

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).

ISACA 2013-2014 Professional Standards and Career Management Committee

Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP	University of North Texas, USA
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Todd Weinman	TheWeinman Group, USA

Guía de Auditoría y Aseguramiento de SI 2006 Competencia

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** Esta guía ofrece orientación para ayudar a los profesionales de auditoría y aseguramiento de SI a adquirir las habilidades y conocimiento necesario y mantener las competencias profesionales en el ejercicio de los trabajos de auditoría.
 - 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 preparados para justificar cualquier desviación y buscar asesoramiento adicional si se considera necesario.
-

1.2 Vinculación con Estándares

- 1.2.1** Estándar 1005 Debido Cuidado Profesional.
 - 1.2.2** Estándar 1006 Competencia.
 - 1.2.3** Estándar 1201 Planificación de la Asignación.
 - 1.2.4** Estándar 1203 Desempeño y Supervisión.
-

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 Competencia profesional.
 - 2.2 Evaluación.
 - 2.3 Alcanzar el nivel de competencia deseado.
-

Guía de Auditoría y Aseguramiento de SI 2006 Competencia

2.1 Competencia Profesional

- 2.1.1 La [competencia profesional](#) implica poseer las habilidades, conocimiento y experiencia, a través de un nivel adecuado de educación y experiencia, para tener la capacidad de realizar adecuadamente un trabajo de auditoría.
- 2.1.2 La gerencia de auditoría y aseguramiento de SI debe comunicar el nivel deseado y/o esperado de competencia profesional, basado en criterios adecuados, para los roles diferentes en los trabajos de auditoría y asegurar que dichos puntos de referencia son revisados y actualizados periódicamente. La gerencia de auditoría y aseguramiento de SI debe documentar la competencia profesional requerida para los distintos niveles de trabajo, por ejemplo formulando una matriz de habilidades que indique la competencia profesional requerida para los distintos niveles de trabajo.
- 2.1.3 La gerencia de auditoría y aseguramiento de SI debe proporcionar aseguramiento razonable de la disponibilidad de recursos competentes requeridos para llevar a cabo los trabajos de auditoría definidos en el plan de auditoría de SI, y se debe confirmar y asegurar la disponibilidad de los recursos competentes antes de comenzar el trabajo de auditoría.
- 2.1.4 La gerencia de auditoría y aseguramiento de SI es responsable de asegurar que los miembros del equipo son competentes para realizar el trabajo de auditoría. La identificación de competencias profesionales básicas de los miembros del equipo ayudará en la utilización eficiente de los recursos disponibles.
- 2.1.5 Los profesionales deben proporcionar aseguramiento razonable de la posesión de los niveles requeridos de la competencia profesional. Deben ser responsables de adquirir las habilidades profesionales y técnicas requeridas y el conocimiento para llevar a cabo cualquier asignación que acepten realizar.
- 2.1.6 Las habilidades y conocimientos requeridos varían según las posiciones y los roles profesionales respecto al trabajo de auditoría. El requerimiento de habilidades y conocimiento de gerencia debe ser acorde con los niveles de responsabilidad.
- 2.1.7 Las habilidades y conocimiento incluyen [competencia](#) en la identificación y administración de riesgos y controles, así como herramientas y técnicas de auditoría. Los profesionales deben poseer conocimiento analítico y técnico junto con habilidades de entrevista, interpersonales y de presentación.
- 2.1.8 Los profesionales deben poseer el conocimiento para identificar, determinar el impacto y comunicar posibles condiciones o desviaciones que son [materiales](#) para el trabajo de auditoría.
- 2.1.9 Los profesionales deben poseer la habilidad de reconocer posibles indicios de fraude.
- 2.1.10 Los profesionales deben tener un conocimiento general de los fundamentos de negocio, por ejemplo, economía, finanzas, contabilidad, tecnología de la información, riesgos, impuestos y leyes para evitarles posibles problemas o deficiencias.
- 2.1.11 Es conveniente que los profesionales compartan sus experiencias, buenas prácticas adoptadas, lecciones aprendidas y conocimientos adquiridos con los miembros del equipo para mejorar las competencias profesionales de los recursos. Las competencias profesionales de los miembros del equipo también mejoran con sesiones de formación de equipos, talleres, conferencias, seminarios, clases y otros modos de interacción.

