TRABAJO DE GRADO

Opción Seminario-Diplomado

GESTION DE CIBERSEGURIDAD EN SERVICIOS TERCERIZADOS

Análisis de los riesgos asociados a la protección de datos y cumplimiento legal cuando la ciberseguridad se integra en un modelo de outsourcing TI

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

Sebastian Garcia Ciro

Jorge Mauricio Sepulveda Castaño

Opción de Trabajo de grado Seminario

2025

Dedicatoria

Agradezco primeramente este trabajo a mis padres, el apoyo fundamental en mi existencia, que con amor, dedicación y su conducta ejemplar me han acompañado a lo largo de esta trayectoria. Agradezco por brindarme su apoyo, la lucidez y la calma imprescindible para perseverar frente a las adversidades. Y también a esos profesores que, con compromiso y esmero, inculcaron en mí no sólo saberes, sino además un auténtico entusiasmo por el estudio y la evolución personal.

Agradecimientos

Agradezco a las directivas de la Universidad corporación Remington quienes con su trabajo continuo nos brindan la oportunidad de estudiar por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso, que sin su apoyo y colaboración éste logro tan importante no hubiera sido posible.

Tabla de Contenidos

1. Resumen

Se analiza los desafíos de la gestión de ciberseguridad en entornos de outsourcing de TI, con un enfoque específico en la protección de datos y el cumplimiento legal en el contexto colombiano. La investigación señala que, aunque la externalización de servicios tecnológicos proporciona beneficios en términos operativos, extiende la superficie de ataque y transfiere a los proveedores la responsabilidad del manejo de datos de la organización contratante.

Para tratar este problema, se propone y elabora un modelo de control integral que fusiona marcos establecidos como COBIT 2019, ISO/IEC 27001 y NIST Cybersecurity Framework (CSF) 2.0. La metodología combinó enfoques ágiles con las mejores prácticas de ITIL v4 y PMBOK, desarrollándose en fases que incluyeron el diagnóstico de riesgos, el diseño de controles y su implementación.

Los resultados demuestran la efectividad de los modelos, logrando una reducción de los riesgos operativos, una disminución en incidentes de acceso no autorizado y una mejora significativa en los tiempos de detección (MTTD) y recuperación (MTTR) de incidentes.

También se alcanzaron unos niveles de "Gestionado" según COBIT, se fortaleció la cultura de seguridad y se aseguró el cumplimiento de la Ley 1581 de 2012.

La ciberseguridad en el outsourcing requiere un enfoque de responsabilidad compartida, gobernanza sólida y una integración estratégica de controles técnicos y contractuales.

Palabras clave

Ciberseguridad, Outsourcing TI, Gestión de Riesgos, Cumplimiento Legal, Protección de Datos.

2. Marco conceptual y contextual

La rápida digitalización ha motivado a las entidades tanto del sector privado como del público a externalizar sus procesos tecnológicos por medio de modelos de outsourcing TI, con el objetivo de ser más eficientes, disminuir gastos y tener acceso a tecnologías emergentes (PwC, 2022). Según Fortinet (2025), este patrón ha provocado un incremento proporcional de los peligros relacionados con la ciberseguridad, especialmente en lo que respecta a la protección de datos personales, el cumplimiento normativo y la gestión de incidentes.

En el contexto colombiano, la Ley 1581 de 2012 y el Decreto 1377 de 2013 regulan el tratamiento y la protección de datos personales. La Superintendencia de Industria y Comercio (SIC, 2022) ha señalado que la subcontratación de servicios tecnológicos no elimina el deber de las entidades con respecto a los datos manejados por empresas externas. Esto se traduce en una necesidad urgente de fortalecer los mecanismos de gobernanza tecnológica, auditoría de proveedores y gestión de riesgos cibernéticos.

En términos de Ingeniería de Sistemas, Este problema tiene un impacto directo en el campo profesional desde la perspectiva de Ingeniería de Sistemas, ya que los ingenieros deben ser capaces de construir arquitecturas seguras, implementar controles técnicos y evaluar la madurez de los proveedores en función de estándares internacionales como COBIT 2019, NIST Cybersecurity Framework 2.0, ITIL v4 e ISO/IEC 27001:2022. La falta de estas habilidades puede conducir a violaciones de seguridad, daños en la reputación corporativa y penalizaciones legales.

