TRABAJO DE GRADO
Opción Seminario-Diplomado.

“Ciberseguridad en Soluciones informáticas”

Informe técnico

Corporación Universitaria Remington.
Nombre de la facultad: ingenierías
Nombre del programa académico: Ingeniería de Sistemas

David Alejandro Quintero Tabares
Johnatan Rios Loaiza
Tutor: Jorge Mauricio Sepúlveda Castaño
Opción de Trabajo de grado Seminario-Diplomado.
2026

Tabla de Contenidos

Contenido

Resumen

Resulta que cuando entregas tus datos y tus sistemas a un tercero, también estás entregando algo de control. Y ahí empiezan los problemas. ¿Qué pasa si ese proveedor no cuida bien la información? ¿O si un ciberataque lo deja fuera de servicio? De repente, lo que parecía una solución se convierte en un riesgo enorme. Pérdida de control sobre los activos críticos, vulnerabilidades que se meten por la cadena de suministro, y para rematar, la posibilidad de que te caiga una multa porque el proveedor no cumplió con alguna norma de protección de datos. No es un escenario agradable.

La idea es mirar con lupa qué está pasando con la ciberseguridad cuando hay un tercero en el medio. Revisamos las amenazas más comunes, tanto las operativas (las del día a día) como las puramente cibernéticas. Y luego, lo más importante, empezamos a pensar en cómo reducir esos riesgos. Para eso nos apoyamos en marcos como el NIST, la ISO 27001 y el COBIT 2019. Suenan muy técnicos, pero en el fondo son como una guía para no improvisar.

También hablamos de herramientas. Porque una cosa es la teoría y otra lo que realmente funciona cuando hay que proteger datos que están en manos de un tercero. Y cerramos con buenas prácticas, esas que uno aprende después de ver qué funcionó y qué no en casos reales. Todo esto, claro está, mirando el contexto colombiano. Porque no es lo mismo hablar de ciberseguridad en un país que en otro, y acá hemos visto casos recientes que dejan enseñanzas.

La conclusión después de todo este recorrido es que no se puede externalizar la responsabilidad. Si una empresa decide tercerizar sus servicios TI, tiene que estar encima. Evaluar al proveedor como si fuera una extensión de la empresa, invertir en tecnología que sí proteja y tener claro que la seguridad no es algo que se firma en un contrato y se olvida. Es un trabajo de todos los días. Si se hace bien, el outsourcing puede ser una gran jugada. Si se hace mal, el costo puede ser muy alto.

Marco conceptual y contextual

1. Marco conceptual

1.1. Definición y Alcance del Outsourcing de Servicios TI

La tercerización de servicios TI u outsourcing no es más que una decisión. Básicamente consiste en tomar procesos, operaciones o funciones tecnológicas que antes hacía la empresa y pasárselas a un proveedor externo que se especializa en ello. Con ello garantizamos optimizar recursos, bajar costos y acceder a capacidades técnicas que por uno mismo sería muy costoso o complicado tener. Esto puede ir desde entregarles la infraestructura completa, los centros de datos, hasta el desarrollo de software, el soporte técnico e incluso los servicios de ciberseguridad (Peña, 2024).

Estas decisiones tienen una consecuencia que a veces no se piensa bien: uno cede control. Y no cualquier control, sino el de los activos de información que son críticos para el negocio. Ahí es donde empieza la cosa a complicarse. Porque lo que se genera es una

relación de interdependencia. Ya no depende todo de lo que uno haga, sino de lo que haga el proveedor también. Y esa dinámica, si no se maneja con cuidado, abre la puerta a vectores de ataque que antes no existían. Por eso toca sentarse a establecer políticas de seguridad robustas, y no solo crearlas, sino evaluarlas de verdad (Johnson, 2024).

1.2. Ciberseguridad: concepto y aplicación general

Conjunto de políticas, procedimientos, controles y herramientas que se ponen en marcha para proteger sistemas, redes y datos contra ataques o accesos que no deberían ocurrir (Fortinet, 2025). La norma ISO/IEC 27032 (2017) lo dice de una manera más técnica: un enfoque integral para garantizar que los activos digitales sigan siendo confidenciales, íntegros y estén disponibles cuando se necesiten.

