Requisito Temático sobre Terceras Partes

Public Consultation Draft

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 sobre los temas. La conformidad con los Requisitos Temáticos aumentará la consistencia con la que se prestan los servicios de auditoría interna y mejorará la calidad y confiabilidad 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 responde a una de las siguientes circunstancias:

A. Es el objeto de un trabajo incluido en el plan de auditoría interna.
B. Es identificado durante la ejecución de un trabajo.
C. 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 requisito 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 mantiene una relación comercial. Una relación con terceras partes puede formalizarse mediante un contrato, acuerdo u otro medio para suministrar a la organización productos o servicios. El uso del término "tercera parte" puede variar en función del sector o de otros contextos. Esta guía utiliza el término "tercera parte" para referirse a vendedores o proveedores, contratistas o subcontratistas, proveedores de servicios externalizados, otras agencias y consultores, e incluye los acuerdos entre una tercera parte y sus subcontratistas, a menudo conocidos como subcontratistas "en cadena".

Este Requisito Temático no pretende abordar las relaciones indirectas, intereses o implicación con la organización principal, tales como empleados, socios financieros, reguladores, agentes o fideicomisarios.

Aunque la organización principal puede contratar a una tercera parte para que le ayude a alcanzar uno o varios de sus objetivos empresariales, la organización principal sigue siendo responsable de los riesgos asociados a la consecución de dichos objetivos. Si el contrato o acuerdo de una tercera parte con la organización le permite subcontratar a una cuarta parte o a otras partes "en cadena", este requisito temático se aplica también a la hora de proporcionar aseguramiento sobre el gobierno y la supervisión de esas relaciones subcontratadas. En estos casos, los auditores internos deben aplicar todos los requisitos según indiquen los resultados de una evaluación de riesgos. Las exclusiones deben estar documentadas.

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. Categorías y ejemplos de riesgos relacionados con terceras partes incluyen:

- Operativos, como interrupciones del servicio o incumplimiento de los objetivos empresariales.
- Ciberseguridad, como datos sensibles comprometidos.
- Financieros, como la insolvencia del proveedor.
- Cumplimiento de los requisitos regulatorios locales, nacionales e internacionales aplicables.
- Jurídicos, como conflictos de interés, disputas y litigios por incumplimiento de contratos.
- Reputacionales, como los daños causados al medio ambiente o a los clientes, consumidores o partes interesadas de la organización principal.

El ciclo de vida de una tercera parte consiste en seleccionar, contratar, incorporar, monitorear y desvincular. Los auditores internos deben tener en cuenta estas fases 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 coherente 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 esta evaluación en una organización.

Gobierno: Evaluación y valoración del gobierno de terceras partes

Requisitos:

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

A. Se establece, aplica y revisa periódicamente un enfoque formal para determinar si se contrata a una tercera parte para que ayude a cumplir un objetivo empresarial mediante el suministro de un producto o servicio. El enfoque incluye criterios adecuados para definir y evaluar los recursos disponibles para cumplir los objetivos.

B. Se establecen políticas, procedimientos y procesos para definir, evaluar y gestionar las relaciones y los riesgos con terceras partes a lo largo de su ciclo de vida. Las políticas, procedimientos y procesos se

ajustan a los requisitos regulatorios aplicables y se revisan y actualizan periódicamente para reforzar el entorno de control.

C. Se definen las funciones y responsabilidades de gestión de terceras partes dentro de la organización, detallando quién selecciona, dirige, gestiona, se comunica con y supervisa a terceras partes, así como quién debe ser informado sobre las actividades de terceras partes. Existe un proceso para garantizar que las personas a las que se asignan funciones y responsabilidades sobre terceras partes tienen los conocimientos, competencias y capacidades adecuados.
D. Los protocolos de comunicación con las partes interesadas pertinentes están definidos e incluyen la información sobre el estado del rendimiento, los riesgos y el cumplimiento de las terceras partes prioritarias. Las partes interesadas pueden ser el consejo de administración, la alta dirección, el área de operaciones, gestión de riesgos, recursos humanos, seguridad de la información, servicios jurídicos, cumplimiento normativo, compras y otros.

GESTIÓN DE RIESGOS: Evaluación y valoración de la gestión de riesgos de terceras partes

Requisitos:

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

A. Los procesos de gestión de riesgos para terceras partes están normalizados y son exhaustivos, incluyen funciones y responsabilidades definidas y abordan suficientemente los riesgos clave (como los financieros, operativos, estratégicos, de ciberseguridad, de cumplimiento, de reputación, éticos, de sostenibilidad, geopolíticos y jurídicos). Se supervisa el cumplimiento de los procesos y se aplican medidas correctoras para cualquier desviación.

B. Se identifican y evalúan los riesgos relacionados con terceras partes a lo largo del ciclo de vida. La evaluación de riesgos se utiliza para clasificar y jerarquizar a terceras partes y priorizar las respuestas a los riesgos. La evaluación 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 poner remedio a la situación, que pueden llegar hasta la rescisión del contrato.

CONTROLES: Evaluación y valoración de los procesos de control de terceras partes

Requisitos:

Los auditores internos deben evaluar los siguientes controles para las terceras partes prioritarias, incluidos los procesos de la dirección para la evaluación y monitoreo continuos de las terceras partes de la organización:

A. Un caso de negocio documentado y aprobado u otro documento pertinente describe y justifica la necesidad y la naturaleza de la relación con una tercera parte.

B. Existe un sólido proceso de diligencia debida para la contratación y selección de terceras partes. El proceso incluye criterios para aspectos importantes, como la revisión de los protocolos de ciberseguridad, la comprobación de los antecedentes financieros y la verificación de los datos bancarios.

C. La contratación y aprobación se realizan de acuerdo con las políticas, procedimientos y procesos de gestión de riesgos de terceras partes e incluyen la colaboración con las partes adecuadas de la organización.

D. Los contratos o acuerdos finales son revisados y aprobados por todas las partes interesadas, incluidos el departamento jurídico y el de cumplimiento normativo, si procede; firmados por personas autorizadas de ambas partes; y almacenados de forma segura. Todos los contratos se asignan a un gestor o administrador responsable.

E. 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.

F. Se establecen y siguen procesos de incorporación documentados para que las terceras partes puedan cumplir las condiciones del contrato o acuerdo.

G. Existen procesos de monitoreo continuo para evaluar si las terceras partes prioritarias actúan de conformidad con los términos del contrato o del acuerdo durante el ciclo de vida y cumplen las 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.

H. 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.

I. Se supervisan las fechas de renovación de los contratos y se adoptan las medidas de renovación necesarias.

J. Para las terceras partes prioritarias, se aplica y se sigue un plan formalizado de desvinculación. 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 almacenados con la tercera parte.
   - Revocar el acceso de la tercera parte a los sistemas, herramientas e instalaciones.

Acerca del Instituto de Auditores Internos

El Instituto de Auditores Internos (The IIA) es una asociación profesional internacional que cuenta con más de 260.000 miembros en todo el mundo y ha concedido más de 200.000 certificaciones Certified Internal Auditor® (CIA®) globalmente. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información, visite www.theiia.org.

Descargo de responsabilidad

Copyright

Febrero de 2025