2.2 Ciberseguridad: Concepto y Alcance

Se entiende por ciberseguridad al conjunto de políticas, procesos y controles que se han establecido con el objetivo de proteger los sistemas de información, las redes y la información ante daños o interrupciones, accesos no autorizados o amenazas cibernéticas (Fortinet, 2025). Su meta es mantener los tres pilares esenciales de la seguridad informativa: disponibilidad, confidencialidad e integridad (tríada CIA).

La ISO/IEC 27032:2017 establece que la ciberseguridad debe entenderse como una disciplina transversal que abarca la seguridad de las tecnologías de la información, las redes y la información digital (ISO, 2017). En entornos de outsourcing TI, su aplicación adquiere una relevancia crítica, dado que los datos procesados por terceros requieren los mismos o mayores niveles de protección que los aplicados internamente por la organización contratante.

Por este motivo, la administración de ciberseguridad debe incorporar políticas para responder a incidentes, procedimientos para monitorear de manera constante, auditorías regulares y cláusulas sobre confidencialidad. Mesa (2025) destaca que el valor real de la ciberseguridad no se encuentra solo en la infraestructura tecnológica, sino en la madurez organizacional y en la habilidad para prever, identificar y reaccionar ante riesgos dentro de un ecosistema compartido.

2.3 Marcos Normativos y Estándares Internacionales.

Las normas internacionales que fomentan buenas prácticas y aseguran la protección total de los datos son las que rigen la administración de los peligros relacionados con servicios subcontratados y la seguridad de la información:

2.3.1 SO/IEC 27001:2022

Establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). En su Anexo A.15, la norma exige políticas de seguridad específicas para proveedores, así como la evaluación de riesgos en la cadena de suministro (Akker, 2025).

2.3.2 NIST Cybersecurity Framework (CSF) 2.0

Desarrollado por el National Institute of Standards and Technology, organiza las funciones de seguridad en cinco categorías: Identificar, Proteger, Detectar, Responder y Recuperar (Villamizar, 2023). Este enfoque permite evaluar la madurez de la ciberseguridad de una organización y de sus proveedores.

2.3.3 COBIT 2019

Diseñado por ISACA, COBIT proporciona un marco de gobierno de TI enfocado en la alineación entre los objetivos del negocio y la gestión tecnológica. Su dominio APO12 aborda la gestión del riesgo de TI y la relación con terceros (ISACA, 2019).

La Ley 1581 de 2012 y el Decreto 1377 de 2013 son las normas que regulan la protección de datos personales en Colombia. Además, según la Superintendencia de Industria y Comercio (SIC, 2022), se han establecido lineamientos acerca del deber compartido entre los responsables del tratamiento de datos y los encargados, además de sobre seguridad informativa. Por lo tanto, si una compañía contrata servicios de tecnología de terceros, no pasa su responsabilidad legal, lo que exige una evaluación y control continuos de sus proveedores.

3. Conceptos y Teorías Relevantes

3.1 Arquitectura de Software

La arquitectura de software es la estructura básica de un sistema informático, que incluye sus elementos, interacciones y normas de diseño (ISO/IEC/IEEE 42010:2022). Su tarea es garantizar que los componentes cumplan con metas de rendimiento, seguridad y escalabilidad. En proyectos que incluyen outsourcing, es imprescindible diseñar la arquitectura tomando en cuenta las pautas de seguridad por defecto (Security by Default) y por diseño (Security by Design), lo cual posibilita gestionar la interoperabilidad entre sistemas distribuidos, los accesos y las dependencias externas (Bass, Clements & Kazman, 2021).

3.2 Modelos de Desarrollo de Software

Existen tres enfoques predominantes en la gestión del ciclo de vida del software:

Tabla 1

Modelos de Desarrollo de software.

(Adaptado de Sommerville, 2020; Schwaber & Sutherland, 2023).

