TRABAJO DE GRADO

Opción Seminario-Diplomado.

Gestión de ciberseguridad en servicios tercerizados

Corporación Universitaria Remington.

Facultad de ciencias básicas e ingeniería

Ingeniería de sistemas

Jefferson Javier Valderrama Rosas

Docente del seminario: Jorge Mauricio Sepúlveda Castaño

Seminario de grado Outsourcing TI

2025

Tabla de Contenidos

Resumen

Este trabajo aborda temas de Gestión de ciberseguridad en servicios tercerizados y los servicios Outsourcing TI como estrategias para las organizaciones, logrando comprende como así la importancia de definir las políticas de seguridad y confidencialidad de la información al momento de contratar proveedores externos para el manejo de la información, se abordan temas a tener en cuenta como la normativa presente para la gestión de la ciberseguridad, que riesgos se puede presentar si no se toman las medidas necesarias desde el primer momento.

En el informe técnico se analizan los conceptos básicos como outsourcing TI, definición de Ciberseguridad, marcos reconocidos como: ISO/IEC 27001: 2022, ISO/IEC 27036, NIST CSF. Asi mismo se socializan procesos para la protección de datos en servicios tercerizados enfatizando nuestro entorno. Con el fin de realizar buenas practicas al momento de realizar el tema contractual con un proveedor de servicio bajo la modalidad de outsourcing con el fin de garantizar la seguridad del mayor activo de una empresa el cual es la información.

De esta forma podemos concluir que es de vital importancia garantizar la protección de lo información cuando se realiza un proceso de contratación para un servicio bajo la modalidad de outsourcing TI.

Palabras clave

(Ciberseguridad, Outsourcing TI, Tercerización, Marco normativo, servicios)

Marco conceptual y contextual

1. Marco conceptual

1.1. Contexto y fundamentos del Outsourcing en la transformación digital

El outsourcing nace en los años 90 debido al gran crecimiento de varias empresas que no eran lo suficientemente grandes, lo cual no les permitía tener sus áreas de atención y soporte. Con esta necesidad se empiezan a crear diversas empresas que con el tiempo empezarían a prestar sus servicios a otras empresas que requerían una solución tercerizada.(De Rafael, 2008)

El outsourcing permite que las empresas puedan dedicarse por completo al Core business de sus negocios, tercerizando así otras actividades que no pertenecen a su actividad principal, por ejemplo: una empresa de desarrollo de paginas web, puede tercerizar sus servicios de infraestructura como seguridad y limpieza. Evitando así gastar parte de sus recursos en la selección de este personal y centrándose mas en sus proyectos de desarrollo.

Uno de los fundamentos del Outsourcing es la externalización de proceso con el fin de reducir costos en las empresas y así acceder a personal capacita que se dedica a los servicios contratados con otras empresas.

1.2. outsourcing y su rol en la transformación digital

"Según el Estudio de Sourcing de Servicios de TI de Eraneos y Whitelane Research, este año las empresas españolas destinarán 53.100 millones de euros a Tecnologías de la Información (TI), lo que supone un crecimiento del 4% respecto al ejercicio anterior. Conforme la digitalización sigue avanzando, el outsourcing en Life Science no solo se mantendrá vigente, sino que se volverá una parte aún más integral de la estrategia." (Ambit Ibera,2024)

1.2.1. Tipos de outsourcing:

Por ubicación geográfica:

Algunos tipos de Outsourcing son: (INEAF, s.f.):

- **Onshore outsourcing:** Cuando ambas empresas pertenecen al mismo país o localidad.
- **Nearshore outsourcing:** Cuando la empresa contratada esta en un país colindante o localidad cercana.
- **Offshore outsourcing:** Cuando la empresa se encuentra en otro país, se contrata con el fin de ahorrar costos o acceso a talento especifico.

Por proceso:

- **IT Outsourcing: Externalización de funciones TI**
- **Business Process Outsourcing:** Externalización de procesos administrativos (contabilidad, infraestructura, etc..) del negocio.

Por modelo de responsabilidad:

- **Staff augmentation:** cuando se contrata personal externo para trabajar como parte de tu equipo, y se gestiona de forma interna.

1.2.2. Beneficios y riesgos del outsourcing :

Dentro de los beneficios de Outsourcing podemos encontrar:

- **Escalabilidad:** permite gestionar de manera muchas mas eficiente los proyectos que requieren demasiado esfuerzo con ayuda externa. (Ambit Iberia, 2024).
- **Enfoque estratégico:** permite externalizar tareas operativas liberando así tiempo y recursos.
- **Mano de obra calificada:** el externalizar una actividad permite dar con una empresa con mano de obra calificada y con experiencia en buenas prácticas normativas.

los riesgos que se pueden presentar son:

- Perdida de control sobre los datos.
- Errores al momento de negociar, una mala planificación para externalizar un servicio de la empresa.
- Inconvenientes en la calidad de los servicios.

