**TRABAJO DE GRADO**

**Opción Seminario-Diplomado.**

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


Corporación Universitaria Remington.

Nombre de la facultad: Facultad de Ingenierías

Nombre del programa académico: Especialización en seguridad de la información
Ingeniería de sistemas

Presentado por:

Erika Andrea Navia

Eblys Giron Rivas

Luis David Medina Sandoval.

Docente: Jorge Mario Sepulveda.



Opción de Trabajo de grado Seminario-Diplomado.

2025.

# Tabla de Contenido

## RESUMEN

La externalización de servicios de Tecnologías de la Información (Outsourcing TI) se ha consolidado como una estrategia clave para organizaciones que buscan optimizar recursos, reducir costos y acceder a capacidades tecnológicas especializadas. No obstante, esta práctica introduce riesgos significativos en materia de ciberseguridad, como la pérdida de control sobre activos críticos, vulnerabilidades en la cadena de suministro y posibles incumplimientos normativos.

Este informe técnico analiza los retos actuales de la ciberseguridad en entornos de outsourcing, revisa las principales amenazas operativas y cibernéticas, y propone estrategias de mitigación basadas en marcos reconocidos como el NIST Cybersecurity Framework y la ISO/IEC 27001 y COBIT 2019. Además, presenta herramientas tecnológicas clave y buenas prácticas para proteger datos y servicios tercerizados, con énfasis en el contexto de amenazas actuales en Colombia y casos recientes de impacto global.

La investigación concluye que una gestión proactiva de riesgos, acompañada de una evaluación exhaustiva de proveedores y el uso de tecnologías de protección avanzada son esenciales para garantizar la seguridad, la continuidad operativa y el cumplimiento normativo en entornos de outsourcing TI.

**Palabras clave**

(Outsourcing TI, Gestión de Riesgos, Ciberseguridad, NIST, ISO/IEC 27001, Infraestructura tecnológica)

# MARCO CONCEPTUAL Y CONTEXTUAL

## 1. Marco conceptual

### 1.1. Definición y Alcance del Outsourcing de Servicios TI

La tercerización u outsourcing de servicios TI consiste en delegar procesos, operaciones o funciones tecnológicas específicas a proveedores externos especializados. Su finalidad es optimizar recursos, reducir costos operativos y acceder a capacidades técnicas avanzadas. Esta práctica puede incluir desde la gestión de infraestructura y centros de datos, hasta el desarrollo de software, soporte técnico y servicios de ciberseguridad (Peña, 2024).

Por su naturaleza, el outsourcing implica ceder parte del control sobre activos de información críticos para la organización. Esto genera una relación de interdependencia entre cliente y proveedor, donde la seguridad de la información depende de ambas partes. Esta dinámica abre la puerta a nuevos vectores de ataque y obliga a establecer y evaluar políticas de seguridad robustas (Johnson, 2024).

### 1.2. Ciberseguridad: concepto y aplicación general

La ciberseguridad es el conjunto de políticas, procedimientos, controles y herramientas tecnológicas diseñadas para proteger sistemas, redes y datos contra ciberataques o accesos no autorizados (Fortinet, 2025). La norma ISO/IEC 27032 (2017) la define como un enfoque integral orientado a garantizar la confidencialidad, integridad y disponibilidad de los activos digitales en entornos interconectados y distribuidos.

En el caso del outsourcing, la ciberseguridad cobra aún más importancia porque aumenta la superficie expuesta a riesgos. Muchas veces, los datos y procesos críticos dejan de estar bajo control directo de la organización, lo que obliga a replantear las estrategias de protección, establecer políticas conjuntas y trabajar de forma coordinada con todos los proveedores involucrados.

### 1.3. Marcos Normativos y Regulatorios

La gestión de riesgos en entornos de outsourcing se apoya en marcos normativos internacionales que definen requisitos específicos de seguridad de la información y control de terceros. Entre los más relevantes destacan:

- **ISO/IEC 27001:2022:** proporciona un enfoque sistemático para el establecimiento de Sistemas de Gestión de Seguridad de la Información (SGSI), incluyendo controles específicos para la gestión de relaciones con proveedores y la seguridad en acuerdos de outsourcing (Akker, 2025). La norma establece controles detallados en su Anexo A.15 para abordar la seguridad en las relaciones con proveedores, incluyendo políticas específicas de seguridad, direccionamiento de la seguridad en acuerdos contractuales y gestión de la cadena de suministro de TIC (Administrator, 2025).
- **NIST Cybersecurity Framework 2.0:** Ofrece un marco flexible basado en riesgos, estructurado en cinco funciones clave: identificar, proteger, detectar, responder y recuperar. Incluye guías específicas para la gestión de riesgos de terceros, como la publicación NIST SP 800-161, que establece metodologías para evaluar y mitigar riesgos en cadenas de suministro (Villamizar, ¿Qué es NIST Cibersecurity Framework? GlobalSuite Solutions., 2023). (barrera, 2021).

