Terceras Partes

Topical Requirement

Requisito Temático

Guía de usuario

The Institute of Internal Auditors

Traducción al Español Auspiciada por:

Instituto de Auditores Internos de España

FLAI Fundación Latinoamericana de Auditores Internos

Contenido

Resumen de los Requisitos Temáticos 2

Aplicabilidad, riesgo y criterio profesional 2

Consideraciones 7

Consideraciones sobre el Gobierno 7

Consideraciones sobre la gestión de riesgos 8

Consideraciones sobre el control 10

Apéndice A. Ejemplos de aplicación práctica 16

Apéndice B. Herramienta de documentación opcional 18

Gobierno de terceras partes 18

Gestión de riesgos de terceras partes 20

Controles de terceras partes 21

Resumen de los Requisitos Temáticos

Los Requisitos Temáticos son un componente esencial del Marco Internacional para la Práctica Profesional®, junto con las Normas Globales de Auditoría Interna™ y las Guías Globales. El Instituto de Auditores Internos exige que los Requisitos Temáticos se utilicen junto con las Normas, que proporcionan la base autorizada de las prácticas requeridas. Las referencias a las Normas aparecen a lo largo de esta guía como una fuente de información más detallada

Los Requisitos Temáticos formalizan cómo los auditores internos abordan las áreas de riesgo prevalentes para promover la calidad y la coherencia dentro de la profesión. Los Requisitos Temáticos establecen una base y proporcionan criterios relevantes para la realización de servicios de aseguramiento relacionados con el tema de un Requisito Temático (Norma 13.4 Criterios de evaluación). La conformidad con los Requisitos Temáticos es obligatoria para los servicios de aseguramiento y recomendada para la evaluación durante los servicios de asesoramiento. Los Requisitos Temáticos no pretenden abarcar todos los aspectos potenciales que deben tenerse en cuenta al realizar trabajos de aseguramiento, sino más bien proporcionar un conjunto mínimo de requisitos que permitan una evaluación coherente y fiable del tema en cuestión.

Los Requisitos Temáticos están claramente vinculados al Modelo de las Tres Líneas del IIA y a las Normas Globales de Auditoría Interna. El gobierno, la gestión de riesgos y los procesos de control son los principales componentes de los Requisitos Temáticos que se ajustan a la Norma 9.1 Comprender los procesos de gobierno, gestión de riesgos y control. En referencia al Modelo de las Tres Líneas, el gobierno se vincula al Consejo/órgano de gobierno, la gestión de riesgos se vincula a la segunda línea, y los controles o procesos de control se vinculan a la primera línea. Mientras que la dirección está representada tanto en la primera como en la segunda línea, la función de Auditoría Interna se representa en la tercera línea como un proveedor de aseguramiento independiente y objetivo, que informa al Consejo/órgano de gobierno (Principio 8 Supervisión del Consejo)

Aplicabilidad, riesgo y criterio profesional

Los Requisitos Temáticos deben cumplirse cuando las funciones de Auditoría Interna realicen trabajos de aseguramiento sobre temas para los que exista un Requisito Temático o cuando se identifiquen aspectos del Requisito Temático en otros trabajos de aseguramiento.

Como se describe en las Normas, la evaluación de los riesgos es una parte importante de la planificación del Director de Auditoría Interna. Determinar los trabajos de aseguramiento a incluir en el Plan de Auditoría Interna requiere evaluar las estrategias, objetivos y riesgos de la organización al menos anualmente (Norma 9.4 Plan de Auditoría Interna). Al planificar trabajos individuales de aseguramiento, los auditores internos deben evaluar los riesgos relevantes para el trabajo (Norma 13.2 Evaluación de riesgos del trabajo).

Cuando el tema de un Requisito Temático se identifica durante el proceso de planificación de auditoría interna basada en riesgos y se incluye en el Plan de Auditoría Interna, entonces los requisitos descritos en el Requisito Temático deben ser utilizados para evaluar el tema dentro de los trabajos aplicables. Además, cuando los auditores internos realicen un trabajo (incluido o no en el Plan) y surjan elementos de un Requisito Temático, deberá evaluarse la aplicabilidad del Requisito Temático como parte del trabajo. Por último, si se solicita un trabajo que no estaba originalmente en el Plan e incluye el tema en cuestión, debe evaluarse la aplicabilidad del Requisito Temático.

El juicio profesional desempeña un papel clave en la aplicación del Requisito Temático. Las evaluaciones de riesgos impulsan las decisiones de los Directores de Auditoría Interna sobre los trabajos que deben incluirse en el Plan de Auditoría Interna (Norma 9.4). Adicionalmente, los auditores internos utilizan su juicio profesional para determinar qué aspectos serán cubiertos dentro de cada trabajo (Normas 13.3 Objetivos y alcance del trabajo, 13.4 Criterios de evaluación, y 13.6 Programa de trabajo).

Deberán conservarse pruebas de que se ha evaluado la aplicabilidad de cada uno de los requisitos del Requisito Temático, incluida una justificación de la exclusión de cualquier requisito que no sea considerado. La conformidad con el Requisito Temático debe documentarse utilizando el juicio profesional de los auditores internos, tal como se describe en la norma 14.6 Documentación de los trabajos.

Aunque el Requisito Temático proporciona una base de procesos de control a considerar, las organizaciones que evalúan el tema de riesgo como muy alto pueden necesitar evaluar aspectos adicionales.

Si la función de auditoría interna no dispone de las competencias necesarias para realizar trabajos sobre un tema de máxima exigencia, el Director de Auditoría Interna debe determinar cómo obtener los recursos y comunicar oportunamente al consejo y a la alta dirección el impacto de las limitaciones y cómo se abordará cualquier déficit de recursos. El Director de Auditoría Interna conserva la responsabilidad última de garantizar la conformidad de la función de Auditoría Interna con los Requisitos Temáticos, independientemente de cómo se obtengan los recursos (Normas 3.1 Competencia, 7.2 Cualificaciones del Director de Auditoría Interna, 8.2 Recursos, 10.2 Gestión de los recursos humanos).

