TRABAJO DE GRADO
Opción Seminario-Diplomado.

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

Corporación Universitaria Remington

Facultad de Ingenierías

Ingneiería de Sistemas

Fabian Ricardo Vargas Diaz

Juan camilo Monroy Montes

Jorge Mauricio Sepúlveda Castaño

Opción de Trabajo de grado Seminario-Diplomado.

2025

Tabla de Contenidos

Resumen

En el contexto actual de transformación digital, las organizaciones han adoptado el outsourcing de servicios de tecnologías de la información (TI) como una estrategia para optimizar recursos, acceder a conocimientos especializados y mejorar la eficiencia operativa. Sin embargo, esta externalización de funciones críticas, como la gestión de infraestructura, plantea desafíos significativos en materia de ciberseguridad.

Este trabajo de grado, desarrollado en el marco del seminario *Gestión de Servicios de Outsourcing en TI* de la Corporación Universitaria Remington, analiza los riesgos asociados a la tercerización de infraestructura tecnológica y propone estrategias de protección alineadas con estándares internacionales. Se toma como referencia la empresa ficticia InnovaCorp S.A.S., dedicada a soluciones digitales para el sector financiero, que ha decidido tercerizar la administración de servidores, redes, almacenamiento y soporte técnico.

A través de una simulación técnica, se identifican riesgos como fuga de datos por mala gestión de credenciales, vulnerabilidad a ransomware en servidores no actualizados, accesos no autorizados, fallas en disponibilidad e incumplimiento normativo. Para mitigar estos riesgos, se propone una arquitectura de seguridad basada en gestión de identidades, monitoreo, auditoría, segmentación de red y gestión de vulnerabilidades.

Además, se presenta una propuesta técnica de soporte tercerizado con atención escalonada (N1, N2, N3), y un Acuerdo de Nivel de Servicio (ANS) que define tiempos de respuesta, métricas de desempeño, disponibilidad, sanciones y mecanismos de mejora continua. El enfoque contractual se complementa con cláusulas de seguridad, auditorías y revisión anual del contrato.

Como resultado, se espera que InnovaCorp S.A.S. fortalezca su postura de ciberseguridad, mejore la continuidad operativa, cumpla con normativas como ISO/IEC 27001, GDPR y Ley 1581, y consolide una relación transparente con su proveedor de servicios TI.

Palabras Clave

- Ciberseguridad
- Outsourcing
- Infraestructura TI
- SLA
- Gestión de riesgos

Marco conceptual y contextual

En la era digital, las organizaciones dependen cada vez más de los servicios de tecnologías de la información (TI) para operar de manera eficiente y competitiva. Esta creciente demanda ha impulsado la adopción del outsourcing como una estrategia clave para optimizar recursos, mejorar la eficiencia operativa y acceder a conocimientos especializados sin incurrir en altos costos de infraestructura o personal (Gonzales Ramirez, Gascó Gascó, & Taverner, 2015).

Sin embargo, la externalización de funciones críticas —como la gestión de infraestructura, almacenamiento de datos o soporte técnico— plantea importantes desafíos en materia de ciberseguridad. Al delegar el control de activos digitales a terceros, las organizaciones se exponen a riesgos como accesos no autorizados, pérdida de datos, vulnerabilidades en la cadena de suministro y cumplimiento normativo insuficiente (TI Rescue, 2023).

Para mitigar estos riesgos, es fundamental que las organizaciones y sus proveedores de servicios cumplan con estándares nacionales e internacionales en seguridad de la información, como la Ley 1581 de 2012 en Colombia (Congreso de Colombia, 2012), el Reglamento General de Protección de Datos (GDPR) (Unión Europea, 2016) en Europa, y normas como ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27017 (ISO, 2022; Sinergias Empresariales, 2023). Además, deben aplicar marcos de

gobierno TI como COBIT (COBIT an ISACA Framework, 2019; Sinergias Empresariales, 2023), que proporcionan lineamientos para la gestión y control de los servicios tercerizados, promoviendo la alineación entre los objetivos del negocio y la tecnología.

