Guía de Auditoría y Aseguramiento de SI 2007 Afirmaciones

La naturaleza especializada de la auditoría y aseguramiento de los sistemas de la información (SI) y de las habilidades necesarias para realizar este tipo de compromisos requiere estándares que apliquen especialmente a las auditorías y aseguramiento de SI. El desarrollo y diseminación de los estándares de auditoría y aseguramiento de SI son la piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen requerimientos obligatorios para la auditoría de SI y presentación de informes e informan a:

- Los profesionales de auditoría y aseguramiento de SI de profesionales del nivel mínimo de desempeño aceptable requerido para cumplir las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- Expectativas de la gerencia y otras partes interesadas de la profesión respecto al trabajo de los profesionales.
- Los poseedores de la Certificación de Auditoría de Sistemas de la Información en Inglés Certified Information Systems Auditor® (CISA®). El incumplimiento de estos estándares puede dar lugar a una investigación sobre la conducta del poseedor del certificado CISA por la Junta Directiva de ISACA o el comité apropiado y, en última instancia, en una acción disciplinaria.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en sus trabajos, donde sea apropiado, indicando que el trabajo ha sido realizado de acuerdo con los estándares de auditoría y aseguramiento de los SI de ISACA o de otros posibles estándares aplicables.

ITAF™, un marco de trabajo de prácticas profesionales para auditoría y aseguramiento de SI, proporciona múltiples niveles de dirección:

- **Estándares**, divididos en tres categorías:
  - Estándares generales (series 1000)-Son los principios rectores bajo los que opera la profesión de auditoría y aseguramiento de SI. Aplican a la realización de todas las tareas, y hacen frente a la ética, independencia, objetividad y debida diligencia del profesional de auditoría y aseguramiento de SI, así como los conocimientos, competencia y habilidades. Las declaraciones de los estándares (en **negrita**) son obligatorias.
  - Estándares de desempeño (series 1200)- Tienen que ver con la forma en que se conduce la asignación, tales como planificación y supervisión, definición del alcance, riesgos y materialidad, la movilización de recursos, supervisión y administración de asignaciones, evidencias de auditoría y aseguramiento, y el ejercicio de su juicio profesional y debida diligencia.
  - Estándares de presentación de informes (series 1400)-Direccionan los tipos de informes, medios de comunicación y la información comunicada.
- **Guías**, apoyan a los estándares y también se dividen en tres categorías:
  - Guías generales (series 2000).
  - Guías de rendimiento (series 2200).
  - Guías de presentación de informes (series 2400).
- **Herramientas y técnicas**, proporcionan una guía adicional para los profesionales de auditoría y aseguramiento de SI, por ejemplo, documento técnico (white paper), programas de auditoría / aseguramiento de SI, los productos de la familia de COBIT® 5.

Se proporciona un glosario en línea de los términos utilizados en ITAF en *www.isaca.org/glossary*.

Aclaración: ISACA ha diseñado esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado exitoso. La publicación no debe considerarse como incluyente de cualquier procedimiento y pruebas o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a obtener los mismos resultados. Para determinar la conveniencia de cualquier procedimiento o prueba específica, los profesionales de controles deben aplicar su propio juicio profesional a las circunstancias de control específicas presentadas por los sistemas particulares o entorno de SI.

El Comité de Estándares Profesionales y Administración de Carreras de ISACA, en Inglés “ISACA Professional Standards and Career Management Committee” (PSCMC) se ha comprometido a una amplia consulta en la preparación de estándares y guías. Antes de emitir cualquier documento, se emite internacionalmente un borrador de la norma para comentar por el público general. Los comentarios pueden también presentarse a la atención del director de desarrollo de estándares profesionales por correo electrónico (*standards@isaca.org*), fax (+1.847. 253.1443) o correo postal (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

La guía se presenta en las siguientes secciones:
1. Propósito de la guía y vinculación con estándares.
2. Contenido de la guía.
3. Relación con estándares y procesos de COBIT 5.
4. Terminología.
5. Fecha de vigencia.

1. Propósito de la Guía y Vinculación con Estándares

1.0 Introducción

Esta sección clarifica:
1.1 Propósito de la guía.
1.2 Vinculación con estándares.
1.3 Uso de términos 'función de auditoría' y 'profesionales'.

1.1 Propósito

1.1.1 El propósito de esta guía es detallar las diferentes afirmaciones, guiar a los profesionales de auditoría y aseguramiento de SI en asegurar que el criterio, contra los que se evalúa la materia, es compatible con las afirmaciones y proporcionan orientación para formular una conclusión y redacción de un informe sobre las afirmaciones.