Desempeño, documentación e informes

Al aplicar los Requisitos Temáticos, los auditores internos también deben ajustarse a las Normas, realizando su trabajo de acuerdo con el Dominio V: Desempeño de los Servicios de Auditoría Interna. Las normas del Dominio V describen la planificación de los trabajos (Principio 13 Planificar eficazmente los trabajos), la realización de los trabajos (Principio 14 Ejecución de los trabajos) y la comunicación de los resultados de los trabajos (Principio 15 Comunicar las conclusiones del trabajo y monitorear los planes de acción).

Los Requisitos Temáticos están diseñados para apoyar prácticas de auditoría interna coherentes y de alta calidad. Las leyes locales, las regulaciones, las expectativas de supervisión y otros marcos reconocidos profesionalmente pueden imponer requisitos adicionales o más específicos. Los auditores internos deben comprender y acatar las leyes y/o regulaciones pertinentes a la industria y jurisdicciones en las que opera la organización, incluyendo hacer las divulgaciones requeridas, de acuerdo con la Norma 1.3 Comportamiento legal y ético. Es posible que los auditores internos ya hayan integrado estos requisitos

adicionales en los programas de auditoría y en los procedimientos de comprobación, y deben cotejarlos con el Requisito Temático para garantizar una cobertura adecuada.

La cobertura del Requisito Temático puede documentarse en el Plan de Auditoría Interna o en los papeles de trabajo, basándose en el juicio profesional de los auditores internos. Uno o más trabajos de auditoría interna pueden cubrir los requisitos. Además, puede que no todos los requisitos sean aplicables. Deben conservarse pruebas de que se ha evaluado la aplicabilidad del Requisito Temático, incluida una justificación que explique cualquier exclusión.

Aseguramiento de la Calidad

Las Normas exigen que el Director de Auditoría Interna desarrolle, implemente y mantenga un Programa de Aseguramiento y Mejora de la Calidad que abarque todos los aspectos de la función de Auditoría Interna (Norma 8.3 Calidad). Los resultados deben comunicarse al Consejo y a la Alta Dirección. Las comunicaciones deben informar sobre la conformidad de la función de Auditoría Interna con las Normas y el logro de los objetivos de desempeño.

La conformidad con los Requisitos Temáticos se evaluará en las evaluaciones de calidad.

Terceras partes

Una tercera parte es una persona, grupo o entidad externa con la que una organización ("la organización principal") establece una relación comercial para obtener productos o servicios. La relación puede formalizarse a través de un contrato, acuerdo u otro medio para proporcionar a la organización productos, servicios, mano de obra, fabricación o soluciones informáticas, como almacenamiento, procesamiento y mantenimiento de datos.

> Nota
>
> Los Requisitos Temáticos utilizan la terminología general de auditoría interna definida en las Normas Globales de Auditoría Interna. Los lectores deben consultar los términos y definiciones en el glosario de las Normas.

El término "tercera parte" puede utilizarse de forma diferente en función del sector o de otros contextos. Cada función de Auditoría Interna tiene la flexibilidad de utilizar su criterio en la aplicación del Requisito Temático según cómo la organización principal (la organización que celebra un acuerdo con terceras partes) defina a las terceras partes. En el Requisito Temático sobre Terceras Partes y en la guía de usuario, el término "terceras partes" se refiere a vendedores, proveedores, contratistas, subcontratistas, proveedores de servicios externalizados, otras agencias y consultores. El término "tercera parte" engloba todos los acuerdos de este tipo, incluidos los celebrados entre una tercera parte y sus subcontratistas, a menudo conocidos como subcontratistas "descendentes", o "cuartas partes", "quintas partes" o "enésimas partes"

Este Requisito Temático no pretende abordar las relaciones, intereses o implicaciones externas indirectas con la organización principal, como reguladores, agentes, intermediarios, inversores, fideicomisarios/miembros del consejo, servicios públicos y miembros del público en general, ni las relaciones internas, como empleados o proveedores de servicios intragrupo.

El término "tercera parte" puede definirse y utilizarse de forma diferente en función del sector o de otros contextos. A los auditores internos se les concede flexibilidad y deben basarse en su juicio profesional para adaptar el Requisito Temático a la definición de tercera parte de la organización principal.

La eficacia de los procesos de una organización para gestionar sus relaciones con terceras partes puede evaluarse en toda la organización y/o a nivel de uno o más contratos, acuerdos o relaciones individuales. Los auditores internos deben emplear un enfoque descendente para desarrollar una comprensión de las políticas, procedimientos, procesos, marco y ciclo de vida de terceras partes definidas por la organización. Los auditores internos deben utilizar su juicio para comprender los matices de los riesgos de terceras partes en función de los sectores, las organizaciones y las temáticas de los trabajos. En consonancia con la Norma 5.1 Uso de la información, los auditores internos deben conocer y cumplir las políticas y procedimientos relacionados con la información de terceras partes a la que puedan acceder.

El Requisito Temático se aplica cuando la función de Auditoría Interna realiza trabajos de aseguramiento sobre terceras partes y/o cualquier relación subcontratada, incluidas las de cuarto o ulterior nivel, permitidas por el contrato o acuerdo de la tercera parte con la organización principal. Los auditores internos deben dar prioridad a las terceras partes y a las partes descendentes en función del riesgo, tal y como se describe más adelante en la sección de gestión de riesgos. Los auditores internos deben aplicar todos los requisitos según indiquen los resultados de la evaluación de riesgos, y las exclusiones deben documentarse.