Ahora, ¿por qué esto se vuelve tan importante cuando hablamos de outsourcing? Pues porque la superficie de riesgo se expande. Cuando los datos y los procesos críticos salen del control directo de la organización, las cosas se ponen más difíciles. Ya no basta con tener las defensas bien puestas en la oficina o en los servidores propios. Hay que replantear las estrategias de protección, ponerse de acuerdo con los proveedores, establecer políticas conjuntas y coordinar esfuerzos.

1.3. Marcos Normativos y Regulatorios

Existen marcos normativos internacionales que ya tienen definidos los requisitos específicos para manejar la seguridad de la información y, sobre todo, para controlar a los terceros que entran en la ecuación. Las normas que son más conocidas son:

ISO/IEC 27001:2022: Te da un enfoque sistemático para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). En ello podemos encontrar un apartado específico para el tema de proveedores, el Anexo A.15. Habla de cómo establecer políticas de seguridad con los suministradores, cómo manejar los riesgos en los contratos y cómo gestionar toda la cadena de suministro de TIC (Akker, 2025; Administrator, 2025).

NIST Cybersecurity Framework 2.0: No es una norma de certificación como la ISO, sino un marco de trabajo basado en riesgos. Se organiza en cinco funciones que son muy prácticas: identificar, proteger, detectar, responder y recuperar, tiene publicaciones complementarias, como la NIST SP 800-161, que dan metodologías específicas para evaluar y mitigar riesgos en cadenas de suministro (Villamizar, 2023; barrera, 2021). Este marco no es tan rígido y se puede adaptar a las necesidades de cada empresa.

COBIT 2019: Orientado al gobierno y la gestión de TI, no solo a la seguridad. Su enfoque es alinear la tecnología con los objetivos del negocio. En el contexto del outsourcing, es muy útil porque te da herramientas para gestionar los riesgos, controlar a los proveedores y optimizar los procesos de TI. Lo bueno es que se puede integrar con la ISO 27001 y con el NIST CSF, es flexible porque no es necesario elegir solo uno sino que puedes usarlos combinados para tener una estrategia más completa (ISACA, 2019).

2. Marco contextual

Los conceptos y marcos normativos revisados en la sección anterior proporcionan una base teórica necesaria para abordar la gestión de riesgos en outsourcing. Sin embargo, resulta igualmente importante examinar las condiciones concretas en las que estas amenazas se desarrollan, tanto a nivel global como en Colombia. La distancia entre la teoría y la práctica puede ser significativa, y el análisis del contexto permite dimensionar la magnitud de los desafíos que enfrentan las organizaciones.

2.1. Evolución del Panorama de Amenazas

Anteriormente los ciberataques no eran tan comunes, Actualmente vemos que los atacantes van por un proveedor más pequeño o con menos controles, y desde ahí saltar a los clientes potenciales. Es como si en vez de asaltar un banco, te robaran las llaves del custodio que tiene las cajas de seguridad.

En 2024 se registraron más de 467.000 ciberataques diarios en todo el mundo. Para que se haga una idea, eso es un 14% más que el año anterior (Valladolid, 2025). Y cuando hablamos específicamente de ataques a la cadena de suministro, el número de organizaciones afectadas creció en casi 50.000 casos (Group, 2024). No son cifras menores.

A esta estrategia le llaman "ataque en cascada" (Law, 2024). Y no es teoría. El caso de SolarWinds fue un baldado de agua fría para la industria. Después vino Kaseya. Y más recientemente, el incidente de CrowdStrike, que, aunque fue una actualización fallida más que un ataque, nos dejó una lección: cuando falla un proveedor con el que todos trabajan, el impacto es masivo. Hablamos de 8,5 millones de sistemas afectados en todo el mundo (Alexander Liskin, 2024). Este es un caos a nivel cibernético.

2.2.Panorama en Colombia

El outsourcing de TI sigue creciendo a toda velocidad. El país ya es el tercer mercado de TI más grande de Latinoamérica. Las empresas colombianas han entendido que tercerizar es una forma de acceder a conocimiento especializado que a veces simplemente no consiguen en el mercado local. De hecho, el 86% de las compañías colombianas dice que esa es la razón principal para externalizar procesos tecnológicos (PwC, 2022).

