TRABAJO DE GRADO
Opción Seminario-Diplomado.

Gestión de Ciberseguridad en Servicios Tercerizados (Outsourcing TI)

Corporación Universitaria Remington.
Nombre de la facultad: Facultad de Ingeniería
Nombre del programa académico: Ingeniería de sistemas

Sebastian Gómez Rincón.
Jorge Mauricio Sepúlveda Castaño.
Opción de Trabajo de grado Seminario-Diplomado.
2025.

Dedicatoria

Este estudio está dedicado a las pequeñas empresas que buscan avanzar en su proceso de formalización, con el propósito de visibilizar la importancia y el impacto de la seguridad de la información en los servicios tercerizados.

Agradecimientos

Agradezco a mi tutor por su orientación, acompañamiento y aportes académicos durante el desarrollo de este estudio. Asimismo, expreso mi gratitud a la institución educativa por los conocimientos brindados, los cuales permitieron fortalecer el enfoque técnico y metodológico de esta investigación.

Finalmente, agradezco a mi familia por el respaldo constante a lo largo de este proceso académico.

Tabla de Contenidos

Resumen

Este proyecto aborda la importancia de la gestión de ciberseguridad de empresas pequeñas basadas en modelos “Social Commerce” que buscan tercerizar servicios tecnológicos como estrategia para aumentar su productividad y bajar costos de contratación. Sin embargo, esa tercerización también acarrea riesgos significativos para la información(activos) ya que los proveedores tienen acceso a activos como datos de los clientes, canales de comunicación o sistemas internos y una mala gestión de estos pueden generar impactos severos como filtración de datos, indisponibilidad de servicio o fraudes.

El objetivo de este trabajo es analizar la gestión de ciberseguridad aplicada a los activos de una empresa pequeña que utiliza Social Commerce cuando decide tercerizar servicios TI específicamente respaldos(backups) para su información. Para ello, se desarrolla una revisión conceptual sobre outsourcing, ciberseguridad, gestión de riesgos y controles basados en normas internacionales como ISO 27001 e ISO 27005. La metodología utilizada incluye análisis documental, evaluación de riesgos y la elaboración de un modelo de buenas prácticas adaptado a pequeñas empresas que no cuentan con equipos internos de seguridad.

El proyecto propone un marco de gestión que permite identificar activos sensibles, evaluar los riesgos derivados del acceso del proveedor, definir controles mínimos de protección y establecer acuerdos de nivel de servicio (ANS/SLA), cláusulas de seguridad, monitoreo constante y métricas de desempeño.

En conclusión, el estudio demuestra que una gestión estructurada de ciberseguridad en procesos de outsourcing TI reduce significativamente los

riesgos operativos y de información, mejorando la productividad, eficiencia y costos de las empresas pequeñas, siempre que exista una correcta evaluación de riesgos y una gobernanza adecuada del proveedor.

Palabras clave

(Incluya 5 palabras clave que representen su trabajo de grado)

Gestión de ciberseguridad
Social commerce
Outsourcing TI
ISO 27001/27005
ANS/SLA

Marco conceptual y contextual

Marco conceptual

Social Commerce 1.1.

El Social Commerce es un modelo de comercio electrónico que se basa en el uso de redes sociales con los procesos de compra y venta de productos o servicios. Permite que los usuarios descubran, recomienden, interactúen y adquieran bienes directamente desde las redes sociales, asi como Sánchez Casado y Giraldo Cardona (2015) señalan que el análisis de la actividad en redes sociales permite comprender cómo las marcas utilizan estos entornos digitales como una herramienta de social commerce, integrando la interacción social dentro de las estrategias comerciales.

Outsourcing TI 1.2.

El Outsourcing TI es una buena práctica en temas de costos y beneficios, Devars (2009) define el *outsourcing* como la práctica mediante la cual una organización delega a un tercero especializado determinadas funciones o procesos con el fin de optimizar recursos, reducir costos y enfocarse en sus actividades estratégicas.

