TONE at the TOP®

Proporcionar a la alta dirección, juntas directivas y comités de auditoría, información concisa sobre temas relacionados con la gobernanza.

Edición 127 | Febrero 2025

Una Nueva Herramienta para Monitorear los Riesgos Establecidos

Este mes, el IIA publicó el primero de una serie de nuevos requisitos que respaldarán los esfuerzos de los auditores internos para abordar mejor las áreas de interés actual. El componente más reciente del Marco Internacional de Prácticas Profesionales (IPPF, por sus siglas en inglés) del IIA, los Requisitos Temáticos, garantizarán que todas las funciones de auditoría interna, independientemente de su tamaño, estructura de propiedad o ubicación, apliquen la misma metodología de auditoría al evaluar la efectividad de la gobernanza, la gestión de riesgos y los controles de un área temática en particular.

Los Requisitos Temáticos establecen una línea de base que eleva el trabajo de la función de auditoría interna y el valor de la información y los conocimientos que proporciona a la junta directiva y a la organización. Este documento examinará los Requisitos Temáticos y lo que significan para los miembros de la junta y sus organizaciones.

Preocupaciones Generalizadas y de Alto Riesgo

Los auditores internos proporcionan aseguramiento y asesoramiento independientes y objetivos para mejorar los procesos y la toma de decisiones con el fin de maximizar el valor. Para garantizar que los auditores tengan el conocimiento y las habilidades necesarias para satisfacer las necesidades de las organizaciones, el IIA mejora y actualiza regularmente sus Normas y orientaciones. La introducción de los Requisitos Temáticos es parte del proyecto de evolución del MIPP que también incluye las nuevas Normas Globales de Auditoría Interna™ presentadas el año pasado, así como otras directrices mundiales.

Los Requisitos Temáticos están destinados a "temas globales auditados con frecuencia, que suelen ser de mayor riesgo y de naturaleza generalizada". Los Requisitos Temáticos abordarán las áreas de riesgo maduras y proporcionarán orientación basada en las mejores prácticas establecidas. Uno de los requisitos, sobre ciberseguridad, se publicó a principios de este mes, y otros siete están en desarrollo.

Requisitos temáticos planificados

Los Requisitos Temáticos que se espera que se publiquen en los próximos años incluyen:

Ciberseguridad	Lucha contra la corrupción/soborno
Terceros	Gestión de personas
Cultura	Gestión del riesgo de fraude
Resiliencia Empresarial	Sostenibilidad/ESG

Se dio prioridad a la ciberseguridad como primer Requisito Temático debido a la profunda dependencia de las organizaciones del Internet en la mayoría o en todas sus actividades y debido a la necesidad de proteger su perímetro basado en la web. Los auditores internos son muy conscientes de la amenaza que suponen los problemas de ciberseguridad. En el informe más reciente del IIA global: Risk in Focus, los líderes de auditoría interna no solo citan a la ciberseguridad como el mayor riesgo actualmente y en el próximo año, sino que también dicen que esperan que siga siendo la mayor amenaza para sus organizaciones durante los próximos tres años.

Los encuestados también están preocupados por un tema relacionado, la disrupción digital, incluidos los riesgos asociados con la inteligencia artificial (IA), la IA generativa (GenAI) y otras tecnologías emergentes. Colocan la disrupción digital en el extremo inferior de sus cinco principales riesgos actualmente y en el próximo año, pero la elevan al riesgo número 2 cuando miran hacia el futuro en los próximos tres años. Si bien GenAI puede mejorar la detección de amenazas y vulnerabilidades, también puede facilitar que los actores maliciosos desarrollen ataques más sofisticados y efectivos.