De esta forma podemos obtener una idea del panorama que presenta el Outsourcing ya que con la ayuda de la transformación digital se impulsa la tercerización de servicios

TI, lo cual demanda que las empresas gestionen de mejor forma los riesgos de seguridad. Los riesgos pueden hacer que una empresa piense bien las cosas antes de entrar en el proceso de outsourcing con sus servicios.

1.3. Impacto de la transformación digital en la seguridad de la información

La transformación digital ha impulsado la adopción de nuevas tecnologías como la inteligencia artificial y el almacenamiento en la nube. Estas nuevas tecnologías son bastante eficientes permiten aumentar la productividad de las empresas, pero también se debe asumir con responsabilidad ya que son mas propensas a sufrir ataques si no se cuenta con una buena gestión de la seguridad dentro de las empresas. los inconvenientes de ciberseguridad se vuelven mas frecuentes, por lo cual la ciberseguridad se convierte en un elemento estratégico dentro del Outsourcing. Lo cual permite que algunas empresas que no cuentan con buena infraestructura tecnológica soliciten los servicios de aquellas empresas que solo se dedican a la administración y seguridad de las redes en sus servicios.

1.4. Fundamentos de ciberseguridad

“La ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos

financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciber amenazas.” (Lindemulder & Kosinski, 2024).

De esta forma podemos comprender que la ciberseguridad permite proteger la información critica de las empresas, garantizando su disponibilidad para su consulta reduciendo así los riesgos en los entornos digitales.

Principios de la ciberseguridad:

los tres pilares de la ciberseguridad son preservar la confidencialidad, integridad y disponibilidad de la información, estos garantizan que los datos estén disponibles y sean accesibles solo por personal autorizado. En un entorno de Outsourcing la ciberseguridad se extiende a los proveedores externos, por lo cual es de gran importancia establecer en los contratos de servicios el monitoreo continuo y las políticas de protección necesarias para resguardar la información de la empresa.

1.5. Riesgos y amenazas en materia de ciberseguridad en servicios tercerizados

Un informe en el año 2024 de la empresa de antivirus Kaspersky da a conocer: “Los expertos de Kaspersky han analizado importantes ataques a cadenas de suministro e interrupciones de TI del último año y han explorado posibles escenarios de riesgos futuros, proporcionando ideas clave para ayudar a empresas de todos los tamaños a mejorar su

ciberseguridad, fortalecer su resiliencia y prepararse para las amenazas emergentes en 2025.

De acuerdo al Boletín Anual de Seguridad de Kaspersky, en 2024, los ataques a cadenas de suministro y las interrupciones de TI se consolidaron como preocupaciones predominantes en ciberseguridad, demostrando que prácticamente ninguna infraestructura está exenta de riesgos. Una actualización defectuosa de CrowdStrike afectó a millones de sistemas, mientras que incidentes sofisticados, como la puerta trasera XZ y el ataque a la cadena de suministro de Polyfill.io, expusieron los riesgos inherentes a herramientas ampliamente utilizadas. Estos y otros casos destacados subrayan la necesidad de medidas de seguridad rigurosas, una gestión robusta de parches y actualizaciones, y defensas proactivas para proteger las cadenas de suministro e infraestructuras a nivel global.”(Kaspersky,2024)

Existen muchos riesgos y amenazas actualmente ya que estamos en la era digital la mayoría de las empresas ya están digitalizando todos sus procesos evitando así tener información en físico, lo que obliga a las empresas a buscar un proveedor que se encargue de resguardar su información, es ahí donde entra en operación los servicios de outsourcing permitiendo a las organizaciones optimizar sus recursos para así mismo poder contar a empresas especializadas en el campo de la seguridad, sin embargo, esta práctica pone en riesgo la información de la empresa ya que se debe delegar el control de sistemas críticos a terceros, generando así la perdida en el control de los activos.

1.6. Riesgos Emergentes:

"La gestión de riesgos de terceros (TPRM) es una disciplina de gestión de riesgos que implica identificar, evaluar y mitigar los riesgos asociados al uso de terceros, como socios, proveedores, contratistas y prestadores de servicios. Estos terceros suelen tener acceso a diversos sistemas y datos de su organización y, a menudo, participan activamente en sus operaciones críticas. Por consiguiente, los terceros pueden incrementar su perfil de riesgo cibernético, dado que cualquier problema de seguridad que puedan sufrir puede tener repercusiones en toda la organización."(Rosencrance,2024,parr.20).