1. Conceptos clave

Desarrollo e implementación del aprendizaje

Matriz de riesgos

Ejemplo de riesgo: Fuga de datos por mala gestión de credenciales. Controles recomendados: MFA, rotación de contraseñas, gestores seguros y auditorías periódicas (TI Rescue, 2023).

Diseño de arquitectura de seguridad para infraestructura tercerizada

La arquitectura de seguridad propuesta, siguiendo lineamientos de ITIL y COBIT (COBIT an ISACA Framework, 2019; International Organization for Standardization, 2022), para InnovaCorp S.A.S. se basa en los siguientes pilares:

- **Gestión de identidades y accesos (IAM):** RBAC y MFA (ISO/IEC 27001, 2022).
- **Gestión de vulnerabilidades:** escaneos periódicos y parches (NIST, 2022).

- **Monitoreo y auditoría:** SIEM centralizado y trazabilidad (ISACA, 2019).
- **Gobierno y cumplimiento:** cláusulas contractuales alineadas con GDPR y Ley 1581 (Unión Europea, 2016; Congreso de Colombia, 2012).

Outsourcing en TI o subcontratación de tecnología de la información, es el proceso mediante el cual una empresa contrata a un proveedor externo para gestionar funciones de IT que tradicionalmente se realizarían internamente. Esto puede incluir desde el soporte técnico y la gestión de redes hasta el desarrollo de software y la ciberseguridad (Nordic Stories, s.f.).

Ciberseguridad, La ciberseguridad se refiere a cualquier tecnología, práctica y política para prevenir los ataques cibernéticos o mitigar su impacto (Lindemulder & Kosinski, 2024). Es una realidad que muchas compañías no cuentan con el personal de TI suficiente para encargarse bien de todos los aspectos digitales de un negocio, por lo que muchos líderes recurren a servicios de firmas de IT outsourcing, para buscar apoyo en cuanto a ciberseguridad (Beneficios clave de contratar firmas de IT outsourcing en Colombia para ciberseguridad, s.f.).

2. Contexto del Trabajo

Este trabajo se desarrolla en el marco del seminario “Gestión de Servicios de Outsourcing en TI”, y se enfoca en el análisis de los retos actuales y estrategias de protección en entornos de outsourcing, específicamente en el servicio de gestión de infraestructura.

La empresa ficticia InnovaCorp S.A.S., dedicada a soluciones tecnológicas para el sector financiero, ha decidido tercerizar la gestión de su infraestructura tecnológica con el objetivo de reducir costos operativos y mejorar la disponibilidad de sus servicios. Esta decisión implica delegar la administración de servidores, redes, almacenamiento y sistemas de respaldo a un proveedor externo especializado.

En este contexto, se identifican riesgos como la pérdida de control sobre los activos críticos, la exposición a vulnerabilidades en la cadena de suministro, y la dificultad para garantizar el cumplimiento normativo. Por ello, se propone analizar las estrategias de protección más efectivas para mitigar estos riesgos, incluyendo la implementación de acuerdos de nivel de servicio (SLA), auditorías periódicas, cifrado de datos, y políticas de acceso robustas (Ávila & Ayala, 2023).

Desarrollo e implementación del aprendizaje

1. Contexto de aplicación:

InnovaCorp S.A.S. es una empresa ficticia especializada en soluciones digitales empresariales. Su modelo de operación se apoya en la tercerización de infraestructura TI, incluyendo servidores, redes, almacenamiento, virtualización y soporte técnico. Esta decisión estratégica busca garantizar escalabilidad, disponibilidad continua y cumplimiento normativo, sin incurrir en altos costos de operación interna. La externalización de infraestructura TI implica delegar el control de activos críticos a un proveedor externo.

Esto genera una superficie de ataque ampliada y nuevos vectores de riesgo. Se realizó una simulación de evaluación de riesgos sobre el contrato de outsourcing, considerando aspectos técnicos, operativos y legales.