Guía de Auditoría y Aseguramiento de SI 2006 Competencia

2.1 Competencia Profesional cont.

- 2.1.12** Para asegurar la disponibilidad de las habilidades adecuadas, se deben de evaluar los medios alternativos de adquirir estas habilidades. Incluyendo la subcontratación de recursos específicos, externalizar una parte de las tareas de auditoría y aseguramiento de SI y/o retrasar el trabajo de auditoría hasta que estén disponibles las habilidades necesarias.
 - 2.1.13** El conocimiento externo se puede obtener externalizando parte del trabajo. La colaboración entre recursos externalizados y profesionales internos asegura que el conocimiento y las habilidades también se desarrollarán y mantendrán internamente.
 - 2.1.14** Cuando una parte del trabajo de auditoría se externaliza o se obtiene asistencia experta, se debe proporcionar una seguridad razonable de que la agencia subcontratada o el experto externo posee la competencia profesional requerida.
 - 2.1.15** Cuando se obtiene asistencia experta de forma regular, la competencia profesional de dichos expertos se debe medir, monitorear y revisar periódicamente contra los estándares o parámetros profesionales.
-

2.2 Evaluación

- 2.2.1** Los profesionales deben monitorear continuamente sus habilidades y conocimientos para mantener el nivel adecuado de competencia profesional. La gerencia de auditoría y aseguramiento de SI debe evaluar periódicamente la competencia profesional.
 - 2.2.2** La evaluación del desempeño de los profesionales debe llevarse a cabo de manera justa, transparente, fácil de entender, sin ambigüedades, sin prejuicios y considerada una práctica general aceptable dado el entorno de trabajo.
 - 2.2.3** Se deben definir claramente los criterios y procedimientos de evaluación, pero pueden variar dependiendo de las circunstancias como localización geográfica, clima político, naturaleza de la asignación, cultura o de otras circunstancias similares.
 - 2.2.4** En el caso de un equipo de profesionales, la evaluación debe llevarse a cabo internamente entre los equipos o individuos sobre una base multi funcional.
 - 2.2.5** En el caso de individuos profesionales independientes, la evaluación debe ser realizada en la medida de lo posible por una relación entre iguales. Si una revisión entre iguales no es posible, se debe realizar y documentar una autoevaluación.
 - 2.2.6** La evaluación del desempeño de los profesionales se debe realizar por un nivel de gerencia adecuado.
 - 2.2.7** Las ausencias observadas durante la evaluación deben ser abordadas adecuadamente.
-

Guía de Auditoría y Aseguramiento de SI 2006 Competencia

2.3 Alcanzar el Nivel de Competencia Deseado

- 2.3.1** Se debe registrar y analizar las ausencias observadas basadas en la diferencia entre el nivel actual de y el nivel esperado de competencia profesional. Cuando exista una deficiencia significativa en cualquier recurso, no se debe utilizar dicho recurso en la realización de un trabajo de auditoría.
- 2.3.2** Es importante determinar la causa de las ausencias y tomar las medidas de acción correctivas adecuadas, como entrenamiento y educación profesional continua (CPE), tan pronto como sea posible.
- 2.3.3** Se deben completar las actividades de entrenamiento requeridas para un trabajo de auditoría en tiempo razonable y antes de comenzar la actividad de auditoría.
- 2.3.4** Se debe medir la efectividad del entrenamiento después de un tiempo razonable tras finalizar el entrenamiento.
- 2.3.5** La documentación de las habilidades requeridas, como matriz de habilidades, según se formuló por la gerencia de auditoría y aseguramiento de SI (2.1.2), ayudará a identificar las ausencias y necesidades de entrenamiento. La matriz puede ser una referencia cruzada de recursos disponibles y sus habilidades y conocimientos.
- 2.3.6** Se deben mantener, analizar y referenciar para uso futuro los registros de entrenamiento proporcionado, junto con comentarios sobre la formación y su efectividad.
- 2.3.7** CPE es la metodología adoptada para mantener la competencia profesional y las habilidades y conocimientos actualizados. Los profesionales deben cumplir con los requerimientos de las políticas establecidas de los CPE por sus respectivos colegios profesionales a los que están asociados.
- 2.3.8** Los programas de CPE deben ayudar en la mejora de las habilidades y conocimientos relacionados a los requerimientos profesionales y técnicos de aseguramiento, seguridad y Gobierno de SI. Los colegios profesionales normalmente prescriben eventos elegibles para el reconocimiento de CPE. Los profesionales deben observar las normas prescritas por sus respectivos colegios profesionales.
- 2.3.9** Los colegios profesionales normalmente prescriben la metodología de obtención de los créditos CPE y los créditos mínimos que deben ser obtenidos periódicamente por sus asociados. Los profesionales deben observar dichas normas prescritas por sus respectivos colegios profesionales. Si los profesionales están asociados a más de un colegio profesional, pueden usar su [juicio profesional](#) a efectos de obtener los créditos mínimos haciendo uso común de los créditos CPE según los eventos elegibles, siempre que la misma sea consistente con las reglas / guías enmarcadas dentro del colegio profesional respectivo.
- 2.3.10** ISACA tiene una política integral de CPE, aplicable a sus miembros y poseedores de la designación CISA. Los profesionales con la designación CISA deben cumplir las políticas CPE de ISACA. Los detalles de la política están disponibles en www.isaca.org/CISAcpepolicy.
- 2.3.11** Como establecen los colegios profesionales respectivos, incluyendo ISACA, los profesionales deben mantener registros adecuados de los eventos CPE, conservarlas para los periodos específicos, y de ser necesario, tenerlas disponibles para la auditoría.

