

Estándar de auditoría y aseguramiento de SI 1001 Estatuto de la función de auditoría

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1001 Estatuto de la función de auditoría

Declaraciones

- 1001.1** La función de auditoría y aseguramiento de SI documentará la función de la auditoría de manera adecuada en un estatuto de la función de auditoría, que indique propósito, responsabilidad, autoridad y responsabilidad.
- 1001.2** La función de auditoría y aseguramiento de SI debe tener el estatuto de la función de auditoría acordado y aprobado en el nivel adecuado dentro de la empresa.
-

Aspectos clave

La función de auditoría y aseguramiento de SI debe:

- Preparar un Estatuto de la función de auditoría para definir las actividades de la función interna de auditoría y aseguramiento de SI con los detalles suficientes que comuniquen:
 - La autoridad, el propósito, las responsabilidades y las limitaciones de la función de auditoría y aseguramiento de SI
 - La Independencia y la responsabilidad de la función de auditoría y aseguramiento de SI
 - Las funciones y las responsabilidades del auditado durante la asignación de auditoría o la asignación de aseguramiento de SI
 - Los estándares profesionales que el profesional de auditoría y aseguramiento de SI respetará durante la realización de la asignación de auditoría y aseguramiento de SI
 - Revisar el estatuto de la función de auditoría al menos una vez por año, o con más frecuencia si cambian las responsabilidades.
 - Actualizar el estatuto de la función de auditoría según sea necesario para asegurar que el propósito y las responsabilidades hayan sido, y continúen, documentadas de manera adecuada.
 - Comunicar formalmente el estatuto de la función de auditoría al auditado para cada asignación de auditoría y aseguramiento de SI.
-

Términos

Término	Definición
Asignación de aseguramiento	Examen objetivo de la evidencia con el propósito de brindar una evaluación sobre los procesos de gestión de riesgos, control o gobierno para la empresa. Nota de alcance: Los ejemplos pueden incluir asignaciones de seguridad del sistema, cumplimiento, desempeño y financieras.
Estatuto de la función de auditoría	Documento aprobado por los responsables del gobierno que define el propósito, la autoridad y la responsabilidad de la actividad de auditoría interna. El estatuto debe: • Establecer la posición de la función de auditoría interna dentro de la empresa. • Autorizar el acceso a registros, personal y propiedades físicas relevantes para el desempeño de las asignaciones de auditoría y aseguramiento de SI. • Definir el alcance de las actividades de la función de auditoría.

Estándar de auditoría y aseguramiento de SI 1001 Estatuto de la función de auditoría

Asignación de auditoría	Actividad de revisión, tarea o compromiso de auditoría específica, como una auditoría, revisión de autoevaluación de control, examen de fraude o consultoría. Una asignación de auditoría puede incluir múltiples tareas o actividades diseñadas para lograr un conjunto específico de objetivos relacionados.
Independencia	La libertad de condiciones que amenazan la objetividad o apariencia de la objetividad. Dichas amenazas a la objetividad deben ser gestionadas en los niveles organizacionales, funcionales, de asignación y auditor individual. La independencia incluye Independencia de mente e Independencia en apariencia.

Enlace a los
lineamientos

Tipo	Título
Lineamiento	2001 Estatuto de la función de auditoría

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.



Estándar de auditoría y aseguramiento de SI 1002 Independencia organizacional

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1002 Independencia organizacional

Declaraciones

- 1002.1** La función de auditoría y aseguramiento de SI será independiente del área o actividad que se revise para permitir la ejecución objetiva de la asignación de auditoría y aseguramiento.

Aspectos clave

La función de auditoría y aseguramiento de SI debe:

- Presentar reportes a un nivel dentro de la organización auditada que brinde Independencia y permita que la función de auditoría y aseguramiento de SI lleve a cabo sus responsabilidades sin interferencia.
- Divulgar los detalles del deterioro a las partes apropiadas si la independencia se deteriora de hecho o en apariencia.
- Evitar funciones diferentes de la auditoría en las iniciativas de SI que requieran la asunción de responsabilidades de dirección, ya que dichas funciones podrían impedir una independencia futura.
- Abordar la independencia y la responsabilidad de la función de auditoría en su estatuto y/o carta de asignación de auditoría.

