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

Nombres de los estudiantes autores del trabajo de grado:

Miler Alexis Bolaños

Nombre del Tutor del trabajo de grado (docente del seminario o diplomado).

Jorge Mauriio Sepúñveda Castaño

Opción de Trabajo de grado Seminario-Diplomado:

Seminario

Año de presentación del trabajo de grado:

2026

Dedicatoria

A Zuly, mi compañera incansable y mi fuerza en cada paso. Gracias por tu apoyo incondicional, por tu valentía y tu lucha diaria para sacar adelante este proyecto, y por empujarme a mejorar y a superar cada desafío. Gracias por atravesar conmigo cada momento, por sostenerme en las dudas y celebrar conmigo los logros, y por recordarme siempre que juntos podemos llegar más lejos. Este logro también es tuyo, porque sin ti, nada de esto habría sido posible.

Agradecimientos

Agradezco profundamente a la Corporación Universitaria Remington por brindarme la oportunidad de desarrollar este proyecto en un entorno académico de excelencia, así como por los recursos y la infraestructura que facilitaron su realización.

De manera especial, expreso mi sincero agradecimiento a los profesores por su constante apoyo, orientación y disposición durante todo este proceso, por compartir su conocimiento y experiencia, y por motivarme a superar los desafíos y a alcanzar los objetivos planteados. Su acompañamiento ha sido fundamental para el aprendizaje y la consolidación de este trabajo.

Tabla de Contenido

1. Resumen

El enfoque orientado a la adopción de modelos de outsourcing en tecnologías de la información (TI) ha crecido considerablemente en empresas que buscan las ventajas que este tipo de modelo les ofrece para optimizar costes, mejorar la eficiencia de los procesos, y acceder a capacidades especializadas, etc. No obstante, la externalización también lleva implícitos unos riesgos considerables en el ámbito de la seguridad de la información, especialmente en cuanto a la protección de los datos, la gestión de los accesos y el cumplimiento normativo.

El presente informe tiene como objetivo un análisis de los riesgos que derivan de la gestión de la ciberseguridad en el contexto del outsourcing, así como la evaluación de controles, modelos de responsabilidad compartida, y estándares internacionales aplicables a ello. También se abordarán las estrategias de mitigación en el outsourcing desde el punto de vista de las buenas prácticas: acuerdos de nivel de servicio (SLA), auditorías de seguridad, legislación como la norma ISO/IEC 27001.

Por último, se mostrarán los resultados de una aplicación práctica del conocimiento en el marco del outsourcing, mostrado en un entorno simulado donde quedará demostrado cómo se llevarían a cabo la gestión de incidentes, la gestión de accesos o el trabajo de monitoreo de seguridad, y donde se demostrará la apertura de la vía de validación de los modelos propuestos.

Palabras clave
Ciberseguridad, Protección de datos, Riesgo, SLA (Service Level Agreement) y Estrategias.

2. Marco conceptual y contextual

El presente documento aborda el análisis y aplicación de modelos de outsourcing en tecnologías de la información, integrando definiciones conceptuales que apoyan la narrativa común de la literatura y las temáticas que se han visto en el seminario. El outsourcing no ha hecho sino consolidarse como una manera de operar actualmente, en períodos caracterizados por ser intensamente competitivos, ayudando a las empresas a optimizar recursos, así como a acceder a capacidades especializadas.

Desde el plano conceptual, el outsourcing también ha sido definido con bastante amplitud en la literatura. Como afirman Mary C. Lacity y Leslie P. Willcocks (2012), el outsourcing es transferir el control o la responsabilidad de los procesos o servicios que son internos a los de una organización a los de proveedores externos mediante un acuerdo contractual. En sentido complementario, Ilan Oshri, junto a una relación de coautores, lo define como un servicio tecnológico prestado

por una empresa externa, especializada, y con condiciones fijadas de antemano (Oshri, Kotlarsky & Willcocks, 2015). Igualmente, Robert J. Thierauf también apunta que el outsourcing permite a las organizaciones centrarse en sus competiciones, mientras que las funciones de soporte se las delegan a terceros.

En el contexto de las tecnologías de la información, el outsourcing TI (ITO en inglés), hace referencia a la subcontratación de servicios de tecnologías que pueden englobar, el desarrollo de software, la gestión de la infraestructura, el soporte o los servicios de seguridad. Tal como argumentan Lacity y Willcocks (2012) esta práctica ha evolucionado desde un enfoque centrado en la reducción de costes hacia una práctica orientada a la generación de valor, la innovación y la flexibilidad en la organización.