2. Evaluación de riesgos en infraestructura tercerizada

La externalización de infraestructura TI implica delegar el control de activos críticos a un proveedor externo. Esto genera una superficie de ataque ampliada y nuevos vectores de riesgo. Se realizó una simulación de evaluación de riesgos sobre el contrato de outsourcing, considerando aspectos técnicos, operativos y legales.

Tabla 1. Matriz de Riesgos en Infraestructura TI Tercerizada

Riesgo Identificado	Probabilidad	Impacto	Nivel de Riesgo	Controles Recomendados
Fuga de datos por mala gestión de credenciales	Alta	Alto	Crítico	MFA, rotación de contraseñas, gestores seguros y auditorías periódicas (NIST, 2022)
Ransomware en servidores no actualizados	Alta	Crítico	Muy Alto	Gestión de parches, backups offline, segmentación de red, simulacros (ISO/IEC 27002, 2022)
Accesos no autorizados por falta de controles de acceso	Media-Alta	Alto	Crítico	RBAC, monitoreo de accesos, revisión de permisos (ISACA, 2019)
Fallas en disponibilidad por mala gestión del proveedor	Media	Alto	Alto	SLA claros, monitoreo, penalizaciones contractuales (Axelos, 2020)
Incumplimiento normativo	Media	Alto	Alto	Auditorías, cláusulas contractuales, capacitación (ISO, 2022)

3. Diseño de arquitectura de seguridad para infraestructura tercerizada

La arquitectura de seguridad propuesta para InnovaCorp S.A.S. se basa en los siguientes pilares:

- **Gestión de Identidades y Accesos (IAM):**
  - Implementación de RBAC (Role-Based Access Control).

- Autenticación multifactor (MFA) en todos los accesos administrativos.
- Integración con gestores de credenciales seguros (ej. HashiCorp Vault).

- **Gestión de Vulnerabilidades**
  - Ciclo de parches automatizado con herramientas como WSUS o Ansible.
  - Escaneo mensual de vulnerabilidades con OpenVAS o Nessus.
  - Simulacros de respuesta ante incidentes (ransomware, DDoS, fuga de datos).

- **Monitoreo y Auditoría**
  - SIEM (Security Information and Event Management) para correlación de eventos.
  - Registro de logs centralizado y cifrado.
  - Auditorías trimestrales de cumplimiento de SLA y controles de acceso.

- **Gobierno y Cumplimiento**
  - Contratos con cláusulas de seguridad, confidencialidad y cumplimiento normativo.

- Adopción de estándares ISO/IEC 27001 (ISO, 2022), ISO/IEC 20000-1 y buenas prácticas ITIL.
- Evaluaciones de proveedores con base en criterios de madurez de seguridad.

4. Propuesta técnica de soporte tercerizado

La propuesta técnica de soporte para InnovaCorp S.A.S. contempla un modelo escalonado de atención, orientado a garantizar la continuidad operativa, la trazabilidad de incidentes y la mejora continua del servicio. Este modelo se estructura en tres niveles:

- Nivel 1 (N1): Atención básica para resolución de problemas comunes como desbloqueo de cuentas, configuración de correo, y asistencia en herramientas corporativas (Axelos, 2020).
- Nivel 2 (N2): Soporte especializado para fallos en red interna, errores en software corporativo, y problemas de conectividad (Axelos, 2020) .
- Nivel 3 (N3): Intervención avanzada en servidores, infraestructura crítica o escalamiento a proveedores externos (Axelos, 2020).
- El servicio se presta mediante canales definidos: correo electrónico, sistema de gestión de tickets, línea telefónica y chat

corporativo. Cada solicitud se registra con trazabilidad completa, permitiendo análisis de recurrencias y seguimiento por usuario y equipo.

Se incluye soporte técnico remoto y presencial, mantenimiento preventivo mensual, y atención a incidentes críticos fuera del horario laboral. El proveedor se compromete a mantener un equipo técnico disponible y capacitado, con protocolos de escalamiento automáticos en caso de incumplimiento de tiempos de respuesta.