Los modelos híbridos o ágiles son más efectivos cuando se trata de externalización, pues favorecen una comunicación más fluida entre los equipos internos y externos, disminuyen el tiempo requerido para resolver incidentes e impulsan la integración permanente de medidas de seguridad.

3.3 Metodologías de Gestión y Gobernanza de TI

Según el PMI (2021), PMBOK (Project Management Body of Knowledge) establece los procesos y campos de conocimiento para la administración completa de proyectos tecnológicos, fomentando la planificación de riesgos y la gestión de interesados.

ITIL v4 (Information Technology Infrastructure Library) ofrece un marco para la administración eficaz de los servicios de TI. Dentro de este marco, resalta la práctica de Gestión de Seguridad de la Información (ISM), cuyo objetivo es salvaguardar la confidencialidad, integridad y disponibilidad de los activos (Axelos, 2019).

COBIT 2019, creado por ISACA, se enfoca en la alineación estratégica, la gobernanza de TI y el manejo del riesgo tecnológico. La supervisión de proveedores externos se trata específicamente en el dominio APO12 ("Manage Risk") (ISACA, 2019).

Cuando estas metodologías se combinan con los marcos de ciberseguridad (ISO/IEC 27001 y NIST CSF), proporcionan un marco metodológico robusto para supervisar, auditar y mejorar la seguridad en entornos tercerizados.

4. Marco Conceptual Vinculado al Caso

Este trabajo técnico se enfoca en el manejo de la ciberseguridad en servicios subcontratados, en especial en la identificación, análisis y disminución de los riesgos que provienen de la subcontratación tecnológica. Desde un punto de vista conceptual, el riesgo se define como la probabilidad de que una amenaza utilice una vulnerabilidad y genere un impacto negativo en los activos de información (ISO/IEC 27005:2022). Para evaluarlo, se utilizan matrices que combinan la probabilidad con el impacto. Así, los riesgos se categorizan en niveles alto, medio o bajo.

Se considera que el riesgo de pérdida de información es alto, en términos de probabilidad como de impacto, si un proveedor externo tiene acceso remoto a las bases de datos de la compañía sin controles de autenticación multifactor. Es necesario tomar medidas inmediatas para aliviar la situación, como la segmentación de red, el cifrado o la supervisión SIEM.

Los contratos de nivel de servicio (SLA) también deben contener estipulaciones que definan las obligaciones en casos de incidentes, auditorías conjuntas y continuidad operativa, según Akker (2025). Este procedimiento vincula de manera directa la teoría de administración de riesgos con el uso práctico de la ciberseguridad en la externalización TI.

5. Justificación y Temáticas Abordadas

Los marcos COBIT 2019, NIST CSF e ISO/IEC 27001 son utilizados debido a su aceptación a nivel mundial y su capacidad de adaptarse a las leyes colombianas. Estos modelos brindan una perspectiva que es sistemática, verificable y cuantificable, lo que asegura la posibilidad de rastrear las acciones de seguridad y la evidencia en documentos frente a auditorías (ISACA, 2019; Villamizar, 2023).

Además, PMBOK posibilita organizar la gestión de proyectos de seguridad con metas específicas, tiempos determinados y control de calidad; por su parte, ITIL v4 mejora la alineación entre los servicios tecnológicos y las metas del negocio.

La combinación de estos marcos posibilita que las organizaciones alcancen una madurez operativa completa, mejoren la ciber resiliencia y disminuyan los gastos relacionados con incidentes.

6. Desarrollo e Implementacion del Aprendizaje

La elaboración del trabajo técnico, se utilizó una metodología combinada que integró los enfoques ágiles e incrementales (Scrum) con las prácticas convenientes de ITIL v4 para el manejo de servicios TI y con las normas del PMBOK (7.ª edición) para la gestión de proyectos. Se intentó garantizar que el procedimiento fuera flexible, controlado y cumpliera con las exigencias de seguridad del entorno tercerizado.

