ESTANDAR DE AUDITORÍA DE SI
IRREGULARIDADES Y ACCIONES ILEGALES
DOCUMENTO S9

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para realizarlas, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

- Los **Estándares** definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:
  - Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido 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.
  - Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.
- Las **Directrices** proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.
- Los **Procedimientos** proporcionan ejemplos de procedimientos que podría seguir un auditor de SI durante la ejecución de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de **CobiT®** deben utilizarse como fuente de asesoría con respecto a las mejores prácticas. El *Marco Referencial* de CobiT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno". CobiT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en CobiT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de CobiT para TI, considerando además los criterios de información de CobiT.

Tal como se define en el *Marco Referencial* de CobiT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. CobiT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, con base en estándares de referencia comúnmente comprendidos y respetados. CobiT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Razonamiento práctico y guías sobre “cómo implementar” los objetivos de control
- Directrices de auditoría—Guías para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Guías sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva auto-evaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requerimientos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres sobre auto-evaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

El **glosario** de términos se encuentra en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos cuando sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico (standards@isaca.org), por fax (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue publicado el 1 de julio de 2005.

Irregularidades y acciones ilegales S9

Introducción

01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados en letras en negrita, que son obligatorios junto con la documentación relacionada.

02 El propósito de este estándar de ISACA es establecer y proporcionar asesoría sobre irregularidades y acciones ilegales que el auditor de SI debe tener en cuenta durante el proceso de auditoría.

Estándar

03 Al planificar y realizar la auditoría para reducir el riesgo de auditoría a un nivel bajo, el auditor de SI debe tener en cuenta el riesgo de irregularidades y acciones ilegales.

04 El auditor de SI debe mantener una actitud de escepticismo profesional durante la auditoría, reconociendo la posibilidad de que podrían existir declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales, independientemente de su propia evaluación del riesgo de irregularidades y acciones ilegales.

05 El auditor de SI debe obtener un entendimiento de la organización y su entorno, incluidos los controles internos.

06 El auditor de SI debe obtener evidencia de auditoría suficiente y relevante para determinar si la gerencia u otras personas dentro de la organización tienen conocimientos de cualquier irregularidad y acción ilegal real, sospechada o alegada.

07 Al realizar procedimientos de auditoría para obtener un entendimiento de la organización y su entorno, el auditor de SI debe considerar relaciones inusuales o inesperadas que pueden indicar un riesgo de declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales.

08 El auditor de SI debe diseñar y realizar procedimientos para probar lo adecuado de los controles internos y el riesgo de anulación de los controles por parte de la gerencia.

09 Cuando el auditor de SI identifica una declaración incorrecta, el auditor de SI debe evaluar si tal declaración incorrecta puede indicar la existencia de una irregularidad o acción ilegal. Si existe tal indicación, el auditor de SI debe tener en cuenta las implicaciones en relación con otros aspectos de la auditoría y, en particular, las declaraciones de la gerencia.

10 El auditor de SI debe obtener declaraciones escritas de la gerencia al menos una vez al año o con mayor frecuencia, dependiendo del contrato de auditoría. La gerencia debe:

- **Reconocer su responsabilidad en el diseño e implementación de controles internos para prevenir y detectar irregularidades o acciones ilegales**
- **Revelar al auditor de SI los resultados de la evaluación de riesgos cuando pueda existir una declaración materialmente incorrecta como resultado de una irregularidad o acción ilegal**
- **Revelar al auditor de SI cuando tenga conocimiento de irregularidades o acciones ilegales que estén afectando la organización en relación a:**
  - **La gerencia**
  - **Empleados que tienen funciones significativas en el control interno**
- **Revelar al auditor de SI cuando tenga conocimiento de cualquier declaración de irregularidades o acciones ilegales, o sospechas de irregularidades o acciones ilegales que estén afectando la organización tal como lo hayan comunicado los empleados, ex empleados, funcionarios responsables de la normatividad dentro de la organización y otros**

11 Si el auditor de SI ha identificado una irregularidad material o acción ilegal, u obtiene información de que puede existir una irregularidad material o acción ilegal, el auditor de SI debe comunicarlo sin demora al nivel de dirección apropiado.