La parte preocupante Mientras más empresas tercerizan, más crece la ciberdelincuencia. Un dato que llamó mi atención es que solo el 45% de las organizaciones que externalizan servicios incluyen a sus proveedores en los planes de respuesta a incidentes. O sea, más de la mitad no lo hace. Sí, hay un avance, pero todavía nos falta un montón por mejorar, sobre

todo en implementar medidas preventivas y de control (accenture, 2023). Es como tener un seguro de vida, pero no revisarlo nunca.

El ataque de ransomware a Empresas Públicas de Medellín (EPM) en 2022 fue un antes y un después. No solo afectó a una empresa, sino que paralizó servicios esenciales de una ciudad entera. La gente se quedó sin poder hacer trámites, sin atención al cliente, y en el sector salud, que es todavía más delicado porque hablamos de vidas, también han pasado cosas graves. Los incidentes en Salud Total y la Clínica Keralty, donde se filtraron datos sensibles de pacientes, nos mostraron que nadie está exento (UAO, 2025).

Lo que estos casos nos dejan claro es que las infraestructuras críticas son un blanco, y que la seguridad no puede quedarse solo en las paredes de la empresa. Hay que mirar toda la cadena de valor, y sobre todo a esos proveedores de servicios tecnológicos que tiene acceso a contenido confidencial de la empresa. Si ellos caen, nosotros caemos con ellos.

DESARROLLO E IMPLEMENTACIÓN DEL APRENDIZAJE

A partir de ese análisis, se presentarán estrategias de mitigación fundamentadas en marcos reconocidos, junto con recomendaciones de herramientas tecnológicas y buenas prácticas orientadas a proteger los datos y servicios tercerizados, se planteará un escenario simulado que permita ilustrar la aplicación concreta de estos conceptos.

1. Principales amenazas en la externalización de servicios TI.

La externalización de servicios TI ofrece beneficios innegables: reducción de costos, acceso a talento especializado y mayor flexibilidad operativa. Sin embargo, también introduce riesgos significativos que conviene clasificar en dos grandes categorías: los riesgos operativos y estratégicos, por un lado, y los riesgos de ciberseguridad, por el otro. A continuación, se examinan cada uno de ellos. 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:

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 funciones claves por periodos	El equipo interno deja de conocer la arquitectura del sistema tras años de

	prolongados.	outsourcing.

Riesgo	Descripción	Ejemplo de impacto
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.

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

1.1. Amenazas de ciberseguridad en outsourcing TI

Los riesgos operativos y estratégicos representan un desafío importante para las organizaciones que recurren en el outsourcing. Sin embargo, las implicaciones en materia de ciberseguridad resultan particularmente críticas, pues involucran la protección de activos de información frente a un ecosistema cada vez más hostil. La falta de controles efectivos en los proveedores, el incumplimiento de normativas aplicables o la exposición directa a ciberataques pueden desencadenar consecuencias operativas, financieras y legales de gran magnitud. La Tabla 2 presenta una síntesis de las amenazas más frecuentes en este tipo de esquemas.

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.
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.

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

En Colombia, estas amenazas cobran aún más importancia. De acuerdo con el Barómetro de Riesgos Allianz 2026, la inteligencia artificial y la desinformación se han convertido en el principal riesgo para las empresas del país, alcanzando un 48% de las menciones y escalando desde el décimo lugar en 2025. Los incidentes cibernéticos, aunque descienden al segundo lugar con un 45%, siguen siendo una amenaza crítica, potenciados ahora por el uso de inteligencia artificial para automatizar ataques de ransomware, fraudes digitales y filtraciones de datos a escala sin precedentes (Allianz, 2026). En el caso del outsourcing, estos riesgos se acentúan debido a la estrecha dependencia tecnológica que las organizaciones mantienen con sus proveedores externos, quienes pueden convertirse en el eslabón más débil de la cadena de suministro tecnológica. (Allianz, 2026).