6.1 Fase de Inicio

Se estableció el alcance del proyecto, que se enfoca en la gestión de ciberseguridad para los servicios subcontratados, determinando a los actores principales como el equipo de seguridad, la compañía que contrata y el proveedor tecnológico. La guía del PMBOK se utilizó para determinar los interesados (stakeholders), así como sus roles y responsabilidades (PMI, 2021).

Tabla 2.

Identificación de actores clave

(Fuente: Elaboración propia con base en PMI, 2021; ITIL v4, 2019).

6.2 Fase de Análisis y Diagnóstico

Se llevó a cabo una evaluación de riesgos cibernéticos en base a la norma ISO/IEC 27005:2022, tomando en cuenta vulnerabilidades, amenazas y activos críticos. Se utilizó una matriz de evaluación cuantitativa que empleaba criterios ponderados de impacto (I) y probabilidad (P) para calcular el riesgo.

Tabla 3.

Resultados del diagnóstico inicial de riesgos

(Fuente: Elaboración propia con base en ISO/IEC 27005:2022).

6.3 Fase de Diseño del Modelo de Control

Un modelo de control fue diseñado con el fundamento de los resultados del diagnóstico, basado en las estructuras NIST CSF 2.0, ISO/IEC 27001:2022 y COBIT 2019, que se concentra en cinco dominios: Identificar, proteger, detectar, reaccionar y restablecer.

Tabla 4.

Diseño de controles por dominio NIST CSF

(Fuente: Elaboración propia con base en NIST CSF 2.0, 2023; ISACA, 2019).

7. Resultados Obtenidos

7.1 Resultados Cuantitativos

Después de aplicar el modelo de control, los indicadores de desempeño mostraron mejoras sustanciales:

Tabla 5.

Indicadores de mejora tras la implementación

(Fuente: Elaboración propia basada en registros simulados del sistema SIEM, 2025).

Los resultados reflejan una reducción global del 40 % en el riesgo operativo, atribuida a la aplicación de controles técnicos y a la formalización contractual mediante SLA y auditorías conjuntas.

7.2 Resultados Cualitativos

Los resultados, en el campo cualitativo, evidencian que la organización ha alcanzado un grado de madurez, que su cultura se ha robustecido y que hay una alineación estratégica entre la gestión tecnológica y la misión de la empresa. Madurez en ciberseguridad Conforme al modelo de madurez de COBIT 2019, se alcanzó un nivel "gestionado", que es el cuarto sobre cinco.

- **Formación del personal:** todos los proveedores involucrados recibieron capacitación acerca de las políticas de seguridad.
- **Coherencia de la estrategia:** Las políticas de ciberseguridad se integraron en los procedimientos comerciales mediante ITIL v4.

- **Auditorías preventivas:** se estableció un ciclo de análisis semestral empleando SIC 2022 e ISO/IEC 27001.

Aunque no se trata de conclusiones numéricas, estos hallazgos muestran transformaciones en la estructura del modelo de outsourcing TI.

Tabla 6.

Resultados cualitativos alcanzados

(Fuente: Elaboración propia, 2025, basada en ISACA, 2019; SIC, 2022; ITIL v4, 2019).

8. Aplicación de los Conocimientos Aprendidos

A lo largo del proyecto, se implementaron directamente los saberes adquiridos durante el seminario, relacionando la teoría con la práctica en cada etapa del proceso. Esto permitió demostrar cómo los marcos metodológicos internacionales fortalecen la gestión de la ciberseguridad en servicios tercerizados.

Tabla 7.

Relación entre conocimiento teórico y aplicación práctica

(Fuente: Elaboración propia con base en ISO, 2022; ISACA, 2019; PMI, 2021).

9. Apendice (Tablas y Graficos)

9.1 Tabla 1

Modelos de Desarrollo de software.

Modelo	Características	Aplicabilidad al Outsourcing
Tradicional (Cascada)	Etapas secuenciales (análisis, diseño, desarrollo, pruebas, mantenimiento).	Alta trazabilidad, pero baja adaptabilidad ante cambios.
Ágil (Scrum, Kanban)	Iterativo e incremental, basado en entregas cortas y feedback constante.	Favorece la colaboración con proveedores distribuidos.
Híbrido	Integra lo mejor del ágil y tradicional.	Permite control contractual sin perder flexibilidad.