- **COBIT 2019**: Centrado en el gobierno y la gestión de las tecnologías de la información, COBIT 2019 ofrece principios, objetivos y componentes diseñados para alinear la estrategia tecnológica con los objetivos de negocio. Su enfoque incluye prácticas para la gestión de riesgos, el control de proveedores y la optimización de procesos de TI en entornos de outsourcing. Además, facilita la integración con otros marcos como ISO/IEC 27001 y NIST CSF, fortaleciendo así la gobernanza y la seguridad de la información (ISACA, 2019).

## 2. Marco contextual

Una vez definidos los conceptos y marcos normativos, es fundamental analizar el contexto en el que se desarrollan las amenazas y riesgos asociados al outsourcing TI, tanto a nivel global como en Colombia.

### 2.1. Evolución del Panorama de Amenazas

En los últimos años, las amenazas contra las cadenas de suministro tecnológicas se han sofisticado notablemente. Solo en 2024 se registraron más de 467.000 ciberataques diarios en todo el mundo, lo que representa un aumento del 14% respecto al año anterior (Valladolid, 2025). Además, el número de organizaciones afectadas por ataques a la cadena de suministro creció en casi 50.000 casos (Group, 2024).

Los ciberdelincuentes suelen dirigirse a proveedores con medidas de seguridad más débiles como punto de entrada a múltiples empresas clientes, una táctica conocida como “ataque en cascada” (Law, 2024). Ejemplos claros de este patrón fueron los incidentes de SolarWinds, Kaseya y, más recientemente, el caso de CrowdStrike, que afectó a 8,5 millones de sistemas en todo el mundo (Alexander Liskin, 2024).

## 2.2. Panorama en Colombia

El outsourcing de TI sigue creciendo en Colombia y, con él, también aumentan los riesgos cibernéticos que enfrentan las empresas. El país ya es el tercer mercado de TI más grande de Latinoamérica y, según estudios recientes, el 86% de las compañías colombianas ven en el conocimiento especializado una razón clave para tercerizar procesos tecnológicos (PwC, 2022).

Sin embargo, este crecimiento ocurre en un escenario donde la ciberdelincuencia no deja de aumentar. El 45% de las organizaciones que externalizan servicios incluyen a sus proveedores en los planes de respuesta a incidentes, lo que muestra un avance en la gestión conjunta de riesgos. Aun así, sigue existiendo un amplio margen de mejora, sobre todo en la implementación de medidas preventivas y de control (accenture, 2023).

Colombia ya ha sido escenario de ciberataques de alto perfil que, aunque no siempre vinculados directamente al outsourcing, reflejan la sofisticación de las amenazas. Entre los casos más notorios están el ataque de ransomware a Empresas Públicas de Medellín (EPM) en 2022, que afectó la continuidad de servicios esenciales, y también se encuentran los incidentes contra instituciones de salud (Salud Total y Clínica Keralty), donde se filtraron datos sensibles de varios pacientes (UAO, 2025). Estos casos subrayan las vulnerabilidades de infraestructuras críticas y la necesidad de fortalecer las medidas de ciberseguridad en toda la cadena de valor, incluyendo a los proveedores de servicios tecnológicos.

## DESARROLLO E IMPLEMENTACIÓN DEL APRENDIZAJE

En esta sección se revisan los principales riesgos que implica externalizar servicios de Tecnologías de la Información (TI), abarcando tanto aspectos operativos y estratégicos como las amenazas de ciberseguridad más relevantes. También se presentan estrategias de mitigación basadas en frameworks reconocidos y se recomiendan herramientas y buenas prácticas para reforzar la protección de datos y servicios tercerizados. Finalmente, se muestra cómo aplicar estos conceptos en un escenario simulado, para ilustrar su uso en la práctica.

### 1. Principales amenazas en la externalización de servicios TI.

La externalización de servicios TI aporta beneficios como reducción de costos, acceso a expertos y flexibilidad operativa, pero introduce riesgos significativos que pueden clasificarse en operativos y estratégicos, y de ciberseguridad los cuales veremos a continuación.

### 1.1. Riesgos operativos y estratégicos del outsourcing en TI

En la tercerización de servicios de TI, los riesgos abarcan aspectos operativos y estratégicos que pueden afectar la eficiencia, la calidad del servicio e incluso el cumplimiento de los objetivos del negocio. La siguiente tabla presenta un resumen de los riesgos más comunes en este tipo de contratos:

*Tabla 1. Riesgos operativos outsourcing TI. Fuente: Adaptado de (Mesa, 2025).*

| Riesgo | Descripción | Ejemplo de impacto |
|---|---|---|
| Pérdida de control sobre el servicio | Delegar funciones críticas a un tercero puede disminuir la supervisión directa sobre calidad, tiempos y eficiencia. | Un proveedor incumple los niveles de servicio pactados, afectando la disponibilidad de una plataforma de atención al cliente. |
| Riesgo de concentración | Dependencia de un único proveedor para múltiples servicios, incrementando vulnerabilidad ante sus fallos. | El colapso operativo del proveedor interrumpe varias áreas de la empresa. |
| Costos ocultos o imprevistos | Gastos no contemplados en el contrato, como penalizaciones o tarifas adicionales por cambios. | Cobros extra por ampliación de almacenamiento en la nube. |
| Baja calidad del servicio | Falta de personal capacitado o alineación con los objetivos del cliente. | Entregas tardías de actualizaciones críticas de software. |
| Conflictos y dependencia del proveedor | Dificultades para renegociar o cambiar de proveedor por barreras contractuales. | La empresa debe aceptar incrementos de tarifas para evitar interrupciones de servicio. |
| Pérdida de conocimiento interno | Descapitalización del know-how interno al delegar | El equipo interno deja de conocer la arquitectura del |

| Riesgo | Descripción | Ejemplo de impacto |
|---|---|---|
| | funciones claves por periodos prolongados. | sistema tras años de outsourcing. |
| Riesgo de incumplimiento normativo | Posibles sanciones si el proveedor no respeta regulaciones de protección de datos o ciberseguridad. | Multa por incumplir la Ley 1581 de protección de datos en Colombia. |
| No cumplimiento de objetivos de negocio | El servicio tercerizado no aporta valor ni mejora en los indicadores esperados. | Reducción de la satisfacción del cliente a pesar de externalizar el soporte técnico. |

## 1.2. Amenazas de ciberseguridad en outsourcing TI

Además de estos riesgos operativos y estratégicos, la tercerización de TI implica desafíos significativos en materia de ciberseguridad. La falta de controles efectivos, el incumplimiento de normativas o la exposición a ciberataques pueden desencadenar consecuencias operativas, financieras y legales de gran magnitud. A continuación, se describen las amenazas más relevantes:

*Tabla 2. Amenazas de ciberseguridad en Outsourcing. Fuente Adaptado de (staffboom, 2024).*

| Amenaza cibernética | Descripción | Ejemplo en outsourcing |
|---|---|---|
| Brechas de datos (Data breaches) | Acceso no autorizado, robo o divulgación de información sensible debido a controles de seguridad inadecuados en el proveedor. | Filtración de bases de datos de clientes por vulnerabilidades en la infraestructura del proveedor. |

| Amenaza cibernética | Descripción | Ejemplo en outsourcing |
|---|---|---|
| Ataques de ransomware | Infecciones que cifran la información del proveedor y exigen un pago para su recuperación, afectando la continuidad del negocio. | Bloqueo de sistemas de un proveedor de soporte técnico que paraliza el servicio al cliente. |
| Problemas de cumplimiento normativo | Incumplimiento de leyes o estándares en materia de protección de datos, privacidad o ciberseguridad aplicables en la jurisdicción del cliente. | Sanción por incumplimiento de la Ley 1581 de 2012 de protección de datos en Colombia debido a malas prácticas del proveedor. |
| Problemas de calidad y rendimiento | Deficiencias en el cumplimiento de acuerdos de nivel de servicio (SLA) que afectan la seguridad y disponibilidad de los sistemas. | Retrasos en la aplicación de parches de seguridad que dejan expuestos sistemas críticos. |

En Colombia, estas amenazas cobran aún más importancia. De acuerdo con el Barómetro de Riesgos Allianz 2025, los incidentes cibernéticos como la ciberdelincuencia y la filtración de datos, se han convertido en el principal riesgo para las empresas del país, subiendo del cuarto lugar en 2024 al primero en 2025 con un aumento del 30 % al 34 % en ponderación, lo que evidencia una mayor vulnerabilidad frente a brechas de información y ataques de ransomware. En el caso del outsourcing, este riesgo se acentúa debido a la

estrecha dependencia tecnológica que las organizaciones mantienen con sus proveedores externos (República, 2025).


*Figura 1. Top 10 de riesgos en Colombia. Fuente: tomada de (República, 2025).*

## 2. Estrategias efectivas de mitigación y frameworks de gestión de riesgos

Tras identificar los riesgos operativos, estratégicos y cibernéticos propios del outsourcing de TI, el siguiente paso es definir cómo reducirlos. No se trata solo de reaccionar ante incidentes, sino de anticiparse y fortalecer las defensas antes de que las amenazas se materialicen. Para ello, es clave apoyarse en frameworks de gestión de riesgos

reconocidos y en prácticas probadas que permitan evaluar, controlar y supervisar continuamente a los proveedores externos.