Diversos estudios académica ha evidenciado el crecimiento y la importancia del outsourcing TI. Un ejemplo de ello puede ser la revisión de la literatura realizada por Dibbern et al. (2004); los hallazgos de esta revisión muestran que el outsourcing TI ha sido investigado en las decisiones, la gestión de proveedores y sus riesgos, y otros autores más recientes enfatizan factores como la gobernanza, la confianza y el alineamiento estratégico a la hora del éxito de la práctica de outsourcing (Oshri et al., 2015).

Desde un enfoque contextual, el desarrollo de este informe tiene lugar en un contexto organizacional (simulado) en el que se hacen uso de las competencias adquiridas en el ámbito de la gestión de servicios TI, del gobierno de TI, de la gestión de riesgos, de la ciberseguridad. Si nos encontramos en una organización real es importante describir en qué sector económico opera, el tamaño de la misma, cuál es su estructura organizativa y qué nivel de madurez tecnológica tiene, así como el papel estratégico que poseen las TI a la hora de cumplir con las metas establecidas.

De forma particular, en relación a la ciberseguridad, el outsourcing representa un desafío. Referente a la externalización de servicios, ya que el perímetro de seguridad se expande debido a que los activos de información y los procesos tecnológicos no son ya totalmente controlables por parte de la empresa. Para Kevin W. Knight (2019), esto se traduce en un incremento de la posibilidad de sufrir riesgos derivados de las terceras partes proveedores de la organización, como accesos no deseados, fallos en la cadena de suministro y vulnerabilidades provenientes de la infraestructura externa.

En este contexto, se hace necesario adoptar enfoques de gestión de riesgos de terceros (Third-Party Risk Management) y modelos de responsabilidad compartida, así como establecer acuerdos de nivel de servicio (SLA) que contemplen requisitos de seguridad, cumplimiento normativo y continuidad del negocio. De acuerdo con Lacity y Willcocks (2012), el éxito del outsourcing TI

depende en gran medida de la capacidad de la organización para establecer mecanismos efectivos de control, supervisión y evaluación continua del desempeño de los proveedores.

En este informe se plantea un caso simulado de una organización del sector financiero en Colombia, una organización de tamaño medio que gestiona productos bancarios y prestación de servicios digitales a clientes, que trata información muy sensible, es decir, trata datos personales, financieros, datos transaccionales, etc. Con la finalidad de obtener una mejora en costes y eficiencia operativa, esta organización ha adoptado un modelo de outsourcing de los servicios críticos de TI como infraestructura de nube, gestión de bases de datos y soporte técnico especializado. Entre los activos críticos se incluyen los sistemas de información de clientes, las plataformas transaccionales, la infraestructura alojada en la nube y los sistemas de autenticación y control de acceso. La participación de proveedores externos en la gestión de estos activos críticos incrementa la superficie de ataque y genera riesgos concretos como accesos no autorizados, fuga de información, caídas de disponibilidad de servicio o incumplimientos normativos, con lo que este caso es considerado crítico, donde la implementación de controles de ciberseguridad y mecanismos de seguimiento debe ser la adecuada para proteger la información.

Este escenario corresponde a un entorno de alta criticidad, donde la exposición a riesgos de terceros requiere la implementación de un modelo de seguridad basado en defensa en profundidad, articulando la teoría con su aplicación práctica en entornos organizacionales y permitiendo comprender tanto los beneficios como los riesgos asociados a la adopción del outsourcing en TI.

3. Riesgos de ciberseguridad en servicios tercerizados

3.1 Identificación y análisis de riesgos

La subcontratación de algunos de los procesos de TI implica la delegación de funciones críticas a terceros ajenos a la organización que amplían el perímetro de control y los riesgos de ciberseguridad, los cuales incluyen pero no se limitan a la fuga, pérdida o robo de información, accesos inapropiados o no autorizados, falta de cifrado, manejo incorrecto de credenciales, dependencia de proveedores (Vendor Lock-in), escaso control sobre infraestructuras ajenas, incumplimiento normativo y errores en las auditorías y en la aplicación de la gestión de incidentes, comprometiendo así la confidencialidad, la integridad y la disponibilidad de la información persistiendo en la continuidad de negocio y la resiliencia operativa; así, estos riesgos de ciberseguridad deben ser valorados y gestionados de forma sistemática, y siguiendo estándares de referencia como ISO/IEC 27001, NIST, ITIL 4 y COBIT 2019.