Otros factores de riesgos emergentes que se pueden encontrar podrían ser el uso mal intencionado de la IA y los ataques a los servicios en la web, lo cual representa una amenaza creciente para las empresas.

Constantemente las páginas web publicadas en internet de entidades públicas son atacadas por los ciberdelincuentes con el propósito de robar información de las personas que le permita acceder a las cuentas bancarias y así poder cometer sus crímenes. Para evitar los riesgos de robo de información gran parte de las entidades públicas, tercerizan sus servicios de administración de la red a un proveedor con conocimientos en ciberseguridad.

1.7. Marco normativo:

Las empresas que ofrecen servicios de Outsourcing de deben regir en los diferentes marcos normativos que definen una serie de requisitos específicos para la seguridad de la información por parte de terceros:

- ISO/IEC 27001: 2022: Establece los requisitos para implementar y mantener un sistema de gestión de seguridad de la información. Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgo. Esta norma aplica para todo tipo de organización. (ISO,2022).

- ISO/IEC 27036: Proporciona directrices para la gestión de la seguridad de la información en las relaciones con proveedores. Se centra en la seguridad de la cadena de suministro de hardware, software y servicios (CFE Certification, s.f.).

- NIST CSF: Conjunto de normas, directrices y mejores practicas para la gestión de riesgo de ciberseguridad. Este marco ayuda a las empresas a identificar, proteger, detectar, responder y recuperar frente a incidentes de ciberseguridad. Incluye metodologías para evaluar y mitigar riesgos en cadenas de suministro. (NIST, 2023)

2. Marco contextual

Teniendo claro los diferentes conceptos de outsourcing, ciberseguridad y marcos normativos, ahora se hace necesario analizar el contexto de los servicios de outsourcing TI.

2.1. Contexto global de la ciberseguridad en outsourcing TI

El mercado global del Outsourcing de servicios TI ha crecido de forma constante en la ultima década. Según un análisis reciente, este mercado estaba valorado en aproximadamente USD 600.9 mil millones en 2024 y se proyecta que alcance cerca de USD 835.5 mil millones para el 2033(IMARC Group, 2024).

En base a lo anterior podemos concluir que las empresas continúan confiando cada vez mas en proveedores externos para solucionar sus necesidades tecnológicas, reflejando así una adopción en las nuevas tecnologías y buscando ahorrar eficiencia en costos de operatividad.

2.2. Contexto en Colombia

En Colombia el sector del outsourcing tecnológico ha tenido un auge importante. Se ha consolidado como una potencia en la regional en este ámbito, con un crecimiento anual estimado alrededor del 9.43% hacia 2025 en el mercado Outsourcing TI. Algunas empresas locales y multinacionales encuentran en Colombia mano de obra especializada.(ZInko Colombia Tech, 2025).

Sin embargo, ese crecimiento también plantea desafíos en materia de ciberseguridad y la aplicación de leyes que permitan regular su uso.

- Legislación Colombiana:

En Colombia el marco normativo en ciberseguridad ha evolucionado con el fin de abordar los riesgos emergentes producto de la digitalización y la interconexión de servicios, actualmente no existe una ley única que regule la ciberseguridad en su totalidad.

Pero podemos encontrar normas relacionadas con la protección de datos personales, la seguridad de la información y los delitos cibernéticos las cuales establecen sanciones por incumplimiento.

- “Ley de Protección de Datos Personales: Conocida oficialmente como Ley 1581 de 2012, por muchos años ha sido considerada la principal estrategia nacional de Ciberseguridad. Se centra en la transparencia de las bases de datos y en el derecho del conocimiento por parte del usuario, cuando su información personal será recabada para un determinado fin, especialmente comercial.

