Guía de Auditoría y Aseguramiento de SI
2008 Criterios

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 gestión 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)-Hacen frente a la realización de la asignación, tales como planificación y supervisión, definición del alcance, riesgos y materialidad, la movilización de recursos, supervisión y gestión 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, prueba especifico o control profesional se deben aplicar su propio juicio profesional a las circunstancias de control específicas presentadas por los sistemas particulares o entorno de SI.

El Comite de Estandares Profesionales y Gestión de Carreras de ISACA, en Ingles “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 a seleccionar los criterios, contra los que se evaluará la materia, que son adecuados y proceden de una fuente relevante.

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 1007 Afirmaciones.

1.2.2 Estándar 1008 Criterios.

1.3 Uso de Términos

1.3.1 De aquí en adelante:
- 'Función de auditoría y aseguramiento de SI' esta referenciada como 'función de auditoría'.
- 'Profesionales de auditoría y aseguramiento de SI' esta 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:
2.1 Selección y uso del criterio.
2.2 Idoneidad.
2.3 Aceptabilidad.
2.4 Fuente.
2.5 Cambio en el criterio durante la asignación de la auditoría.

2.1 Selección y Uso de Criterios

2.1.1 Los profesionales deberán seleccionar criterios, contra los que se evaluara la materia. Cuando seleccionen los criterios, los profesionales deberán considerar cuidadosamente la idoneidad, aceptabilidad y fuente de los criterios, como se describe en las secciones 2.2, 2.3 y 2.4 respectivamente.

2.1.2 Los profesionales deben considerar la selección de criterios cuidadosamente. Cumplir con las leyes locales y regulaciones es importante y debe ser considerado un requisito obligatorio. Sin embardo es reconocido que muchas asignaciones de auditoría incluyen áreas, como cambios de gerencia, controles generales de TI y controles de acceso, no cubiertos por leyes o regulaciones. Además, algunas industrias, como la industria de tarjetas de pago, han establecido requisitos obligatorios. Se debe considerar la relevancia de normas locales e internacionales de protección de datos y las regulaciones de privacidad. Cuando los requisitos legislativos están basados en principios, los profesionales deben asegurarse que los criterios seleccionados logran el objetivo de la auditoría.

2.1.3 Se requiere el uso de de criterios adecuados y aceptables para asegurar una evaluación consistente de la materia. Sin el criterio correcto, cualquier conclusión u opinión formada estará abierta a malentendidos e interpretación desde un punto de vista personal del lector.

2.1.4 Los profesionales deben abstenerse de evaluar la materia en base a sus propias expectativas, experiencias o juicios, porque podría no considerarse un criterio adecuado y aceptable.

2.1.5 Cuando los criterios no están fácilmente disponibles, incompletos o sujetos a interpretación profesional se debe incluir una descripción y cualquier otra interpretación necesaria para asegurar que el informe es justo, objetivo y comprensible, y el contexto en que se usa el criterio es claro.

2.1.6 El juicio profesional se debe utilizar para asegurar que el uso de los criterios permitirá el desarrollo de una opinión o conclusión justa y objetiva que no induzca al lector o usuario. Esta reconocido que la gerencia podría poner criterios que no cumplen todos los requerimientos.

2.2 Idoneidad

2.2.1 Los profesionales deben valorar la idoneidad y adecuación de los criterios utilizados para evaluar la materia. El ejemplo de criterio ‘La legislación local estipula que toda la información personal de los clientes debe permanecer siempre privada cuando se realizan transmisiones de datos’ se usa para clarificar los siguientes atributos de los criterios:

- **Objetividad**—Libre de prejuicios que pueden impactar de forma adversa en los hallazgos y conclusiones de los profesionales y, de en consecuencia, pueden inducir a error al usuario del reporte de auditoría, ej.: los criterios son objetivos porque son ratificados por la ley local.
- **Integridad**–Suficientemente completa para que todos los criterios que puedan afectar las conclusiones de los profesionales sobre la materia están identificados y utilizados en la realización de la asignación de la auditoría. Por lo tanto, la integridad de todos los criterios usados debe alcanzarse, dados los objetivos de la asignación de la auditoría.
- **Relevancia**—Relevancia a la materia y contribuir a los hallazgos y conclusiones que cumplen los objetivos de la asignación de la auditoría.

2.2 Idoneidad cont.

Los criterios pueden ser sensibles al contexto, incluso para la misma materia pueden haber diferentes criterios dependiendo de los objetivos y circunstancias de la asignación de auditoría, ej.: los criterios se consideran relevantes porque las transacciones de datos están en el alcance de la asignación de auditoría.

- **Mensurabilidad**—Permitir la medición constante de la materia y el desarrollo de conclusiones consistentes cuando se aplica por profesionales diferentes en circunstancias similares, ej.: el criterio es mesurable porque cada transacción de datos con información personal desprotegida puede ser identificada únicamente y por lo tanto medida constantemente.
- **Comprensibilidad**—Comunicado claramente y no sujeta a interpretaciones diferentes principalmente por los usuarios previstos, ej.: el criterio es comprensible porque esta sección de la ley ha estado sujeta ya a múltiples sentencias de los tribunales, ayudando a establecer una clara comprensión sobre la ejecución práctica e interpretación de la ley.