1.1.2 Los profesionales de auditoría y aseguramiento de SI deben considerar esta guía para determinar cómo implementar el estándar, uso del juicio profesional en su aplicación, estar preparado para justificar cualquier desvío y buscar guías adicionales si se considera necesario.

1.2 Vinculación con Estándares

1.2.1 Estándar 1007 Afirmaciones.
1.2.2 Estándar 1008 Criterios.
1.2.3 Estándar 1204 Materialidad.
1.2.4 Estándar 1206 Uso del Trabajo de Otros Expertos.
1.2.5 Estándar 1401 Reportes.

1.3 Uso de Términos

1.3.1 De aquí en adelante:
- 'Función de auditoría y aseguramiento de SI' está referenciada como 'función de auditoría'.
- 'Profesionales de auditoría y aseguramiento de SI' está referenciada como 'profesionales'.

2. Contenido de la Guía

2.0 Introducción

La sección del contenido de la guía está estructurada para proporcionar información sobre los siguientes temas de compromiso clave de auditoría y aseguramiento de SI:
2.1 Afirmaciones.
2.2 Materia y criterios.
2.3 Afirmaciones desarrolladas por terceros.

2.4 Conclusión e informe

2.1 Afirmaciones

2.1.1 Las afirmaciones son toda declaración o conjunto de declaraciones si la materia se basa en la conformidad con los criterios seleccionados. Los profesionales deben tener en cuenta estas afirmaciones durante la ejecución de un trabajo de auditoría, obtener aseguramiento de su logro y expresarlas en un informe de auditoría.

2.1.2 Las afirmaciones comunes que se pueden considerar son:

- **Confidencialidad**—Preservar las restricciones autorizadas al acceso y divulgación, así como medios para proteger la privacidad y la propiedad de la información.
- **Completitud**—Todas las actividades, información y otros datos que deberían haberse registrado están registrados, por ejemplo, todos los cambios a los sistemas de TI promovidos a producción se registran en la aplicación de seguimiento de gerencia del cambio.
- **Precisión**—Los importes, fechas y otros datos relacionados con las actividades registradas se han registrado adecuadamente, por ejemplo, datos relacionados a la promoción de cambios en los sistemas de TI en producción se muestran correctamente en los registros de cambios de la aplicación de seguimiento de gerencia del cambio.
- **Integridad**—La información, evidencias y otros datos recibidos provienen de fuentes confiables, por ejemplo, los registros de cambios solicitados por los profesionales se reciben desde el gerente de cumplimiento, una fuente de confianza y fiable dentro de la empresa.
- **Disponibilidad**—La información, evidencias y otros datos requeridos para el trabajo de auditoría existen y son accesibles, por ejemplo, los registros de solicitud de cambios existen y son de fácil acceso en la aplicación de seguimiento de gerencia del cambio.
- **Cumplimiento**—La información, evidencias y otros datos han sido grabados de acuerdo a la empresa, regulaciones o de otras estipulaciones aplicables, por ejemplo, los campos necesarios, de acuerdo a las estipulaciones aplicables, están presentes en los registros de cambios de la aplicación de seguimiento de gerencia del cambio.

2.1.3 La gerencia es responsable de definir y aprobar la materia y afirmaciones relacionadas. Los profesionales deben asegurarse que cualquier afirmación desarrollada por la gerencia es lo que un lector o usuario experto podrían esperar comparado a los estándares de pronunciamientos autorizados.

2.1.4 Una precondición previa para que el profesional acepte el trabajo de auditoría debe ser la confirmación de la gerencia que comprende completamente su responsabilidad de proporcionar toda la información necesaria respecto a la materia y las afirmaciones de los profesionales. Si los profesionales creen que la gerencia no será capaz de cumplir esta responsabilidad, deben:

- Informar a la gerencia de auditoría y aseguramiento de SI y a los encargados del Gobierno de las cuestiones identificadas.
- No aceptar el trabajo de auditoría propuesto.

2.1 Afirmaciones cont.

2.1.5 Los profesionales deben revisar las afirmaciones seleccionadas para el trabajo de auditoría y asegurar que son:

- **Suficientes**—Para cumplir el propósito del trabajo de auditoría, que está expresando una opinión o conclusión de la materia en el alcance.
- **Validas**—Capaz de ser probadas, dada la materia en el alcance.
- **Relevante**—Tener una conexión directa a la materia en el alcance y contribuir al cumplimiento de la finalidad del trabajo de auditoría.

