Estándar de auditoría y aseguramiento de SI 1008 Criterios

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 1008 Criterios

Declaraciones

1008.1 **Los profesionales de auditoría y aseguramiento de SI deben seleccionar criterios con los que será evaluado el tema, que sean objetivos, completos, relevantes, medibles, comprensibles, ampliamente reconocidos, autorizados y comprendidos por, o disponibles para, todos los lectores y usuarios del reporte.**

1008.2 **Los profesionales de auditoría y aseguramiento de SI deben considerar la fuente de los criterios y centrarse en aquellos emitidos por organismos autorizados relevantes antes de aceptar criterios menos reconocidos.**

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Considerar la selección de Criterios detenidamente y poder justificar su selección.
- Utilizar el buen juicio profesional para asegurar que, si corresponde, el uso de los criterios pueden permitir el desarrollo de una conclusión u opinión objetiva y justa que no ocasione una interpretación errónea por parte del lector o usuario. Hay que admitir que la dirección podría presentar criterios que no cumplan con todos los requerimientos.
- Considerar la idoneidad y disponibilidad de los criterios al determinar los requerimientos de la asignación.
- Cuando los criterios no están fácilmente disponibles, están incompletos o sujetos a interpretación, incluir una descripción y cualquier otra información necesaria para asegurar que el reporte sea justo, objetivo y comprensible, y que se incluya en el reporte el contexto en el que se utilizan los criterios.

Lo adecuado y apropiado de los criterios de evaluación del tema deben ser evaluados en función de los siguientes cinco criterios de idoneidad:

- **Objetividad**: Los criterios no deben tener sesgo que pudiera afectar adversamente los hallazgos y las conclusiones del profesional y, en consecuencia, pudieran ocasionar una interpretación errónea por parte del usuario del reporte.
- **Completitud**: Los criterios deben ser lo suficientemente completos de modo que se puedan identificar y utilizar todos los criterios que pudieran afectar a las conclusiones de los profesionales cuando se realiza la asignación de auditoría o aseguramiento de SI.
- **Relevancia**: Los criterios deben ser relevantes para el tema y contribuir a los hallazgos y las conclusiones que cumplan con los objetivos de la asignación de auditoría o aseguramiento de SI.
- **Mensurabilidad**: Los criterios deben permitir una medición consistente del tema, así como el desarrollo de conclusiones coherentes cuando sean aplicados por diferentes profesionales en circunstancias similares.
- **Comprensibilidad**: Los criterios deben comunicarse claramente y no ofrecer ocasión a interpretaciones significativamente diferentes a sus usuarios.

La aceptación de los criterios se ve afectada por la disponibilidad de los criterios para los usuarios del reporte de los profesionales, de modo que los usuarios entiendan la base de la actividad de aseguramiento y la relevancia de los hallazgo y las conclusiones. Las fuentes pueden incluir aquellas que son:

- **Reconocidas**: Los criterios deben ser suficientemente bien reconocidos para que su uso no sea cuestionado por los usuarios previstos.

Aspectos clave Continúa

- **Autorizadas**: Deben buscarse criterios que reflejen pronunciamientos autorizados dentro del área y que sean adecuados para el tema. Por ejemplo, los pronunciamientos autorizados pueden provenir de organismos profesionales, grupos industriales, gobierno y reguladores.
- **Públicamente disponibles**: Los criterios deben estar disponibles para los usuarios del reporte de los profesionales. Los ejemplos incluyen estándares desarrollados por organismos de auditoría y contabilidad profesionales como ISACA, la Federación Internacional de Contadores (IFAC) y otros organismos profesionales o gubernamentales reconocidos.
- **Disponibles para todos los usuarios**: Cuando los criterios no están públicamente disponibles, éstos deben ser comunicados a todos los usuarios mediante afirmaciones que formen parte del reporte de los profesionales. Las afirmaciones consisten en declaraciones sobre el tema que cumplen con los requerimientos de criterios adecuados para que puedan ser auditados.

Además de la idoneidad y la disponibilidad, la selección de criterios de aseguramiento de SI debe considerar la fuente, en términos de su uso y posible audiencia. Por ejemplo, cuando se trata de regulaciones gubernamentales, los criterios basados en las afirmaciones desarrolladas a partir de la legislación y las regulaciones que se aplican al tema pueden ser más apropiados. En otros casos, los criterios de la asociación de comercio o industria pueden ser relevantes. Las posibles fuentes de criterios, enumeradas con el fin de consideración, son:

- **Criterios establecidos por ISACA**: Éstos son criterios públicamente disponibles y estándares que han sido expuestos para revisión por parte de compañeros y un exhaustivo proceso de debida diligencia por expertos internacionales reconocidos en gobierno, control, seguridad y aseguramiento de TI.
- **Criterios establecidos por otros organismos de expertos**: Similares a los criterios y estándares de ISACA, éstos son relevantes para el tema y han sido desarrollados y expuestos para revisión de compañeros y un exhaustivo proceso de debida diligencia por expertos en varios campos.
- **Criterios establecidos por leyes y regulaciones**: Si bien las leyes y regulaciones pueden brindar la base de los criterios, debe tenerse cuidado en su uso. Frecuentemente, la terminología es compleja y acarrea un significado legal específico. En muchos casos, puede ser necesaria para reafirmar los requerimientos como afirmaciones. Además, expresar una opinión sobre la legislación está normalmente restringido a los miembros de la profesión legal.
- **Criterios establecidos por empresas que no respetan el debido proceso**: Éstos incluyen criterios relevantes desarrollados por otras empresas que no respetaron el debido proceso y no han sido sujetos a debate y consulta pública.
- **Criterios desarrollados específicamente para la asignación de auditoría o aseguramiento de SI**: Si bien los criterios desarrollados específicamente para la asignación de auditoría o aseguramiento de SI pueden ser apropiados, debe tenerse especial cuidado para asegurar que estos criterios cumplan con los criterios de idoneidad, completitud particular, mensurabilidad y objetividad. Los criterios desarrollados específicamente para una asignación de auditoría o aseguramiento de SI están en forma de afirmaciones.

Los criterios de selección deben ser considerados con cuidado. Si bien el cumplimiento con las regulaciones y leyes locales es importante y debe considerarse como un requerimiento obligatorio, se reconoce que muchas asignaciones de auditoría y aseguramiento de SI incluyen áreas, tales como gestión de cambios, controles de acceso y controles generales de TI, no cubiertas por regulaciones o leyes. Además, algunas industrias, como la industria de tarjetas de pagos, han establecido requerimientos obligatorios establecidos que deben cumplirse. Cuando los requerimientos legislativos están basados en principios, el profesional debe asegurar que los criterios seleccionados cumplan con el objetivo de la asignación.

A medida que avanza la asignación, la información adicional puede resultar en ciertos criterios que no son necesarios para cumplir con los objetivos. En esas circunstancias, no es necesario el trabajo adicional relacionado con los criterios.

Términos

Término	Definición
Criterios	Estándares y análisis comparativos (benchmarks) utilizados para medir y presentar el tema y en el que un auditor de SI evalúa el tema. Los criterios deben ser: • Objetivos: Sin sesgo • Completos: Incluyen todos los factores relevantes para llegar a una conclusión • Relevantes: Se relacionan con el tema • Medibles: Brindan medición coherente En una asignación de testación, los análisis comparativos (benchmarks) de acuerdo con los que se puede evaluar la afirmación escrita de la dirección sobre el tema. El profesional formula una conclusión sobre el tema al consultar los criterios adecuados.

Enlace a los lineamientos

Tipo	Título
Lineamiento	2008 Criterios

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.