5. Acuerdo de Nivel de Servicio (ANS)

El ANS formaliza los compromisos entre InnovaCorp S.A.S. y el proveedor TechSoluciones S.A.S., estableciendo métricas claras de desempeño, disponibilidad y calidad del servicio.

Tabla 2. Tiempos de respuesta y resolución

Tipo de Incidente	Ejemplo	Tiempo de Respuesta	Tiempo de Resolución
Crítico	Caída de sistema central	≤ 1 hora	≤ 4 horas
Alto	Fallo en múltiples estaciones	≤ 4 horas	≤ 8 horas
Medio	Error en software de usuario	≤ 6 horas	≤ 16 horas
Bajo	Solicitud de instalación	≤ 8 horas hábiles	≤ 3 días hábiles

- **Métricas de desempeño**
  - FCR (First Contact Resolution): ≥ 70%
  - CSAT (Satisfacción del Usuario): ≥ 85%
  - NPS (Net Promoter Score): Medición mensual
  - Cumplimiento de SLA: ≥ 95% mensual
- **Disponibilidad del servicio**
  - Horario estándar: lunes a viernes, 7:00 a.m. – 7:00 p.m.
  - Incidentes críticos: Atención fuera de horario garantizada en ≤ 1 hora.
- **Sanciones e indemnizaciones**
  - Penalización del 1% del valor mensual por cada incidente fuera de SLA.

- Compensaciones en horas de soporte, capacitaciones o servicios adicionales.
- Revisión contractual si la disponibilidad mensual cae por debajo del 93%.

- **Mejora continua**
  - Reuniones mensuales de revisión de indicadores.
  - Retroalimentación del cliente y ajustes operativos.
  - Revisión anual del contrato y del ANS.

6. Gobierno y cumplimiento

La gestión contractual y normativa en entornos de outsourcing de infraestructura TI es un componente esencial para garantizar la seguridad, la trazabilidad y la responsabilidad compartida entre cliente y proveedor. En el caso de InnovaCorp S.A.S., se han definido mecanismos de gobierno que permiten supervisar el cumplimiento de los acuerdos establecidos y asegurar la alineación con estándares internacionales.

Entre las medidas implementadas se destacan:

- Contratos con cláusulas específicas de seguridad, confidencialidad, cumplimiento normativo y gestión de incidentes.

- Adopción de estándares internacionales como ISO/IEC 27001 para seguridad de la información, ISO/IEC 20000-1 (International Organization for Standardization, 2022)para gestión de servicios, y buenas prácticas ITIL para operación y mejora continua.
- Evaluaciones periódicas de proveedores, basadas en criterios de madurez de seguridad, cumplimiento de SLA, y calidad del soporte técnico.
- Derecho a auditoría técnica y documental, incluyendo revisiones de accesos, gestión de vulnerabilidades y cumplimiento de políticas de respaldo.
- Revisión anual del contrato y del ANS, con posibilidad de ajustes según evolución tecnológica, necesidades operativas y desempeño del proveedor.

Estas prácticas permiten a InnovaCorp S.A.S. mantener el control estratégico sobre sus activos digitales, reducir la exposición a riesgos legales y operativos, y fomentar una relación transparente y colaborativa con el proveedor de servicios tercerizados.

7. Resultados esperados

La implementación de la arquitectura de seguridad, el modelo de soporte técnico y el acuerdo de nivel de servicio en el entorno tercerizado de InnovaCorp S.A.S. permitirá alcanzar los siguientes resultados:

- Reducción significativa de riesgos críticos, como fuga de datos, ransomware y accesos no autorizados.
- Mejora en la disponibilidad y continuidad operativa de los servicios digitales, gracias a protocolos de atención escalonada y monitoreo constante.
- Cumplimiento efectivo de normativas nacionales e internacionales, evitando sanciones legales y fortaleciendo la reputación corporativa.
- Mayor trazabilidad y control sobre los servicios tercerizados, mediante auditorías, métricas de desempeño y cláusulas contractuales claras.
- Fortalecimiento de la confianza interna y externa en la gestión de infraestructura TI, promoviendo una cultura de seguridad y responsabilidad compartida.