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.

Título del Estándar	Declaración Estándar Relevante
1005 Debido Cuidado Profesional	Los profesionales de auditoría y aseguramiento de SI ejercerán debido cuidado, incluyendo la observación de estándares de auditoría profesional aplicables, en la planificación, desarrollo y presentación de los resultados de los trabajos.
1006 Competencia	<p>Los profesionales de auditoría y aseguramiento de SI, colectivamente con otros asistentes de la asignación, deben poseer habilidades y competencia adecuadas en la realización de trabajos de auditoría y aseguramiento de SI y ser profesionalmente competentes para realizar el trabajo requerido.</p> <p>Los profesionales de auditoría y aseguramiento de SI, junto con otros que ayuden en el trabajo, deberán poseer el conocimiento adecuado de la materia.</p> <p>Los profesionales de auditoría y aseguramiento de SI deberán mantener competencia profesional a través de la adecuada formación profesional continua y de entrenamiento.</p>
1201 Planificación de la Asignación	<p>Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir:</p> <ul style="list-style-type: none"> • Objetivo(s), alcance, línea de tiempo y entregables. • Cumplimiento con leyes aplicables y estándares de auditoría profesionales. • Uso de enfoque basado en riesgos, cuando sea adecuado • Cuestiones específicas del trabajo. • Requisitos de documentación y presentación de informes. <p>Los profesionales de auditoría y aseguramiento de SI deberán desarrollar y documentar un plan de proyecto del trabajo de auditoría o aseguramiento de SI, describiendo:</p> <ul style="list-style-type: none"> • La naturaleza, objetivos, línea de tiempo y recursos requeridos del trabajo.

Guía de Auditoría y Aseguramiento de SI 2006 Competencia

Título del Estándar	Declaración Estándar Relevante
	<ul style="list-style-type: none"> Tiempos y grado de los procedimientos de auditoría para completar el trabajo.
1203 Desempeño y Supervisión	<p>Los profesionales de auditoría y aseguramiento proporcionaran supervisión al personal de auditoría de SI para quienes tienen la responsabilidad de supervisar, para cumplir los objetivos de auditoría y cumplir con los estándares de auditoría profesional aplicables.</p> <p>Los profesionales de auditoría y aseguramiento de SI aceptarán sólo tareas que están dentro de su conocimiento y habilidades o para los que tienen expectativas razonables de adquirir las habilidades durante el trabajo o lograr la tarea bajo supervisión.</p>

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
EDM04 Asegurar la optimización de los recursos.	Asegurar que se cumplen las necesidades de recursos de la empresa de forma óptima, costes de TI optimizados, y hay mayor probabilidad de aumentar los beneficios y prepararse para el cambio futuro.
APO07 Administración de recursos humanos.	Optimizar las capacidades de los recursos humanos para cumplir los objetivos empresariales.
MEAO2 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 desde auditoría y aseguramiento de SI:

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

4. Terminología

Término	Definición
Competencia	Poseer habilidades y experiencia.
Competencia profesional	Nivel probado de capacidad, junto con experiencia profesional, a menudo vinculado a las calificaciones emitidas por cuerpos profesionales pertinentes y el cumplimiento de sus códigos de práctica y estándares.
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.
Materialidad	Un concepto de auditoría respecto de la importancia de una información respecto a su impacto o efecto en el sujeto auditado. Una expresión del significado o importancia relativa de una materia particular en el contexto del encargo o la empresa en su conjunto.

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.