12 Si el auditor de SI ha identificado una irregularidad material o acción ilegal que involucra a la gerencia o a empleados que tienen funciones significativas en el control interno, el auditor de SI debe comunicarlo sin demora a los responsables del gobierno corporativo.

13 El auditor de SI debe dar recomendaciones al nivel apropiado de la gerencia y a aquellos responsables del gobierno corporativo sobre las debilidades materiales en el diseño e implementación del control interno para prevenir y detectar irregularidades y acciones ilegales que el auditor de SI pueda haber notado durante la auditoría.

14 Si el auditor de SI encuentra circunstancias excepcionales que afectan su capacidad para continuar ejecutando la auditoria debido a una declaración materialmente incorrecta o una acción ilegal, el auditor de SI debe tener en cuenta la responsabilidad legal y profesional aplicable en tales circunstancias, incluyendo que pueda existir el requisito para el auditor de SI de notificar a aquellos que celebraron el contrato o, en algunos casos, a los responsables del gobierno corporativo o a las autoridades responsables de la normatividad dentro de la organización o incluso considerar retirarse del contrato.

15 El auditor de SI debe documentar todas las comunicaciones, planeación, resultados, evaluaciones y conclusiones relacionadas con irregularidades materiales y acciones ilegales que han sido notificadas a la gerencia, a los responsables del gobierno corporativo, autoridades responsables de la normatividad dentro de la organización y otros.

Comentario

16 El auditor de SI debe consultar la Directriz de Auditoría de SI G19, Irregularidades y Acciones Ilegales, para obtener la definición de que constituye una irregularidad y una acción ilegal.

17 El auditor de SI debe obtener una garantía razonable de que no existen declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales. Un auditor de SI no puede tener garantía absoluta con base en factores tales como el buen juicio, el alcance de las pruebas y las limitaciones inherentes de los controles internos. La evidencia de auditoría de que disponga el auditor de SI durante una auditoría debe ser de naturaleza persuasiva y no concluyente.

18 El riesgo de no detectar una declaración materialmente incorrecta que surge de una acción ilegal es mayor que el riesgo de no detectar una declaración materialmente incorrecta que surge de una irregularidad o error, porque las acciones ilegales pueden involucrar esquemas complejos diseñados para ocultar eventos o declaraciones intencionalmente incorrectas ante el auditor de SI.

19 La experiencia previa del auditor de SI y su conocimiento de la organización deben ayudarle al auditor de SI durante la auditoría. Al hacer investigaciones y realizar procedimientos de auditoría, no se espera que el auditor de SI descarte por completo su experiencia previa, pero se espera que mantenga un nivel de escepticismo profesional. El auditor de SI no debe estar satisfecho con evidencia de auditoría que sea menos que persuasiva basándose en la creencia de que la gerencia y los responsables del gobierno corporativo son honestos e íntegros. El auditor de SI y el equipo involucrado deben discutir la susceptibilidad de la organización a irregularidades y acciones ilegales como parte del proceso de planeación y durante la auditoría.

20 Para evaluar el riesgo de la existencia de irregularidades materiales y acciones ilegales, el auditor de SI debe considerar el uso de:
- Sus conocimientos y experiencia previos con la organización (incluida su experiencia con respecto a la honestidad e integridad de la gerencia y los responsables del gobierno corporativo)
- Información obtenida al entrevistar a la gerencia
- Declaraciones de la gerencia y verificaciones firmadas de los controles internos
- Otra información confiable obtenida durante el curso de la auditoría
- La evaluación de la gerencia del riesgo de irregularidades y acciones ilegales, y su proceso para identificar y responder a tales riesgos

21 Debe consultarse la documentación siguiente para obtener mayor información sobre irregularidades y acciones ilegales:
- Directriz de Auditoría de SI G5, Estatuto de auditoría
- Marco Referencial de COBIT, objetivos de control DS3, DS5, DS9, DS11 y PO6
- Ley Sarbanes-Oxley de 2002
- Ley sobre Prácticas Extranjeras Corruptas 1977

Fecha de Vigencia

22 Este estándar de ISACA estará en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de septiembre de 2005.