El Requisito Temático sobre Terceras Partes y la guía de usuario hacen referencia a las etapas de la relación de una organización con sus terceras partes, también conocidas como etapas del ciclo de vida: selección, contratación, incorporación, supervisión y desvinculación (dar de baja). Estas etapas se utilizarán a efectos de Requisito Temático sobre Terceras Partes y la guía de usuario, aunque algunas industrias tengan sus propias versiones del ciclo de vida. Las etapas son:

- Selección: incluye procesos para determinar la necesidad de una tercera parte, el plan para su uso y la diligencia debida para la selección. Además, la selección debe incluir la evaluación de los riesgos de terceras partes potenciales y contratadas.
- Contratación: incluye los procesos de diligencia debida para redactar, negociar, aprobar y aplicar un acuerdo legal con la tercera parte.
- Incorporación: comienza cuando se firma el contrato para iniciar la relación y sienta las bases para que las terceras partes cumplan los términos del contrato o acuerdo.
- Supervisión: incluye procesos de gestión "durante la vida útil" y supervisión continua de la tercera parte una vez establecido y aprobado el contrato. El planteamiento suele ser sistemático y basarse en los riesgos, y debe tener en cuenta la mejora continua. El seguimiento incluye la renovación de los contratos o acuerdos en curso con terceras partes cuando sea necesario.
- Desvinculación (dar de baja): incluye procesos para poner fin a contratos y acuerdos, mantener una estrategia de salida para terceras partes que se hayan priorizado en función del riesgo y poner fin a las relaciones cuando sea necesario. Los procesos suelen utilizar un enfoque basado en el riesgo y pueden implicar un plan de salida formal.

La organización principal sigue siendo responsable de los riesgos asociados a la consecución de sus objetivos, incluso cuando contrata a una tercera parte para que le ayude a alcanzar uno o más de esos objetivos. La contratación de terceras partes puede reducir algunos de los costes de la organización para llevar a cabo los procesos. Sin embargo, puede introducir riesgos operativos porque la organización principal tiene menos visibilidad y autoridad sobre los procesos de control de la tercera parte. Si una

tercera parte no cumple lo contratado, participa en prácticas poco éticas o experimenta una interrupción del negocio, la organización principal puede sufrir repercusiones.

La organización principal debe identificar, evaluar y gestionar los riesgos mediante procesos adecuados de gobierno, gestión de riesgos y control. Las categorías y ejemplos de riesgos relacionados con terceras partes incluyen:

- Estratégicos, como la capacidad de cumplir la misión de la organización y/o los objetivos de alto nivel o de gestionar las repercusiones de las fusiones y adquisiciones.
- Reputacionales, como los daños causados al medio ambiente o a la relación y confianza de la organización principal con clientes, consumidores y partes interesadas.
- Éticos, como faltas de integridad, conflictos de intereses, sobornos y corrupción.
- Operacionales, como la seguridad física y de la información, el riesgo por actores internos, las interrupciones del servicio y la no consecución de los objetivos.
- Financieros, como la insolvencia de terceras partes y el fraude.
- Cumplimiento de los requisitos regulatorios locales, nacionales e internacionales aplicables.
- Ciberseguridad y otros tipos de protección de datos, como la filtración de datos sensibles o que éstos se encuentren comprometidos.
- Tecnologías de la información, como la falta de servicios de apoyo a operaciones críticas.
- Jurídicos, como conflictos de interés, disputas y litigios por incumplimiento de contratos.
- Sostenibilidad medioambiental, social y de gobierno. Algunos ejemplos son los riesgos relacionados con el impacto de una organización en el entorno natural y los riesgos relativos a las interacciones de una organización con las comunidades.
- Geopolíticos, como disputas comerciales/sanciones e inestabilidad política.

Los auditores internos deben tener en cuenta cada etapa del ciclo de vida de las terceras partes al evaluar los requisitos de los procesos de gobierno, gestión de riesgos y control.

Los requisitos del Requisito Temático sobre Terceras Partes se dividen en tres secciones de acuerdo con la Norma 9.1 Comprender los Procesos de gobierno, gestión de riesgos y control:

- Gobierno: objetivos y estrategias básicos claramente definidos para utilizar a terceras partes en apoyo de los objetivos, políticas y procedimientos de la organización.
- Gestión de riesgos: procesos para identificar, analizar, gestionar y supervisar los riesgos de recurrir a terceras partes, incluido un proceso para escalar los incidentes con prontitud.
- Controles: procesos de control establecidos por la dirección y evaluados periódicamente para mitigar los riesgos cuando se recurre a terceras partes.

Además del Requisito Temático y de esta guía de usuario, los auditores internos pueden consultar orientaciones profesionales adicionales sobre terceras partes, como las Guías Globales del MIPP y recursos específicos de la industria.

Consideraciones

Las siguientes consideraciones pueden ayudar a los auditores internos a aplicar los requisitos del Requisito Temático sobre Terceras Partes. Las afirmaciones con letras en cada sección a continuación reafirman o parafrasean los requisitos correspondientes del Requisito Temático. Estas consideraciones no obligatorias son ilustrativas para ofrecer ejemplos de formas de evaluar los requisitos. Los auditores internos deben aplicar su juicio profesional a la hora de determinar qué incluir en sus evaluaciones.

Consideraciones sobre el Gobierno

Para evaluar cómo se aplican los procesos de gobierno, incluida la supervisión del consejo, a los objetivos de terceras partes, los auditores internos pueden revisar pruebas de:

A. Un enfoque o estrategia formalizados y documentados basados en el riesgo para determinar si se debe recurrir a una tercera parte. El planteamiento se revisa periódicamente e incluye:

- Un proceso claramente definido y normalizado para aplicar el enfoque, aprobado por la organización para su uso.
- Recursos presupuestados basados en un análisis coste-beneficio para justificar la contratación de una tercera parte, garantizando la alineación estratégica y la eficiencia de los recursos.
- Evaluación por la dirección de los riesgos y controles, incluidos los relativos a cuestiones con terceras partes.
- Recursos adecuados para contratar, gestionar y supervisar el rendimiento de terceras partes.
- La integración de las opiniones de las partes interesadas en el planteamiento o la estrategia.