Términos

Término	Definición
Deterioro	Condición que causa una debilidad o capacidad disminuida para ejecutar los objetivos de la auditoría. El deterioro de la independencia organizacional y objetividad individual puede incluir conflictos de interés personales; limitaciones del alcance; restricciones al acceso de registros, personal, equipos o instalaciones; y limitaciones de recursos (como fondos o personal).
Independencia	La libertad de condiciones que amenazan la objetividad o apariencia de la objetividad. Dichas amenazas a la objetividad deben ser gestionadas en los niveles organizacionales, funcionales, de asignación y auditor individual. La independencia incluye Independencia de mente e Independencia en apariencia.
Independencia en apariencia	La evasión de hechos y circunstancias que son tan significativos que sería probable que un tercero informado y razonable concluya, ponderando todos los hechos y las circunstancias específicas, que la integridad, objetividad o escepticismo profesional de una firma, función de auditoría o miembro del equipo de auditoría han sido comprometidos.
Independencia de mente	El estado de mente que permite la expresión de una conclusión sin ser afectada por influencias que comprometan el buen juicio profesional, permitiendo, de ese modo, que un individuo actúe con integridad y ejerza la objetividad y el escepticismo profesional.
Objetividad	La capacidad de ejercer el buen juicio, expresar opiniones y presentar recomendaciones con imparcialidad.

Estándar de auditoría y aseguramiento de SI 1002 Independencia organizacional

Enlace a los
lineamientos

Tipo	Título
Lineamiento	2002 Independencia organizacional

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.



Estándar de auditoría y aseguramiento de SI 1003 Independencia profesional

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de *ITAF™* para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1003 Independencia profesional

Declaraciones

1003.1 Los profesionales de auditoría y aseguramiento de SI deben ser independientes y objetivos, tanto en actitud como en apariencia, en todos los asuntos relacionados con las asignaciones de auditoría y aseguramiento.

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Realizar la asignación de auditoría y aseguramiento de SI de forma imparcial al abordar asuntos de aseguramiento y alcanzar conclusiones.
 - Ser independientes de hecho pero también parecer ser independientes en todo momento.
 - Divulgar los detalles del deterioro a las partes apropiadas si la independencia se deteriora de hecho o en apariencia.
 - Evaluar la independencia periódicamente con la dirección y el comité de auditoría, si está establecido.
 - Evitar funciones diferentes de la auditoría en las iniciativas de SI que requieran la asunción de responsabilidades de dirección porque dichas funciones podrían impedir una independencia futura.
-

Términos

Término	Definición
Deterioro	Condición que causa una debilidad o capacidad disminuida para ejecutar los objetivos de la auditoría. El deterioro de la independencia organizacional y objetividad individual puede incluir conflictos de interés personales; limitaciones del alcance; restricciones al acceso de registros, personal, equipos o instalaciones; y limitaciones de recursos (como fondos o personal).
Independencia	La libertad de condiciones que amenazan la objetividad o apariencia de la objetividad. Dichas amenazas a la objetividad deben ser gestionadas en los niveles organizacionales, funcionales, de asignación y auditor individual. La independencia incluye Independencia de mente e Independencia en apariencia.
Independencia en apariencia	La evasión de hechos y circunstancias que son tan significativos que sería probable que un tercero informado y razonable concluya, ponderando todos los hechos y las circunstancias específicas, que la integridad, objetividad o escepticismo profesional de una firma, función de auditoría o miembro del equipo de auditoría han sido comprometidos.
Independencia de mente	El estado de mente que permite la expresión de una conclusión sin ser afectada por influencias que comprometan el buen juicio profesional, permitiendo, de ese modo, que un individuo actúe con integridad y ejerza la objetividad y el escepticismo profesional.
Objetividad	La capacidad de ejercer el buen juicio, expresar opiniones y presentar recomendaciones con imparcialidad.