Estos resultados consolidan la capacidad de InnovaCorp S.A.S. para operar de manera segura, eficiente y alineada con las exigencias del entorno digital actual.

Conclusiones

La implementación de estrategias de ciberseguridad en entornos de outsourcing representa un reto técnico y contractual, como señalan Gonzales Ramírez, Gascó & Taverner (2015) en relación con la evolución del outsourcing en TI. Requiere planificación, monitoreo y alineación con estándares internacionales.

El análisis de riesgos permitió identificar vulnerabilidades críticas que deben ser gestionadas desde el diseño del contrato y la operación técnica. La propuesta de soporte escalonado y el ANS aportan claridad, trazabilidad y responsabilidad compartida entre cliente y proveedor.

Se concluye que el outsourcing no debe verse como una pérdida de control, sino como una oportunidad para fortalecer la gestión tecnológica mediante alianzas estratégicas. La clave está en establecer mecanismos de gobierno, auditoría y mejora continua que garanticen la protección de los activos digitales y el cumplimiento normativo.

Referencias

Axelos. (2020). ITIL® Foundation: ITIL 4 Edition. The Stationery Office

Beneficios clave de contratar firmas de IT outsourcing en Colombia para ciberseguridad. (s.f.). Obtenido de Rootstack: https://rootstack.com/es/blog/it-outsourcing-firmas-colombia-ciberseguridad

Congreso de Colombia. (2012). *Ley 1581 de 2012*. Obtenido de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

International Organization for Standardization. (2022). *ISO/IEC 27001:2022*. Obtenido de ISO : https://www.iso.org/standard/27001

Lindemulder, G., & Kosinski, M. (12 de Agosto de 2024). *¿Qué es la ciberseguridad?* Obtenido de IBM: https://www.ibm.com/mx-es/topics/cybersecurity

Nordic Stories. (s.f.). *Outsourcing de TI: Ventajas y Desventajas*. Obtenido de Nordic Solutions: https://www.nordicsolutions.es/outsourcing-de-ti-ventajas-y-desventajas/

TI Rescue. (15 de Noviembre de 2023). *Ciberseguridad a Escala Global: Normas Internacionales - TI Rescue*. Obtenido de TI RESCUE: https://tirescue.com/ciberseguridad-a-escala-global-normas-internacionales/

Ávila, C. J., & Ayala, J. C. (2023). Análisis de la ciberseguridad a la infraestructura tecnológica de la empresa Señal X.

Rootstack. (s. f.). Beneficios clave de contratar firmas de IT outsourcing en Colombia para ciberseguridad. https://rootstack.com/es/blog/it-outsourcing-firmas-colombia-ciberseguridad

ISACA. (2019). COBIT an ISACA Framework. https://www.isaca.org/resources/cobit

Congreso de Colombia. (2012). Ley 1581 de 2012. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Gonzales Ramírez, M. R., Gascó Gascó, J. L., & Taverner, J. L. (2015). Outsourcing de sistemas de información: situación actual, evolución y tendencias.

International Organization for Standardization. (2022). ISO/IEC 27001:2022. https://www.iso.org/standard/27001

ISO. (2022). Seguridad de la información. https://www.iso.org

Lindemulder, G., & Kosinski, M. (2024, agosto 12). ¿Qué es la ciberseguridad? IBM. https://www.ibm.com/mx-es/topics/cybersecurity

Microsoft. (2025). Asistencia de IA para revisión y sugerencias en documentos técnicos (Copilot). https://copilot.microsoft.com

Nordic Solutions. (s. f.). Outsourcing de TI: ventajas y desventajas. https://www.nordicsolutions.es/outsourcing-de-ti-ventajas-y-desventajas/

Sinergias Empresariales. (2023). ¿Qué normas ISO regulan la ciberseguridad?

TI Rescue. (2023, noviembre 15). Ciberseguridad a escala global: normas internacionales. https://tirescue.com/ciberseguridad-a-escala-global-normas-internacionales/

Unión Europea. (2016). Reglamento general de protección de datos (RGPD). https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html