## 2.1. Estrategias para mitigar riesgos operativos

Para fortalecer la gestión del outsourcing, las organizaciones deben implementar acciones que garanticen una coordinación eficiente con los proveedores y un control efectivo sobre los servicios delegados, a continuación, se describen las principales estrategias de mitigación adaptadas de (Dodds, 2024):

- **Evaluación exhaustiva del proveedor:** Antes de contratar, se debe realizar una investigación profunda sobre el historial, estabilidad financiera, cumplimiento normativo y medidas de seguridad del proveedor. Esto incluye verificar experiencia en el sector, referencias de clientes y certificaciones (como, por ejemplo: ISO 27001, SOC 2).
- **Selección de proveedores con experiencia probada:** Priorizar aquellos con trayectoria sólida en la industria y en las tecnologías requeridas, reduciendo la curva de aprendizaje y los riesgos asociados a inexperiencia.
- **Contratos claros y detallados:** Definir de forma precisa el alcance, entregables, plazos, KPIs, mecanismos de auditoría, resolución de disputas y cláusulas de terminación. Incluir obligaciones específicas sobre seguridad, confidencialidad y cumplimiento regulatorio.
- **Comunicación efectiva y canales acordados:** Establecer plataformas y frecuencias de comunicación, como reuniones periódicas, reportes de avance y

herramientas colaborativas, para alinear expectativas y detectar problemas tempranamente.

- **Monitoreo y supervisión continua:** Implementar revisiones de desempeño, auditorías y evaluaciones de riesgo periódicas, asignando un responsable interno que actúe como enlace entre la empresa y el proveedor.

## 2.2. Estrategias para riesgos de ciberseguridad

La creciente complejidad de los ciberataques y el intercambio de datos críticos con proveedores externos exigen medidas específicas para gestionar la seguridad en entornos de outsourcing. Siguiendo las recomendaciones adaptadas de (staffboom, 2024) se destacan las siguientes estrategias:

- **Evaluación integral de riesgos:** Identificar amenazas y vulnerabilidades específicas que puedan afectar a los socios de outsourcing, evaluando la probabilidad e impacto de cada riesgo. Utilizar frameworks como NIST Cybersecurity Framework o ISO/IEC 27005 para guiar el análisis.
- **Fortalecimiento del marco de gobernanza:** Definir responsabilidades y roles claros, establecer políticas de seguridad documentadas y realizar auditorías periódicas para verificar su cumplimiento. Incluir en los contratos cláusulas específicas y sanciones por incumplimientos en materia de ciberseguridad.
- **Protección y privacidad de datos:** Implementar cifrado en tránsito y en reposo, autenticación multifactor, controles de acceso y copias de seguridad seguras. Cumplir con la normativa vigente y garantizar el consentimiento informado antes de compartir datos.

- **Gestión de diferencias culturales y comunicación:** Reconocer y abordar las diferencias culturales que puedan influir en la gestión de la seguridad, promoviendo una comunicación clara para prevenir malentendidos y errores operativos.
- **Planes de contingencia y continuidad de negocio:** Preparar protocolos ante interrupciones por ciberataques, desastres naturales o crisis políticas. Mantener proveedores alternativos, sistemas de respaldo y procedimientos de recuperación probados regularmente.
- **Monitoreo continuo y métricas de seguridad:** Definir indicadores clave (KPIs) y acuerdos de nivel de servicio (SLAs) enfocados en la seguridad, supervisando su cumplimiento y fomentando la mejora continua.

## 2.3. Frameworks de Gestión de Riesgos

Tras identificar amenazas como filtraciones de datos, ransomware, incumplimientos regulatorios y problemas de calidad del servicio, es fundamental adoptar un enfoque estructurado basado en marcos de trabajo reconocidos. Estos frameworks proporcionan lineamientos claros y probados para gestionar riesgos en entornos con terceros.

### 2.3.1. NIST Cybersecurity Framework

Este marco define cinco funciones clave que pueden adaptarse a la relación con proveedores externos, adoptadas de (Villamizar, GlobalSuite Solutions, 2023) y que se desarrollan de la siguiente manera:

- **Identificar (ID):** Realizar un inventario completo de proveedores, clasificación por nivel de riesgo y análisis de dependencias críticas.

- **Proteger (PR):** Cláusulas contractuales y SLAs robustos que especifiquen requisitos de seguridad (cifrado de datos en tránsito y en reposo), tiempos de respuesta ante incidentes, derecho a auditar al proveedor y penalizaciones por incumplimiento. Principio de mínimo privilegio para asegurar que el proveedor solo tenga el acceso estrictamente necesario.
- **Detectar (DE)**: Monitoreo continuo y logs compartidos. Exigir al proveedor compartir logs de seguridad relevantes e integrarlos en el sistema SIEM de la organización cliente.
- **Responder (RS)**: Plan de respuesta a incidentes conjunto que defina roles, responsabilidades y canales de comunicación entre cliente y proveedor.
- **Recuperar (RC)**: Planes de continuidad del negocio (BCP/DRP) que verifiquen que el proveedor tenga planes sólidos de recuperación compatibles con los de la organización cliente.