Uso de los Requisitos Temáticos

Los Requisitos Temáticos formalizan cómo los auditores internos abordan las áreas de riesgo prevalentes. Los requisitos:

- Establecer una línea de base para que las funciones de auditoría interna la utilicen en sus esfuerzos por mitigar el riesgo en la organización.
- Son obligatorios para los servicios de aseguramiento pertinentes y se recomiendan para ser considerados para los servicios de asesoramiento.
- Exigir que la aplicabilidad de un Requisito Temático se determine mediante un plan de auditoría basado en riesgos. Teniendo en cuenta que la evaluación del riesgo es una parte importante de la planificación del director ejecutivo de auditoría, piden que esa determinación se haga sobre la base de una evaluación de las estrategias, los objetivos y los riesgos de la organización.
- Establecer un enfoque globalmente coherente de la auditoría dentro de cada área temática, lo que mejorará la fiabilidad de los servicios y resultados de la auditoría interna.
- Proporcionar criterios relevantes para la prestación de servicios de aseguramiento de la ciberseguridad.
- Se deben aplicar a nivel de entidad u organización en áreas que tienen un impacto en toda la organización.
- Identificar los riesgos generalizados que deberían estar al menos en el radar de una organización.
- Agregar valor al garantizar una cobertura y consistencia adecuadas de los riesgos cibernéticos.
- No están destinados a cubrir todos los aspectos que se deben considerar en un compromiso de aseguramiento. Más bien, establecen requisitos mínimos para una evaluación consistente y fiable del tema.

Los requisitos están diseñados para permitir que los auditores internos los utilicen juiciosamente. Para comprender cómo se pueden poner en práctica los requisitos, considere una situación en la que la ciberseguridad se ha identificado como un riesgo generalizado o extenso para la organización durante el proceso de planificación de la auditoría interna, y se realizará una auditoría del tema. Ese es claramente un caso en el que se debe aplicar el Requisito Temático, pero no todos los casos serán tan claros.

Tomemos, por ejemplo, un equipo de auditoría interna que realiza una auditoría de cuentas por pagar y se entera de los riesgos cibernéticos asociados con un proceso de solicitud de órdenes de compra basado en la web. Incluso si la ciberseguridad no se identificara como un riesgo general de la organización en el plan de auditoría, la auditoría interna seguiría aplicando el Requisito Temático, pero de manera más específica. Es posible que el equipo dedique más tiempo a la parte de los controles de ciberseguridad de la auditoría que a la gobernanza o la gestión de riesgos. Los auditores internos documentarían sus razones para limitar el encargo a una pieza específica.

Sobre El IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin fines de lucro que presta servicios a más de 245,000 miembros globales y ha otorgado más de 200,000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Establecido en 1941, el IIA es reconocido globalmente como líder de la profesión de auditoría interna en estándares, certificaciones, educación, investigación y orientación técnica. Para más información, visite: **theiia.org.**

El IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Suscripciones Complementarias

Visite **theiia.org/Tone** para registrarse y acceder a la suscripción.

Feedback del Lector

Envíe sus preguntas/comentarios a: **Tone@theiia.org.**

Gobernanza, Gestión de Riesgos y Controles de Ciberseguridad.

Como se ha señalado, los Requisitos Temáticos cubrirán la gobernanza, la gestión de riesgos y los controles de cada área temática. Bajo el paraguas de la gobernanza, los auditores internos deben evaluar si los procesos de gobernanza de la organización abordan adecuadamente la ciberseguridad. La gobernanza de la ciberseguridad define objetivos y estrategias relacionados que promueven las metas, políticas y procedimientos de la empresa.

La sección de comunicación del requisito cubre los tipos de materiales que recibe la junta sobre la estrategia, el riesgo, los objetivos y los controles de ciberseguridad, y considera si la iniciativas estratégicas apoyan a la ciberseguridad. Esta sección también cubre las políticas y procedimientos, así como las funciones y responsabilidades creadas para lograr los objetivos de ciberseguridad, el compromiso con las partes interesadas y los requisitos de recursos para cumplir los objetivos de ciberseguridad.

La sección de gestión de riesgos de ciberseguridad establece la necesidad de un proceso para identificar, analizar, gestionar y monitorear las amenazas cibernéticas, incluido un proceso para escalar rápidamente el reconocimiento de los riesgos cibernéticos. El objetivo principal es garantizar que la gestión de riesgos de ciberseguridad sea una prioridad desde el punto de vista de la gestión de riesgos empresariales.