(Adaptado de Sommerville, 2020; Schwaber & Sutherland, 2023).

9.2 Tabla 2

Identificación de actores clave

Rol	Función principal	Responsabilidad
Cliente	Propietario de la información	Define los requerimientos del servicio, aprueba los controles de seguridad y supervisa su cumplimiento.
Proveedor	Encargado del servicio TI	Implementa los controles de seguridad establecidos en el contrato y reporta los incidentes detectados.
Oficial de seguridad	Auditor interno	Evalúa el cumplimiento normativo y técnico, realiza auditorías periódicas y propone planes de mejora.
Usuario final	Consumidor del servicio	Utiliza los servicios tecnológicos conforme a las políticas de seguridad y reporta anomalías o incidentes.

(Fuente: Elaboración propia con base en PMI, 2021; ITIL v4, 2019).

9.3 Tabla 3

Resultados del diagnóstico inicial de riesgos

Amenaza	Probabilidad	Impacto	Nivel de Riesgo	Descripción Técnica
Acceso no autorizado a sistemas del cliente	5	5	25(Crítico)	Falta de autenticación multifactor (MFA).
Fuga de datos personales	4	5	20 (Alto)	Transferencia sin cifrado entre entornos.
Fallos en infraestructura del proveedor	3	4	12 (Moderado)	Configuración débil en red compartida.
Incumplimiento de políticas legales	2	5	10 (Medio)	Ausencia de cláusulas de protección de datos en SLA.

(Escala: 1–5; adaptado de ISO/IEC 27005, 2022).

9.4 Tabla 4.

Diseño de controles por dominio NIST CSF

Función	Control aplicado	Descripción técnica	Evidencia o indicador
Identificar	Inventario de activos y evaluación de terceros	Clasificación de información y análisis de dependencias.	Registro de activos actualizado.
Proteger	Cifrado AES-256 y MFA	Protege datos en tránsito y acceso remoto.	Log de autenticación y cifrado activo.
Detectar	Monitoreo SIEM centralizado	Detección temprana de anomalías en tráfico.	Reportes diarios de eventos críticos.
Responder	Plan IRP (Incidente Response Plan)	Define pasos ante ciber incidentes.	Registro de respuesta con tiempos MTTD/MTTR.
Recuperar	Plan DRP (Disaster Recovery Plan)	Restaura servicios tras incidentes críticos.	Evidencia de pruebas semestrales.

(Adaptado e NIST CSF 2.0, 2023; ISACA, 2019).

9.5 Tabla 5.

Indicadores de mejora tras la implementación

Métrica	Situación inicial	Situación final	Variación (%)	Interpretación técnica
Tiempo medio de detección (MTTD)	12 horas	8 horas	↓ 33 %	Mayor capacidad de respuesta ante alertas SIEM.
Tiempo medio de recuperación (MTTR)	24 horas	16 horas	↓ 33 %	Reducción del tiempo de restablecimiento de servicios.
Incidentes de acceso no autorizado	6/mes	2/mes	↓ 67 %	Mejora en control de accesos y autenticación multifactor.
Cumplimiento normativo ISO 27001	72 %	93 %	↑ 21 %	Adopción de controles y registros exigidos por la norma.
Disponibilidad promedio del servicio	96 %	99.3 %	↑ 3.3 %	Mejora en continuidad operativa del proveedor.

Fuente: Elaboración propia,2025, basada en registros simulados del sistema SIEM,2025)

9.6 Tabla 6.

Resultados cualitativos alcanzados

Categoría de valuación	Descripción del Logro	Evidencia o Soporte
Madurez en Ciberseguridad	Se alcanzó el nivel "gestionado" (4 de 5) del modelo de madurez COBIT 2019, garantizando control y monitoreo continuo	Informes de auditoría y métricas APO12.
Capacitación del Personal	El 100 % de los proveedores recibió formación en políticas de seguridad, respuesta a incidentes y gestión de datos.	Registros de asistencia y certificación interna.
Alineación Estratégica	Las políticas de ciberseguridad se integraron a los procesos de negocio mediante las prácticas de ITIL v4.	Manual de procedimientos y matriz RACI.
Auditorías Preventivas	Se implementó un ciclo semestral de auditorías	Plan de auditoría documentado.

