

Norma de Auditoría de SI

Documento S 7 REPORTES

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.

Renuncia: ISACA ha definido este asesoramiento 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 hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio

profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

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.

S7 Reporte

Introducción

01. Las Normas de Auditoría de SI de ISACA contienen 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 y proporcionar asesoría sobre la generación del informe, a fin de que el auditor de SI pueda cumplir con esta responsabilidad.

Estándar

03. El auditor de SI debe suministrar un informe, en un formato apropiado, al finalizar la auditoría. El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.
04. El informe de auditoría debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.
05. El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor de SI tuviese en cuanto al alcance de la auditoría.
06. El auditor de SI debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.
07. Al emitirse, el informe del auditor de SI debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.

Comentario

08. El formato y contenido del informe generalmente varían según el tipo de servicio o contrato. Un auditor de SI puede realizar cualquiera de las siguientes acciones:
 - Auditoría (de manera directa o como testigo)
 - Revisión (de manera directa o como testigo)
 - Procedimientos acordados
09. Cuando se requiera que el auditor de SI proporcione una opinión sobre el entorno de control y exista evidencia de auditoría sobre una debilidad material o significativa, el auditor de SI no deberá concluir que los controles internos son eficaces. El informe del auditor de SI debe describir la debilidad material o significativa y el efecto en el logro de los objetivos de los criterios de control.

10. El auditor de SI debe comentar el contenido del informe en borrador con la gerencia del área bajo revisión antes de la finalización y divulgación, e incluir los comentarios de la gerencia en el informe final cuando corresponda.
11. Cuando el auditor de SI encuentre deficiencias significativas en el entorno de control, el auditor de SI debe informar sobre estas deficiencias al comité de auditoría o a la autoridad responsable y comentar en el informe que se han comunicado dichas deficiencias significativas.
12. Cuando el auditor de SI emita informes separados, el informe final deberá hacer referencia a todos los informes separados.
13. El auditor de SI debe considerar y evaluar si comunicará a la gerencia acerca de las deficiencias en los controles internos de menor magnitud que las deficiencias significativas. En tales casos, el auditor de SI debe informar al comité de auditoría o a la autoridad responsable que se han comunicado a la gerencia dichas deficiencias del control interno.
14. El auditor de SI debe solicitar y evaluar la información sobre los hallazgos, las conclusiones y las recomendaciones de informes anteriores a fin de determinar si se han implementado las acciones apropiadas de manera oportuna.
15. Debe consultarse la siguiente documentación para obtener más información sobre la generación del informe:
 - ☐ Guía de Auditoría de SI G20, Reporte
 - ☐ *Marco Referencial de COBIT*, Objetivos de control M4.7 y M4.8

Fecha de operación

16 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.

Junta Normativa de la Asociación de Auditoría y Control de Sistemas de Información 2004-2005

Presidente, Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay

Svein Aldal Aldal Consulting, Noruega

John Beveridge, CISA, CISM, CFE, CGFM, CQA Oficina del Auditor del Estado de Massachusetts, EE.UU.

Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP Value Partners, Italia

Christina Ledesma, CISA, CISM Citibank NA Sucursal, Uruguay

Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Consejo Municipal de Brisbane, Australia

V. Meera, CISA, CISM, ACS, CISSP, CWA Microsoft Corporation, EE.UU.

Ravi Muthukrishnan, CISA, CISM, FCA, ISCA NextLinx India Private Ltd., India

Peter Niblett, CISA, CISM, CA, CIA, FCPA WHK Day Neilson, Australia

John G. Ott, CISA, CPA Aetna Inc., EE.UU.

Thomas Thompson, CISA Ernst & Young, UAE

© Copyright 2004

Information Systems Audit and Control Association

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 EE.UU.

Teléfono: +1.847.253.1545

Fax: +1.847.253.1443

Correo electrónico: standards@isaca.org

Sitio web: www.isaca.org