Tabla 1: Identificación y análisis de riesgos

Riesgo	Categoría	Impacto / Normativa
Pérdida o fuga de información	Información	Alto. Riesgo de filtración de datos sensibles. Normativa aplicable: ISO/IEC 27001 (gestión de información), GDPR (protección de datos), NIST SP 800-53 (controles de seguridad).
Acceso indebido por proveedor o accesos no autorizados	Acceso	Alto. Riesgo de intrusión externa o interna. Normativa aplicable: ISO/IEC 27001 (control de accesos), NIST SP 800-53 (gestión de identidades y accesos), COBIT 2019 (seguridad y gobernanza de TI).
Falta de cifrado en transmisión o almacenamiento	Información	Alto. Datos vulnerables a intercepciones. Normativa aplicable: ISO/IEC 27001 (cifrado de información), GDPR (protección de datos en tránsito y reposo), NIST SP 800-175B.
Credenciales mal gestionadas o falta de autenticación multifactor	Acceso	Medio-Alto. Facilita intrusiones. Normativa aplicable: ISO/IEC 27001 (gestión de identidades), NIST SP 800-63B (autenticación digital), PCI DSS (si aplica para datos financieros).
Dependencia del proveedor (Vendor Lock-in) y dificultad para migrar servicios	Gestión de proveedor	Medio. Dificulta cambios estratégicos. Normativa aplicable: ISO/IEC 38500 (gobernanza de TI), ITIL 4 (gestión de proveedores y contratos).
Falta de control sobre infraestructuras externas	Gestión de proveedor	Alto. Supervisión limitada de sistemas críticos. Normativa aplicable: ISO/IEC 27001 (control de operaciones y monitoreo), ISO/IEC 27036 (seguridad de proveedores).
Incumplimiento normativo y violación de leyes de protección de datos	Información	Alto. Riesgo de sanciones legales. Normativa aplicable: GDPR, Leyes locales de protección de datos (ej. Ley 1581 de 2012 en Colombia), ISO/IEC 27001.
Falta de auditorías y protocolos claros	Gestión de proveedor	Medio. Reduce capacidad de detección de vulnerabilidades. Normativa aplicable: ISO/IEC 27001 (auditorías internas y externas), COBIT 2019 (control y supervisión).
Gestión inadecuada de incidentes y tiempos de respuesta elevados	Gestión de proveedor	Alto. Impacta la continuidad del negocio. Normativa aplicable: ISO/IEC 27001 (gestión de incidentes), NIST SP 800-61 (gestión de incidentes de seguridad informática), ITIL 4 (gestión de incidentes y continuidad).

Fuente: Elaboración propia.
Dicha revisión posibilita establecer un sistema de prioridades entre los distintos riesgos existentes en función de su probabilidad de ocurrencia e importancia, y sirve de soporte para la configuración de los controles y los procedimientos de mitigación, como pueden ser los SLA, el seguimiento continuo, las auditorías periódicas o la toma de normas internacionales de seguridad, como ISO/IEC 27001. La categorización de los distintos riesgos y su puesta en orden simplifican comprenderlos y la planificación de acciones preventivas en un esquema de outsourcing TI.

3.2 Cumplimiento normativo y estándares

La eficaz gestión de los riesgos relativos a la ciberseguridad en el caso de los servicios tercerizados debe estar acompañada de la aplicación de marcos normativos y estándares ampliamente reconocidos que sirvan para garantizar la protección de la información y de la continuidad de las operaciones. Los más relevantes son:

La ISO/IEC 27001 (2013) establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información, ofreciendo un marco estructurado que permite proteger la confidencialidad, integridad y disponibilidad de los activos de información dentro de la organización. Como complemento, la ISO/IEC 27017 (2015) proporciona controles específicos para servicios en la nube, orientados a la segregación de clientes, la gestión de privilegios y la definición clara de responsabilidades entre proveedor y cliente en entornos cloud.