B. Políticas, procedimientos y otra documentación pertinente utilizada para definir, evaluar y gestionar las relaciones con terceras partes a lo largo del ciclo de vida. Las políticas y procedimientos pueden incluir:

- Herramientas y plantillas normalizadas para facilitar los procesos clave de gobierno, gestión de riesgos y control.
- Procesos para evaluar periódicamente las políticas y procedimientos, determinar su adecuación y actualizarlos en caso necesario.
- Establecimiento de criterios para seleccionar, contratar, incorporar, supervisar y desvincular (dar de baja) a terceras partes.
- La identificación y revisión periódica de los requisitos reglamentarios aplicables para alinearlos con las políticas y procedimientos.
- Realización de ejercicios de evaluación comparativa para identificar y comparar las principales prácticas de gestión de terceras partes.

C. Funciones y responsabilidades definidas que apoyan la consecución de los objetivos de terceras partes. Otras pruebas pueden ser:

- Procesos para evaluar si los valores, la ética y la responsabilidad social corporativa de la tercera parte coinciden con los principios de la organización principal. El proceso debe incluir cómo abordar con prontitud posibles conflictos de intereses o prácticas poco éticas.
- Formación regular del personal que desempeña funciones de gestión de terceras partes y evaluación periódica de sus competencias.
- Un proceso para evaluar si se ha impartido formación para concienciar a toda la organización sobre terceras partes.
- Las funciones y responsabilidades se ajustan al Modelo de las Tres Líneas.

D. Comunicación y compromiso oportunos con las partes interesadas pertinentes a lo largo de todo el ciclo de vida de la tercera parte (por ejemplo, el consejo, la alta dirección, la contratación, las operaciones, la gestión de riesgos, el cumplimiento, el departamento jurídico, la tecnología de la información, la seguridad de la información, los recursos humanos y otros), lo que incluye:

- Información sobre riesgos de terceras partes y vulnerabilidades potenciales conocidas en actas de reuniones, informes o correos electrónicos.
- Intercambio de información sobre la gestión de terceras partes y fomento de la colaboración (por ejemplo, mediante reuniones periódicas interfuncionales).

Consideraciones sobre la gestión de riesgos

Para evaluar cómo se aplican los procesos de gestión de riesgos a los objetivos de terceras partes, los auditores internos pueden revisar evidencias de que:

A. Los procesos estandarizados y exhaustivos de gestión de riesgos para el usuario de servicios de terceras partes incluyen funciones y responsabilidades definidas y abordan suficientemente los riesgos clave relevantes para la organización:

- Los procesos de evaluación y gestión de los riesgos de terceras partes incluyen el modo en que se evalúan los riesgos clave:
  - Inicialmente identificado e informado
  - Analizados para evaluar su impacto en la capacidad de alcanzar los objetivos de la organización
  - Mitigado, incluyendo planes de acción para reducir el riesgo a un nivel aceptable.
  - Supervisado, incluida la detección y respuesta a las alertas tempranas y un plan de información continua hasta que las amenazas se hayan resuelto por completo.
- Se supervisa el cumplimiento de los procesos y la aplicación de medidas correctoras en caso de desviaciones, para evitar socavar los objetivos o la estrategia a largo plazo de la organización.
- Un comité de gestión de riesgos u otro grupo se encarga de la supervisión directa de terceras partes y de las aportaciones al consejo. El comité tiene un objetivo definido y se reúne periódicamente. Las pruebas pueden incluir las actas de las reuniones.

B. Los riesgos relacionados con terceras partes a lo largo del ciclo de vida se identifican y evalúan periódicamente. La evaluación de riesgos clasifica y prioriza a las terceras partes. Las respuestas a los riesgos se clasifican y priorizan.

- La organización principal tiene en cuenta factores como su tamaño, madurez y número de terceras partes contratadas a la hora de desarrollar una evaluación de riesgos de terceras partes.
- La evaluación de riesgos está documentada e identifica los riesgos inherentes y residuales.
- La organización sigue un proceso de diligencia debida para revisar y actualizar la evaluación de riesgos.
- Se establecen criterios para clasificar y priorizar a las terceras partes en función de los riesgos. Algunos ejemplos de estos criterios son:
  - Los servicios prestados son fundamentales para el funcionamiento de la organización.
  - El valor financiero del acuerdo es importante.
  - La relación es nueva, se inicia rápidamente y/o su duración es larga.
  - Intervienen varias partes externas.
  - La tercera parte tiene previsto subcontratar parte o la totalidad del trabajo.
- La organización se adhiere a prácticas de evaluación de riesgos ampliamente aceptadas, incluyendo que la evaluación de riesgos se realice en la fase más temprana posible, normalmente cuando se analiza la propuesta durante la fase de selección, y antes de la incorporación.
- Los proveedores rellenan un cuestionario para determinar su clasificación y prioridad en función de los riesgos inherentes. La organización se asegura de que los cuestionarios son cumplimentados por el personal pertinente y son revisados para garantizar su exactitud.
- La organización obtiene información periódica sobre la gestión de riesgos de terceras partes de áreas funcionales, como tecnología de la información, compras, gestión de riesgos empresariales, recursos humanos, jurídico, cumplimiento, operaciones, contabilidad y finanzas.

C. Las respuestas al riesgo, como mitigación, aceptación, eliminación y reparto, se identifican y son proporcionales a la clasificación del riesgo.

- Las respuestas a los riesgos se documentan e incluyen la consideración del entorno de control de la tercera parte.
- Documentación de que las respuestas a los riesgos que superan la tolerancia al riesgo de la organización principal se revisan para comprobar su idoneidad, especialmente cuando se aceptan los riesgos. Las respuestas incluyen las relativas a posibles conflictos de intereses con terceras partes.