Estándar de auditoría y aseguramiento de SI 1003 Independencia profesional

Enlace a los
lineamientos

Tipo	Título
Lineamiento	2003 Independencia profesional

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1004 Expectativa razonable

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1004 Expectativa razonable

Declaraciones

- 1004.1** Los profesionales de auditoría y aseguramiento de SI deben tener una expectativa razonable de que la asignación puede ser realizada de conformidad con los estándares de auditoría y aseguramiento de SI y, cuando se requiera, otros estándares industriales o profesionales adecuados o regulaciones aplicables, y brindar una conclusión u opinión profesional.
- 1004.2** Los profesionales de auditoría y aseguramiento de SI deben tener una expectativa razonable de que el alcance de la asignación permite la conclusión sobre el tema y abordar cualesquiera restricciones.
- 1004.3** Los profesionales de auditoría y aseguramiento de SI deben tener una expectativa razonable de que la dirección entiende sus obligaciones y responsabilidades en relación a la provisión de información apropiada, relevante y oportuna requerida para realizar la asignación.
-

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Realizar la asignación de auditoría o aseguramiento de SI sólo si el trabajo puede completarse satisfactoriamente en conformidad con los estándares profesionales.
 - Realizar la asignación de auditoría o aseguramiento de SI sólo si el tema de la asignación puede evaluarse con los criterios relevantes.
 - Revisar el alcance de la asignación de auditoría o aseguramiento de SI para determinar que esté claramente documentada y permite que se llegue a una conclusión sobre el tema.
 - Identificar y abordar cualquier restricción sobre la asignación que se realiza, incluyendo el acceso a la información apropiada, relevante y oportuna.
 - Considerar si el alcance es suficiente para permitir que se exprese la Opinión del auditor sobre el tema. Las limitaciones del alcance pueden ocurrir cuando la información requerida para realizar la asignación no está disponible, cuando el plazo incluido en la asignación del aseguramiento del auditor de SI no es suficiente o cuando la dirección intenta limitar el alcance de las áreas seleccionadas. En estos casos, pueden considerarse otros tipos de asignaciones, tales como respaldar declaraciones financieras auditadas, revisiones de controles, cumplimiento de los estándares y las prácticas requeridas o cumplimiento con acuerdos, licencias, legislación y regulación.
-

Términos

Término	Definición
Opinión del auditor	Declaración formal expresada por el profesional de auditoría o aseguramiento de SI que describe el alcance de la auditoría, los procedimientos utilizados para producir el reporte y si los hallazgos respaldan o no que los criterios de auditoría se hayan cumplido. Los tipos de opiniones son: • Opinión no calificada: No observa excepciones o ninguna de las excepciones observadas conforma una deficiencia significativa

Estándar de auditoría y aseguramiento de SI 1004 Expectativa razonable

	• Opinión calificada: Observa excepciones que conforman una deficiencia significativa (pero no una debilidad material) • Opinión adversa: Observa una o más deficiencias significativas que conforman una debilidad material Nota: Se emite una abstención de opinión cuando el auditor no puede obtener evidencia de auditoría suficiente y adecuada en la cual basar una opinión o si es imposible formular una opinión debido a las interacciones potenciales de múltiples incertidumbres y su posible impacto acumulativo.
--	---

Enlace a los
lineamientos

Tipo	Título
Lineamiento	2004 Expectativa razonable

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1005 Debido cuidado profesional

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1005 Debido cuidado profesional

Declaraciones

1005.1 Los profesionales de aseguramiento y auditoría de SI deben ejercer el debido cuidado profesional, que incluye la observancia de los estándares de auditoría profesional, al planificar, realizar y presentar los reportes sobre los resultados de las asignaciones.

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Realizar las asignaciones con integridad y cuidado.
- Demostrar una comprensión y competencia suficiente para lograr los objetivos de la asignación.
- Mantener la Escepticismo profesional durante la asignación.
- Mantener la competencia profesional manteniéndose informado sobre, y cumpliendo con, los desarrollos en estándares profesionales.
- Comunicar a los miembros del equipo sus funciones y responsabilidades y garantizar el cumplimiento del equipo con los estándares adecuados al realizar las asignaciones.
- Abordar todas las preocupaciones encontradas con respecto a la aplicación de los estándares durante la realización de la asignación.
- Mantener comunicaciones efectivas con las partes interesadas relevantes durante la asignación.
- Tomar medidas razonables para proteger la información obtenida o derivada durante la asignación de divulgación inadvertida a partes no autorizadas.
- Realizar todas las asignaciones con el concepto de aseguramiento razonable en mente. El nivel de pruebas variará con el tipo de asignación.

Nota: El debido cuidado profesional implica competencia y cuidado razonable, no desempeño extraordinario o infalibilidad.

