# NORMA DE AUDITORÍA DE SI

## PLANEACIÓN

**DOCUMENTO N° S5**

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, 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 asesoramiento:

- Los **Estándares** definen requisitos obligatorios para la auditoría y el reporte de SI. 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 asesoramiento en 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 en el curso de un contrato de 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 asesoramiento 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 utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. CobiT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre “cómo implementar” los objetivos de control
- Directrices de auditoría—Asesoramiento 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—Asesoramiento 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 autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, 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.

Se puede encontrar el **glosario** de términos 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 esto 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 a (standards@isaca.org), por fax a (+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 emitido el 15 de octubre de 2004.

## S5 Planeación

**Introducción**

01 Los Estándares de Auditoría de SI de ISACA contienen los principios básicos y procedimientos esenciales, identificados en letras en negrita, los cuales son obligatorios, junto con la documentación relacionada.

02 El propósito de esta Norma de Auditoría de SI es establecer normas y brindar asesoría sobre la planeación de una auditoría.

**Estándar**

**03 El auditor de SI debe planear la cobertura de la auditoría de sistemas de información para cubrir los objetivos de la auditoría y cumplir con las leyes aplicables y las normas profesionales de auditoría.**

**04 El auditor de SI debe desarrollar y documentar un enfoque de auditoría basado en riesgos.**

**05 El auditor de SI debe desarrollar y documentar un plan de auditoría que detalle la naturaleza y los objetivos de la auditoría, los plazos y alcance, así como los recursos requeridos.**

**06 El auditor de SI debe desarrollar un programa y/o plan de auditoría detallando la naturaleza, los plazos y el alcance de los procedimientos requeridos para completar la auditoría.**

**Comentario**

07 Para una función de auditoría interna, debe desarrollarse/actualizarse un plan, al menos una vez al año, para las actividades permanentes. El plan debe servir como marco de referencia para las actividades de auditoría y servir para abordar las responsabilidades establecidas por el estatuto de auditoría. El nuevo/actualizado plan debe ser aprobado por el comité de auditoría, en caso de que éste haya sido establecido.

08 Para el caso de una auditoría externa de SI, normalmente debe prepararse un plan para cada una de las tareas, sean o no de auditoría. El plan debe documentar los objetivos de la auditoría.

09 El auditor de SI debe obtener un entendimiento de la actividad que está siendo auditada. El grado del conocimiento requerido debe ser determinado por la naturaleza de la organización, su entorno y riesgos, y por los objetivos de la auditoría.

10 El auditor de SI debe realizar una evaluación de riesgos para brindar una garantía razonable de que todos los elementos materiales serán cubiertos adecuadamente durante la auditoría. En este momento, es posible establecer las estrategias de auditoría, los niveles de materialidad y los recursos necesarios.

11 El programa y/o plan de auditoría puede requerir ajustes durante el desarrollo de la auditoría para abordar las situaciones que surjan (nuevos riesgos, suposiciones incorrectas o hallazgos en los procedimientos ya realizados) durante la auditoría.

12 Debe consultarse la siguiente documentación para obtener más información sobre la preparación de un plan de auditoría.

- Guía de Auditoría de SI G6, Conceptos de materialidad para la auditoría de SI
- Guía de Auditoría de SI G15, Planeación
- Guía de Auditoría de SI G13, Uso de la evaluación de riesgos en la planeación de la auditoría
- Guía de Auditoría de SI G16, Efecto de terceros en los controles de TI de una organización
- *Marco Referencial de* CobiT, Objetivos de control

**Fecha operativa**

13 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.