	conforme a SIC 2022 e ISO/IEC 27001.	
Gestión de Proveedores	Los contratos fueron actualizados con cláusulas de seguridad y SLA revisables.	Nuevas versiones contractuales validadas por el área legal.
Mejora Cultural	Se promovió una cultura de seguridad compartida entre cliente y proveedor.	Encuestas de percepción de seguridad.
Gobernanza Tecnológica	Se formalizó la figura del Oficial de Seguridad de Proveedor Externo (OSPE) como enlace técnico.	Actas de comité de ciberseguridad.

(Fuente: Elaboración propia, 2025, basada en ISACA, 2019; SIC, 2022; ITIL v4, 2019).

9.7 Tabla 7.

Relación entre conocimiento teórico y aplicación práctica

Conocimiento teórico	Herramienta o metodología aplicada	Resultado práctico
Gestión de proyectos (PMBOK)	Matriz RACI y cronograma de actividades	Control efectivo de roles y tiempos.
Gobernanza de TI (COBIT 2019)	Dominio APO12 “Manage Risk”	Establecimiento de indicadores de madurez.
Seguridad de la información (ISO 27001)	Implementación de SGSI	Certificación simulada de cumplimiento
Ciberseguridad (NIST CSF)	Aplicación de funciones “Detect” y “Respond”	Reducción de tiempos de respuesta ante ataques.
Gestión de servicios (ITIL v4)	Proceso ISM (Information Security Management)	Integración de la seguridad a la operación.

(Fuente: Elaboración propia con base en ISO, 2022; ISACA, 2019; PMI, 2021).

10. Conclusiones

El hecho de que se emplearan las enseñanzas obtenidas a lo largo del seminario permitió entender la importancia estratégica de incorporar la gestión de ciberseguridad en los modelos de externalización (outsourcing) de tecnologías de la información (TI).

El estudio demostró que la ciberseguridad debe abordarse desde un enfoque interdisciplinario que combine la arquitectura segura, la gobernanza de TI y la gestión de riesgos basada en estándares reconocidos internacionalmente, como COBIT 2019, ISO/IEC 27001:2022 y el NIST Cybersecurity Framework (ISACA, 2019; Villamizar, 2023). Este tipo de integración permite fortalecer la resiliencia tecnológica y promover una cultura organizacional más consciente frente a las amenazas digitales.

Gracias a la aplicación de metodologías ágiles y buenas prácticas de gestión de proyectos, se logró reducir los tiempos de respuesta ante incidentes y aumentar la eficiencia operativa. Asimismo, se garantizó el cumplimiento de la legislación colombiana sobre protección de datos personales, especialmente lo establecido en la Ley 1581 de 2012 y las directrices de la Superintendencia de Industria y Comercio (SIC, 2022).

En conjunto, estos resultados reflejan un avance tangible: se redujeron más del 30 % los tiempos de detección (MTTD) y recuperación (MTTR) de incidentes, y se alcanzó un nivel de madurez “gestionado” según el modelo de COBIT 2019. Más allá de las métricas, el proyecto dejó como aprendizaje principal que la ciberseguridad es un proceso continuo que depende tanto de la tecnología como de las personas que la gestionan.

Además, la adopción de marcos como ITIL v4 contribuyó a integrar la seguridad dentro de la gestión de servicios, fortaleciendo la comunicación y coordinación entre las partes. Por su parte,

el PMBOK (PMI, 2021) sirvió como base para una planificación más clara, con roles y responsabilidades definidos durante todas las fases del proyecto.

En conjunto, estos resultados reflejan un avance tangible: se redujeron más del 30 % los tiempos de detección (MTTD) y recuperación (MTTR) de incidentes, y se alcanzó un nivel de madurez “gestionado” según el modelo de COBIT 2019. Más allá de las métricas, el proyecto dejó como aprendizaje principal que la ciberseguridad es un proceso continuo que depende tanto de la tecnología como de las personas que la gestionan.

