Guía de Auditoría y Aseguramiento de SI 2005 Debido Cuidado Profesional

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).

Guía de Auditoría y Aseguramiento de SI 2005 Debido Cuidado Profesional

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 clarificar el término 'debido cuidado profesional' que se aplica a la realización de un trabajo de auditoría con integridad y cuidado en el cumplimiento con los Códigos de Ética Profesional de ISACA.

1.1.2 Esta guía explica como los profesionales de auditoría y aseguramiento de SI deben aplicar el debido cuidado profesional en la planificación, realización y presentación de informes en un trabajo de auditoría.

1.1.3 Los profesionales de auditoría y aseguramiento de SI deben considerar esta guía para determinar cómo implementar el estándar, usen el juicio profesional en su aplicación, estar preparado para justificar cualquier desvío y buscar asesoramiento adicional si se considera necesario.

1.2 Vinculación con Estándares

1.2.1 Estándar 1002 Independencia Organizacional.
1.2.2 Estándar 1003 Independencia Profesional.
1.2.3 Estándar 1005 Debido Cuidado Profesional.
1.2.4 Estándar 1006 Competencia.
1.2.5 Estándar 1205 Evidencia de Auditoría.

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 2005 Debido Cuidado Profesional

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 El escepticismo y competencia profesional.
2.2 Aplicación.
2.3 Ciclo de vida del trabajo.
2.4 Comunicación.
2.5 Administración de la información.

2.1 El Escepticismo y Competencia Profesional

2.1.1 El debido cuidado profesional está relacionado al ejercicio del juicio profesional en la conducta del trabajo realizado. El debido cuidado profesional implica que los profesionales deben abordar los asuntos requeridos al juicio profesional con escepticismo profesional, diligencia, integridad y cuidado. Deben mantener su actitud durante todo el trabajo.

2.1.2 Los profesionales deben mantener la competencia, independencia y un estado objetivo de la mente en todos los asuntos relacionados a la realización del trabajo de auditoría. Deben ser honestos, imparciales y objetivos para abordar los problemas y alcanzar las conclusiones.

2.1.3 El Ejercicio del cuidado profesional debe hacer a los profesionales considerar la posible existencia de ineficiencias, malos usos, errores y exclusiones, incompetencia, conflictos de intereses o fraude. También debe hacer que los profesionales estén atentos a condiciones específicas o actividades en los que pueden ocurrir estos errores.

2.1.4 Al mantener informados y cumplir con la evolución de estándares profesionales, demuestran suficiente comprensión y competencia profesional para alcanzar los objetivos de auditoría y aseguramiento de SI. Se puede encontrar una guía detallada en el Estándar 1006 Competencia.

2.1.5 Los profesionales deben llevar a cabo el trabajo de auditoría con diligencia mientras se adhieren a estándares y profesionales y requisitos legales y reglamentarios.

2.2 Aplicación

2.2.1 Debe extenderse el debido cuidado profesional a todos los aspectos de la auditoría, incluyendo, pero sin limitarse a, evaluar los riesgos de auditoría, aceptando asignaciones de auditoría, establecer el alcance de la auditoría, formular objetivos de auditoría, planificar la auditoría, llevar a cabo la auditoría, asignación de recursos a la auditoría, seleccionando pruebas de auditoría, evaluando resultados de las pruebas, documentando la auditoría, llegando a las conclusiones de auditoría, presentando y entregando los resultados de la auditoría. Al hacer esto, los profesionales deben determinar o evaluar:

- Tipo, nivel, habilidad y competencia de los recursos necesarios para cumplir con los objetivos de auditoría y aseguramiento de SI.
- Importancia del riesgo identificado y el efecto potencial de tal riesgo sobre el sujeto de la auditoría.

2.2 Aplicación cont.

- Suficiencia, validez y relevancia de las pruebas de auditoría reunidas
- Competencia, integridad y conclusiones de otros en los que se puede confiar de su trabajo.

2.2.2 El debido cuidado profesional también requiere que los profesionales realicen todos sus trabajos con el concepto de seguridad razonable en mente.

