023).

- **COBIT 2019**: Centrado en el gobierno y la gestión de las tecnologías de la información, COBIT 2019 ofrece principios, objetivos y componentes diseñados para alinear la estrategia tecnológica con los objetivos de negocio. Su enfoque incluye prácticas para la gestión de riesgos, el control de proveedores y la optimización de procesos de TI en entornos de outsourcing. Además, facilita la integración con otros marcos como ISO/IEC 27001 y NIST CSF, fortaleciendo así la gobernanza y la seguridad de la información (ISACA, 2019).

2. Marco contextual

El contexto actual resalta la necesidad de una selección y auditoría robusta, dado el aumento de la dependencia tecnológica y la complejidad de los riesgos.

2.1. Entorno global tercerización de servicios

En el entorno empresarial actual, caracterizado por la digitalización y la globalización de los mercados, el outsourcing TI ha adquirido una importancia estratégica. Las organizaciones recurren a proveedores externos para acelerar la innovación, reducir costos operativos y acceder a tecnologías avanzadas como inteligencia artificial, big data, computación en la nube y ciberseguridad gestionada.

Sin embargo, esta práctica también incrementa la exposición a riesgos tecnológicos y de seguridad, lo que hace indispensable la implementación de procesos robustos de evaluación y auditoría de proveedores.

2.2. Entorno local Tercerización de Servicios

En América, la tercerización de servicios ha experimentado un crecimiento constante en los últimos años, debido a que se han ido digitalizando y a la necesidad de mejorar la utilización de los recursos tecnológicos.

En Colombia, la necesidad de soporte técnico remoto, desarrollo de software y servicios en la nube ha crecido.

Sin embargo, el hecho de que muchas organizaciones todavía no tengan estructuras formales para la auditoría y evaluación provoca riesgos relacionados con la falta de control sobre los datos, las brechas de seguridad y el incumplimiento normativo.

El outsourcing TI, es un plan estratégico en las organizaciones que buscan reducir costos, adquirir conocimientos especializados y mejorar la eficiencia operativa. Sin embargo, la tercerización de servicios tecnológicos conlleva riesgos significativos asociados a la seguridad de la información, la calidad del servicio y la dependencia del proveedor.

Por lo tanto, resulta prudente establecer criterios técnicos y metodológicos para la selección y auditoría continua de los proveedores de outsourcing TI.

1. Recomendación para la selección de proveedores

En la necesidad de implementar una supervisión y gobernanza constante sobre terceros que manejan procesos, datos y activos fundamentales para las empresas se realizan las auditorias de selección de proveedores.

Esta auditoría de proveedores de Outsourcing TI va más allá del cumplimiento de los contratos y se transforma en una herramienta proactiva para manejar el riesgo en la cadena tecnológica y de ciberseguridad.

En Este marco, las auditorías a los proveedores de outsourcing TI se transforman en un instrumento fundamental para asegurar que los servicios contratados satisfagan las metas estratégicas del organismo, las reglas de seguridad de la información, los estándares de calidad y los convenios de nivel de servicio (SLA).

Las sugerencias para la auditoría de proveedores se presentan como una guía metodológica y práctica para planificar, implementar y evaluar auditorías eficaces.

1.1. Capacidad técnica y experiencia comprobada

El proveedor de outsourcing de Tecnologías de la Información debe contar con las competencias, recursos, conocimientos, metodologías, certificaciones y trayectoria práctica que demuestran su habilidad para diseñar, implementar, operar y mantener soluciones tecnológicas alineadas con las necesidades y estándares de la empresa contratante.

La combinación demostrable de habilidades, conocimientos, infraestructura tecnológica, el talento humano calificado y la madurez organizacional busca asegurar que el proveedor cuenta con los recursos necesaria para ofrecer servicios de TI de manera eficiente, segura y sostenible.