### 2.3.2. ISO/IEC 27001:2022

La norma ISO/IEC 27001 establece un Sistema de Gestión de Seguridad de la Información (SGSI) que incluye controles específicos para las relaciones con proveedores, descritos en el Anexo A.15 tomado de (López, 2025):

- **15.1.1 Política de seguridad de la información para suministradores:** Se deben acordar y documentar los requisitos de seguridad de la información necesarios para proteger los activos de la organización frente a los riesgos derivados del acceso de proveedores y terceros.

- **15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores:** Los contratos con proveedores deben incluir todos los requisitos de seguridad pertinentes para la manipulación, procesamiento, almacenamiento o transmisión de información de la organización, así como para el suministro de componentes de infraestructura tecnológica.
- **15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones**: Los acuerdos con proveedores deben incluir cláusulas específicas para abordar los riesgos de seguridad de la información asociados a la cadena de suministro de servicios y productos de tecnologías de la información y comunicaciones.

### 2.3.3. COBIT 2019: Gobierno y Gestión de TI Empresarial

Este marco se orienta en el gobierno corporativo de la información y la tecnología, con aplicación directa en entornos de tercerización de servicios TI. Este enfoque permite alinear los objetivos tecnológicos con las metas estratégicas de la organización, asegurando que el outsourcing aporte valor y minimice riesgos. A continuación, se presentan los Principios del Sistema de Gobierno de COBIT 2019 aplicados al outsourcing:

- **Valor para las partes interesadas:** Asegura que la información y tecnología proporcionen el valor necesario para todas las partes interesadas.
- **Enfoque holístico:** Reconoce que la TI está compuesta por múltiples componentes interrelacionados que deben gestionarse como un todo.
- **Sistema de gobierno dinámico:** Permite adaptar la gobernanza ante cambios en el entorno o en los factores de diseño del negocio.

- **Separación de gobierno y gestión:** Define con claridad las funciones, estructuras y responsabilidades para dirigir (gobernar) y operar (gestionar) la TI.
- **Ajustado a la necesidad empresarial:** Utiliza factores de diseño para adaptar la implementación a las prioridades y contexto específico de la organización.
- **Cobertura extremo a extremo:** Abarca toda la empresa, más allá de la función de TI, incluyendo proveedores y terceros críticos.

Adicionalmente, el COBIT 2019 incluye un objetivo específico para la gestión de riesgos (APO12) que aborda:

- Identificación y mitigación de riesgos en toda la cadena de valor.
- Cumplimiento normativo y regulatorio.
- Gestión de riesgos de terceros y proveedores.
- Optimización de recursos y mejora de confianza

En la siguiente ilustración se presenta una comparación visual de los tiempos promedio de implementación de distintos marcos de trabajo de ciberseguridad y gestión de riesgos. Esta referencia permite dimensionar el esfuerzo y la planificación necesarios para adoptar cada framework, considerando que las diferencias no solo responden a la complejidad técnica, sino también al alcance organizacional, los recursos asignados y los requisitos normativos que cada uno implica.