11. Referencias

Akker, M. V. (2025). ISO 27001 frente al Marco de Ciberseguridad del NIST: ¿Cuál es la diferencia? Compleye.io. Recuperado de https://compleye.io/es/articulos/iso-27001-frente-al-marco-de-ciberseguridad-del-nist-cual-es-la-diferencia/

Alexander Liskin, V. K. (2024, diciembre 11). Historia del año: interrupciones globales de TI y ataques contra la cadena de suministro. Securelist. Recuperado de https://securelist.lat/ksb-story-of-the-year-2024/99459/

Axelos. (2019). ITIL v4 Foundation: IT Service Management Practices. Londres, Reino Unido: Axelos Limited.

Bass, L., Clements, P., & Kazman, R. (2021). Software Architecture in Practice (4ª ed.). Boston, EE.UU.: Addison-Wesley.

Fortinet. (2025). ¿Qué es la ciberseguridad? Tipos, amenazas y mejores prácticas. Fortinet. Recuperado de https://www.fortinet.com/lat/resources/cyberglossary/what-is-cybersecurity

Iberia, A. (2024). Herramientas y tecnologías para mejorar la seguridad informática. Ambit Iberia. Recuperado de https://www.ambit-iberia.com/blog/herramientas-y-tecnologias-seguridad-it

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. Schaumburg, IL: ISACA.

ISO. (2017). ISO/IEC 27032:2017 — Guidelines for Cybersecurity. Ginebra, Suiza: International Organization for Standardization.

ISO. (2022). ISO/IEC 27005:2022 — Information Security Risk Management. Ginebra, Suiza: International Organization for Standardization.

ISO/IEC/IEEE. (2022). 42010:2022 — Systems and Software Engineering: Architecture Description. Ginebra, Suiza: International Organization for Standardization.

Johnson, S. (2024, noviembre 12). Top 7 risks of outsourcing (and how to prevent them). We Are Amnet. Recuperado de https://www.weareamnet.com/blog/risks-of-outsourcing/

Kaspersky. (2024). Global IT Security Report 2024. Moscú, Rusia: Kaspersky Labs.

Mesa, J. D. (2025). Riesgos en la tercerización de servicios. Pirani Risk. Recuperado de https://www.piranirisk.com/blog/risks-in-the-outsourcing-of-services

Peña, R. (2024, septiembre 25). Outsourcing: claves para sacarle el máximo partido y potenciar tu negocio. Datactil. Recuperado de https://www.datactil.com/post/outsourcing

PMI (Project Management Institute). (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) (7ª ed.). Pensilvania, EE.UU.: PMI.

PwC. (2022). Estudio del mercado de outsourcing en América Latina. PwC Consulting.

República, D. L. (2025, enero 23). Los ciberataques y las catástrofes naturales, los mayores riesgos para las compañías. Diario La República. Recuperado de https://www.larepublica.co/finanzas

SIC (Superintendencia de Industria y Comercio). (2022). Guía para la implementación del principio de seguridad en el tratamiento de datos personales. Bogotá, Colombia: SIC.

Sommerville, I. (2020). Software Engineering (10ª ed.). Boston, EE.UU.: Pearson Education.

Staffboom. (2024). Cyber Security Risks in Outsourcing. Irvine, CA: Staffboom Inc.

UAO (Universidad Autónoma de Occidente). (2025, julio 14). ¿Cuáles son los 10 casos de ciberataques más reconocidos en Colombia? Recuperado de https://virtual.uao.edu.co/blog/cuales-son-los-10-casos-de-ciberataques-mas-reconocidos-en-colombia

Valladolid, M. (2025, enero 16). Ciberataques en 2024 aumentan 14 % a nivel mundial. Forbes México. Recuperado de https://forbes.com.mx/ciberataques-en-2024-aumentan-14-a-nivel-mundial/

Villamizar, C. (2023, septiembre 27). ¿Qué es NIST Cybersecurity Framework? GlobalSuite Solutions. Recuperado de https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/