1.2. Seguridad y confidencialidad de la información

En el proceso de selección, la auditoría se centra en verificar si el proveedor tiene la experiencia, los controles y las certificaciones necesarias para proteger la información del cliente, garantizando que los servicios tercerizados se presten en un entorno seguro, controlado y conforme a la normativa vigente**,** lo cual es esencial para preservar la confianza, la reputación y la continuidad operativa de ambas partes**.**

La auditoría debe concluir si los controles de seguridad y confidencialidad proveedor son los requeridos por la empresa.

1.3. Capacidad de gestión y continuidad operativa

Es la capacidad que tiene el proveedor de servicios TI, para planificar, organizar, controlar y mantener la prestación continua de los servicios tecnológicos contratados, incluso ante situaciones adversas o imprevistas, constituye un factor esencial para garantizar la confiabilidad, sostenibilidad y estabilidad de los servicios que se requieran contratar.

Con el objetivo de asegurar que los servicios subcontratados se mantengan disponibles, sean estable y sean en dirección con las metas trazadas del cliente, este criterio revisa la capacidad operativa del proveedor, la eficacia de los procesos de gestión y el grado de madurez del proveedor

1.4. Cumplimiento legal y regulatorio

Se trata de un criterio marca en la auditoría de proveedores ya que otorga al proveedor responsabilidad en todo aquello que respecta a la custodia y al uso de la información bajo las leyes que regulan el servicio. El objetivo es auditar este cumplimiento para mitigar los riesgos de sanciones, juicios, pérdidas financieras y daño a la reputación de la empresa dueña del contrato. El proveedor de servicios de TI será responsable por 7. Identificar e implantar los controles necesarios para garantizar que sus actividades, sus procesos y el manejo de los datos de clientes están en cumplimiento con todas las leyes aplicables, regulaciones, normas de la industria y contratos.

1.5. Reputación y referencias de desempeño

Este aspecto da la posibilidad a la empresa de evaluar y analizar el desempeño del proveedor en el mercado, su capacidad de respuesta frente a incidentes, su cumplimiento de acuerdos de nivel de servicio (SLA) la satisfacción general de sus clientes, esto proporciona una perspectiva real sobre la calidad, la confiabilidad y la ética del proveedor.

La reputación del proveedor en un contexto empresarial que es altamente competitivo y crítico y desde el punto de vista tecnológico, es signo de madurez organizacional, garantizando la fortaleza de las operaciones y el compromiso con la mejora continua.

2. Auditoria de proveedores

Con el fin de comprobar la seguridad de la información, verificar el cumplimiento de los acuerdos de nivel de servicio (SLA) y la continuidad operativa y la calidad del servicio se realizan auditorías periódicas a los proveedores de servicios de outsourcing TI.

Estas auditorías deben centrarse en el análisis de los riesgos, controles técnicos, organizativos y contractuales que garantizan la disponibilidad, confidencialidad, integridad y cumplimiento normativo de los servicios tercerizados que se han contratados.

2.1. Planificación de auditorias

Es el procedimiento de analizar, planificar y organizar todas las actividades requeridas para llevar a cabo una auditoria de servicios, garantizando que se cumplan todos los objetivos definidos, dentro del alcance establecido

2.1.1. Elementos claves de la planificación

ELEMENTO	DESCRIPCION
OBJETIVOS	Organizar, planificar y estructurar el proceso de auditoría técnica al proveedor de outsourcing TI, asegurando que se cumplan los acuerdos de nivel de servicio (SLA), la seguridad de la información y las políticas organizacionales.
ALCANCE	La auditoría incluye el análisis técnica, operativo y de seguridad del proveedor de servicios TI seleccionado para el proyecto.

CRITERIOS	las normas internacionales ISO 27001, COBIT, ITIL, las cláusulas y SLA establecidos en el contrato firmado, las Política internas de seguridad de la información, Ley de Protección de Datos Personales (**Ley 1581 de 2012)** y el Decreto 1377 de 2013, se utilizarán como referencia para evaluar al auditado.
EQUIPO AUDITOR	Se asigna un coordinador encargado de la planificación y ejecución para Evaluar cumplimiento de procesos, políticas, estándares y Facilita la información, las evidencias y el acceso a documentación.
METODOLOGÍA	Se puede utilizar herramientas como Revisión documental, entrevistas con jefes y personal operativo, observación directa de procesos, muestreo de registros y evidencias, evaluación de cumplimiento de SLA y controles.
RECURSOS Y HERRAMIENTAS	Se requiere acceso a los documentos contractuales y técnicos del proveedor, al espacio físico o virtual para entrevistas y revisión documental. Las herramientas de auditoría tales como checklists, software de gestión, hojas de control y soporte del área de TI y del proveedor auditado.