Ciberseguridad 1.3.

Fernández Bermejo y Martínez Atienza (2018) entienden la ciberseguridad como la protección de los activos de información frente a las amenazas que se materializan en el ciberespacio, mediante la aplicación de medidas orientadas a prevenir, detectar y responder a riesgos. Su función es garantizar la confidencialidad, integridad y disponibilidad (CIA) de los activos de información.

Análisis y gestión de riesgos (ISO 27005) 1.4.

Según la ISO/IEC 27005 (2018), el análisis y la gestión de riesgos constituyen un proceso sistemático orientado a identificar, evaluar, tratar, monitorear y comunicar los riesgos que afectan a la seguridad de la información.

Mediante una matriz de riesgo se puede identificar las amenazas, el impacto y la probabilidad con el fin de tomar decisiones en la empresa.

ANS/SLA 1.5.

Los acuerdos de nivel de servicio permiten establecer niveles de calidad y desempeño medibles que alinean las expectativas entre proveedores y clientes, contribuyendo a la competitividad organizacional (Ramírez, 2016). Los ANS/SLA son parte crucial del proceso de outsourcing.

Contrato de Outsourcing TI 1.6.

El Contrato de Outsourcing TI es el acuerdo legal con un documento formal en donde se define todo lo que tiene que ver con el servicio, tal es su importancia que Según Valero y Salvador (2008)**,** los proyectos de outsourcing total de TI tienden a fracasar a mediano plazo si no se establecen claramente los niveles de servicio, los contratos relacionales y mecanismos de adaptación al cambio.

Copias de seguridad (Backup) TI 1.7.

La información corporativa puede resultar dañada o perdida debido a ataques, errores humanos o fallos tecnológicos, por lo que es necesario contar con copias de respaldo que aseguren su recuperación (Santos, 2011).

Se ha interpretado por mucho tiempo que el mayor activo de las empresas es la infromacion, es por eso que tener un sistema de respaldo es crucial para el conituo funcionamiento del negocio.

Metodología OCTAVE-S 1.8.

OCTAVE-S es una metodología de autoevaluación orientada al análisis del riesgo de la seguridad de la información, que permite a las organizaciones identificar riesgos sobre sus activos críticos en función de los objetivos del negocio (Alberts et al., 2005) y cuenta con 3 fases las cuales son construcción de perfiles de amenaza basados en activos, identificación de vulnerabilidades de la infraestructura y desarrollo de estrategias y planes de seguridad.

Marco contextual

El estudio se realiza con una empresa ficticia.

Nombre de la empresa 2.1.

SuppEnjoy

Sector TI 2.2.

Comercio (Retail)

Modelo de operación 2.3.

Social commerce.

¿Por qué necesita tercerizar? 2.4.

La empresa está en una etapa de transformación digital para aumentar su productividad y automatizar procesos importantes como respaldar su información.

Riesgos 2.5.

Al tercerizar servicios, la empresa le da acceso a información delicada a el proveedor por lo que una mala gestión al momento del contrato y del acuerdo a nivel de servicios puede impactar de forma negativa como filtración de datos, indisponibilidad de servicio o fraudes.

Descripción del marco contextual 2.5.

Actualmente SuppEnjoy es una empresa (Pyme) de venta de suplementos deportivos que labora con un modelo social commerce con cuentas personales de WhatsApp e Instagram como sus principales canales de servicio demostrando la madurez de la empresa siendo esta informal y manual y es por eso que en busca de una mayor eficiencia, formalización y oportunidad de crecimiento, la empresa da el siguiente paso a una transformación digital, priorizando en su primera etapa puntos relacionados con riesgos legales o de cumplimiento incluido la gestión de manera correcta la información de sus clientes como lo son los datos personales.

A partir de esto, SuppEnjoy analiza los costos de la contratación interna y toma la decisión de subcontratar a un tercero la gestión de los dos puntos anteriores.