El NIST Cybersecurity Framework (2018), desarrollado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos, propone un enfoque estructurado para que las organizaciones identifiquen, protejan, detecten, respondan y recuperen información frente a incidentes de ciberseguridad. En el ámbito local, la Ley 1581 de 2012 de Colombia y sus decretos reglamentarios definen los principios y obligaciones sobre el tratamiento de datos personales, regulando la forma en que deben recolectarse, almacenarse y protegerse los datos sensibles de los ciudadanos. La ISO/IEC 27018 (2019) complementa estos marcos al orientar la protección de información personal identificable (PII) en servicios de nube pública.

Para la gobernanza y gestión de TI, el COBIT 2019 proporciona principios, prácticas y métricas que facilitan la gestión de riesgos y la alineación estratégica de TI, mientras que el PCI DSS (2022) establece los requisitos de seguridad para organizaciones que manejan información de tarjetas de pago, aplicable especialmente cuando se externalizan servicios financieros. Adicionalmente, la

ISO/IEC 22301 (2019) orienta la gestión de la continuidad del negocio, asegurando la resiliencia de los servicios tercerizados frente a incidentes críticos.

Según Kaspersky (2019), la confianza en los proveedores no debe basarse en suposiciones, sino en procesos continuos de verificación y control. Esto implica que la relación con terceros requiere mecanismos permanentes de supervisión, auditoría y evaluación del cumplimiento de políticas y estándares de seguridad, garantizando que los servicios externalizados cumplan con los niveles de protección y confiabilidad esperados.

4. Desarrollo e implementación del aprendizaje

4.1 Gestión de accesos y control de proveedores

La ciberseguridad en un modelo de outsourcing TI implica realizar un control de accesos a la información y a los sistemas de negocio necesarios. En la práctica y en el entorno simulado, se implementaron mecanismos de gestión de accesos por roles (RBAC) y autenticación multifactor (MFA), asegurando que los empleados de la empresa y los proveedores únicamente tengan permisos estrictamente necesarios para el cumplimiento de sus funciones. En los proveedores, se definieron accesos temporales y auditorías regulares de credenciales y privilegios que permiten garantizar la trazabilidad y el control de la utilización de los recursos.

Los Acuerdos de Nivel de Servicio (ANS), por su parte, incluyen simples y explícitas métricas de rendimiento, protocolos de operación y flujos de escalado de los incidentes, indicando las responsabilidades contractuales y los mecanismos de medición del cumplimiento. Permitiendo así garantizar la calidad del servicio y proteger los activos críticos asegurando la continuidad operacional.