Top 10 risks in Colombia

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 226. Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2025 rank	Trend
1	Artificial intelligence *(e.g., implementation challenges, liability exposures, misinformation / disinformation)*	48%	*10 (13%)*	↗
2	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	45%	*1 (34%)*	↘
3	Political risks and violence *(e.g., war, political instability, terrorism, polarization, coup d'état, civil commotion, strikes, riots, looting)*[1]	26%	*9 (15%)*	↗
4	Changes in legislation and regulation *(e.g., tariffs, new directives, sustainability requirements)*	26%	*4 (24%)*	→
5	Business interruption *(incl. supply chain disruption)*	19%	*2 (30%)*	↘
6	Climate change *(e.g., physical, operational and financial risks as a result of extreme weather)*	14%	*6 (18%)*	→
7	Fire, explosion	12%	*5 (20%)*	↘
8	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire)*	11%	*3 (25%)*	↘
9	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	10%	*7 (16%)*	↘
10	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	9%	*8 (15%)*	↘

1 Political risks and violence ranks higher than changes in legislation and regulation based on the actual number of responses

Figura 1. Top 10 de riesgos en Colombia. Fuente: tomada de (Allianz, 2026).

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

Una vez identificados los riesgos operativos, estratégicos y cibernéticos asociados al outsourcing de TI, No basta con reaccionar cuando algo sale mal. Reaccionan cuando el proveedor ya tuvo una filtración o cuando el servicio lleva horas caído. La idea es anticiparse y fortalecer las defensas antes de que las amenazas se materialicen.

Para lograrlo, los frameworks de gestión de riesgos son una herramienta clave. NIST, ISO 27001, COBIT 2019. No son la única opción, pero son los más reconocidos. Ayudan a estructurar la evaluación, el control y la supervisión de los proveedores externos.

2.1. Estrategias para mitigar riesgos operativos

La gestión de riesgos operativos en entornos de outsourcing requiere un enfoque sistemático que combine controles preventivos con mecanismos de supervisión continua. Diversos marcos de referencia y estudios especializados coinciden en señalar un conjunto de prácticas que resultan determinantes para reducir la exposición de las organizaciones frente a fallos o desviaciones en el desempeño de sus proveedores externos.

- **Evaluación exhaustiva del proveedor:** Antes de suscribir cualquier acuerdo, la organización debe adelantar un proceso de debida diligencia que vaya más allá de la revisión de precios o capacidades técnicas. El NIST SP

800-161 (National Institute of Standards and Technology, 2022) recomienda evaluar aspectos como la estabilidad financiera del proveedor, su historial de cumplimiento normativo y la madurez de sus controles internos. La profundidad de esta evaluación debe ser proporcional al nivel de riesgo que el proveedor representará para la organización.

- **Selección de proveedores con experiencia probada:** La experiencia previa del proveedor en el sector de la organización contratante constituye un factor que reduce significativamente los riesgos operativos. Cuando el proveedor ya ha trabajado en industrias reguladas o con tecnologías específicas, la curva de aprendizaje se acorta y disminuye la probabilidad de errores derivados del desconocimiento del contexto. La norma ISO/IEC 27001:2022, enfatiza la importancia de que los acuerdos con proveedores consideren no solo las capacidades técnicas, sino también la alineación con los requisitos sectoriales aplicables.
- **Formalización contractual con enfoque en seguridad:** El contrato constituye el principal instrumento para gestionar las expectativas y establecer los límites de la relación. Más allá de definir alcances, plazos e indicadores, los acuerdos deben incluir cláusulas que regulen aspectos críticos como la propiedad de la información, las condiciones de auditoría, los procedimientos de escalamiento ante incidentes y las causales de terminación.
- **Definición de canales y frecuencias de comunicación:** La experiencia muestra que una proporción significativa de los conflictos en outsourcing

tiene su origen en fallas de comunicación más que en deficiencias técnicas. Por esta razón, resulta recomendable establecer desde el inicio canales formales de interacción, frecuencias definidas para reuniones de seguimiento y mecanismos claros para el escalamiento de problemas. El COBIT 2019, destaca la necesidad de definir roles y responsabilidades específicos para la interacción con terceros, de modo que no queden espacios de ambigüedad en la coordinación diaria.

- **Supervisión continua y gestión de la relación:** La firma del contrato no marca el final del proceso de gestión, sino el inicio de una relación que requiere monitoreo permanente. Las organizaciones con mejores resultados en outsourcing asignan un responsable interno con dedicación específica a la gestión del proveedor (vendor manager), que revisa periódicamente los indicadores de desempeño, coordina las auditorías técnicas y actúa como punto de contacto único para la resolución de problemas. El enfoque de mejora continua que propone el NIST Cybersecurity Framework, en su función de identificación y protección, refuerza la necesidad de mantener una supervisión activa que permita ajustar los controles a medida que evoluciona la relación.