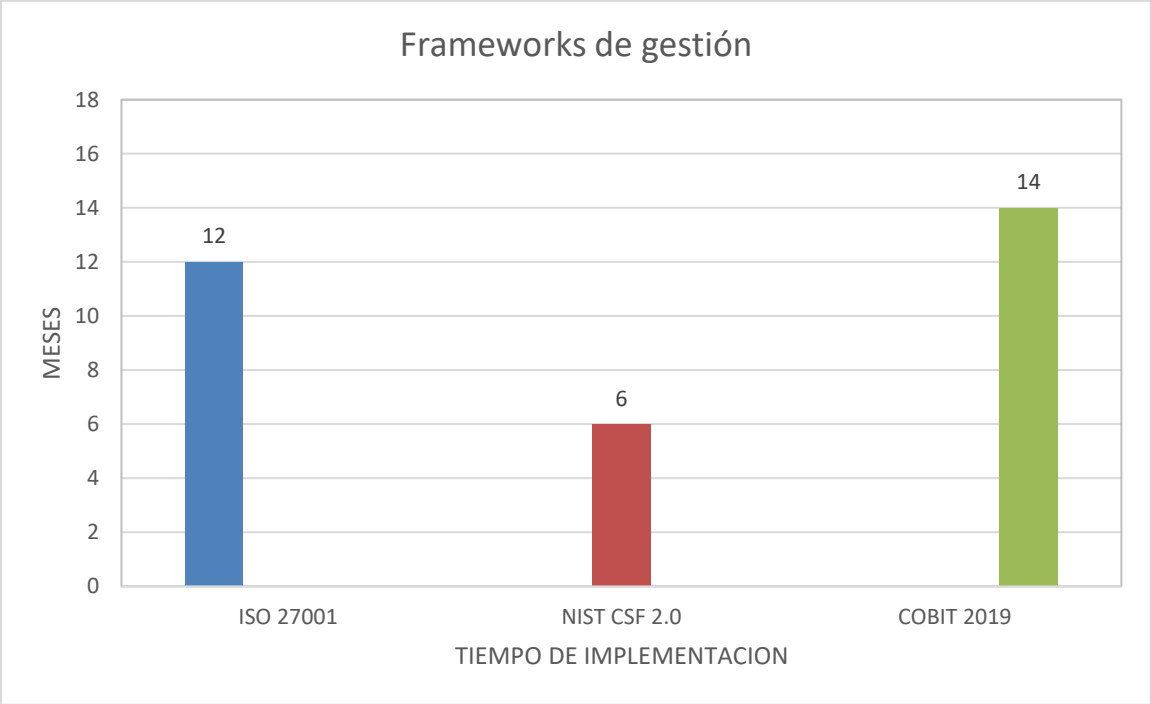


*Figura 2. Top 10 de riesgos en Colombia. Fuente: propia.*

## 3. Herramientas tecnológicas recomendadas y mejores prácticas para proteger información y datos críticos.

La implementación exitosa de las estrategias de mitigación requiere un ecosistema tecnológico integral que aborde todos los tipos de riesgos identificados en entornos de outsourcing. Las organizaciones modernas necesitan soluciones que no solo protejan contra amenazas de ciberseguridad, sino que también gestionen riesgos operacionales, financieros y regulatorios. A continuación, presentamos las herramientas tecnológicas y mejores prácticas de protección en entornos de Outsourcing.

## 3.1. Herramientas Tecnológicas de seguridad para Outsourcing

*Tabla 3. Herramientas tecnológicas de seguridad. Fuente: Adaptado de (Iberia, 2024)*

| Herramientas | Descripción | Casos de uso en Outsourcing |
|---|---|---|
| **Gestión de Acceso Privilegiado (PAM)** Soluciones: CyberArk, BeyondTrust, Thycotic. | Controla, supervisa y audita el uso de cuentas privilegiadas, aplicando políticas de mínimo privilegio y rotación automática de credenciales. | Acceso remoto seguro para proveedores con monitoreo de sesiones en tiempo real; gestión automatizada de credenciales con rotación programada; auditoría completa para cumplir ISO 27001 y NIST CSF. |
| **Data Loss Prevention (DLP)** Soluciones: Symantec DLP, Forcepoint DLP, Trellix DLP. | Detecta y bloquea la transferencia no autorizada de información sensible en redes, endpoints y entornos cloud. | Evitar que un proveedor externo transfiera documentos confidenciales fuera del perímetro corporativo; aplicar políticas de bloqueo en dispositivos USB para terceros. |
| **Security Information and Event Management (SIEM)** Soluciones: Wazuh, Splunk, QRadar. | Centraliza la recolección, correlación y análisis de logs de seguridad, con alertas ante comportamientos anómalos. | Monitorizar en tiempo real las actividades de un proveedor que administra bases de datos críticas; detectar intentos de acceso no autorizado. |
| **Endpoint Detection and Response (EDR)** | Supervisa el comportamiento de endpoints para detectar, contener y responder a amenazas avanzadas. | Detectar y aislar un equipo de un contratista infectado con malware antes de que se propague a la red corporativa. |

| Herramientas | Descripción | Casos de uso en Outsourcing |
|---|---|---|
| Soluciones: CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint. | | |
| **Gestión de Identidades y Accesos (IAM)** Soluciones: Okta, Azure AD, Ping Identity. | Gestiona la autenticación, autorización y el ciclo de vida de usuarios, incluyendo MFA y control de acceso basado en roles. | Habilitar acceso temporal y seguro a aplicaciones críticas para personal de outsourcing, con autenticación multifactor y caducidad automática. |
| **Soluciones de cifrado y protección de datos** Soluciones: Vormetric, BitLocker, VeraCrypt. | Protegen la información cifrándola en reposo y en tránsito para evitar filtraciones. | Cifrar datos sensibles antes de transferirlos a un proveedor de almacenamiento en la nube. |
| **Sistemas de Prevención de Intrusiones (IPS) y Firewalls de Próxima Generación (NGFW)** Soluciones: Palo Alto Networks, Fortinet, Suricata. | Combinan inspección profunda de paquetes, filtrado basado en aplicaciones y detección de amenazas en tiempo real. | Controlar y filtrar tráfico entre el proveedor y los sistemas del cliente; inspección de túneles seguros; aplicar microsegmentación para limitar alcance de incidentes. |

## 3.2. Mejores prácticas para proteger información y datos críticos en entornos de outsourcing.

La protección de información y datos críticos requiere no solo de tecnología, sino de un conjunto de prácticas operativas y políticas sólidas que reduzcan la probabilidad de

incidentes y mejoren la capacidad de respuesta ante amenazas. Las siguientes recomendaciones están alineadas con estándares internacionales y casos de éxito en la industria.

