Terceras Partes

Topical Requirement

Requisito Temático

The Institute of Internal Auditors

Traducción al Español Auspiciada por:

Instituto de Auditores Internos de España

FLAI Fundación Latinoamericana de Auditores Internos

Requisito Temático sobre Terceras Partes

El Marco Internacional para la Práctica Profesional (International Professional Practices Framework®), comprende las Normas Globales de Auditoría Interna (Global Internal Audit Standards™), los Requisitos Temáticos y las Guías Globales. Los Requisitos Temáticos son obligatorios y deben utilizarse junto con las Normas, que proporcionan la base autorizada para las prácticas requeridas.

Los Requisitos Temáticos proporcionan expectativas claras para los auditores internos mediante el establecimiento de una base mínima para la auditoría de temas específicos de riesgo. El perfil de riesgo de la organización puede requerir que los auditores internos consideren aspectos adicionales del tema abordado.

La conformidad con los Requisitos Temáticos aumentará la consistencia con la que se prestan los servicios de auditoría interna y mejorará la calidad y fiabilidad en los servicios y resultados de auditoría interna. En última instancia, los Requisitos Temáticos elevan la profesión de auditoría interna.

Los auditores internos deben aplicar los Requisitos Temáticos en conformidad con las Normas Globales de Auditoría Interna. La conformidad con los Requisitos Temáticos es obligatoria para los servicios de aseguramiento y recomendada para los servicios de asesoramiento. El Requisito Temático es aplicable cuando el tema en cuestión corresponde a una de las siguientes situaciones:

1. Es el objeto de un trabajo incluido en el plan de auditoría interna.
2. Se ha identificado durante la ejecución de un trabajo.
3. Es objeto de una solicitud de trabajo que no figura en el plan de auditoría interna original.

Deben documentarse y conservarse pruebas de que se ha evaluado la aplicabilidad de cada exigencia del Requisito Temático. Es posible que no todos los requisitos individuales se apliquen en todos los trabajos; si se excluyen requisitos, deberá documentarse y conservarse una justificación. La conformidad con los Requisitos Temáticos es obligatoria y se evaluará durante 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 mediante un contrato, un acuerdo u otros medios. Este Requisito Temático utiliza el término "tercera parte" para referirse a vendedores, proveedores, contratistas, subcontratistas, proveedores de servicios externalizados, otras agencias y consultores. El término incluye los acuerdos entre la tercera parte y sus subcontratistas, a menudo conocidos como subcontratistas "descendentes".

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 indicados por los resultados de la evaluación de riesgos, y las exclusiones deben documentarse.

Este Requisito Temático no pretende abordar las relaciones, intereses o implicaciones externas indirectas con la organización principal, como reguladores, agentes, fideicomisarios/miembros del consejo de administración, ni las relaciones internas, como empleados.

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 organización principal (la organización que suscribe un acuerdo con una tercera parte) 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 varios de esos objetivos. Trabajar con terceras partes introduce riesgos que deben identificarse, evaluarse y gestionarse mediante procesos adecuados de gobierno, gestión de riesgos y control, tal y como se indica en este Requisito Temático. 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. Las categorías y ejemplos de riesgos relacionados con terceras partes incluyen:

- Estratégicos, como la capacidad de cumplir la misión de la organización principal 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 estos 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.

El ciclo de vida de una tercera parte consiste en seleccionarla, contratarla, incorporarla, supervisarla y desvincularla (darla de baja). Los auditores internos deben tener en cuenta estas etapas al evaluar los requisitos de los procesos de gobierno, gestión de riesgos y control.

Evaluación y valoración de los procesos de gobierno, gestión de riesgos y procesos de control de terceras partes

Este Requisito Temático proporciona un enfoque consistente y exhaustivo para evaluar el diseño y la aplicación de los procesos de gobierno, gestión de riesgos y control de terceras partes. Los requisitos representan una base mínima para la evaluación.

GOBIERNO

Requisitos:

Los auditores internos deben evaluar los siguientes aspectos del gobierno de terceras partes por parte de la organización principal, incluida la supervisión del consejo:

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.

C. Se definen las funciones y responsabilidades de la organización sobre la gestión de terceras partes, detallando quién selecciona, dirige, gestiona, se comunica con ellas y las supervisa, 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 regulaciones) de las terceras partes prioritarias. Se priorizan 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 y recursos humanos, entre otros.

GESTIÓN DE RIESGOS

Requisitos:

Los auditores internos deben evaluar los siguientes aspectos de la organización en cuanto a la gestión de riesgos de terceras partes:

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. Se identifican y evalúan periódicamente los riesgos relacionados con terceras partes a lo largo de su ciclo de vida. La evaluación de riesgos se utiliza para clasificar y priorizar a las terceras partes, incluidas las 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 de terceras partes que surjan, 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

Requisitos:

Los auditores internos deben evaluar los siguientes controles para las terceras partes priorizadas por riesgo. La evaluación debe incluir los procesos de la dirección de la organización para la evaluación y supervisión continuas de las terceras partes.

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 la organización para la gestión de riesgos de terceras partes e incluyen la colaboración entre las partes apropiadas 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.

F. Existen procesos de supervisión continua para evaluar si las terceras partes actúan de acuerdo con los términos del contrato o acuerdo a lo largo del 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.

Copyright

Septiembre de 2025

The Institute of Internal Auditors

Sede mundial
Instituto de Auditores Internos
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, EE.UU.
Teléfono: +1-407-937-1111
Fax: +1-407-937-1101