2.2. Estrategias para riesgos de ciberseguridad

Cuando una organización decide externalizar servicios TI, los datos que antes estaban en servidores propios, pasan a estar en manos de un tercero. No es

que el proveedor vaya a actuar de mala fe, pero la realidad es que la organización pierde visibilidad directa sobre lo que ocurre con su información. Y esa pérdida de visibilidad es, probablemente, el riesgo más difícil de gestionar en ciberseguridad.

Varias estrategias aparecen de manera recurrente en la literatura y en las guías prácticas de organizaciones como el NIST o la ISO. No son soluciones mágicas, pero ayudan a reducir la exposición.

Hacer una evaluación de riesgo antes de contratar: Muchas empresas se enfocan en el precio y en las capacidades técnicas del proveedor, pero se deja a un lado entender qué riesgos introduce esa relación. ¿Qué información sensible va a manejar el proveedor? ¿Qué tan críticos son los sistemas a los que va a tener acceso? ¿Qué controles de seguridad tiene implementados?

El NIST SP 800-30 (National Institute of Standards and Technology, 2012) propone una metodología para hacer este tipo de evaluaciones, hay que identificar los activos críticos, analizar las amenazas que podrían afectarlos y valorar el impacto si algo sale mal. Este ejercicio no es algo que se hace una sola vez. El riesgo cambia con el tiempo, y la evaluación debería actualizarse periódicamente.

Definir responsabilidades desde el principio: En la práctica, uno de los problemas más comunes en outsourcing es que nadie tiene la culpa. El contrato dice cosas generales, pero cuando ocurre un incidente de seguridad, el proveedor dice que eso es responsabilidad del cliente, y el cliente dice que eso

lo cubría el proveedor. Mientras se resuelve quién tiene la culpa, el problema sigue ahí, simplemente para no responder por multas o daños.

La norma ISO/IEC 27001:2022 aborda esto en su control A.5.2 (Segregación de funciones). Básicamente, plantea que las responsabilidades deben estar definidas de manera clara y documentada.

Proteger los datos con medidas concretas: Cuando se hace la entrega de la documentación a outsorcing, la organización tiene que asegurarse de que se apliquen medidas técnicas que reduzcan el riesgo, independientemente de la confianza que se tenga en el proveedor.

Con ello uno de los más comunes son la autenticación multifactor para todos los accesos. Controles de acceso que limiten lo que cada usuario puede hacer. Copias de seguridad cifradas y probadas periódicamente. Son el mínimo aceptable en cualquier esquema de outsourcing.

En Colombia, además, la Ley 1581 de 2012 establece obligaciones específicas para el tratamiento de datos personales. Si el proveedor maneja mal esos datos, la sanción recae sobre la empresa contratante. Por eso las medidas técnicas no son solo una buena práctica, son una exigencia legal.

No subestimar las diferencias culturales: Lo que para una empresa es un incidente grave que requiere escalamiento inmediato, para otra puede ser un asunto menor que se resuelve en la reunión semanal. Las expectativas sobre

tiempos de respuesta, los niveles de formalidad en la comunicación, la disposición a reportar errores, todo varía de acuerdo a la empresa a contratar.

El COBIT 2019 (ISACA, 2019), sugiere que se establezcan desde el inicio mecanismos de comunicación claros, definir canales, frecuencias de reunión, procedimientos de escalamiento. Parece algo administrativo, pero ayuda a prevenir que las diferencias culturales se conviertan en conflictos operativos.

Preparar la respuesta conjunta: Los ciberataques no son una posibilidad remota. En Colombia, como se vio con los casos de EPM, caso de Bancolombia o las clínicas afectadas por ransomware, los incidentes ocurren y su impacto puede ser masivo. Por eso los planes de respuesta no pueden ser solo de la organización. Tienen que ser conjuntos con el proveedor.

El proveedor debe tener sus propios planes de recuperación ante desastres (DRP) y continuidad del negocio (BCP), y esos planes deben ser compatibles con los de la organización. También vale la pena identificar proveedores alternativos para los servicios críticos, porque si la opción A falla, el outsorcing debe tener la opción B, Tener en cuenta que los simulacros son importantes.

