Guía de Auditoría y Aseguramiento de SI
2001 Estatuto de Auditoría

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 Ingles Certified Information Systems Auditor® (CISA®) la designación de requisitos. 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 ej., 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 Comitéde 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 ayudar a los profesionales de auditoría y aseguramiento de SI en la preparación del Estatuto de auditoría. El Estatuto de auditoría define el propósito, responsabilidad, autoridad y responsabilidad final de la función de auditoría y aseguramiento de SI.

1.1.2 Los profesionales de auditoría y aseguramiento de SI deben considerar esta guía para determinar cómo implementar el estándar, uso de su 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 1001 Estatuto de auditoría.
1.2.2 Estándar 1002 Independencia organizacional.
1.2.3 Estándar 1003 Independencia profesional.

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 clave de compromiso clave de auditoría y aseguramiento de SI:
2.1 Mandato.
2.2 Contenido del Estatuto de auditoría.

Guía de Auditoría y Aseguramiento de SI 2001 Estatuto de Auditoría

2.1 Mandato

2.1.1 Los profesionales deben tener un claro mandato para realizar la función de auditoría. Este mandato está documentado normalmente en un Estatuto de auditoría que debe ser formalmente aprobado por los encargados del Gobierno, ej., consejo de administración y comité de auditoría. Donde exista un Estatuto de auditoría para la función de auditoría como un conjunto, se debe incorporar el mandato de auditoría y aseguramiento de SI.

2.2 Contenido del Estatuto de Auditoría

2.2.1 El Estatuto de auditoría debe direccionar claramente los cuatro aspectos de propósito, responsabilidad, autoridad y responsabilidad final. Estos aspectos se exponen en las siguientes secciones.

2.2.2 **Propósito** del Estatuto de auditoría y función de auditoría debe contener las siguientes secciones:

- Objetivos / Metas del Estatuto de auditoría proporcionan un marco de trabajo funcional y organizacional en el que opera la función de auditoría.
- La declaración de la misión y objetivos de la función de la auditoría trae un enfoque estructurado para evaluar y mejorar el diseño y efectividad operacional de los procesos de administración de riesgos, sistemas de control interno y estructuras de gobierno de los sistemas de la información.
- El ámbito de la función de auditoría es para la empresa entera o para una organización específica dentro de la empresa.
- El Gobierno detalla el organismo que autoriza el Estatuto de auditoría y la función de auditoría.

2.2.3 **Responsabilidad** de la función de auditoría debe contener las siguientes secciones:

- Principios operativos proporcionan una enumeración más detallada y cuantitativa de los diferentes objetivos de la función de auditoría.
- Independencia detalla la implementación del requerimiento de la función de auditoría y profesionales, tal como se describe en el estándar 1002 Independencia Organizacional y 1003 Independencia Profesional.
- Relaciones con la auditoría externa detalla la relación de la función de auditoría con el auditor externo:
  - Reunión con los auditores externos para coordinar el esfuerzo de trabajo para minimizar duplicación de esfuerzos.
  - Proporcionar acceso a los papeles de trabajo profesionales, documentación y evidencia.
  - Tener en cuenta el trabajo planificado por los auditores externos cuando se elabore el plan de auditoría para el próximo periodo.
- Expectativas del auditado detalla los servicios y entregables que los auditados pueden esperar de la función de auditoría y profesionales:
  - Descripción de problemas identificados, consecuencias y posibles resoluciones relacionadas con el área de responsabilidad del auditado.
  - Posibilidad de incluir administración de respuestas y acciones correctivas adoptadas sobre los hallazgos en el informe de

2.2 Contenidos del Estatuto de Auditoría cont.

auditoría. Esto incluye referencias a los niveles de servicio relacionados (SLAs) para elementos tales como entrega de informes, respuesta a las quejas del auditado, calidad del servicio, revisión del desempeño, proceso de presentación de informes y acuerdo de los hallazgos.

- Requerimientos del auditado detalla la responsabilidad de la entidad auditada, por ej., se requiere que todos los auditados estén disponibles y asistan a la función de auditoría y profesionales en el cumplimiento de las responsabilidades asignadas.
- Comunicación con los auditados detalla la frecuencia y canales de comunicación a través de los cuales la función de auditoría se comunicará con los auditados.

2.2.4 **Autoridad** de la función de auditoría debe contener las siguientes secciones:

- Derecho de acceso a información relevante, sistemas, personal y locales por los profesionales cuando realicen un compromiso de auditoría. La función de auditoría, representada por los profesionales:
  - Está autorizada, completa, libre y sin restricciones de acceso a todos los registros, documentación, sistemas y localidades cuando se realiza un encargo de auditoría y puede obtener asistencia de la gerencia ejecutiva en la obtención de este acceso.
  - Tiene la autoridad para obtener todos los datos de un empleado, consultor o contratista cuando se realiza un encargo de auditoría.
- Limitaciones de autoridad de la función de auditoría y profesionales, en su caso.
- Procesos a ser auditados, que la función de auditoría está autorizada para auditar, por ej., la función de auditoría es libre de determinar los procesos que auditará, basada en el plan de auditoría basado en los riesgos.