  Destaca por ser una de las primeras leyes de este tipo en Latinoamérica, marcando un precedente sobre la importancia de la integridad de la información, la transparencia y la gestión del riesgo durante el manejo de datos.” (NE Digital, 2025)

- “Ley 1273 de 2009: Esta ley establece normas sobre delitos informáticos en Colombia y define los tipos penales relacionados con el acceso no autorizado a sistemas informáticos, daño informático, sabotaje informático, uso de software malicioso, entre otros.” (NE Digital, 2025)

- “Decreto 620 de 2019: Este decreto reglamenta la Ley 1273 de 2009 y establece disposiciones específicas sobre la protección de la información y los sistemas de información en el ámbito de las entidades públicas. Fue un punto de inflexión para que en Colombia se empezara a entender amenazas como ataques de denegación de servicios (DDoS), seguridad digital en general, vulnerabilidad de infraestructuras críticas, entre otros temas de seguridad.” (NE Digital, 2025)

- “Decreto 620 de 2020: Complementa el Decreto 620 de 2019 y establece los lineamientos para la implementación de medidas de seguridad de la información en el sector privado.” (NE Digital, 2025)

2.3. Problemática actual

El crecimiento de Outsourcing de servicio TI en las empresas trae consigo problemas a nivel de la contratación ya que, a nivel de contratos, acuerdos de nivel de servicios y clausulas se seguridad, no son analizadas ni tenidas en cuenta al momento de

cerrar una negociación lo cual deja un espacio para la fuga de datos, accesos no autorizados o problemas con el servicio.

En ocasiones la seguridad de los proveedores tercerizados es insuficiente, cuando un proveedor presenta una falla operativa, es el cliente es que termina siendo afectado directamente por lo cual se deben tomar enserio los términos en cuanto a las políticas de seguridad.

Desarrollo e implementación del aprendizaje

En esta sección se abordan los principales riesgos en materia de ciberseguridad que pueden afrontar las empresas al momento de tercerizar sus servicios, abordando temas operativos, estratégicos. Atreves de casos de empresas que fueron victimas de ciberataques lograr analizar las posibles causas y factores a tener en cuenta al momento de tercerizar los servicios con el fin de entender que la seguridad de la información es compartida y la importancia de definir a nivel contractual las clausulas necesarias que garanticen la seguridad de la información en los servicios de outsourcing TI

1. Identificación de vulnerabilidades en la externalización de TI

1.1. Riesgos operativos y estratégicos

La pérdida de control directo sobre los procesos críticos es uno de los mayores retos al momento de tercerizar los servicios y mas si tienen que ver con migración de información a la nube con servidores externos, la mayoría de las organizaciones dependen de proveedores externos para la administración de su información y la continuidad de su negocio. Esto puede generar riesgos operativos, como fallos en los servicios, incumplimientos en los contratos.

Ejemplo, si un proveedor no mantiene un plan de continuidad del negocio, al presentarse un incidente que tenga que ver con un ataque a los servidores podría detener completamente las operaciones del cliente. Para lo cual es importante realizar auditorias de seguimiento, KPI y acuerdos de nivel de servicio con sus responsables definidos ante fallos operativos.

2. Amenazas de ciberseguridad en servicios tercerizados

Una de la principales amenazas que encontramos en los servicios tercerizados es la falta de control sobre los accesos autorizados que maneja un proveedor. Un caso muy particular es el incidente de vulnerabilidades como SolarWinds y Kaseya revelaron como los atacantes aprovecharon actualizaciones comprometidas para infiltrarse en sistemas en los sistemas de los clients(Ruiz,2025)

Estos ataques incluyeron accesos no autorizados, fugas de datos, phishing dirigido a proveedores. Por eso e importante el cumplimiento de las normas de ciberseguridad, implementar multifactorial y cifrado de datos.

3. Estrategias para reducir riesgos operativos

Con el fin de reducir riesgos operativos de la empresa el área encargada de contratar los servicios de Outsourcing debe realizar una evaluación completa de la información que manejan y los niveles de seguridad que tiene con el fin de poder negociar con el proveedor los controles necesarios para garantizar su información. Definiendo roles y responsabilidades claras tanto del cliente como del proveedor.

Dentro de los contratos deben incluir clausulas especificas sobre tiempos de respuesta, niveles de disponibilidad y mecanismos de compensación por incumplimiento.

4. Estrategias para minimizar riesgos de ciberseguridad

Con el fin de reducir los posibles riesgos de ataques cibernéticos en la contratación de servicios Outsourcing TI, se deben implementar medidas técnicas como la autenticación multifactor (MFA), segmentación de la red, cifrado de datos. Esto con el propósito de minimizar los riesgos de ataques cibernéticos.

También es importante realizar capacitación al personal sobre phishing, el manejo seguro de contraseñas y las diferentes políticas de acceso.

5. Marcos y estándares de gestión de riesgo

Los marcos de referencia ayudan a estructurar la gestión de riesgo de los servicios de Outsourcing TI. Entre los mas utilizados se encuentra ISO/IEC 27001 la cual define un sistema de gestión de seguridad de la información, ISO/27036, enfocada en relaciones con proveedores.