2.3 Aceptabilidad

2.3.1 La aceptabilidad de los criterios está afectada por la disponibilidad de los criterios a los usuarios del reporte de auditoría, así los usuarios comprenden la base de la actividad de aseguramiento y la relevancia de los hallazgos y conclusiones. Las fuentes pueden incluir los criterios siguientes:

- **Reconocido**—Suficientemente bien reconocido por lo que su uso no se cuestiona por los usuarios previstos.
- **Autorizado**—Refleja pronunciamientos autoritativos dentro del área y son apropiados para la materia, ej.: pronunciamientos autoritativos pueden venir de cuerpos profesionales, grupos de la industria, Gobierno y reguladores.
- **Disponibles públicamente**—Incluye estándares desarrollados por organismos profesionales de contabilidad y auditoría como ISACA, Federación Internacional de Contables (IFAC) y otros cuerpos reconocidos del Gobierno, legales o profesionales.
- **Disponible para todos los usuarios**—Cuando no están disponibles públicamente, los criterios deben ser comunicados a todos los usuarios a través de las afirmaciones que forman parte del reporte de auditoría. Las afirmaciones consisten en declaraciones acerca de la materia que logran los objetivos de "criterios adecuados" por lo que pueden ser auditados, como se describe en el Estándar 1007 Afirmaciones.

2.3.2 Los profesionales deben asegurar que los criterios utilizados en una asignación de auditoría son:

- **Aceptado Externamente**—Reconocido, autorizado y disponible públicamente.
- **Confirmado Externamente**—Criterios desarrollados por la gerencia (para una asignación de auditoría especifica) no se consideran reconocidos, autorizados y disponibles públicamente. Antes de su uso, estos criterios requieren validaciones externas por un tercero independiente reconocido para asegurar que la gerencia no impone implícitamente un resultado deseado de la asignación de auditoría.

2.4 Fuente

2.4.1 Además de su idoneidad y disponibilidad, la selección de los criterios de aseguramiento de SI debe considerar también su fuente, en términos de sus usos y la audiencia potencial. Por ejemplo, cuando se trata de regulaciones del Gobierno, los criterios basados en afirmaciones desarrolladas desde la legislación y regulaciones que le aplican a la materia debe ser lo más apropiado. En otros casos, los criterios de la industria o asociaciones comerciales pueden ser relevantes. Las posibles fuentes de criterios, en orden de consideración, son:

- **Criterios establecidos por ISACA**—Criterios y estándares públicamente disponibles que se han expuesto a la revisión por pares y a través de un proceso de debida diligencia reconocido por expertos internacionales en Gobierno, control, seguridad y aseguramiento de TI.
- **Criterios establecidos por otros cuerpos de expertos**—Similar a los estándares y criterios de ISACA, son relevantes para la materia y han sido desarrollados y expuestos a revisiones por pares y a través de procesos de debida diligencia por expertos en diferentes campos.
- **Criterios establecidos por leyes y regulaciones**—Mientras las leyes y regulaciones pueden proporcionar las bases de los criterios, se debe tener cuidado en su uso. Frecuentemente, la redacción es compleja y tiene un significado legal específico. En muchos casos, puede ser necesario repetir los requerimientos como afirmaciones. Además, expresar una opinión sobre la legislación está restringido normalmente para miembros de la profesión jurídica.
- **Criterios establecidos por entidades que no siguieron los procesos debidos**—Incluyen los criterios relevantes desarrollados por otras entidades que no siguieron procesos debidos y no han sido sujetas a consulta y debate público.
- **Criterios desarrollados específicamente para la asignación de la auditoría**—Mientras los criterios desarrollados específicamente para la asignación de la auditoría pueden ser apropiados, tenga especial cuidado para asegurar que esos criterios son adecuados, especialmente objetivos, completos y medibles. Los criterios desarrollados específicamente para una asignación de auditoría están en forma de afirmaciones. Suelen estar desarrollados para referirse a las necesidades de un usuario específico. Ej.: se pueden usar diferentes marcos de trabajo como criterios establecidos para evaluar la efectividad de los sistemas de control internos; un determinado usuario, sin embargo, puede desarrollar un conjunto de criterios que logren las necesidades específicas, ej.: una jerarquía de aprobaciones autorizadas. Los profesionales deben mencionar claramente en el reporte de auditoría que ciertos criterios son desarrollados específicamente para la asignación de auditoría. Ellos deben considerar si los criterios de desarrollo podrían inducir a error al usuario previsto y, si es necesario, proporcionar más información sobre los criterios. Considerando que estos criterios fueron desarrollados por la gerencia, se debe buscar y mencionar en el reporte la confirmación externa, como se describe en 2.3.2.

2.5 Cambio en el Criterio Durante la Asignación de Auditoría

2.5.1 Según progresa la auditoría, la información adicional y la visión sobre la materia puede resultar en un cambio de los criterios seleccionados:

- Ciertos criterios podrían no ser necesarios más para lograr el objetivo de la auditoría. Es estas circunstancias, no es necesario un trabajo adicional de auditoría relacionada a los criterios.
- Podría haber una necesidad de establecer criterios adicionales para conseguir el objetivo de la auditoría. En estas circunstancias, serán seleccionados los criterios extra y se llevara a cabo el trabajo de auditoría en relación a los criterios.

---

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
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.
1008 Criterios	Los profesionales de auditoría y aseguramiento seleccionaran criterios, contra los que se evaluará 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.

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 del 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.
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 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

Termino	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.

Termino	Definición
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.