

S16 E-COMMERCE

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las habilidades necesarias para ejecutarla, requiere de estándares que sean específicamente aplicables a la auditoría de SI. Uno de los objetivos de ISACA[®] es promover estándares globalmente aplicables 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 de 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 a demás interesados en las expectativas de la profesión con respecto al trabajo de sus profesionales
 - Los poseedores del Certificado de Auditor 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 al cumplimiento de los Estándares de Auditoría de SI.
- Los **Procedimientos** proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso 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.

Objetivos de Control para Información y Tecnología Relacionada (Control Objectives for Information and related Technology, COBIT[®]) es un marco de referencia de dirección de tecnología de información (TI) y conjunto herramientas de apoyo que permite a los gerentes superar las diferencias entre los requisitos de control, cuestiones técnicas y riesgos del negocio. COBIT permite un desarrollo claro de políticas y buenas prácticas para el control de TI a lo largo de organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido a partir de TI, permite el alineamiento y simplifica la implementación de los conceptos de la estructura COBIT.

COBIT está destinado a 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, en base a una estructura comúnmente comprendida y bien respetada. COBIT está disponible para su descarga del sitio Web de ISACA: www.isaca.org/cobit. Tal como se define en la estructura de COBIT, cada uno de los siguientes productos y/o elementos está organizado de acuerdo con el proceso de administración/gestión de TI:

- **Objetivos de control**—Declaraciones genéricas de un mínimo buen control en relación con los procesos de TI
- **Directrices de gestión**—Guías sobre evaluación y mejora de ejecución del proceso de TI, utilizando modelos de madurez, cuadros RACI (quién es Responsable de, quién rinde cuentas A, a quién se le Consulta y/o a quién se le Informa), metas y métricas. Proporcionan un marco de referencia de gestión orientado hacia una continua y proactiva auto-evaluación del control, enfocada específicamente en:
 - Medición del rendimiento/desempeño
 - Perfil de control de TI
 - Concienciación
 - Benchmarking
- **Prácticas de control de COBIT**—Declaraciones de riesgo y valor y guías sobre 'cómo implementar' los objetivos de control
- **Guía de garantía de TI**—Guías para cada área de control sobre cómo obtener un entendimiento, juzgar cada control, evaluar su conformidad y validar el riesgo de que los controles no se cumplan

El **glosario** de términos se encuentra en el sitio web de ISACA www.isaca.org/glossary. Las palabras "auditoría" y "revisión" se usan de manera indistinta en los Estándares, las Directrices y los Procedimientos de Auditoría de SI.

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 como 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, el profesional de control debe utilizar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de tecnologías 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 habilidad 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 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 estándares de investigación y relaciones académicas. Este material fue emitido el 1 de diciembre de 2007.

S16 Comercio electrónico

Introducción

- 01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados con letra negrita, que junto con la documentación relacionada son obligatorios.
- 02 El propósito de este estándar de ISACA es el de establecer normas y proporcionar guías relativas a la revisión de entornos de comercio electrónico.

Estándar

- 03 **El auditor de SI debe evaluar los controles aplicables, y cotejar los riesgos al revisar entornos de comercio electrónico, para asegurar que las transacciones de comercio electrónico están correctamente controladas.**

Comentario

- 04 El comercio electrónico se define como aquellos procesos, a través de los cuales, las organizaciones realizan negocios por medios electrónicos con sus clientes, proveedores y otros socios comerciales externos, utilizando Internet como una tecnología habilitadora. Por lo tanto, incluye modelos de comercio electrónico de negocio a negocio (B2B), y de negocio a consumidor (B2C).
- 05 El auditor de SI debe utilizar una técnica o enfoque apropiado de evaluación de riesgos para desarrollar el plan general de auditoría de SI debe cubrir los entornos de comercio electrónico.
- 06 El auditor de SI debe considerar la utilización de técnicas de análisis de datos, incluida la utilización de una garantía continua, que permita a los auditores de SI monitorizar la fiabilidad del sistema de forma continua, y recoger evidencias selectivas de auditoría por medio del ordenador/computadora, al revisar las actividades de comercio electrónico.
- 07 El nivel de habilidad y conocimiento requerido, para comprender las implicaciones de control y administración/gestión de riesgos del comercio electrónico, varía con la complejidad de las actividades de comercio electrónico de la organización.
- 08 El auditor de SI debe comprender la naturaleza y la criticidad del proceso del negocio soportado por la aplicación de comercio electrónico antes de comenzar la auditoría, de modo que los resultados puedan evaluarse en el contexto apropiado.
- 09 Debe consultarse la guía siguiente para obtener mayor información con respecto al comercio electrónico:
 - Guía G21 Revisión de sistemas de planificación de recursos empresariales (Enterprise Resource Planning, ERP)
 - Guía G22 Revisión de comercio electrónico del negocio al consumidor (B2C)
 - Guía G24 Banca en Internet
 - Guía G25 Revisión de redes privadas virtuales (Virtual Private Networks, VPN)
 - Guía G33 Consideraciones generales respecto al uso de Internet
 - Procedimiento P6 Cortafuegos (firewalls)
 - Marco de referencia COBIT y objetivos de control

Fecha de Vigencia

- 10 Este estándar de ISACA entrará en vigor para las auditorías de sistemas de información que comiencen a partir del 1 de febrero de 2008.

Junta de Estándares de ISACA 2007-2008

Presidente, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA Capco IT Services India Private Limited, India
Brad David Chin, CISA, CPA Google Inc., EE.UU.
Sergio Fleginsky, CISA ICI Paints, Uruguay
María González, CISA Oficina Principal, España
John Ho Chi, CISA, CISM, CBCP, CFE Ernst & Young, Singapur
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Consejo Municipal de Brisbane, Australia
John G. Ott, CISA, CPA AmerisourceBergen, EE.UU.
Jason Thompson, CISA, CIA KPMG LLP, EE.UU.
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA Microsoft Corp., EE.UU.

© 2007 ISACA. Todos los derechos reservados.

ISACA

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