D. Los procesos para gestionar y escalar los riesgos de terceras partes, incluyendo cómo se evalúa, asigna y prioriza el nivel de amenaza o riesgo. La revisión puede incluir la identificación de:

- Definiciones y explicaciones de los niveles de riesgo de la organización -como alto, moderado y bajo- y procedimientos de escalado para cada categoría de riesgo.
- Lista de terceras partes priorizadas por riesgos identificados y el estado de mitigación de cualquier evento de riesgo
- Requisitos legales, reglamentarios y de cumplimiento aplicables
- Impacto de los riesgos, tanto financieros como no financieros (por ejemplo, reputación)
- Procesos para comunicar los riesgos de terceras partes a la dirección y a los empleados, incluida la información periódica del perfil de riesgo al consejo (u otro órgano apropiado). Las comunicaciones deben incluir actualizaciones sobre la corrección de cualquier problema observado con terceras partes prioritarias.
- Procesos para reevaluar la clasificación y el establecimiento de prioridades cuando cambien el apetito de riesgo y los niveles de tolerancia al riesgo de la organización principal.

Consideraciones sobre el control

Para evaluar cómo se aplican los procesos de control a las relaciones con terceras partes, los auditores internos pueden revisar pruebas de que:

A. Existe un sólido proceso de diligencia debida para la contratación y selección de terceras partes, con un estudio de viabilidad documentado y aprobado u otra documentación pertinente que describa y justifique la necesidad y la naturaleza de la relación con la tercera parte.
    - El caso de negocio también puede:
        - Abordar los riesgos para la capacidad de la tercera parte de cumplir las expectativas y las posibles repercusiones para la organización.
        - Incluir un análisis detallado de costes y beneficios.
    - Se siguen los procesos de contratación establecidos, como licitaciones, solicitudes de propuestas y contratación única. Los procesos incluyen:
        - Criterios para aspectos importantes, como la revisión de protocolos de ciberseguridad, la verificación de datos bancarios, la comprobación de antecedentes financieros y la investigación de la estructura organizativa de la tercera parte, sus antecedentes penales y legales, su historial de conducción, sus actividades políticas y sus vínculos con actividades delictivas.
        - Criterios de selección bien definidos que incluyan la evaluación de los resultados anteriores, las referencias, la reputación y los costes del contrato.
        - Diligencia debida para garantizar la selección adecuada de los proveedores, como la formación de equipos interfuncionales para revisar las propuestas. Para mitigar el riesgo de parcialidad, los controles de los equipos de revisión incluyen procedimientos para la creación de equipos y requisitos para la divulgación de posibles conflictos de intereses.
        - Diligencia debida en la evaluación del entorno de control de la tercera parte; por ejemplo, realizando una visita a las instalaciones o revisando los siguientes aspectos en relación con la tercera parte:

- Informes de control de sistemas y organizaciones (SOC).
- Estabilidad financiera.
- Escritura de constitución o certificado de vigencia.
- Transparencia en la toma de decisiones de los principales directivos y partes interesadas.
- Estructura organizativa.
- Estabilidad operativa.
- Protocolos de ciberseguridad.
- Cumplimiento de las leyes, regulaciones y normas pertinentes.
- Ética.
- Historial con la organización principal.
- Reputación.

o Pruebas de que los posibles vendedores o contratistas sólo pasan a la fase de contratación del ciclo de vida después de que se hayan llevado a cabo los procesos de diligencia debida pertinentes y se hayan analizado los resultados.

B. Se establecen y aplican políticas y procedimientos de contratación.

- Los contratos se redactan en términos inequívocos.
- Los principales riesgos se tienen en cuenta durante la fase de redacción del contrato y se incluyen las cláusulas pertinentes. En esta fase se comunican a la tercera parte las cuestiones que deben resolverse.
- Los elementos esenciales de los contratos se determinan en función de las políticas y procedimientos de contratación de la organización y del nivel de prioridad de la tercera parte. Los elementos pueden incluir:
  - Acuerdos de confidencialidad (privacidad).
  - Cláusulas de rescisión y parámetros definidos para el acceso a los datos.
  - Requisitos de ciberseguridad, incluidos los de acceso y puesta en común de todos los datos y notificación de incidentes o violaciones en un plazo determinado.
  - Requisitos para las notificaciones de una violación que afecte a los datos de la organización principal.
  - Un proceso estandarizado para verificar la identificación de la tercera parte, incluido su nombre legal completo, dirección, ubicación(es) física(s) y sitio web. Una práctica habitual es utilizar una lista de comprobación durante el proceso de identificación y revisar la exactitud de la información.
  - Acuerdos de nivel de servicio claramente definidos, en los que se especifiquen los resultados esperados y los derechos, obligaciones, penalizaciones, recompensas y responsabilidades de cada parte, incluida la responsabilidad de pagar los costes laborales (incluidos los subcontratistas posteriores).

- Una cláusula de derecho de auditoría que incluya a los subcontratistas en sentido descendente, o la exigencia de pruebas de que un proveedor de aseguramiento independiente y acreditado ha auditado a las partes. Sin una cláusula de derecho de auditoría, la capacidad de la función de auditoría interna para obtener o proporcionar garantías puede verse limitada.

- La organización principal tiene acceso a los informes de evaluación de control de los auditores independientes; por ejemplo, los relativos a la seguridad financiera, de cumplimiento y de los datos, como los informes de las Normas Internacionales sobre Encargos de Aseguramiento o SOC.
  - Si se confía en el trabajo de los proveedores de aseguramiento externos de la tercera parte, se revisan los documentos para garantizar su fiabilidad.
  - Los informes SOC se utilizan para identificar procesos inadecuados de gestión de riesgos y cambios.