Al contactarse con el proveedor, este le recomienda un servicio de respaldo de información en la nube por medio de copias de seguridad(backup) y su gestión.

Como podemos observar SuppEnjoy comienza el proceso de outsourcing TI, en donde se debe tener en cuenta el gran impacto en riesgos de seguridad, riesgos operativos y riesgos legales o de cumplimiento que conlleva un servicio de outsourcing.

La seguridad se puede tratar de diferentes maneras, pero uno de los primeros acercamientos seria en cómo la empresa gestiona el ANS/SLA y el contrato de la propuesta del servicio que presta el proveedor.

Para concluir, en este caso de estudio se analizarán dos partes, la primera parte será lo relacionado con el proceso de outsourcing siendo enfático en lo relacionado con la seguridad y la segunda parte se describirán puntos de cómo se debe analizar y gestionar la información en temas de ciberseguridad aplicándolos en el outsourcing TI.

Etapa 1: Servicio de respaldo de información en la nube tercerizado (Backup)

En esta etapa se aborda el proceso del caos de estudio al conciliar el servicio de respaldo de información (Backup).

Madurez de la empresa.

Tabla 1. Matriz de análisis de beneficios de outsourcing TI.

Criterio	Análisis
Nuevos Avances Tecnológicos	La empresa no cuenta con un sistema de ventas, su inventario es manual (no automatizado) y mucho menos cuenta con un ecommerce por lo que el outsourcing será una estrategia muy beneficiosa para su escalabilidad.
Disponibilidad 7 x 24	La disponibilidad es crucial para su funcionamiento y al depender totalmente del tiempo de respuesta del dueño, con

	outsourcing se puede implementar un e-commerce continuo y además se puede incluir chatbots como soporte técnico 7/24.
Seguridad y cumplimiento	El modelo Social Commerce puede llevar a que en temas de seguridad sea bastante informal y que carezca de buenas practicas de seguridad, incluso que sean nulas, con la subcontratación de personal TI calificado se podrían asegurar datos de clientes implementando copias de seguridad en la nube(respaldo) ya que es necesario cumplir con las regulaciones de la industria y ciertos estándares.
Aumentar la productividad.	El modelo actual hace que la mayoría de las funciones sean totalmente manuales lo que puede llevar a errores y/o ralentizaciones constantemente, con outsourcing por medio de la automatización de ventas de en línea, catalogo, inventario aumentaría exponencialmente la eficiencia.
Reducir riesgos	La informalidad y la gestión manual persiste lo que representa altos riesgos que la empresa no puede controlar, pero con una
	implementación de una infraestructura gestionada externamente puede minimizarlos exponencialmente.
Adaptabilidad	La limitación actual de crecimiento es clara, por medio de la implementación de outsourcing se podrán solucionar muchas de esas limitaciones principalmente la

	gestión manual de los diferentes procesos.
Eliminar barreras	Sistematizar y automatizar muchos de los procesos de la empresa que se vienen haciendo manual o que incluso no existen es posible con la implementación de outsourcing que eliminará todas esas barreras que impide el crecimiento.
Planificar costos de área de TI	Los costos son relativos, poco controlables lo que se convierten en costos impredecibles, mientras que con un servicio tercerizado permite costos fijos controlados lo que es una excelente opción y más cuando actualmente la empresa está en las primeras etapas de transformación digital.

La tabla de anterior demuestra la madurez de la empresa y nos da paso para comenzar con la implementación de servicios tercerizados.

ANS/SLA.

Especificación de los servicios 4.1

El proveedor de servicios de TI (outsourcing) será responsable de la gestión completa del proceso de copias de seguridad de la información crítica de la empresa cliente, garantizando la integridad, disponibilidad y recuperación de datos en caso de incidentes.