2.2 Materia y Criterios

2.2.1 La materia de un trabajo de auditoría está determinada por la gerencia y los encargados del Gobierno. Normalmente, la materia del trabajo de auditoría de SI no será definida con tanta precisión como lo es en los trabajos de auditoría financiera. Por ejemplo, la materia de la asignación de auditoría y aseguramiento de SI puede variar de un sistema y sus interfaces, a los procesos (cubriendo múltiples sistemas e interfaces), o incluso todas las operaciones relativas a SI de un cierto departamento.

2.2.2 Los profesionales deben evaluar la materia del trabajo de auditoría contra los criterios predeterminados para expresar una opinión o conclusión sobre la materia. Los profesionales deben evaluar estos criterios para asegurar que respaldan las afirmaciones relevantes.

2.2.3 Un criterio puede vincular a múltiples afirmaciones. Por otra parte, una afirmación puede también ser apoyada por múltiples criterios que todos proporcionan una parte de la seguridad en la consecución de la afirmación.

2.2.4 En caso que los profesionales concluyan que los criterios no soportan completamente todas las afirmaciones relevantes, deben hacer sugerencias para modificar los criterios existentes o para añadir criterios adicionales. La gerencia de auditoría y aseguramiento de SI revisa y aprueba o rechaza los criterios nuevos o modificados.

2.2.5 Tras evaluar que los criterios soportan totalmente las afirmaciones relevantes, los profesionales deben evaluar que los criterios pueden ser sujeto de aun análisis objetivo y medible, como se detalla en el Estándar 1008 Criterios.

2.3 Afirmaciones Desarrolladas por Terceros

2.3.1 Las empresas que externalizan operaciones a terceros recibirán informes sobre el entorno de control de las operaciones externalizadas. La gerencia revisara cada informe para determinar si:

- El informe es emitido por una entidad profesional independiente relevante.
- La opinión de auditoría es cualificada o no cualificada.
- El alcance de los objetivos de control cubre adecuadamente los controles requeridos por la empresa.
- El periodo auditado este en línea con las expectativas de la empresa.
- Las deficiencias de controles específicos (que no conducen a una calificación global del informe) son relevantes para la empresa.
- Las afirmaciones utilizadas están en línea con las afirmaciones requeridas.

2.3 Afirmaciones Desarrolladas por Terceros cont.

La gerencia de auditoría y aseguramiento de SI debe documentar el análisis realizado y las conclusiones alcanzadas. Los profesionales deben asegurarse que las afirmaciones están verificadas y aprobadas formalmente por la gerencia, como parte de un trabajo de auditoría que tiene en el alcance las operaciones externalizadas. El estándar 1206 Uso del Trabajo de Otros Expertos proporciona mas orientación sobre este tema.

2.4 Conclusión e Informe

2.4.1 Después de evaluar la materia del trabajo de auditoría contra los criterios, los profesionales deben formar una conclusión sobre cada afirmación, basada en la suma de los hallazgos contra los criterios relacionados, junto con el juicio profesional.

2.4.2 Tras formar una conclusión, los profesionales deben emitir un informe indirecto o directo sobre la materia:

- **Informe indirecto**—En las afirmaciones sobre la materia. Por ejemplo, en la afirmación 'completitud', para un componente en la materia: 'Basado en nuestras pruebas de efectividad operativa, en nuestra opinión los cambios de sistemas de TI promocionan a producción, en todos los aspectos materiales de acuerdo a los criterios seleccionados, han sido completamente registrados en la aplicación de seguimiento de gerencia del cambio'.
- **Informe directo**—En la materia en sí misma. Por ejemplo, sobre la materia entera: 'Basado en nuestras pruebas, en nuestra opinión los cambios en los sistemas de TI están siguiendo, en todos los aspectos materiales de acuerdo a los criterios seleccionados, los procedimientos de gerencia del cambio requeridos'.

---

3. Relación con Estándares y Procesos de COBIT 5

3.0 Introducción

Esta sección proporciona una visión general relevante de:
3.1 Relación con Estándares.
3.2 Relación con los procesos de COBIT 5.
3.3 Otras guías.

3.1 Relación con Estándares

La tabla proporciona una visión general de:

- Los estándares más relevantes de auditoría y aseguramiento de SI de ISACA que está directamente soportado por esta guía.
- Las declaraciones estándar más relevantes para esta guía.

Nota: Sólo se enumeran las declaraciones estándar más relevantes para esta guía.

Titulo del Estándar	Declaración Estándar Relevante
1007 Afirmaciones	Los profesionales de auditoría y aseguramiento de SI revisaran las afirmaciones contra las que la materia será evaluada para determinar que tales afirmaciones son susceptibles de ser auditadas y que las afirmaciones son suficientes, validas y relevantes.