- **Clasificación y etiquetado de la información:** Se debe establecer un esquema de clasificación adecuada de la información según su nivel de criticidad y sensibilidad, como por ejemplo: “Pública”, “Interna”, “Confidencial” y “Crítica”; Esto facilita priorizar recursos y medidas de seguridad. Podemos tomar como referencia la ISO/IEC 27002:2022 – Control 5.12 (International Organization for Standardization, 2022).
- **Políticas de acceso basado en roles (RBAC):** Otorgar permisos únicamente según el rol funcional y la necesidad operativa, evitando accesos genéricos o permanentes a sistemas críticos. Esto ayuda a reducir la superficie de ataque y el riesgo de abuso de privilegios. Esta práctica está alineada con los controles AC-2 y AC-3 descritos en el NIST SP 800-53 (National Institute of Standards and Technology, 2020).
- **Principio de mínimo privilegio y control de sesiones privilegiadas:** Asegurar que los usuarios, tanto internos como externos, cuenten solo con el acceso estrictamente necesario para cumplir su función, y supervisar en tiempo real las sesiones privilegiadas para identificar comportamientos anómalos. Esta recomendación sigue el enfoque definido en el control 3.1.5 del NIST SP 800-171 (National Institute of Standards and Technology, 2020).
- **Cifrado de datos en tránsito y en reposo:** Aplicar protocolos seguros como TLS 1.3 para proteger las comunicaciones y algoritmos robustos como AES-256 para el

almacenamiento, de forma que, incluso si los datos son interceptados o robados, resulten ilegibles. Este enfoque está respaldado por las recomendaciones criptográficas de (ENISA, 2023).

- **Auditorías y revisiones periódicas de permisos:** Realizar revisiones trimestrales o semestrales de los accesos otorgados a terceros, eliminando credenciales inactivas y detectando privilegios no justificados. Esta práctica sigue la orientación del control A.9.2 de la norma ISO/IEC 27001:2022 (International Organization for Standardization, 2022).
- **Capacitación continua en seguridad de la información:** Capacitar tanto al personal interno como al externo en el uso seguro de la información, el reconocimiento de amenazas como phishing y la correcta respuesta ante incidentes. Tal como plantea el NIST NICE Framework, la fortaleza de la seguridad depende en gran medida del conocimiento del equipo humano (National Initiative for Cybersecurity Education, 2020).
- **Integración de pruebas de seguridad y simulacros:** Incorporar pruebas de penetración, ejercicios de ingeniería social y simulacros de respuesta a incidentes en los que participen los proveedores, para asegurar que las medidas de seguridad funcionan en escenarios reales. Este enfoque está alineado con las recomendaciones del NIST SP 800-84 sobre programas de prueba, entrenamiento y ejercicios (National Institute of Standards and Technology, 2016).

# CONCLUSIONES

La externalización de servicios de Tecnologías de la Información (Outsourcing TI) constituye una estrategia empresarial ampliamente adoptada para optimizar recursos, acceder a conocimientos especializados y mejorar la eficiencia operativa. Sin embargo, como se evidenció en este análisis, también implica desafíos significativos en materia de ciberseguridad, especialmente relacionados con la pérdida de control sobre datos críticos, las vulnerabilidades en la cadena de suministro y el riesgo de incumplimiento normativo por parte de terceros.

La implementación de marcos internacionales como el NIST Cybersecurity Framework, la norma ISO/IEC 27001 y COBIT 2019 se presenta como un pilar fundamental para la gestión de riesgos, ya que proporciona lineamientos estructurados para la identificación, protección, detección, respuesta y recuperación ante incidentes en entornos tercerizados. El estudio demuestra que la evaluación rigurosa de proveedores, la inclusión de cláusulas de ciberseguridad en los contratos, y el monitoreo continuo de la relación comercial son prácticas determinantes para garantizar la seguridad de la información y la continuidad del negocio.

Asimismo, las organizaciones que externalizan servicios TI deben adoptar un enfoque proactivo en la gestión de la seguridad, implementando herramientas tecnológicas como soluciones (PAM), sistemas de detección y prevención de intrusiones (IDS/IPS), plataformas de gestión de identidad y acceso (IAM), soluciones SIEM para el monitoreo integral, entre otras tecnologías, las cuales junto con las mejores prácticas alineadas a

estándares internacionales resultan esenciales para proteger activos críticos y garantizar la continuidad operativa frente a amenazas cada vez más sofisticadas.

Finalmente, las organizaciones que adopten un enfoque proactivo y preventivo, integrando gestión estratégica del riesgo, inversión en tecnología de protección avanzada y fortalecimiento de la cultura de seguridad, estarán en mejores condiciones para garantizar la continuidad del negocio, el cumplimiento normativo y la confianza de sus partes interesadas en un panorama digital cada vez más complejo.