2.2. Ejecución y enfoque de auditorias

La ejecución de auditorías consiste en llevar a cabo la fase operativa en la que se aplica el plan de auditoría de la etapa anterior, con el fin de obtener**,** verificar **y** analizar evidencias que permitan determinar el grado de cumplimiento de los criterios definidos, durante esta fase, los auditores aplican las diferentes técnicas de recolección de evidencias.

2.2.1. Recolección de evidencias y trabajo de campo

Se aplican técnicas de auditorías planificadas para obtener la evidencia, en esta fase el equipo auditor obtiene y valida la información, la evidencia debe ser objetivas, suficientes, pertinentes y verificable y provienen de diversas fuentes

2.2.2. Documentación y análisis de hallazgos

Se documentan detalladamente todos los hallazgos encontrados, se organiza para respaldar cada conclusión, es importante que el equipo auditor identifique y confirme el hallazgo con los dueños del proceso en el proveedor para confirmar la exactitud de los hechos.

2.3. Evaluación de riesgos

Es el proceso mediante el cual las organizaciones identifica, analiza y valora los Riesgos asociados a la contratación y operación tecnológica proporcionada por terceros, permitiendo al equipo auditor enfocar sus recursos en las áreas más críticas, en este contexto del proceso permite determinar la probabilidad de que ocurra un evento adverso y el impacto que tendría en la organización contratante si los controles del proveedor fallaran.

2.3.1. Identificación del riesgo

Es el proceso fundamental y sistemático dentro de la evaluación del riesgo que consiste en detectar, reconocer y describir los elementos que, si se materializan, podrían afectar negativamente el logro de los objetivos de la organización contratante en el contexto del Outsourcing de TI.

2.3.2. Análisis y evaluación del riesgo

En este punto del proceso donde se revisa la gestión y se evalúa los riesgos con el objetivo de entender la naturaleza del mismo y determinar el nivel calculando así la probabilidad de que una amenaza se materialice y el efecto que tendrá.

Tras la evaluación de los riesgos, se determinan si los controles del proveedor son adecuados para disminuir el riesgo inherente a un nivel residual que sea satisfactorio para la empresa contratante, se establecen niveles de prioridad en función de un posible impacto sobre los riesgos con alta severidad, los cuales deben abordarse con controles inmediatos o medidas contractuales específicas, mientras que los de menor impacto pueden gestionarse atreves de un monitoreo periódico.

2.4. Seguimiento y reportes

Es la etapa final del proceso de auditoría a proveedores de outsourcing TI y son fundamentales para asegurar que los hallazgos detectados en el proceso de auditoria se traduzcan en acciones concretas que mitiguen los riesgos y fortalezcan la relación con el proveedor.

2.4.1. Reporte de auditoria

Es el documento formal donde se resumen los resultados de la evaluación, hallazgos, conclusiones y recomendaciones donde su propósito es comunicar a la dirección de la empresa contratante y al proveedor auditado el grado en que los controles y procesos evaluados cumplen con los criterios establecidos.

2.4.2. Plan de acción correctiva

Un plan de acción correctiva es un documento formal y organizado que se utiliza para definir las actividades programadas que se realizan con el fin de eliminar las causas de las no conformidades, desviaciones o deficiencias encontradas durante una auditoría, evaluación o proceso de control. Este plan detalla las medidas que el proveedor debe seguir para solucionar los hallazgos encontrados, especificando qué acciones se realizarán, quién es el responsable, los plazos de implementación y la evidencia de cumplimiento.

El auditor o el departamento del área de gestión correspondiente debe verificar y monitorear este plan para asegurar que las medidas tomadas sean eficaces y sostenibles en el tiempo.