Los controles de ciberseguridad son procesos que se evalúan periódicamente para mitigar los riesgos cibernéticos. Los siete procesos de control cubren aspectos importantes y básicos que los auditores internos deben evaluar al realizar una auditoría de ciberseguridad.

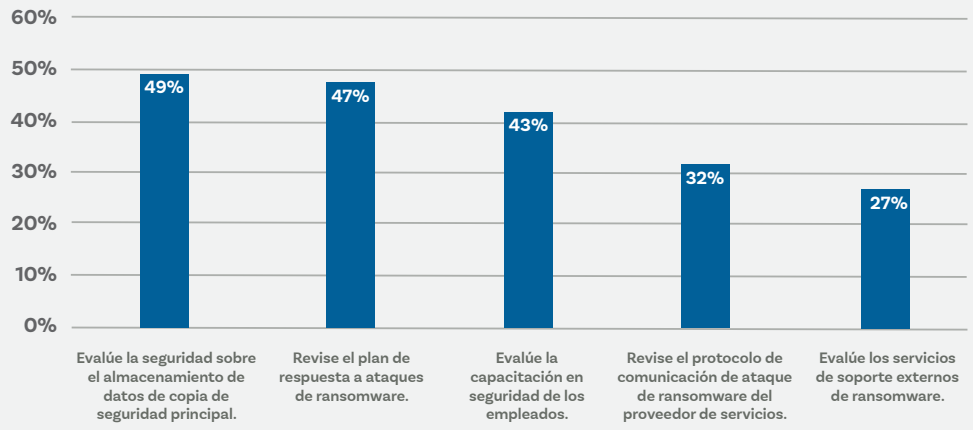
Abordar los Riesgos Comunes y en evolución

Dado su conocimiento profundo y holístico, los auditores internos están excepcionalmente calificados para reconocer ciertos riesgos que tienen más probabilidades de afectar a la organización. El gráfico "Participación de la auditoría interna en la ciberseguridad" muestra muchas de las áreas en las que la auditoría interna ya está involucrada en proporcionar aseguramiento e información.

Desarrollados por un grupo global de líderes de auditoría interna y otros expertos de una variedad de sectores, los Requisitos Temáticos impulsarán el trabajo de la profesión de auditoría interna, permitiendo a los auditores abordar mejor los riesgos comunes y en evolución.

Participación de la Auditoría Interna en la Ciberseguridad

"La práctica de los equipos de auditoría interna evaluando de forma independiente la seguridad de la información, ya sea internamente o con la ayuda de un tercero, se ha mantenido constante año tras año", según la firma de consultoría y reclutamiento Jefferson Wells. Sin embargo, el siguiente gráfico, que muestra el porcentaje de empresas que utilizan equipos de auditoría interna para ciertos compromisos relacionados con la ciberseguridad, indica que muchas organizaciones no están aprovechando al máximo la información y el asesoramiento que la auditoría interna puede proporcionar.