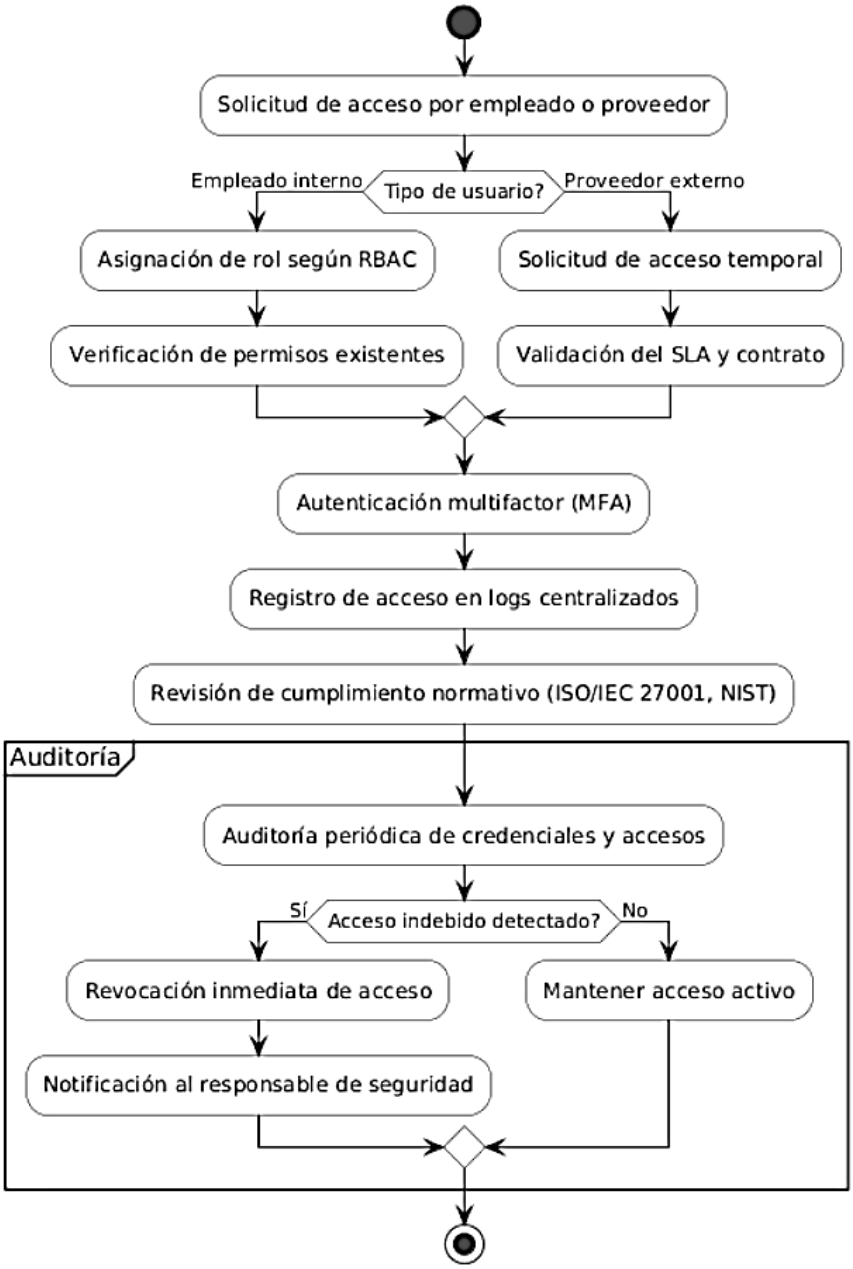

Diagrama 1. Flujo de gestión de accesos
Fuente: Elaboración propia, basado en la norma ISO/IEC 27001:2013 (International Organization for Standardization, 2013) y prácticas recomendadas de RBAC y MFA en entornos de outsourcing TI.

4.2 Gestión de incidentes

La gestión de incidentes de seguridad se ha formalizado como un proceso de trabajo que cubre la detección, la contención, el análisis y, finalmente, la recuperación ante los incidentes de seguridad. Por ejemplo, si se detecta un acceso no autorizado, el sistema es capaz de generar alertas automáticas para bloquear la cuenta vulnerable, de realizar un análisis de los logs a partir de herramientas de monitorización en continuo (SIEM), notificar la situación, en caso de que la misma lo requiera, al proveedor de terceros implicados y solicitar las medidas correctoras necesarias para restaurar la seguridad, así como para minimizar el impacto sobre los activos críticos.

Este proceso de trabajo engloba, a su vez, procedimientos operativos bien definidos, flujos de escalado y la coordinación entre equipos de trabajo internos y externos.

