



## Guía de Auditoría y Aseguramiento de SI 2004 Expectativa Razonable

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](http://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](mailto: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 2004 Expectativa Razonable

La guía se presenta en las siguientes secciones:

1. Propósito de la guía y vinculación con estándares.
  2. Contenido de la guía.
  3. Referencias a 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 asistir a los profesionales de auditoría y aseguramiento de SI en implementar el principio de expectativa razonable en la ejecución de encargos de auditoría. Las principales características sobre las que los profesionales deben tener expectativa razonable son:
    - El trabajo de auditoría se puede realizar de acuerdo con estas normas, otros estándares o reglamentos aplicables, y dar lugar a una opinión o conclusión profesional.
    - El alcance del trabajo de auditoría permite expresar una opinión o conclusión sobre el sujeto.
    - La administración les proporcionará información apropiada, relevante y oportuna requerida para realizar el trabajo de auditoría.
  - 1.1.2** Esta guía ayuda también a los profesionales de auditoría y aseguramiento de SI a abordar las limitaciones del alcance y proporciona orientación para aceptar un cambio en los términos.
  - 1.1.3** Los profesionales de auditoría y aseguramiento de SI deben considerar esta guía cuando determinen como implementar el estándar, uso de juicio profesional en su aplicación, estar preparado para justificar cualquier desvío y buscar orientación adicional si se considera necesario.
- 

### 1.2 Vinculación con Estándares

- 1.2.1** Estándar 1001 Estatuto de Auditoría.
  - 1.2.2** Estándar 1004 Expectativa Razonable.
- 

### 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'.
-

# Guía de Auditoría y Aseguramiento de SI 2004 Expectativa Razonable

## 2. Contenido de la Guía

<b>2.0 Introducción</b>	<p>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:</p> <ul style="list-style-type: none"><li>2.1 Estándares y reglamentos.</li><li>2.2 Alcance.</li><li>2.3 Limitaciones del alcance.</li><li>2.4 Información.</li><li>2.5 Aceptación de un cambio en los términos de compromiso.</li></ul> <hr/>
<b>2.1 Estándares y Reglamentos</b>	<ul style="list-style-type: none"><li><b>2.1.1</b> El Estatuto de Auditoría determinará a qué estándares se adherirá la función de auditoría y los profesionales, como se describe en el Estándar 1001 Estatuto de Auditoría.</li><li><b>2.1.2</b> Los profesionales deben reunir y evaluar todos los estándares y regulaciones aplicables en el Estatuto de Auditoría antes del trabajo de auditoría y volver a ellos durante el trabajo para determinar si tienen expectativa razonable de poder completar el trabajo de auditoría de acuerdo con los estándares y regulaciones, y que el trabajo de auditoría se traducirá en una opinión o conclusión profesional.</li><li><b>2.1.3</b> En caso de que los profesionales determinen que el trabajo de auditoría no puede ser completado de acuerdo con uno o más de los estándares y regulaciones aplicables y expresando que no será posible una opinión o conclusión, deben:<ul style="list-style-type: none"><li>• Informar a la gerencia de auditoría y aseguramiento de SI y a los encargados del Gobierno, de los asuntos de cumplimiento identificados con los estándares y regulaciones.</li><li>• Proponer un cambio en los términos del trabajo o que el trabajo propuesto no se acepta.</li></ul></li></ul> <hr/>
<b>2.2 Alcance</b>	<ul style="list-style-type: none"><li><b>2.2.1</b> Antes de emprender el trabajo de auditoría, los profesionales deben revisar el alcance del trabajo de auditoría. Deben determinar que el alcance de la auditoría está claramente documentada y permite una opinión o conclusión profesional que puede extraerse del sujeto.</li><li><b>2.2.2</b> El alcance del trabajo de auditoría debe estar claramente documentado, sin margen para la interpretación de qué áreas (por ejemplo, procesos, actividades, sistemas) están en el alcance del trabajo. Un alcance que esté descrito muy vagamente no permitirá a los profesionales formar una opinión o conclusión profesional, porque no hay certeza de que se evalúan todas las áreas del alcance.</li><li><b>2.2.3</b> En caso de que los profesionales determinen que el ámbito del trabajo de auditoría no les permite expresar una opinión o conclusión profesional, deben:<ul style="list-style-type: none"><li>• Informar a la gerencia de auditoría y aseguramiento y a los encargados del Gobierno de los asuntos identificados en el alcance.</li><li>• Proponer un cambio en los términos del encargo o no aceptar el trabajo de auditoría propuesto.</li></ul></li></ul>

# Guía de Auditoría y Aseguramiento de SI 2004 Expectativa Razonable

---

## 2.3 Limitaciones del Alcance

- 2.3.1** Antes o durante el trabajo de auditoría pueden suceder limitaciones al alcance específicas. Estas limitaciones al alcance pueden estar influenciadas por diferentes factores, como:
- Información adecuada, pertinente y oportuna requerida para completar el trabajo de auditoría no está disponible.
  - Los auditados (clave) no están disponibles.
  - El marco de tiempo incluido es insuficiente para completar el alcance completo del trabajo de auditoría.
  - La gerencia trata de limitar el alcance del trabajo de auditoría a las áreas seleccionadas.
  - El alcance del trabajo de auditoría es demasiado pequeño o grande para llegar a una conclusión de la materia.
  - El nivel de descentralización hace difícil llegar a una conclusión sobre la totalidad de la materia.
  - La disponibilidad de un número suficiente de profesionales debidamente cualificados para realizar el trabajo de auditoría con el alcance actual.
  - La estructura de presentación de informes de la función de auditoría, por ejemplo, si la función de auditoría no informa al nivel apropiado dentro de la empresa, puede no ser dirigida a evaluar ciertos elementos del alcance.
- 2.3.2** Los profesionales deben considerar si estas limitaciones al alcance todavía permiten una expectativa razonable de que el trabajo de auditoría resultará en una opinión o conclusión profesional. En caso de determinar que esta condición no se cumple, no deben aceptar el trabajo.
- 2.3.3** En caso de que los profesionales concluyan que tienen expectativa razonable de que, a pesar de las limitaciones al alcance, el trabajo resultará en una opinión o conclusión profesional, los profesionales deberán aceptar o continuar el trabajo de auditoría. Las limitaciones al alcance deben ser descritas explícitamente en el informe de la asignación de auditoría y aseguramiento de SI.
- 