6. Implementación de controles y buenas prácticas de seguridad

Entre las mejores practicas podemos encontrar las políticas y privacidad bien definidas al momento de realizar el contrato con el proveedor que va prestar el servicio tercerizado, detener claridad en los protocolos de respuesta a incidente, también se debe aplicar el principio de responsabilidad compartida donde ambas partes son responsables de la seguridad de los datos.

En conjunto con el proveedor del servicio tercerizado se debe trabajar para capacitar a los usuarios finales, como medidas extremas mantener los sistemas actualizados, tener presente los respectivos parches de seguridad y realizar auditorías.

Conclusiones

Podemos concluir que la tercerización de los servicios por medio del Outsourcing TI es de gran ayuda para las empresas ya que les permito tercerizar servicios de los cuales no tienen mucha mano de obra calificada y así mismo liberarse de esas actividades que no pertenecen al Core búshines de la empresa.

Es de tener en cuenta que en la actualidad el panorama con la tercerización de servicios en la mayoría de las empresas a crecido debido a que ahorra costos en contratación de personal capacitado, pues las empresas pueden desviar sus requerimientos a un proveedor que este dispuesto a solucionar sus problemas con personal capacitado y eso les ahorra tiempo y dinero.

La falta de controles y la falta de supervisión a los contratos bajo la modalidad de tipo Outsourcing, aumentan los factores de vulnerabilidad de las empresas. Con el fin de evitar estos inconvenientes siempre se recomienda integrar desde el inicio de la relación contractual las políticas de seguridad basada en normas como la ISO/27001, NIST CSF, entre otras las cuales establecen buenas prácticas para la protección y seguridad de los datos garantizando la operatividad en caso de un ataque cibernético.

Finalmente podemos concluir que las empresas que deseen aprovechar las ventajas del Outsourcing deben asumir un compromiso activo con la ciberseguridad.

Referencias

Ambit Iberia. (2024, noviembre, 29). *El impacto del outsourcing de la transformación digital del sector Life Science*. Ambit Ibera. https://www.ambit-iberia.com/blog/impacto-outsourcing-en-la-transformacion-digital

INEAF. (s.f). *Outsourcing* [Glosario jurídico]. Sitio web https://www.ineaf.es/glosario-juridico/outsourcing

Lidemulder, G., & Kosinski, M. (2024, 12 de agosto). *Ciberseguridad*. IBM Think. Sitio web: https://www.ibm.com/es-es/think/topics/cybersecurity

Kaspersky. (2024, octubre 21*). Kaspersky analiza posibles riesgos de interrupciones de TI y cadenas de suministro en 2025*. Kaspersky Latam. Kaspersky analiza posibles riesgos de interrupciones de TI y cadenas de suministro en 2025

ISO. (2022, octubre). ISO/IEC 27001:2022 – *Informacion security management systems – Requeriments.* Sitio web: https://www.iso.org/es/norma/27001

CFE Certification. (s.f.). *ISO/IEC 27036 Cybersecurity Standard Series*. Sitio web: https://cfecert.com/iso-iec-27036-cybersecurity-standard-series/

NIST. (2023). *NIST Cybersecurity Framework (CSF) 2.0* National Institute of Standards and Technology. https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

IMARC Group. (2024, 27 noviembre). *Global IT outsourcing market statistics, Outlook and regional análisis 2025-2033*. https://www.imarcgroup.com/it-outsourcing-market-statistics

ZInko Colombia Tech.(2025, 30septiembre). *Colombia lidera el outsourcing en Latinoamérica: Datos y Ventajas competitivas 2025*. https://zinkocolombia.com/colombia-lidera-el-outsourcing-tecnologico-en-latinoamerica-datos-y-ventajas-competitivas-2025

Rosencrance, L.(2024,junio21). 5 *Biggest risks of using third-party service providers*. Sitio web: https://www.csoonline.com/article/574543/5-major-risks-third-party-services-may-bring-along-with-them.html

Ruiz, V. (2025). *CrowdStrike, SolarWinds, Kaseya, Okta y Log4j*: estamos en riesgo. Linkedln. https://es.linkedin.com/pulse/crowdstrike-solarwinds-kaseya-okta-y-log4j-estamos-un-v%C3%ADctor-ruiz-j7ejf

NE Digital, (2025, febrero 15). *Ciberseguridad en Colombia: leyes, estrategias y retos*. Sitio Web https://www.nedigital.com/es/blog/ciberseguridad-en-colombia

De Rafael, J. (2008). El outsourcing como palanca de crecimiento de las empresas. Asociacion Española de Empresas de Consultoria (AEC). Sitio web https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/374/65.pdf