Los componentes del servicio incluyen:

- Respaldos automáticos programados de bases de datos, archivos operativos y documentación relevante.
- Almacenamiento seguro en la nube con cifrado en tránsito y reposo.
- Retención de versiones históricas según política definida (mínimo 30 días).
- Monitoreo continuo del estado de las copias (éxito, fallos, alertas).
- Pruebas de restauración periódicas (al menos 1 cada trimestre).
- Soporte técnico para recuperación ante incidentes de pérdida de información.
- Cumplimiento normativo relacionado con protección de datos (Ley 1581 de 2012, ISO 27001, ISO 27040).

Gestión del servicio 4.2

El proveedor deberá llevar a cabo las siguientes actividades:

1. Administración de la plataforma de Backup**,** incluyendo configuración de políticas, cifrado y retención.
2. Monitoreo 24/7 del estado de los respaldos.
3. Gestión de incidentes relacionados con fallas en copias de seguridad o pérdida de datos.
4. Reportes mensuales al cliente sobre:
    - Estado de los backups.
    - Intentos de restauración.
    - Incidentes y medidas correctivas.
5. Mantenimiento preventivo de la infraestructura de respaldo.

6. Gestión de cambios cuando se modifique el entorno, estructura de datos o necesidades del cliente.
7. Atención de requerimientos como restauraciones parciales o completas.

Métricas de rendimiento 4.3

• Tasa de éxito de backups: mínimo 98% mensual.

• Tiempo medio de restauración (RTO): máximo 4 horas para información crítica.

Métricas de calidad de trabajo 4.4

• Integridad de datos verificada: 100% de los backups deben completarse con verificación automática.

• Pruebas de restauración exitosas: 90% mínimo trimestral.

Métricas de velocidad de respuesta 4.5

• Tiempo de atención a incidentes de respaldo**:** máximo 1 hora desde la notificación.

• Tiempo de inicio de restauración solicitado por el cliente: máximo 2 horas.

Métricas de eficiencia 4.6

• Uso óptimo del almacenamiento**:** alertas cuando supere el 80% de capacidad.

• Optimización de versiones: eliminación automática de versiones caducas según política.

Disponibilidad del servicio 4.7

El servicio deberá estar disponible 99.5% mensual, considerando:

- Disponibilidad de la plataforma en la nube.
- Ejecución de procesos automatizados.
- Acceso a reportes y panel de control.
- Disponibilidad del equipo de soporte.

No se descontarán los tiempos planificados por mantenimiento programado

notificados con mínimo 48 horas de anticipación.

Sanciones e indemnizaciones 4.8

Si el proveedor no cumple con el ANS acordado, aplicarán las siguientes sanciones:

- Incumplimiento de disponibilidad (<99.5%):
  - Descuento del 10% del valor mensual del servicio.
- Falla en la ejecución de backups críticos sin recuperación exitosa:
  - Penalidad del 20% del valor mensual.
- Incumplimiento del tiempo de restauración (RTO):
  - Penalidad del 15% del valor mensual.
- Pérdida de datos por negligencia comprobada del proveedor:
  - Indemnización equivalente al valor económico estimado de los datos afectados, acordado mediante acta de impacto.
- Falta de entrega de informes mensuales:
  - Descuento del 5%.

El proveedor deberá establecer un plan de contingencia y asumir los costos operativos derivados de su incumplimiento cuando corresponda.

Etapa 2: Análisis y gestión de ciberseguridad

En esta etapa se aborda el análisis y la gestión de riesgos que representan adquirir un servicio tercerizado que tenga impacto en ciberseguridad. Se debe tener en cuenta que mientras más grande la empresa más estricta se debe ser con los siguientes puntos.

Identificación de riesgos específicos 5.1.