- Las políticas y procedimientos abordan cualquier componente esencial para organizaciones o tipos de contratos específicos:
  - Cláusulas medioambientales y de sostenibilidad.
  - Protocolos de denuncia de irregularidades.
  - Requisitos para las evaluaciones de las medidas de desempeño.
  - Comprobación del plan de continuidad de la actividad para terceras partes.
  - Utilización de la inteligencia artificial en la prestación de servicios.
  - Identificación, divulgación, condiciones y alcance claros de cualquier trabajo subcontratado.
  - Proceso de gestión de cambios, que describe cómo gestionar los cambios en el alcance, las condiciones o los requisitos operativos (como cambios en la tecnología o actualizaciones normativas) durante la vigencia del contrato.
  - Límites en el número de órdenes de cambio o importes que pueden facturarse.

- Las políticas y procedimientos exigen la aceptación formal de los productos finales antes de efectuar el pago o liberar cualquier retención.

- Las terceras partes deben compartir sus políticas éticas o código de conducta y/o adherirse a los de la organización principal.

- Cuando la tercera parte proporciona el contrato, la organización principal ha llevado a cabo una revisión legal, y los riesgos clave se comprenden y se apoyan en una estrategia adecuada de mitigación de riesgos.

C. Los contratos o acuerdos finalizados son revisados y aprobados por las partes interesadas pertinentes, incluidos el departamento jurídico y el de cumplimiento normativo, se conservan de forma segura y se asignan a un gestor o administrador de contratos para que asuma su responsabilidad.

- Un contrato u otro documento oficial que establezca una relación de externalización y la obligación de la tercera parte, y pruebas de cualquier revisión legal y de cumplimiento exigida.

D. Se mantiene un listado preciso, completo y actualizado de todas las relaciones con terceras partes, por ejemplo, en un sistema centralizado de gestión de contratos.

- Un proceso para añadir nuevos contratos o acuerdos con terceras partes al listado o al sistema.
- Un proceso para introducir posibles terceras partes en el sistema de proveedores y eliminarlos si no se aprueba el contrato.
- Un proceso para eliminar contratos o acuerdos de terceras partes de la lista o del sistema.
- Un sistema de seguimiento para documentar problemas con contratistas o proveedores concretos para futuras consultas.
- Un proceso de revisión para determinar si la población de terceras partes es exacta y completa.

E. Se establecen y siguen procesos de incorporación documentados para que las terceras partes puedan cumplir las condiciones del contrato o acuerdo. Las revisiones pueden incluir la verificación de si:

- Los procedimientos normalizados de incorporación garantizan que se complete toda la documentación, formación y revisiones de cumplimiento necesarias.
- Los sistemas y procesos de la tercera parte pueden integrarse perfectamente con la tecnología de la organización principal.
- Los sistemas compartidos son compatibles y seguros. Las pruebas pueden incluir controles complementarios de la entidad usuaria como parte de los informes SOC.
- La organización principal evalúa los planes de continuidad de la actividad de la tercera parte, que garantizan la continuidad del servicio en caso de emergencia. Se incluyen planes de contingencia para hacer frente a posibles perturbaciones.

F. Procesos para la supervisión continua del desempeño del proveedor en relación con los objetivos del contrato o acuerdo, incluidas las evaluaciones de los indicadores clave de desempeño.

- Los procesos de supervisión informan la evaluación de riesgos de terceras partes, y las deficiencias de control identificadas se revisan, se elevan y se abordan según sea necesario.
- Informes u observaciones de los procesos, tecnologías y herramientas establecidos para gestionar la supervisión en tiempo real.
- Procesos para garantizar que los pagos se realizan de acuerdo con los términos del contrato o acuerdo, como el cumplimiento de los plazos del proyecto, los hitos y los requisitos de comunicación. Los pagos sólo se efectúan a los contratistas autorizados que han completado la fase de incorporación y han sido introducidos en el sistema de pago a proveedores. Cuando los entregables se especifican en el contrato, los pagos finales sólo se realizan una vez que se han verificado los entregables.

- Seguimiento para controlar los costes asociados a los acuerdos con terceras partes para garantizar el valor y determinar el rendimiento de la inversión. Los resultados de los análisis coste-beneficio se utilizan para renegociar los contratos.
- Procesos para evaluar las sanciones por incumplimiento de cualquier acuerdo de nivel de servicio en el contrato o acuerdo. Las sanciones se calculan y cobran cuando se producen.
- La clasificación de terceras partes prioritarias basada en el riesgo se reevalúa periódicamente, cuando se producen cambios en un acuerdo y cuando un contrato está próximo a su vencimiento o renovación automática.
- Revisiones de terceras partes prioritarias, como revisiones empresariales in situ o trimestrales, para validar los controles y la integridad operativa.
- Entre las pruebas de supervisión continua adicional pueden figurar:
  - Análisis de la estabilidad financiera de la tercera parte.
  - Evaluación de reclamaciones contra terceras partes.
  - Revisiones por parte de la dirección de informes de auditores independientes, como la Norma Internacional sobre Trabajos de Aseguramiento, las Declaraciones sobre Normas para Trabajos de Atestiguamiento, informes financieros, de auditoría, de cumplimiento y de seguridad de datos proporcionados por terceras partes; certificaciones ISO.
  - Las revisiones por parte de la dirección de las pruebas de resistencia empresarial realizadas por la tercera parte, incluidos los problemas significativos identificados.
  - Condiciones y restricciones para el uso de subcontratados o subcontratistas.
  - Evaluaciones de los valores éticos, la cultura y la conducta de terceras partes.
  - Respuestas a preguntas de los medios de comunicación.
  - Evaluaciones de los protocolos de privacidad y ciberseguridad para proteger el almacenamiento y la transferencia de datos e información de la organización principal, incluido el uso de tecnologías avanzadas como la inteligencia artificial.
  - La identificación por parte de la organización de oportunidades para la mejora continua del desempeño y el cumplimiento de los objetivos del contrato o acuerdo.
  - Revisión de la segregación de funciones.

G. Protocolos para iniciar acciones correctivas sobre incidentes identificados cuando una tercera parte no cumple los requisitos de un contrato o acuerdo, o si las acciones de terceras partes aumentan el riesgo para la organización principal.