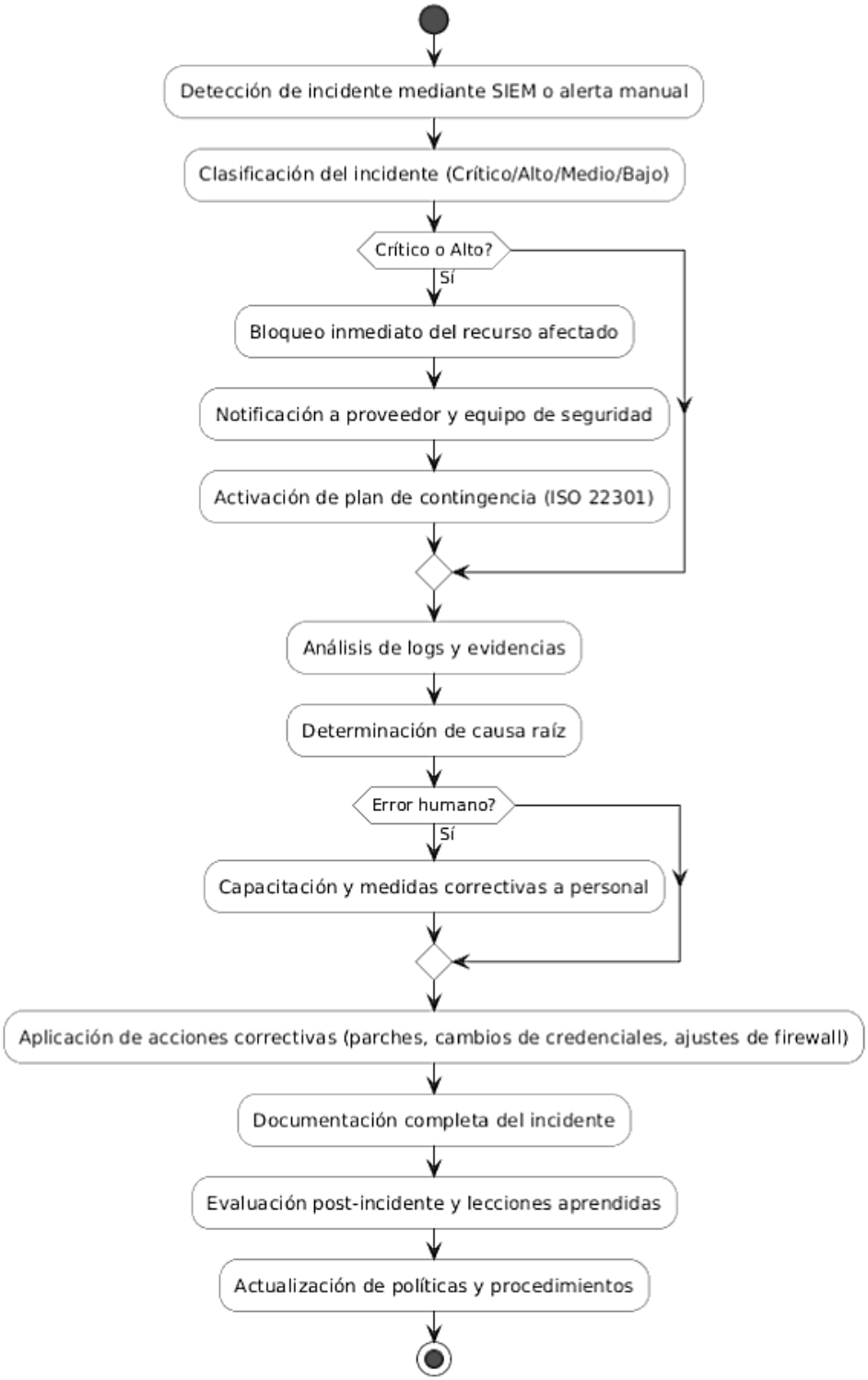

Diagrama 2. Flujo de gestión de incidentes
Fuente: Elaboración propia, basado en NIST SP 800-61 Rev.2 (National Institute of Standards and Technology, 2012) y ITIL 4.

4.3 Monitoreo continuo y KPIs de desempeño

El monitoreo de los servicios tercerizados se realiza mediante dashboards y herramientas de SIEM que permiten la detección temprana de anomalías y el seguimiento de eventos de seguridad. Para medir el desempeño, se definieron Indicadores Clave de Desempeño (KPIs) que evalúan la disponibilidad del servicio, los tiempos de respuesta ante incidentes, la revisión de accesos, el cumplimiento normativo y la capacitación del personal. Estos KPIs se incorporan en los ANS y proporcionan una herramienta objetiva para el seguimiento, control y mejora continua del servicio.

Tabla 2. KPIs de desempeño en ANS

Categoría	KPI	Objetivo	Frecuencia de revisión
Disponibilidad del servicio	% up-time mensual	≥ 99.9%	Mensual
Tiempo de respuesta ante incidentes	Tiempo promedio de resolución	≤ 2 horas	Mensual
Gestión de accesos	% de cuentas revisadas y auditadas	100% cuentas críticas	Mensual
Cumplimiento normativo	% de cumplimiento de controles internos	≥ 98%	Trimestral
Capacitación de personal	% de empleados capacitados	100% personal crítico	Semestral

Fuente: Elaboración propia

4.4 Evaluación y mitigación de riesgos

La evaluación de riesgos se ha hecho mediante el uso de matrices de probabilidad e impacto, los cuales permiten identificar qué riesgos son los más críticos de la externalización de TI, estimar la probabilidad de este y evaluar el impacto sobre los activos críticos. Los riesgos incluyen la fuga de información sensible, accesos no autorizados por parte de los proveedores, incumplimientos de SLA, vulnerabilidades en la infraestructura externa, errores humanos y dependencia excesiva del proveedor-. Cada uno de los riesgos tiene medidas de mitigación técnicas, organizacionales y humanas, que incluyen cifrar, segmentar la red, auditorías periódicas, capacitación o planes de contingencia.