Estos son algunos de los riesgos a tener en cuenta al usar outsourcing TI con impacto en ciberseguridad:

Riesgos de seguridad:

- Acceso no autorizado del proveedor a información confidencial
- Filtraciones de datos o fugas internas
- Robo o pérdida de información
- Configuraciones inseguras hechas por el proveedor
- Malware introducido por malas prácticas del proveedor

- Ataques a la cadena de suministro (supplier attack)

Riesgos operativos:

- Dependencia del proveedor
- Incapacidad del proveedor para responder a incidentes
- Fallas en disponibilidad del servicio (caídas, interrupciones)

Riesgos legales o de cumplimiento:

- Incumplimiento de leyes (Ley 1581 en Colombia, eventualmente GDPR si manejas ciudadanos UE)
- Mal uso de información personal
- No cumplir acuerdos de confidencialidad

Evaluación de riesgo 5.2.

Aquí es posible usar algún método como ISO 27005, OCTAVE Allegro, u otro.

Puntos a evaluar:

- Probabilidad de que un riesgo ocurra.
- Impacto si ocurre.
- Nivel de riesgo total.

Por ejemplo:

Tabla 2. Matriz de evaluación de riesgos.

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Incumplimiento normativo por manejo de datos personales	Baja	Alto	Medio
Caída del servicio del proveedor cloud	Media	Alto	Alto
Fallo en la recuperación durante incidente	Media	Alto	Alto

Establecer controles de seguridad 5.3.

Existen varios controles de la información, pero en este contexto se tendrá en cuenta controles contractuales que es pieza clave en el outsourcing ya que estos puntos se definen en el contrato o en el ANS/SLA, por ejemplo:

- Cláusulas de confidencialidad (NDA).
- Controles de acceso.
- Reglas para manejo de datos personales.
- Requerimientos de cumplimientos (ISO 27001, PCI DSS).
- Políticas de backups.
- Tiempos de respuesta a incidentes.
- Penalidades de incumplimiento.
- Retorno o destrucción de datos cuando termina el contrato.

Gestión de terceros (TPRM) 5.4.

La empresa debe tener en cuenta las 3 etapas de tercerización de servicios: antes de contratar, durante el contrato y al terminar el contrato.

Antes de contratar un servicio debes revisar certificaciones del proveedor como ISO 27001 o SOC 2, revisar historial de incidentes y verificar madurez en seguridad.

Durante la contratación el monitoreo de la ANS/SLA, revisión de reportes mensuales, revisión de logs de accesos y validación del cumplimiento de controles hacen parte de un proceso continuo que es crucial.

Al terminar el contrato destruir o retornar datos, deshabilitar accesos y algún tipo de certificado de eliminación de la información que puede ser requerido como requisito contractual.

Monitoreo continuo y respuesta a incidentes 5.5.

La empresa no debe delegar totalmente la seguridad, aunque haya outsourcing, los riesgos siguen siendo de la empresa, la responsabilidad final siempre será de la misma empresa. Tener canales de comunicación 24/7, monitoreo (SIEM/SOC) o pruebas periódicas ayudaran a tener una respuesta de incidentes si es necesario.

Cumplimiento legal 5.6.

En Colombia la ley 1581 de 2012 se encarga de la protección de datos personales lo que implica que el proveedor debe proteger datos personales, tener medidas de seguridad adecuadas, actuar solo bajo autorización y no usar datos para otros fines.

En Europa se tiene un marco más rígido conocido como el GDPR, pero solo aplica en situaciones donde se manejan datos de clientes europeos.

Documentación 5.7.

Se genera un documento formal que incluya:

- Alcance del outsourcing
- Identificación de riesgos
- Evaluación (matriz)
- Controles de mitigación
- Políticas aplicadas
- Roles y responsabilidades
- Resultados de auditorías
- Plan de mejora continua

Esto sirve como evidencia para auditorías y cumplimiento.

Metodologías 5.8.

No es suficiente gestionar el riesgo de la seguridad de la información solo con la norma ISO 27005. Es necesario apoyarse de una metodología para el análisis y gestión del riesgo, como por ejemplo OCTAVE-s (Espinosa et al., 2014).

La norma permite y recomienda apoyarse en métodos o metodologías específicas para realizar el análisis y valoración del riesgo.