- Protocolos de escalado de incidentes basados en la gravedad del incidente y la prioridad de la tercera parte.
- Revisión posterior al incidente, incluido el análisis de la causa raíz.

H. Procesos para proporcionar alertas de contratos y acuerdos que se acercan a su vencimiento o renovación automática. Los procesos de renovación automática incluyen la revisión de:

- La actuación de la tercera parte.
- Condiciones del contrato o acuerdo y posibles cláusulas adicionales.
- Factores de riesgo.

I. Se aplica y se sigue un plan formalizado de desvinculación para garantizar que los requisitos contractuales relativos a plazos y expectativas se abordan adecuadamente, incluso para los subcontratistas posteriores.

- Listas de comprobación o entrevistas con las principales partes interesadas para garantizar la eficacia de las medidas de seguridad.
- Se ha devuelto o destruido información o datos organizativos bajo custodia de terceras partes.
- Se ha revocado el acceso de la tercera parte a los datos, sistemas o instalaciones de la organización.
- Se han devuelto los activos de la organización principal, como dispositivos, licencias de software, propiedad intelectual y documentación.
- Cuando se despide a una tercera parte por causa justificada, se identifican las circunstancias atenuantes o los riesgos y se elevan a la alta dirección y/o al consejo.
- Cuando se rescinde el contrato de una tercera parte prioritaria, se le sustituye sobre la base de la misma evaluación de riesgos, a menos que el contrato haya finalizado o ya no sea necesario.

Apéndice A. Ejemplos de aplicación práctica

Los siguientes ejemplos describen escenarios en los que sería aplicable el Requisito Temático sobre Terceras Partes:

Ejemplo 1: Un trabajo de auditoría interna del Plan de Auditoría Interna incluye un servicio o resultado que actualmente presta una tercera parte.

Cuando la función de Auditoría Interna complete su proceso de planificación basado en el riesgo e incluya uno o más trabajos en el Plan de Auditoría Interna de servicios o productos que actualmente son prestados por terceras partes en virtud de un contrato o acuerdo, se exigirá el Requisito Temático.

No todas las exigencias del Requisito Temático pueden aplicarse en todos los trabajos. Cuando los auditores internos apliquen su juicio profesional y determinen que uno o más requisitos del Requisito Temático sobre Terceras Partes no son aplicables y, por lo tanto, deben excluirse de un trabajo, los auditores internos deben documentar y conservar la justificación para excluir dichos requisitos. Por ejemplo, la razón para excluir ciertos requisitos podría ser que la función de Auditoría Interna haya determinado que el nivel de dependencia de la organización hacia terceras partes para servicios críticos es baja, o que se trata de una relación establecida con escaso impacto financiero.

Ejemplo 2: Los riesgos de terceras partes se identifican durante un trabajo de aseguramiento sobre un tema distinto de terceras partes o gestión de contratos.

Los auditores internos pueden identificar un riesgo significativo de terceras partes al evaluar un proceso que inicialmente no se había determinado que estuviera relacionado con terceras partes o con la gestión de contratos. Por ejemplo, al planificar un trabajo para evaluar el almacenamiento de datos, los auditores internos se enteran de que los servicios en la nube se alojan a través de una tercera parte. Durante las entrevistas con la dirección de los servicios prestados por terceras partes, los auditores internos identifican riesgos de ciberseguridad relacionados con la tercera parte.

Una vez identificados los riesgos relevantes, los auditores internos deben revisar tanto el Requisito Temático sobre Terceras Partes como el de Ciberseguridad y determinar qué requisitos de éstos son aplicables. Los auditores internos pueden excluir el proceso de gobierno de terceras partes o el proceso de gestión de riesgos de terceras partes del alcance del trabajo y centrarse en los controles de terceras partes sobre los servicios auditados. Este mismo juicio profesional se aplica a la aplicación del Requisito Temático de Ciberseguridad. Los auditores internos deben documentar, en los papeles de trabajo del trabajo de auditoría, la justificación de la exclusión de cualquier requisito de los Requisitos Temáticos sobre terceras partes o ciberseguridad y conservar la documentación.

Ejemplo 3**:** Se necesita un trabajo de terceras partes que no estaba incluido originalmente en el Plan de Auditoría Interna.

Surge un problema en la organización relacionado con una tercera parte prioritaria que requiere la atención inmediata de la función de Auditoría Interna. Se trataba de un fallo de control. El Director de Auditoría Interna debe comunicarse con el consejo para replantear las prioridades del Plan de Auditoría Interna y los recursos de la función de Auditoría Interna a fin de adaptarse a la necesidad. El auditor interno debe comprometerse con la dirección afectada a desarrollar objetivos del trabajo para evaluar la situación y hacer recomendaciones para prevenir futuras incidencias. El Directo de Auditoría Interna debe revisar los Requisitos Temáticos para delimitar el alcance del trabajo, determinar qué requisitos son de aplicación y documentar las exclusiones en consecuencia.

Apéndice B. Herramienta de documentación opcional

Se espera que los auditores internos ejerzan su juicio profesional para determinar la aplicabilidad de los requisitos, basándose en la evaluación de riesgos y documenten adecuadamente las exclusiones de determinados requisitos. El Requisito Temático puede documentarse en el Plan de Auditoría Interna o en los papeles de trabajo del trabajo de auditoría basándose en el juicio profesional del auditor interno. Uno o más trabajos de auditoría interna pueden cubrir los requisitos. Además, puede que no todos los requisitos sean aplicables. El formulario imprimible que figura a continuación ofrece una opción para documentar la conformidad con el Requisito Temático sobre Terceras Partes, pero su uso no es obligatorio.