El NIST Cybersecurity Framework en sus funciones de respuesta y recuperación, enfatiza la necesidad de coordinar estos planes con los terceros que hacen parte de la cadena de suministro.

Puntos de control: Si no se definen indicadores de seguridad para el proveedor, es difícil saber si está cumpliendo.

Algunos indicadores que aparecen con frecuencia como por ejemplo porcentaje de vulnerabilidades críticas parcheadas a tiempo, tiempo de respuesta ante incidentes, disponibilidad de los sistemas, resultados de auditorías de seguridad. Estos indicadores deberían estar en los acuerdos de nivel de servicio (SLA). Si no se miden, no se pueden exigir.

2.3. Frameworks de Gestión de Riesgos

Los marcos de trabajo no son una camisa de fuerza, pero ayudan. Proporcionan una estructura y un lenguaje común que facilita la gestión con terceros.

Uno de los más utilizados es el NIST Cybersecurity Framework. Se organiza en cinco funciones que se pueden aplicar a la relación con proveedores. La primera es identificar, es saber qué proveedores se tienen y qué información es la que manejan. Luego proteger poniendo controles, contratos, SLAs, acceso limitado al cifrado. Después detectar y no basta con que el proveedor diga que está seguro, hay que tener visibilidad, exigir logs, integrarlos. También tener planes conjuntos, roles definidos, canales de comunicación establecidos antes de la crisis. Y finalmente recuperar, en ello verificar que el proveedor tenga sus propios planes de continuidad y que sean compatibles con los del cliente.

La ISO/IEC 27001:2022 tiene un enfoque más centrado en los controles, tiene un anexo que está dedicado a las relaciones con proveedores. La norma exige que los requisitos de seguridad para proveedores estén documentados y plantea que los contratos deben incluir todas las obligaciones de seguridad relevantes.

El COBIT 2019 aporta una mirada más desde el gobierno corporativo. Sus principios son útiles para pensar el outsourcing no solo como un tema técnico, sino como una decisión estratégica. Plantea que el outsourcing debe generar valor, no solo reducir costos y que la seguridad no se puede gestionar de forma aislada, porque todo está conectado, tener en cuenta que los riesgos cambian, y la gobernanza también tiene que cambiar. Que la dirección define políticas de gobierno y el equipo operativo las ejecuta, y que en outsourcing la responsabilidad es compartida pero la rendición de cuentas sigue siendo de la organización contratante y tener en cuenta que no pueden haber puntos ciegos, el gobierno de TI debe cubrir a todos los actores, incluidos proveedores y subcontratistas.

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, asegurar que el proveedor solo tenga

el acceso estrictamente necesario.

- **Detectar (DE)**: Exigir al proveedor compartir logs de seguridad relevantes e integrarlos en el sistema de monitoreo de la organización del 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 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.

- **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, asícomo

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.

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.