OCTAVE-S es una metodología de autoevaluación orientada al análisis del riesgo de la seguridad de la información, que permite a las organizaciones identificar riesgos sobre sus activos críticos en función de los objetivos del negocio (Alberts et al., 2005). OCTAVE-S tiene 3 fases las cuales son construcción de perfiles de amenaza basados en activos, identificación de vulnerabilidades de la infraestructura y desarrollo de estrategias y planes de seguridad.

Un aspecto relevante de la metodología OCTAVE-S es que uno de los criterios para su aplicación es que la organización tenga externalizadas todas o la mayoría de sus funciones de tecnología de la información. No obstante, la propia metodología advierte que no existe evidencia empírica que respalde su uso en proyectos individuales o líneas de negocio con el fin de integrar los resultados y obtener una visión organizacional completa del riesgo (Alberts et al., 2005).

Esto quiere decir que, aunque la metodología es complementaria se debe partir de los estándares y normas de referencia.

Conclusiones

A partir del análisis realizado, se concluye que optar por un modelo de outsourcing TI conlleva grandes impactos en temas de seguridad de la información, pero con una buena gestión por parte de la empresa en las etapas del modelo, específicamente en los ANS/SLA y el contrato, aseguran un buen control de los servicios adquiridos. Adicionalmente es importante destacar que la responsabilidad final es de la empresa y no del proveedor, por eso la importancia de adoptar estándares como ISO 27001/27005 complementadas de metodologías formales de gestión y análisis del riesgo para mantener el control y la responsabilidad sobre la seguridad de la información, aun cunado haya un modelo outsourcing TI.

Referencias

Huang, Z., & Benyoucef, M. (2013). *From e-commerce to social commerce: A close look at design features*. Electronic Commerce Research and Applications, 12(4), 246–259. https://doi.org/10.1016/j.elerap.2012.12.003

Lacity, M. C., & Willcocks, L. P. (2014). Nine keys to world-class business process outsourcing. Bloomsbury Publishing.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

International Organization for Standardization. (2018). *ISO/IEC 27005: Information security risk management*. ISO.

Office of Government Commerce. (2011). ITIL Service Design. TSO (The Stationery Office).

International Organization for Standardization. (2016). ISO/IEC 27036-1:2016 — Information security for supplier relationships — Overview and concepts. ISO.

Chapple, M., Stewart, J., & Gibson, D. (2022). CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide (9th ed.). Wiley.

Espinosa, D., Martínez, J., & Amador, S. (2014). Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso

de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC. Revista Ingenierias USBmed, 5(2), 33-43.

Alberts, C. J., Dorofee, A. J., Stevens, J. F., & Woody, C. (2005). OCTAVE-S Implementation Guide, Version 1.0. Software Engineering Institute, Carnegie Mellon University.

Sánchez Casado, N., & Giraldo Cardona, C. M. (2015). Análisis de la actividad en redes sociales de marcas del sector moda como herramienta de social commerce.

Devars, J. A. (2009). Ventajas y desventajas del outsourcing. CNN expansión.

Fernández Bermejo, D., & Martínez Atienza, G. (2018). Ciberseguridad, ciberespacio y ciberdelincuencia (pp. 1-236). Thomson Reuters Aranzadi.

RAMIREZ, M. V. V. (2016). Los acuerdos de nivel de servicio (ANS) como elementos generadores de competitividad organizacional. Universidad militar Nueva Granada.

Valero, S., & Salvador, R. (2008, September). Claves del éxito para la utilización de estrategias de Outsourcing en el área de Sistemas de Información. In II International Conference on Industrial Engineering and Industrial Management (pp. 667-674).

Santos, J. C. (2011). Seguridad y Alta Disponibilidad (GRADO SUPERIOR). Ra-Ma Editorial.

OpenAI. (2025). ChatGPT (Modelo GPT-5.1) [Modelo de lenguaje grande]. https://chat.openai.com/