Gobierno de terceras partes

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
A. Se establece, aplica y revisa periódicamente un planteamiento formal para determinar si se contrata a una tercera parte. El enfoque incluye criterios apropiados para definir y evaluar los recursos necesarios y disponibles para cumplir los objetivos mediante el suministro de un producto o servicio.		
B. Se establecen políticas y procedimientos para definir, evaluar y gestionar las relaciones y los riesgos con terceras partes a lo largo de todo el ciclo de vida de éstas. Las políticas y procedimientos se ajustan a los requisitos normativos aplicables y se revisan y actualizan periódicamente para reforzar el entorno de control.		

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
C. Se definen las funciones y responsabilidades de gestión de terceras partes de la organización, detallando quién selecciona, dirige, gestiona, se comunica con y supervisa a las terceras partes, y quién debe estar informado sobre las actividades de éstas. Existe un proceso para garantizar que las personas asignadas a funciones y responsabilidades sobre terceras partes tienen las competencias adecuadas.		
D. Se definen protocolos de comunicación con las partes interesadas pertinentes, que incluyen la información puntual sobre el estado de los resultados, los riesgos y el cumplimiento (en concreto, las infracciones de leyes y reglamentos) de las terceras partes prioritarias. Se da prioridad a las terceras partes en función del riesgo. Las partes interesadas pueden ser el consejo de administración, la alta dirección, los departamentos de compras, operaciones, gestión de riesgos, cumplimiento, jurídico, tecnologías de la información, seguridad de la información, recursos humanos y otros.		

Gestión de riesgos de terceras partes

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
A. Los procesos para la gestión de riesgos de terceras partes y sus servicios están estandarizados y son exhaustivos, incluyen funciones y responsabilidades definidas y abordan suficientemente los riesgos clave relevantes para la organización (como los estratégicos, de reputación, éticos, operativos, financieros, de cumplimiento, de ciberseguridad, de tecnologías de la información, jurídicos, de sostenibilidad y geopolíticos). Se supervisa el cumplimiento de los procesos y se aplican medidas correctoras para cualquier desviación.		
B. Los riesgos relacionados con terceras partes a lo largo del ciclo de vida se identifican y evalúan periódicamente. La evaluación de riesgos se utiliza para clasificar y priorizar a terceras partes, incluidos los descendentes. También se clasifican y priorizan las respuestas a los riesgos. La evaluación de riesgos se revisa y actualiza periódicamente.		
C. Las respuestas a los riesgos son adecuadas y precisas, acordes con la clasificación. Las respuestas a los riesgos se aplican, revisan, aprueban, monitorean, evalúan y ajustan según sea necesario.		
D. Existen procesos para gestionar y elevar, en caso necesario, los problemas que surjan de terceras partes, garantizando la responsabilidad de los resultados y aumentando la probabilidad de cumplir los términos de los contratos u otros acuerdos. Si una tercera parte no responde a las preocupaciones planteadas, existen procesos para que la dirección evalúe los riesgos de su relación comercial en curso y adopte nuevas medidas, remedie la situación o ponga fin a la relación, según proceda.		

Controles de terceras partes

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
A. Existe un sólido proceso de diligencia debida para la contratación y selección de terceras partes, con un estudio de viabilidad documentado y aprobado u otro documento pertinente que describa y justifique la necesidad y la naturaleza de la relación con la tercera parte.		
B. La contratación y aprobación se realizan de acuerdo con las políticas y procedimientos de gestión de riesgos de la organización sobre terceras partes e incluyen la colaboración entre los actores implicados dentro de la organización.		
C. Los contratos o acuerdos finales son revisados y aprobados por todas las partes interesadas, incluidos el departamento jurídico y el de cumplimiento normativo, firmados por personas autorizadas de ambas partes y conservados de forma segura. Se asigna a un gestor o administrador de contratos la responsabilidad de cada contrato.		
D. Se mantiene un listado preciso, completo y actualizado de todas las relaciones con terceras partes, por ejemplo, en un sistema centralizado de gestión de contratos.		
E. Se establecen y siguen procesos de incorporación documentados para sentar las bases para que las terceras partes cumplan las condiciones del contrato o acuerdo.		

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
F. Existen procesos de supervisión continua para evaluar si las terceras partes actúan de acuerdo con los términos del contrato o acuerdo durante todo el ciclo de vida y si las terceras partes cumplen sus obligaciones contractuales. Los procesos incluyen la verificación de la fiabilidad de la información facilitada y la reevaluación periódica de los resultados y siempre que cambie el acuerdo.		
G. Se establecen protocolos para iniciar acciones correctivas si una tercera parte no cumple las expectativas o plantea un riesgo mayor o inesperado. Los protocolos incluyen el escalado de incidentes en función de su gravedad, la realización de revisiones posteriores a los incidentes y el análisis de su causa raíz.		
H. Se supervisan las fechas de vencimiento y renovación de los contratos, y se adoptan las medidas de renovación necesarias.		
I. Se pone en marcha y se sigue un plan formalizado de desvinculación para garantizar que se abordan adecuadamente los requisitos contractuales relativos a plazos y expectativas. Los procesos incluyen aspectos cómo: • Dar de baja a la tercera parte. • Sustituir a la tercera parte si es necesario. • Reasignar la custodia y devolver o destruir los datos sensibles de la organización conservados por la tercera parte. • Revocar el acceso de la tercera parte a los sistemas, herramientas e instalaciones de la organización principal.		

Acerca del Instituto de Auditores Internos

El IIA® es una asociación profesional internacional que cuenta con más de 265.000 miembros en todo el mundo y ha concedido más de 200.000 certificaciones Certified Internal Auditor® (CIA®) en todo el mundo. Establecido en 1941, The IIA es reconocido en todo el mundo como líder de la profesión de auditoría interna con respecto a las normas, certificaciones, educación, investigación y orientación técnica. Para más información puede visitar: theiia.org.

Descargo de responsabilidad

El IIA publica este documento con fines informativos y educativos. Este material no pretende dar respuestas definitivas a circunstancias individuales específicas y, como tal, sólo pretende servir de guía. El IIA recomienda buscar asesoramiento experto independiente relacionado directamente con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Copyright

Septiembre de 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101