## 2.4 Información

- 2.4.1** El Estatuto de Auditoría determinará el derecho de acceso a la información, sistemas, personal y locales relevantes al desarrollo del trabajo de auditoría, como se describe en el Estándar 1001 Estatuto de Auditoría.
- 2.4.2** Antes de emprender el trabajo de auditoría, los profesionales necesitan identificar y abordar cualquier restricción impuesta a su derecho de acceso adecuado, pertinente y oportuno al trabajo de auditoría. Deben tener una expectativa razonable de que sus derechos de acceso razonables para el trabajo de auditoría están conformes con lo establecido en el Estatuto de Auditoría, o esas desviaciones potenciales de esas estipulaciones no se oponen a los profesionales para alcanzar una opinión o conclusión sobre la materia.
- 2.4.3** La realización de un trabajo de auditoría o aseguramiento puede incluir la evaluación de actividades realizadas por la alta dirección y gerencia

# Guía de Auditoría y Aseguramiento de SI 2004 Expectativa Razonable

## 2.4 Información cont.

ejecutiva. La posibilidad de que tales eventos sucedan debe ser evaluada antes de la ejecución del trabajo de auditoría, así como que los profesionales sean desafiados en sus necesidades de acceso a estos individuos o información relacionada. Algunas de las medidas necesarias de mitigación antes de la ejecución del trabajo de auditoría serían:

- Asegurar que el Estatuto de Auditoría proporciona autoridad adecuada a la función de auditoría y los profesionales.
- Obtener el soporte explícito y escrito de los encargados del Gobierno, por ejemplo, consejo de administración y comité de auditoría.
- La asistencia de un miembro del consejo o de la gerencia ejecutiva cuando se requiera acceso a ejecutivos o altos directivos.

**2.4.4** En caso que los profesionales concluyan que su derecho de acceso a la información no les permite expresar una opinión o conclusión profesional, deben:

- Informar a la gerencia de auditoría y aseguramiento de SI y a los encargados del Gobierno de los elementos identificados con su derecho de acceso a la información apropiada, relevante y oportuna.
- Proponer un cambio en los términos del trabajo o no aceptar el trabajo de auditoría propuesto.

---

## 2.5 Aceptación de un Cambio en los Términos de Compromiso

**2.5.1** Los profesionales no deben aceptar un cambio en los términos del compromiso de auditoría cuando no haya justificación para hacerlo, basándose en su juicio profesional.

**2.5.2** Si a los profesionales, antes de la finalización del compromiso de auditoría, se les solicita un cambio en términos que disminuye el nivel de aseguramiento, deben determinar si hay justificación para hacerlo, basándose en su juicio profesional.

**2.5.3** Si se cambian los términos del compromiso de auditoría, deberán ser registrados y aprobados formalmente tanto por los profesionales como por los gerentes de auditoría y aseguramiento de SI. Tras completar el compromiso de auditoría, el informe de la asignación de auditoría y aseguramiento de SI debe mencionar este cambio de forma explícita.

**2.5.4** Si los profesionales no aceptan un cambio en los términos del compromiso de auditoría y la gerencia no les permite continuar el compromiso de auditoría original, en consulta con la gerencia de auditoría y aseguramiento deben:

- Retirarse del compromiso de auditoría.
  - Determinar, de acuerdo con su juicio profesional, la necesidad de informar las circunstancias a los encargados del Gobierno, el consejo de administración o incluso a los reguladores.
-

# Guía de Auditoría y Aseguramiento de SI 2004 Expectativa Razonable

## 3. Referencias a 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 están directamente soportados 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
1001 Estatuto de Auditoría	La función de auditoría y aseguramiento de SI deberá documentar la función de auditoría apropiadamente en un Estatuto de Auditoría, indicando propósito, responsabilidad, autoridad y responsabilidad final.  La función de auditoría y aseguramiento de SI deberá tener aceptada y aprobado el Estatuto de Auditoría a un nivel apropiado dentro de la empresa.
1004 Expectativa Razonable	Los profesionales de auditoría y aseguramiento de SI tendrán una expectativa razonable de que se podrá completar el trabajo de acuerdo con los estándares de auditoría y aseguramiento de SI y, cuando se requiera, otros estándares o reglamentos aplicables profesionales o de la industria apropiados y dará lugar a una opinión o conclusión profesional.  Los profesionales de auditoría y aseguramiento de SI deben tener expectativa razonable que el alcance del trabajo permite concluir sobre la materia y se ocupa de las restricciones.  Los profesionales de auditoría y aseguramiento de SI tendrán expectativa razonable de que la gerencia comprende sus obligaciones y responsabilidades respecto a la provisión de información apropiada, pertinente y oportuna requerida para realizar el trabajo.

---

# Guía de Auditoría y Aseguramiento de SI 2004 Expectativa Razonable

- 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
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.
MEAO3 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	Asegurar que la empresa cumple con todos los requerimientos externos.

- 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) de áreas de auditoría de SI y aseguramiento.

## 4. Terminología

Término	Definición
(Ninguno)	

## 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.