2.2.5 **Responsabilidad final** de la función de auditoría debe contener las siguientes secciones:

- Estructura organizacional, incluyendo líneas de responsabilidad a la dirección o gerencia ejecutiva, de la función de auditoría, por ej., la función de auditoría debe tener acceso libre y sin restricciones a la junta directiva y sus miembros.
- Informe que detalla el formato, contenido y destinatarios de la comunicación de los resultados de cada trabajo de auditoría, por ej., un informe escrito de auditoría será emitido por la función de auditoría después de cada trabajo de auditoría y distribuido a los interesados apropiados, incluyendo el alcance, acciones realizadas, hallazgos, recomendaciones, respuesta de la dirección y las acciones correctivas tomadas.
- El desempeño de la función de auditoría que detalla el proceso de presentación de informes periódicos de la función de auditoría comparado con el plan de auditoría y presupuesto, por ej., la función de auditoría informará trimestralmente a la dirección de su propósito, responsabilidad y autoridad, así como de su rendimiento relativo al plan de auditoría y presupuesto.

2.2 Contenidos del Estatuto de Auditoría cont.

- Cumplir con los estándares que detalla los estándares a los que se adhiere la función de auditoría y profesionales, por ej., la función de auditoría y profesionales se adherirá y actuará de acuerdo con todos los Estándares de Auditoría y aseguramiento y Guías de SI de ISACA.
- Proceso de aseguramiento de la calidad (ej., entrevistas, encuestas de satisfacción del cliente, encuestas de desempeño de la asignación) que establece una comprensión de las necesidades y expectativas. relevantes del auditado con la función de auditoría. Estas necesidades deben ser evaluadas contra el Estatuto de auditoría con una visión para mejorar el servicio o el cambio de la prestación del servicio o Estatuto de auditoría, según sea necesario. Revisiones externas de calidad permiten a la función de auditoría evaluar su cumplimiento con los estándares aplicables, el marco de trabajo de riesgos de la empresa y control, uso óptimo de recursos y uso de las buenas prácticas. Se debe realizar una revisión de calidad externa independiente de la función de auditoría al menos cada cinco años para mantener la conformidad con los Estándares de Auditoría y Aseguramiento de SI de ISACA.
- Reglas de dotación de personal para trabajos de auditoría. por ej., establecer un periodo de tiempo mínimo previo en el que los profesionales no estarán empleados en trabajos de auditoría en áreas donde realizaron servicios distintos de la auditoría que perjudican la independencia. El Estatuto de auditoría también debe establecer si se permite participar a los profesionales en la realización de los servicios distintos de la auditoría y carácter general, oportunidad y alcance de dichos servicios, para asegurar que la independencia no se ve afectada. Esto puede eliminar o minimizar la necesidad para obtener mandatos específicos para cada servicio no auditado en una base caso por caso.
- El compromiso de educación continua de la función de auditoría a los profesionales, por ej., la función de auditoría se compromete a proporcionar a los profesionales con un mínimo de 40 horas de formación anuales.
- Acciones acordadas en relación a la función de auditoría y la conducta de los profesionales, por ej., sanciones cuando alguna de las partes no cumple con sus responsabilidades.

2.2.6 Otros aspectos a tener en cuenta para añadir al Estatuto de auditoría son:

- Revisión y modificación de la carta, que es responsabilidad de la función de auditoría. Se debe evaluar periódicamente si el propósito, responsabilidad, autoridad y responsabilidad final, como se define en el Estatuto de auditoría, continua siendo adecuada y comunicado el resultado de la evaluación al comité de auditoría.
- Obtener la aprobación de las modificaciones al Estatuto de auditoría de los encargados del Gobierno.
- Incluir documentos de referencia relacionados como estándares, guías, políticas, marcos de trabajo, manuales, etc.

Guía de Auditoría y Aseguramiento de SI 2001 Estatuto de 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 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.

Titulo 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 aceptado y aprobado el Estatuto de auditoría a un nivel apropiado dentro de la empresa.
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.

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
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 de la empresa.
- Gerentes.
- Órganos de gobierno dentro de la empresa, ej., comité de auditoría.
- Organizaciones profesionales.
- Otras guías profesionales (por ej., libros, papeles, otras guías) de áreas de auditoría de SI y aseguramiento.

4. Terminología

Término	Definición
Estatuto de auditoría	Un documento aprobado por los encargados del Gobierno que define el propósito, autoridad y responsabilidad de la actividad de auditoría y aseguramiento de SI interna. La carta debe: • Establecer la posición de la función de auditoría y aseguramiento de SI interna dentro de la empresa. • Autorizar acceso a registros, personal y los bienes relevantes para la realización del encargo de auditoría y aseguramiento de SI. • Definir el alcance de las actividades de la función de auditoría y aseguramiento de SI.
Compromiso de Auditoría	Una asignación, tarea o actividad de revisión de auditoría específica, como por ej. una auditoría, revisión de control de autoevaluación, examen de fraude o consultoría. Un trabajo de auditoría puede incluir múltiples tareas o diseño de actividades para llevar a cabo un conjunto específico de objetivos relacionados.
Independencia	La ausencia de condiciones que amenazan la objetividad o apariencia de objetividad. Estas amenazas a la objetividad deben ser gestionadas a nivel de auditor individual, compromiso, funcional y organizacional. La independencia incluye independencia de criterio e independencia en apariencia.

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.