La clasificación del nivel de riesgo se establece a partir del valor obtenido en la evaluación cuantitativa, de acuerdo con los siguientes rangos: valores entre 1 y 5 corresponden a un nivel de riesgo bajo; entre 6 y 10, a un nivel medio; entre 11 y 15, a un nivel alto; y entre 16 y 25, a un nivel crítico. Esta categorización permite priorizar la implementación de controles en función de la severidad del riesgo identificado.

Tabla 3. Matriz de riesgos: probabilidad e impacto

Riesgo	Probabilidad (1-5)	Impacto (1-5)	Valor	Nivel de riesgo
Fuga de información sensible	5	5	25	Crítico
Accesos no autorizados por proveedor	3	5	15	Alto
Vulnerabilidades en infraestructura externa	3	4	12	Alto
Error humano / gestión incorrecta de datos	4	4	16	Crítico
Incumplimiento de SLA	3	3	9	Medio
Dependencia excesiva del proveedor (Vendor Lock-in)	3	3	9	Medio
Ataques de phishing dirigidos	4	4	16	Crítico
Fallos en disponibilidad del servicio	3	5	15	Alto
Configuración incorrecta en la nube	3	4	12	Alto
Falta de monitoreo continuo	2	4	8	Medio

Fuente: Elaboración propia, basada en ISO/IEC 27005:2018 para gestión de riesgos.

La adopción del modelo cuantitativo 5x5, no sólo permite establecer la priorización de los riesgos del estudio, sino que también hace evidente que los riesgos con mayor valoración requieren de una atención especial y controles exhaustivos. De los resultados mostrados en la tabla anterior se concluye que los riesgos críticos se asocian fundamentalmente a factores humanos, accesos y gestión de la información, reforzando así el enfoque holístico de seguridad en la organización. En este sentido, la mitigación del riesgo debe complementarse con técnicas de monitoreo continuo, refuerzo de las políticas, procedimientos y desarrollo de una cultura organizacional que fomente la protección de la información, permitiendo así una gestión consciente del riesgo en el outsourcing TI.

4.5 Seguridad informática y equipos especializados

La seguridad se ve reforzada por la participación de equipos especializados para esta actividad: el Blue Team que participa en la defensa y monitorea la situación de la infraestructura; el Red Team que simula ataques y evalúa el estado de las vulnerabilidades existentes; y el Purple Team que consolida las enseñanzas de ambos equipos para continuar adaptando y mejorando la postura de seguridad con la que cuenta la organización. La coordinación de estos equipos permite que los incidentes sean detectados, mitigados y registrados de manera sistemática, aumentando la disponibilidad de los servicios tercerizados y garantizando planes de acción que los eviten a futuro.