CONCLUSIONES

La auditoría de proveedores ha venido evolucionando al pasar de los años de ser una simple revisión de cumplimiento contractual a un listado profundo estratégico de gestión. En el presente debido a la transformación digital y las amenazas de ciberseguridad, las empresas deben optar por subcontratar con proveedores que son aliados estratégicos en la mejora continua de los procesos operativos. Por lo tanto, el éxito del outsourcing no solo se mide por la reducción de costos, sino también por la capacidad de la empresa proveedora de mitigar los riesgo, delegar funciones vitales y proteger la información sensible.

Los riesgos se deben mitigar antes de que el proveedor empiece a trabajar en las operaciones contratadas. La selección de los proveedores y la planificación de la auditoría son puntos importantes en la subcontratación, se debe revisar la reputación y desempeño de las empresas seleccionadas para verificar el respaldo tecnológico y profesional que ofrecen los cuales deben ser proporcionales a la necesidad del servicio. Una planificación inadecuada con lleva a auditorías poco profundas, que no identifican algunos puntos débiles dejando a la empresa expuesta a riesgos costosos y potencialmente peligrosos.

Con un buen plan de acción Correctiva y un seguimiento riguroso la selección de proveedores tendrá un éxito definido, optando siempre por no solo realizar un excelente informe de auditoría si no también colocar en practica las acciones correctivas necesarias. El plan de acción correctiva - PAC ordena al proveedor de eliminar el origen de los riesgos. Por lo tanto, la fase de seguimiento y verificación es esencial para garantizar la mejora continua y para que la auditoría sirva como una herramienta proactiva, asegurando que el proveedor mantenga los estándares de seguridad y desempeño pactados a lo largo del tiempo.

REFERENCIAS

It.Nova. (s.f.). *Outsourcing tecnológico: ¿qué es y cómo beneficia a las empresas?* Obtenido de It.Nova: https://it-nova.co/outsourcing-tercerizacion-de-servicios/

Administrator. (25 de Julio de 2025). *ISO 27001 – Anexo A.15: Relaciones con proveedores.* Obtenido de es.isms.online: https://es.isms.online/iso-27001/annex- a-15-supplier-relationships/

Talmatic. (s.f.). La guía definitiva para elegir a su proveedor ideal de externalización de TI Obtenido de Talmatic: https://talmatic.com/blog/offshore-team/it-outsourcing-vendor-selection-criteria/

Conekta. (02 de agosto 2023). Claves para la evaluación y selección de proveedores para tu empresa. Obtenido de conekta: https://www.conekta.com/blog/seleccion-de-proveedores

Vorecol. (28 de agosto 2024). Estrategias efectivas para seleccionar y gestionar proveedores de outsourcing. Obtenido de Vorecol: https://blogs-es.vorecol.com/articulo-estrategias-efectivas-para-seleccionar-y-gestionar-proveedores-de-outsourcing-33312

Auditol (10 de enero 2023). El auditor y los riesgos con los proveedores. Obtenido de Auditol: https://www.auditool.org/blog/auditoria-interna/el-auditor-y-los-riesgos-con-los-proveedores

TechTarget. (29 de agosto 2023). auditoría de TI (auditoría de tecnología de la

información) información). Obtenido de Techtarget: https://www.techtarget.com/searchcio/definition/IT-audit-information-technology-audit

Orca. (22 de julio de 2021). ¿Cómo hacer una auditoría a tus proveedores de TI? Obtenido de Orca: **https://blog.orcagrc.com/auditoria-informatica-proveedores-de-ti**

Evoluciona Consultores. (s.f.). Cómo elaborar un plan de acciones correctivas en 7 pasos. Obtenido de Evoluciona Consultores: **https://www.evolucionaconsultores.es/plan-acciones-correctivas/**

Td Synnex. (s.f.)**.** Externalización en TI: oportunidades y amenazas para empresas. Obtenido de Td Synnex: **https://blog-es.lac.tdsynnex.com/externalizacion-en-ti-oportunidades-y-amenazas-para-empresas/**