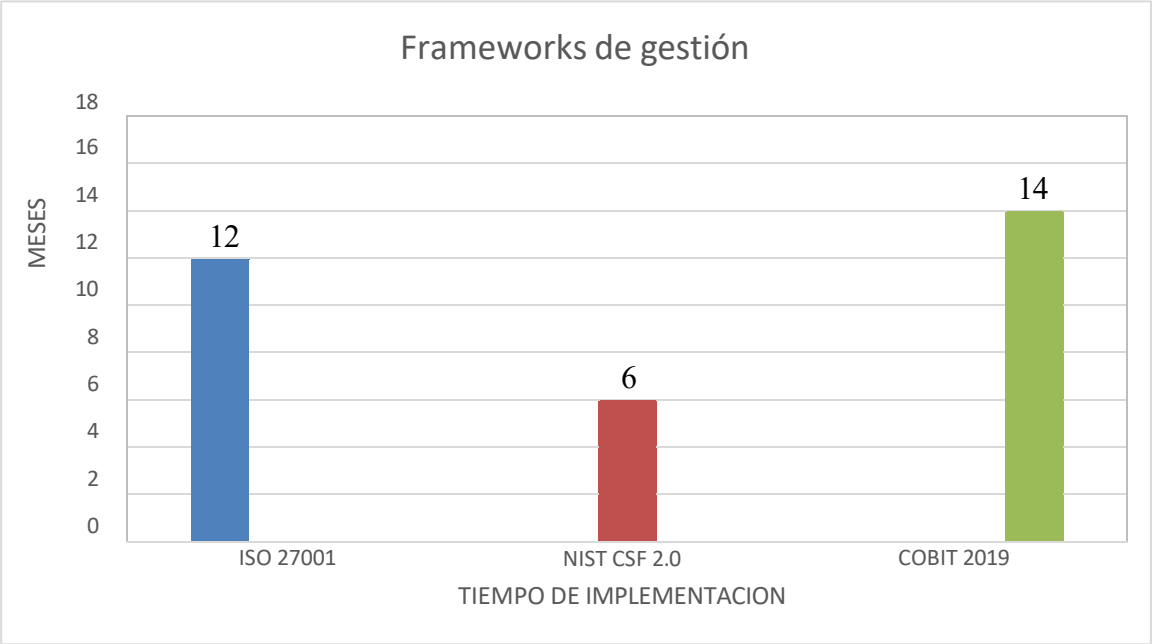

Figura 2. Top 10 de riesgos en Colombia. Fuente: propia.

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

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.

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

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

La protección de la información en esquemas de outsourcing no depende exclusivamente de la tecnología. Por más avanzadas que sean las herramientas, si las prácticas operativas y las políticas no están bien definidas, el riesgo es alto. Las siguientes recomendaciones recogen estándares internacionales y experiencias documentadas en la industria. No son una lista exhaustiva, pero cubren los aspectos que con mayor frecuencia aparecen en las guías especializadas.

- **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.

- **Políticas de acceso basado en roles (RBAC):** Otorgar permisos de acceso sin criterios claros es una de las formas más comunes de aumentar la superficie de ataque. Cuando un proveedor o un contratista tiene acceso a más información de la que realmente necesita para cumplir su función, se introduce un riesgo innecesario.
- **Principio de mínimo privilegio y control de sesiones privilegiadas:** En el contexto del outsourcing, esto cobra especial relevancia porque los proveedores suelen requerir acceso remoto a sistemas críticos. La práctica recomendada incluye la supervisión en tiempo real de las sesiones privilegiadas, de modo que cualquier comportamiento anómalo pueda identificarse y detenerse antes de que cause daño.
- **Cifrado de datos en tránsito y en reposo:** El cifrado es una de las medidas más efectivas para proteger la información, especialmente cuando los datos salen del perímetro controlado por la organización. Si los datos están cifrados, incluso en caso de interceptación o robo, resultan ilegibles para quien no tenga las claves.

  Para las comunicaciones, se recomienda utilizar protocolos seguros como TLS 1.3, que garantizan la confidencialidad e integridad de los datos en

tránsito. Para el almacenamiento, algoritmos robustos como AES-256 ofrecen un nivel de seguridad ampliamente aceptado.

- **Auditorías y revisiones periódicas de permisos:** Los accesos tienen una tendencia natural a acumularse. Un proveedor que inicialmente requería acceso a un sistema específico, con el tiempo puede terminar con permisos sobre otros sistemas que no le corresponden. Las cuentas inactivas también representan un riesgo, porque pueden ser utilizadas por personas que ya no forman parte de la organización.

  Por esta razón, las auditorías periódicas de permisos son una práctica necesaria. Revisiones trimestrales o semestrales permiten identificar cuentas inactivas, detectar privilegios no justificados y ajustar los accesos según las necesidades actuales.
- **Capacitación continua en seguridad de la información:** La tecnología puede tener fallas, pero el eslabón más débil en cualquier esquema de seguridad suele ser el factor humano. Por eso la capacitación continua es tan importante como cualquier control técnico.
- **No se trata de hacer una charla anual y olvidarse del tema:** La formación debe incluir la identificación de amenazas como el phishing, el manejo seguro de la información y los procedimientos de respuesta ante incidentes. Tanto el personal interno como el de los proveedores deben estar incluidos en estos programas. El NIST NICE Framework (National Initiative for Cybersecurity Education) plantea que la fortaleza de la seguridad depende en gran medida

del conocimiento y las competencias del equipo humano, y ofrece una estructura para desarrollar programas de capacitación efectivos.