2.2.3 Los profesionales deben servir en beneficio de los interesados de forma legal y honesta, mientras que mantienen altos estándares de conducta y carácter, y no deben participar en actos en detrimento de la profesión.

2.3 Ciclo de Vida del Trabajo

2.3.1 Los profesionales deben planificar el trabajo de auditoría completamente y en tiempo y forma mediante el ejercicio del debido cuidado profesional para asegurar la disponibilidad de los recursos apropiados y finalizar a tiempo el trabajo de auditoría. Los profesionales asignados al proyecto en conjunto deben poseer las habilidades, conocimiento y competencias pertinentes necesarias para realizar el trabajo de auditoría.

2.3.2 Los profesionales deben realizar el trabajo de auditoría aplicando el debido cuidado profesional, por ejemplo, siguiendo los estándares profesionales adecuados para asegurar calidad y conclusiones u opiniones de la auditoría completas.

2.4 Comunicación

2.4.1 Los roles y responsabilidades definidos deben ser comunicados a los miembros del equipo antes de empezar el proyecto para asegurar que el equipo se adhiere a los estándares profesionales adecuados durante el trabajo de auditoría.

2.4.2 Durante el trabajo de auditoría los profesionales deben comunicar adecuadamente con los auditados e interesados pertinentes para asegurar su cooperación.

2.4.3 Los profesionales deben dirigir sus hallazgos a los auditados del trabajo de auditoría.

2.4.4 Los profesionales deben documentar y comunicar las preocupaciones relativas a la aplicación de los estándares profesionales a las partes adecuadas para resolver inquietudes.

2.4.5 Los profesionales deben ejercitar el debido cuidado profesional mientras informan a las partes adecuadas del resultado del trabajo realizado.

2.5 Obtener y Administrar la Información

2.5.1 Los profesionales deben tener expectativas razonables que la gerencia comprende sus obligaciones y responsabilidades en la provisión de información adecuada, pertinente y oportuna requerida para el desarrollo del trabajo de auditoría.

2.5.2 Los profesionales deben tomar las medidas razonables para mantener la privacidad y confidencialidad de la información obtenida en el ejercicio de sus funciones salvo que la divulgación sea requerida por las autoridades legales. Tal información no debe ser utilizada para beneficio personal ni revelada a partes inapropiadas.

2.5 Obtener y Administrar la Información cont.

2.5.3 La información debe ser retenida y desechada adecuadamente de acuerdo con las políticas organizacionales y leyes, normas y reglamentos pertinentes.

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
1002 Independencia Organizacional	La función de auditoría y aseguramiento de SI deberá ser independiente del área o actividad a ser revisada para permitir llevar a cabo objetivamente la asignación de auditoría y aseguramiento.
1003 Independencia Profesional	Los profesionales de auditoría y aseguramiento de SI deberán ser independientes y objetivos, tanto en actitud como en apariencia en todas las materias relacionadas al trabajo de auditoría y aseguramiento.
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	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. Los profesionales de auditoría y aseguramiento de SI, junto con otros que ayuden en el trabajo, deberán poseer el conocimiento adecuado de la materia. Los profesionales de auditoría y aseguramiento de SI deberán mantener competencia profesional a través de la adecuada formación profesional continua y de entrenamiento.

Titulo del Estándar	Declaración Estándar Relevante
1205 Evidencia de Auditoría	Los profesionales de auditoría y aseguramiento deberán obtener evidencia suficiente y adecuada para llegar a conclusiones razonables sobre las qué basar los resultados del trabajo. Los profesionales de auditoría y aseguramiento de SI deberán evaluar la suficiencia de la evidencia obtenida para apoyar las conclusiones y lograr los objetivos del trabajo.

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 de Gobierno de los miembros del consejo.
APO07 Administración de recursos humanos.	Optimizar las capacidades de los recursos humanos para cumplir los objetivos empresariales.
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.
MEA03 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
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.
Escepticismo profesional	Una actitud que incluye una mente inquisitiva y una evaluación critica de la evidencia de auditoría. Fuente: American Institute of Certified Public Accountants (AICPA) AU 230.07.
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.

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.