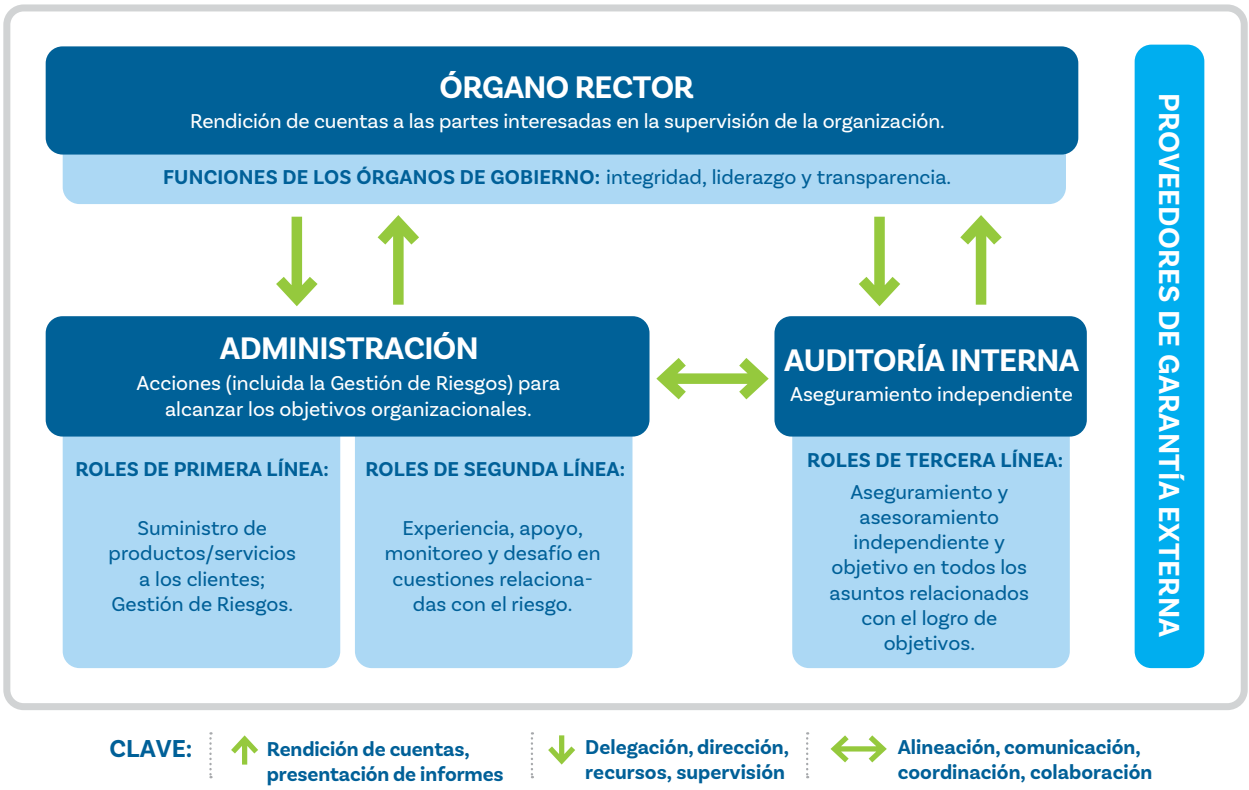
Fuente: Encuesta Anual de Prioridades de Auditoría Interna 2024, Jefferson Wells.

The Institute of Internal Auditors

Los Requisitos Temáticos y su Relación con el Modelo de las Tres Líneas

El IIA utilizó el Modelo de las Tres Líneas para desarrollar los Requisitos Temáticos. Los elementos de gobernanza y supervisión de los requisitos se relacionan con el órgano de gobierno de la organización, el elemento de gestión de riesgos con la segunda línea, los controles y procesos de control con la primera línea, y la función de auditoría interna, como tercera línea, proporciona aseguramiento independiente.

El Modelo de las Tres Líneas del IIA



PREGUNTAS PARA LOS MIEMBROS DE LA JUNTA

1. ¿Cuáles son nuestras mayores vulnerabilidades?
2. ¿Qué tipos de ciberataques podría sufrir la organización?
3. ¿Qué tipo de adversarios podrían estar detrás de ellos?
4. ¿Qué estaría tratando de lograr el adversario: la interrupción del negocio, el robo de datos o activos de información comercial, el cobro de un rescate o algún otro propósito?
5. ¿Cómo llevarían a cabo un ataque?
6. ¿Cómo sabremos que se ha producido un ataque? ¿Estamos preparados para dar una respuesta inmediata?
7. ¿Estamos haciendo el mejor uso del aseguramiento y el asesoramiento que la auditoría interna puede ofrecer para abordar los riesgos de ciberseguridad?
8. ¿Estamos utilizando la inteligencia artificial (IA) para ayudar con la ciberseguridad? Si es así, ¿de qué manera? Si no es así, ¿nos hemos planteado el uso de la IA?