Estándar de auditoría y aseguramiento de SI 1202 Evaluación de riesgo en planificación

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de *ITAF*™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
  - **Estándares generales (serie 1000):** Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
  - **Estándares de desempeño (serie 1200):** Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
  - **Estándares de reportes (serie 1400):** Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
  - Lineamientos generales (serie 2000)
  - Lineamientos de desempeño (serie 2200)
  - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en *www.isaca.org/glossary*.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (*standards@isaca.org*), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Estándar de auditoría y aseguramiento de SI 1202 Evaluación de riesgo en planificación

Declaraciones

1202.1 **La función de auditoría y aseguramiento de SI debe utilizar un enfoque de evaluación de riesgo adecuado y metodología de respaldo para desarrollar el plan completo de auditoría de SI y determinar las prioridades para la asignación efectiva de los recursos de auditoría de SI.**

1202.2 **Los profesionales de auditoría y aseguramiento de SI deben identificar y evaluar el riesgo relevante al área de revisión, cuando planifican asignaciones individuales.**

1202.3 **Los profesionales de auditoría y aseguramiento de SI deben considerar el riesgo del tema, el riesgo de la auditoría y la exposición relativa de la empresa.**

Aspectos clave

Al planificar las actividades continuas, la función de auditoría y aseguramiento de SI debe:

- Realizar y documentar, al menos una vez al año, una Evaluación de riesgo para facilitar el desarrollo del plan de auditoría de SI.
- Incluir, como parte de la evaluación de riesgo, los objetivos y planes estratégicos organizacionales y las iniciativas y marco de gestión de riesgo empresarial.
- Para cada asignación de auditoría y aseguramiento de SI, cuantificar y justificar la cantidad de recursos de la auditoría de SI necesarios para cumplir con los requerimientos de la asignación.
- Utilizar las evaluaciones de riesgo en la selección de áreas e ítems de interés de la auditoría y las decisiones para diseñar y realizar asignaciones particulares de auditoría y aseguramiento de SI.
- Buscar la aprobación de la evaluación de riesgo por parte de las partes interesadas en la auditoría y otras partes apropiadas.
- Priorizar y programar el trabajo de auditoría y aseguramiento de SI en base a las evaluaciones de riesgo.
- En función a la evaluación de riesgo, desarrollar un plan que:
  - Actúe como marco para las actividades de auditoría y aseguramiento de SI
  - Considere actividades y requerimientos de auditoría y aseguramiento que no sean de SI
  - Sea actualizado al menos una vez al año y aprobado por los órganos de gobierno
  - Aborde responsabilidades establecidas por el Estatuto de la función de auditoría

Al planificar una asignación individual, los profesionales de auditoría y aseguramiento de SI deben:

- Identificar y evaluar el riesgo relevante al área bajo revisión.
- Realizar una evaluación preliminar del riesgo relevante al área bajo revisión para cada asignación. Los objetivos para cada asignación específica deben reflejar los resultados de la evaluación del riesgo preliminar.
- Al considerar las áreas de riesgo y planificar una asignación específica, considerar auditorías anteriores, revisiones y hallazgos, que incluyen cualquier actividad correctiva. También considerar el proceso de evaluación de riesgo de gran alcance del Consejo.
- Intentar reducir el Riesgo de auditoría a un nivel aceptable y cumplir con los

objetivos de la auditoría por una evaluación apropiada del tema de SI y controles relacionados, a medida que se planifica y realiza la auditoría de SI.
- Al planificar un procedimiento de auditoría de SI específico, reconocer que mientras más bajo sea el umbral de Materialidad, más precisas son las expectativas de la auditoría y mayor es el riesgo de la auditoría.
- Para reducir el riesgo de mayor materialidad, compensar ampliando las pruebas de controles (reducir el riesgo de control) y/o ampliando los procedimientos de Pruebas sustantivas(reducir el riesgo de detección) para obtener aseguramiento adicional.

Términos

Término	Definición
Estatuto de la función de auditoría	Documento aprobado por los responsables del gobierno que define el propósito, la autoridad y la responsabilidad de la actividad de auditoría interna. El estatuto debe: • Establecer la posición de la función de auditoría interna dentro de la empresa. • Autorizar el acceso a registros, personal y propiedades físicas relevantes para el desempeño de las asignaciones de auditoría y aseguramiento de SI. • Definir el alcance de las actividades de la función de auditoría.
Riesgo de auditoría	El riesgo de alcanzar una conclusión incorrecta en base a los hallazgos de auditoría. Los tres componentes del riesgo de auditoría son: • Riesgo de control • Riesgo de detección • Riesgo inherente
Riesgo del tema de la auditoría	Riesgo relevante al área bajo revisión: • Riesgo de negocio (capacidad del cliente para pagar, solvencia, factores del mercado, etc.) • Riesgo contractual (responsabilidad, precio, tipo, penalizaciones, etc.) • Riesgo del país (político, entorno, seguridad, etc.) • Riesgo del proyecto (recursos, conjunto de habilidades, metodología, estabilidad del producto, etc.) • Riesgo de tecnología (solución, arquitectura, red de infraestructura de hardware y software, canales de entrega, etc.) Ver riesgo inherente.
Riesgo de control	Riesgo de que exista un error material que no sea prevenido o detectado de manera oportuna por el sistema de control interno. (Ver riesgo inherente.)
Riesgo de detección	Riesgo de que los procedimientos sustantivos del profesional de auditoría o aseguramiento de SI no detecten un error que pudiera ser material, individualmente o en combinación con otros

	errores. Ver riesgo de auditoría.
Riesgo inherente	Nivel o exposición al riesgo sin tomar en cuenta las acciones que la dirección ha tomado o podría tomar (por ej., implementar controles). Ver riesgo de control.
Materialidad	Un concepto de auditoría sobre la importancia de un ítem de información con respecto a su impacto o efecto en el funcionamiento de la entidad que está siendo auditada. Una expresión de importancia relativa de un tema particular en el contexto de la empresa como un todo.
Evaluación de riesgo	Proceso utilizado para identificar y evaluar los riesgos y sus posibles efectos. Las evaluaciones de riesgo son utilizadas para identificar aquellos ítems o áreas que presentan la exposición, la vulnerabilidad o el riesgo más alto para la empresa para la inclusión en el plan de auditoría anual de SI. Las evaluaciones de riesgo también se utilizan para gestionar el riesgo de beneficios del proyecto y entrega del proyecto.
Pruebas sustantivas	Obtención de evidencia de una auditoría sobre la integridad, precisión o existencia de actividades o transacciones realizadas durante el período de la auditoría.

Enlace a los lineamientos

Tipo	Título
Lineamiento	2202 Evaluación de riesgo en planificación

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