## REFERENCIAS

accenture. (13 de Junio de 2023). *Aligning Cybersecurity to Business Objectives Helps Drive Revenue Growth and Lower Costs of Breaches, Accenture Report Finds.* Obtenido de accenture: https://newsroom.accenture.com/news/2023/aligning-cybersecurity-to-business-objectives-helps-drive-revenue-growth-and-lower-costs-of-breaches-accenture-report-finds

Administrator. (25 de Julio de 2025). *ISO 27001 – Anexo A.15: Relaciones con proveedores.* Obtenido de es.isms.online: https://es.isms.online/iso-27001/annex-a-15-supplier-relationships/

Akker, M. V. (24 de Marzo de 2025). *ISO 27001 frente al Marco de Ciberseguridad del NIST: ¿Cuál es la diferencia?* Obtenido de compleye.io: https://compleye.io/es/articulos/iso-27001-frente-al-marco-de-ciberseguridad-del-nist-cual-es-la-diferencia/

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

Álvarez, R. A. (2025). *Gestión de Riesgos de Seguridad de la Información en Proyectos de.* Bogotá: Universidad EAN.

barrera, m. (26 de Agosto de 2021). *Metodología NIST SP 800 – 30 para el análisis de Riesgos en SGSI.* Obtenido de PMG SSI - ISO 27001: https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/

Dodds, M. (16 de Octubre de 2024). *Compex IT.* Obtenido de Cybersecurity risks of outsourcing and staying FCA compliant: https://compexit.co.uk/understanding-the-cyber-security-risks-of-outsourcing-and-remaining-fca-compliant/

ENISA. (2023). *ENISA*. Obtenido de Recommendations on cryptographic algorithms. European Union Agency for Cybersecurity: https://www.enisa.europa.eu

Fortinet. (07 de Agosto de 2025). *¿Qué es la ciberseguridad? | Tipos, amenazas y mejores prácticas*. Obtenido de Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-cybersecurity

Group, I. D. (4 de Septiembre de 2024). *El número de víctimas de ciberataques a la cadena de suministro aumenta en casi 50.000.* Obtenido de IT Digital Security: https://www.itdigitalsecurity.es/infraestructuras-criticas/2024/09/el-numero-de-victimas-de-ciberataques-a-la-cadena-de-suministro-aumenta-en-casi-50000

Iberia, A. (09 de Julio de 2024). *ambit-iberia.* Obtenido de Herramientas y Tecnologías para Mejorar la Seguridad Informática: https://www.ambit-iberia.com/blog/herramientas-y-tecnologias-seguridad-it

International Organization for Standardization. (2022). *ISO/IEC 27001:2022-Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO.

ISACA. (2019). *ISACA.* Obtenido de Gobernanza de TI eficaz a su alcance: https://www.isaca.org/resources/cobit

Johnson, S. (12 de Noviembre de 2024). *Top 7 risks of outsourcing (And How to Prevent Them)*. Obtenido de We Are Amnet: https://www.weareamnet.com/blog/risks-of-outsourcing/

Law, S. S. (2024). *NFORME SOBRE CIBERSEGURIDAD y SU IMPACTO EN LAS EMPRESAS.* España.

López, A. (10 de 08 de 2025). *iso27000.* Obtenido de Relación con los Proveedores | Anexo 15 - ISO 27001: https://www.iso27000.es/iso27002_15.html

Mesa, J. D. (17 de Febrero de 2025). *Risks in the outsourcing of services.* Obtenido de piranirisk: https://www.piranirisk.com/blog/risks-in-the-outsourcing-of-services

National Initiative for Cybersecurity Education. (2020). *Cybersecurity Workforce Framework. NIST*. Obtenido de NIST: https://www.nist.gov/nice

National Institute of Standards and Technology. (2016). *NIST SP 800-84 – Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.* doi: https://doi.org/10.6028/NIST.SP.800-84

National Institute of Standards and Technology. (2020). *NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations.* doi:https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2020). *NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations.*

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

PwC. (2022). *Outsourcing/BPO Survey Colombia: Sembrando una relación para la transformación del negocio.* Obtenido de PwC Colombia: https://www.pwc.com/co/es/publicaciones/outsourcing-survey/outsourcing-2022-survey-colombia.pdf

República, D. L. (23 de Enero de 2025). *Diario La República.* Obtenido de Los ciberataques y las catástrofes naturales, los mayores riesgos para las compañías.: https://www.larepublica.co/finanzas/los-ciberataques-y-las-catastrofes-naturales-los-mayores-riesgos-para-las-companias-4043889

staffboom. (16 de Febrero de 2024). *2024 Cyber Security Risks in Outsourcing.* Obtenido de staffboom: https://www.staffboom.com/blog/cyber-risks-in-outsourcing/

UAO. (14 de Julio de 2025). *¿Cuáles son los 10 casos de ciberataques más reconocidos en Colombia?* Obtenido de uao: https://virtual.uao.edu.co/blog/cuales-son-los-10-casos-de-ciberataques-mas-reconocidos-en-colombia

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

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

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