Titulo del Estándar	Declaración Estándar Relevante
1008 Criterios	Los profesionales de auditoría y aseguramiento seleccionaran criterios, contra los que se evaluara la materia, que son objetivos, completos, relevantes, medibles, comprensibles, ampliamente reconocidos, autorizadas y comprendidas por, o disponibles para, todos los lectores y usuarios del informe.
1204 Materialidad	Los profesionales de auditoría y aseguramiento revelaran lo siguiente en el informe de auditoría: • Ausencia de controles o controles inefectivos. • Importancia de la deficiencia de los controles. • Probabilidad de que estas debilidades resulten en una deficiencia significativa o material.
1206 Uso del Trabajo de Otros Expertos	Los profesionales de auditoría y aseguramiento deberán asesorar, revisar y evaluar el trabajo de otros expertos como parte del trabajo, y documentar la conclusión sobre el grado de uso y confianza en su trabajo.
1401 Reportes	Los profesionales de auditoría y aseguramiento de SI deberán presentar un informe para comunicar los resultados una vez finalizado el trabajo, incluyendo: • Identificación de la empresa, destinatarios y cualquier restricción al contenido y circulación. • El alcance, objetivos de trabajo, periodo de cobertura y naturaleza, tiempos y alcance de los trabajos realizados. • Los hallazgos, conclusiones y recomendaciones. • Cualquier cualificación o limitación al alcance que el profesional de auditoría y aseguramiento de SI tiene respecto al trabajo. • Firma, fecha y distribución de acuerdo a los términos de la Estatuto de Auditoría o carta de compromiso.

3.2 Relación con los Procesos de COBIT 5

La tabla proporciona una visión general de los más relevantes:

- Procesos de COBIT 5.
- Propósito de los procesos de COBIT 5.

Se encuentran actividades específicas realizadas como parte de la ejecución de estos procesos en *COBIT 5: Habilitación de Procesos*.

Procesos de COBIT 5	Propósito de los Procesos
EDM01 Asegurar el establecimiento y mantenimiento del marco de Gobierno.	Proporcionar un enfoque consistente integrado y alineado con el enfoque de Gobierno de la empresa. Para asegurar que las decisiones relacionadas con TI se hacen en línea con las estrategias y objetivos de la empresa, asegurando que los procesos relacionados con TI son supervisados de forma efectiva y transparente, se confirma el cumplimiento con los requerimientos legales y regulatorios, y se cumplen los requerimientos del Gobierno de los miembros del consejo.

Procesos de COBIT 5	Propósito de los Procesos
MEA02 Monitorear y evaluar el sistema de controles internos.	Obtener transparencia para los interesados clave en la adecuación de los sistemas de control interno y, por tanto, proporcionar confianza en las operaciones, confianza en el logro de objetivos empresariales y una adecuada comprensión del riesgo residual.

3.3 Otras Guías

En la implementación de estándares y guías, se insta a los profesionales a buscar otras guías cuando se considere necesario. Esto podría ser con el apoyo de:

- Colegas dentro y fuera de la empresa, por ejemplo, a través de asociaciones profesionales o grupos de redes sociales profesionales.
- Gerentes.
- Órganos del Gobierno dentro de la empresa, ejemplo, comité de auditoría.
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías).

4. Terminología

Término	Definición
Afirmación	Cualquier declaración formal o conjunto de declaraciones sobre la materia hecha por la gerencia. Las afirmaciones deben ser generalmente por escrito y comúnmente tener una lista de atributos específicos sobre la materia o sobre un proceso involucrando la materia.
Criterios	Los estándares y puntos de referencia utilizados para medir y presentar la materia y contra el cual el auditor de SI evalúa la materia. Los criterios deben ser: • Objetivos—Libres de prejuicios. • Completos—Incluir todos los factores relevantes para alcanzar una conclusión. • Relevante—Relacionado a la materia. • Medible—Proporcionar una medición coherente. • Comprensible. En un trabajo de certificación, los puntos de referencia contra los que la aserción por escrito de la gerencia en la materia puede ser evaluada. El facultativo forma una conclusión sobre la materia haciendo referencia a criterios adecuados.
Juicio profesional	La aplicación de conocimientos y experiencias relevantes para tomar decisiones informadas acerca de los cursos de acceso que son apropiados en las circunstancias del encargo de la auditoría y aseguramiento de SI.
Materia	La información específica objeto de un informe de un auditor de SI y los procedimientos relacionados, que puede incluir cosas tales como el diseño o la operación de controles internos y cumplimiento de las practicas de privacidad, estándares, legislación y regulaciones especificas (área de actividad).

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para toda asignación de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.