- **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.

Conclusiones

Lo primero que descubre es que el outsourcing TI es un tema que genera opiniones encontradas. Por un lado, las empresas colombianas lo están usando cada vez más. El país es el tercer mercado de TI de Latinoamérica y el 86% de las compañías dice que terceriza para acceder a conocimiento especializado (PwC, 2022). Pero cuando uno empieza a mirar con cuidado cómo se gestiona la seguridad en esas relaciones, la cosa cambia.

Encontré un dato que me llamó la atención durante la investigación. Solo el 45% de las organizaciones que externalizan servicios incluyen a sus proveedores en los planes de respuesta a incidentes (accenture, 2023). Eso significa que más de la mitad no lo hace y es altamente preocupante, porque si el proveedor sufre un ataque y usted no lo tiene contemplado en su plan, no sabríamos que paso seguir. Y mientras tanto, sus datos, que están en manos de ese tercero, pueden estar comprometidos.

Con los marcos normativos pasa algo curioso. NIST, ISO 27001, COBIT 2019. Todos aparecen en la literatura como la solución (Akker, 2025; Villamizar, 2023; ISACA, 2019). Y en teoría lo son. Le dan a uno una estructura para no improvisar. Pero en la práctica, implementarlos no es tan sencillo. Yo diría que es casi un lujo para muchas

empresas colombianas, sobre todo para las medianas y pequeñas. Porque requiere tiempo, gente dedicada, recursos. Y eso no siempre está. Es una limitación real que hay que reconocer.

Las herramientas tecnológicas que se recomiendan son necesarias. No hay duda. Pero también hay que decir algo que no siempre se menciona en los informes técnicos, ponerlas a funcionar bien, monitorearlas, mantenerlas actualizadas, eso cuesta. No solo en dinero, sino en capacidad operativa (Iberia, 2024). Una empresa pequeña puede comprar un software de monitoreo pero, quien estará 24/7 realizándolo para cuando algo pase. Ese es el tipo de preguntas que uno se hace después de revisar la teoría y confrontarla con la realidad.

Me parece importante mencionar los casos colombianos. El ataque a EPM en 2022, los incidentes en Salud Total, Bancolombia y la Clínica Keralty (UAO, 2025). Son ejemplos que uno encuentra cuando investiga y que sirven para recordar que esto no es teoría. Es real. Y en todos esos casos, la cadena de suministro tecnológica jugó un papel. No fueron solo empresas aisladas. Fueron sistemas completos que fallaron, con afectación a usuarios, a pacientes, a ciudades enteras.

La seguridad en el outsourcing no se resuelve con un contrato bien redactado. El contrato es importante, claro. Pero sin supervisión, sin monitoreo, sin una relación donde ambas partes entiendan que es una responsabilidad compartida, cualquier papel se queda corto.

Quien escribe esto cree que las empresas en Colombia tienen un reto grande por delante. Van a seguir tercerizando. Pero la pregunta no es si tercerizar o no. La pregunta es cómo hacerlo sin perder el control de lo crítico. Y eso, me parece, sigue siendo un tema abierto.

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/

Allianz. (2026). *Allianz Risk Barometer 2026: Top business risks for Colombia*. Allianz Commercial.https://www.allianz.co/sala-de-prensa/comunicados/inteligencia-artificial-y-desinformacion-amenaza-empresas-colombianas.html

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

COBIT 2019 (ISACA, 2019) https://www.isaca.org/about-us/newsroom/press-releases/2019/isaca-introduces-cobit-2019-training-resources

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 (European Union Agency for Cybersecurity). (2021). Recommendations on cryptographic algorithms. https://www.enisa.europa.eu/publications/algorithms-key-length-and-protocols-report-2021

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 (ISO). (2022). *ISO/IEC 27001:2022 Information security management systems*. https://www.iso.org/standard/27001

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

ISO/IEC 27001:2022) https://www.isms.online/iso-27001/annex-a-2013/annex-a-15-supplier-relationships-2013/

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

NIST Cybersecurity Framework (funciones Identify y Protect) https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

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

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). *GlobalSuite Solutions.* Obtenido de ¿Qué es NIST Cibersecurity Framework?:

https://www.globalsuitesolutions.com/es/que- es-nist-cibersecurity-framework