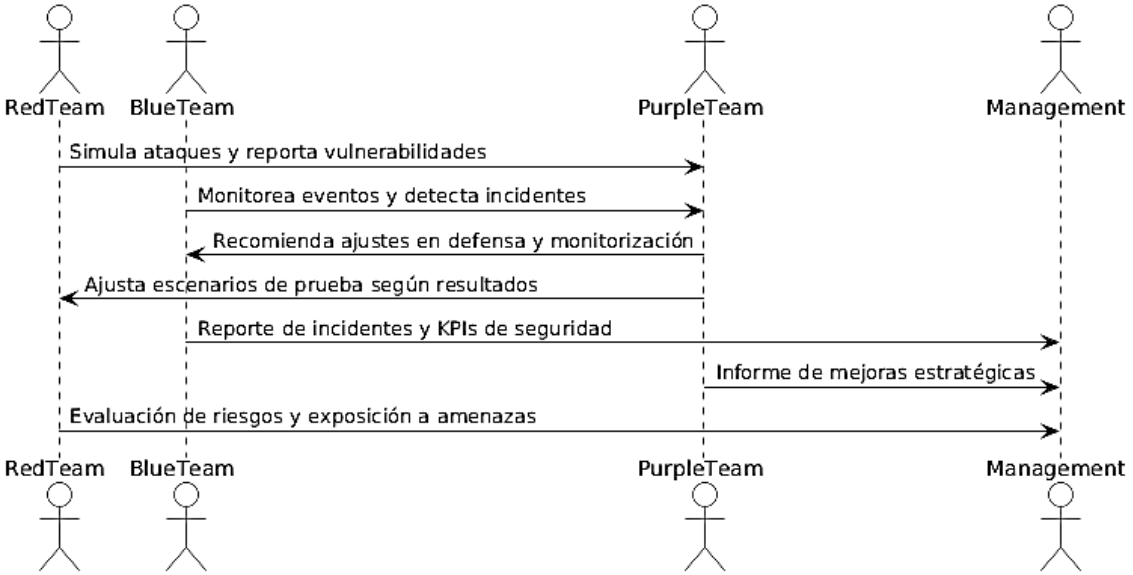

Diagrama 3. Coordinación de equipos de seguridad
Fuente: Elaboración propia, inspirado en NIST Cybersecurity Framework (National Institute of Standards and Technology, 2018) y prácticas de seguridad ofensiva y defensiva coordinada.

5. Conclusiones

El análisis realizado evidencia cómo la adopción de determinados modelos de outsourcing de las tecnologías de la información, si bien suponen una estrategia eficaz para la optimización de recursos y el acceso a capacidades específicas, presenta riesgos relevantes de ciberseguridad que es necesario gestionar de forma adicional. La externalización de procesos extiende el perímetro de la seguridad de la compañía, generando una mayor exposición a amenazas potenciales derivadas de accesos no autorizados, fuga de información, riesgos de terceros, etc.

De acuerdo con el caso simulado, la investigación pudo determinar que los riesgos más relevantes están especialmente asociados al ámbito humano de la administración de los accesos y la protección de la información, todo lo cual implica la necesidad de controles no sólo tecnológicos, sino también organizacionales y culturales. En este marco, la implementación del modelo cuantitativo 5x5 permitió la priorización de riesgos de forma objetiva que facilitó el proceso de toma de decisiones para la mitigación de riesgos a partir de los más graves.

De la misma forma, la inclusión de mecanismos como los Acuerdos de Nivel de Servicio (ANS), la definición de KPIs o bien la adopción de marcos normativos internacionales como ISO/IEC 27001, NIST Y COBIT 2019, fortalecen la gobernanza de la seguridad y permiten conseguir relaciones de confianza soportadas en la verificación continua con los proveedores. La propia implementación estructurada de procesos para la gestión de accesos, de incidentes o bien la posibilidad de realizar un monitoreo continuo demuestran la necesidad de tener una línea de actuación que demuestre un enfoque sistemático y medible en la protección de activos críticos.

Por otra parte, la implementación de equipos especializados como el Blue Team, Red Team o Purple Team con estrategias de defensa en profundidad prueban que la ciberseguridad en entornos de outsourcing debe tratarse desde una óptica proactiva, colaborativa y con un enfoque crítico en la mejora continua. En consecuencia, la seguridad de esta información no depende únicamente de la tecnología implementada, sino de la propia articulación de procesos, de personas y herramientas que valoran la resiliencia organizacional frente a un entorno de amenazas cada vez más complejo.

Referencias

- Axelos. (2019). *ITIL Foundation: ITIL 4 edition*. The Stationery Office.
- Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information systems outsourcing: A survey and analysis of the literature. *ACM SIGMIS Database*, 35(4), 6–102. https://doi.org/10.1145/1035233.1035236
- International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. ISO.
- International Organization for Standardization. (2015). *ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. ISO.
- International Organization for Standardization. (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. ISO.
- International Organization for Standardization. (2019a). *ISO/IEC 27018:2019 Information technology — Security techniques — Protection of personally identifiable information (PII) in public clouds*. ISO.
- International Organization for Standardization. (2019b). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*. ISO.
- ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- Kaspersky, E. (2019). *Cybersecurity insights report*. Kaspersky Lab.
- Lacity, M. C., & Willcocks, L. P. (2012). *Advanced outsourcing practice: Rethinking ITO, BPO and cloud services*. Palgrave Macmillan.
- National Institute of Standards and Technology. (2012). *Computer security incident handling guide (SP 800-61 Rev. 2)*. NIST.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*. NIST.
- Oshri, I., Kotlarsky, J., & Willcocks, L. (2015). *The handbook of global outsourcing and offshoring* (3rd ed.). Palgrave Macmillan.
- PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard (PCI DSS), version 4.0*. PCI SSC.
- Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Protección de datos personales*. Diario Oficial No. 48.587.