Términos

Término	Definición
Escepticismo profesional	Actitud que incluye una mente interrogativa y una evaluación crítica de la evidencia de la auditoría. Fuente: Instituto Americano de Contadores Públicos Certificados (AICPA) AU 230.07

Enlace a los lineamientos

Tipo	Título
Lineamiento	2005 Debido cuidado profesional

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1006 Competencia

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de *ITAF*™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1006 Competencia

Declaraciones

- 1006.1** Los profesionales de auditoría y aseguramiento de SI, junto con otras personas que ayudan en la asignación, deben poseer las habilidades y la competencia adecuadas para realizar las asignaciones de auditoría y aseguramiento de SI y ser profesionalmente aptos para realizar el trabajo requerido.
- 1006.2** Los profesionales de auditoría y aseguramiento de SI, junto con otras personas que ayudan en la asignación, deben poseer el conocimiento adecuado sobre el tema.
- 1006.3** Los profesionales de auditoría y aseguramiento de SI deben mantener la aptitud profesional mediante la capacitación y el entrenamiento profesional continuo y adecuado.
-

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Demostrar que las Aptituds profesionales suficientes (habilidades, conocimiento y experiencia relevante a la asignación planificada) se encuentran disponibles antes del comienzo del trabajo.
 - Evaluar medios alternativos para adquirir las habilidades, que incluyen subcontratación, externalizar una parte de las tareas, demorando la asignación hasta que esas habilidades se encuentren disponibles o asegurando, de alguna otra manera, que las habilidades adecuadas se encuentren disponibles.
 - Asegurar que los miembros del equipo que no poseen CISA ni otra designación profesional relevante y que están involucrados en la asignación de auditoría y aseguramiento de SI tengan suficiente educación, capacitación y experiencia laboral.
 - Proporcionar un aseguramiento razonable, cuando lidera un equipo que realiza una asignación de auditoría o aseguramiento de SI, de que todos los miembros del equipo cuenten con el nivel adecuado de competencia profesional para el trabajo que llevan a cabo.
 - Tener suficiente conocimiento en las áreas clave para permitir la realización de la asignación de auditoría o aseguramiento de SI de manera efectiva y eficaz, junto con cualquier especialista utilizado y otros miembros del equipo.
 - Cumplir con los requerimientos de desarrollo o educación profesional continua de CISA u otras designaciones profesionales relevantes.
 - Actualizar constantemente el conocimiento profesional mediante cursos educativos, seminarios, conferencias, webcasts y capacitación en el sitio de trabajo para brindar un nivel de servicio profesional que sea proporcional a los requerimientos de la función de auditoría o aseguramiento de SI.
-

Términos

Término	Definición
Aptitud	La capacidad de realizar una tarea específica, acción o función con éxito.
Competencia	Poseer habilidades y experiencia.

Estándar de auditoría y aseguramiento de SI 1006 Competencia

Enlace a los
lineamientos

Tipo	Título
Lineamiento	2006 Competencia

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1007 Afirmaciones

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1007 Afirmaciones

Declaraciones

1007.1 Los profesionales de auditoría y aseguramiento de SI deben revisar las afirmaciones con las que el tema será evaluado para determinar que dichas afirmaciones sean capaces de ser auditadas y que las afirmaciones sean suficientes, válidas y relevantes.

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Evaluar los criterios con los que el tema será evaluado para asegurarse de que respaldan las Afirmación.
- Determinar si se pueden auditar las afirmaciones y si están respaldadas por información de corroboración.
- Determinar si las afirmaciones están basadas en criterios que son determinados de manera apropiada y están sujetos a análisis objetivo y medible.
- Cuando las afirmaciones han sido desarrolladas por la dirección, asegurar que, si son comparadas con otros estándares de pronunciamientos autorizados, las afirmaciones son suficientes con respecto a lo que esperaría un lector o usuario con conocimiento.
- Cuando las afirmaciones han sido desarrolladas por terceros que operan controles en nombre de la empresa, asegurar que las afirmaciones son verificadas y aceptadas por la dirección.
- Presentar reportes del tema directamente (reporte directo) o mediante una afirmación sobre el tema (reporte indirecto).
- Formular una conclusión sobre cada afirmación, en base al agregado de los hallazgos empleando los criterios junto con el buen juicio profesional.

Términos

Término	Definición
Afirmación	Cualquier declaración formal o conjunto de declaraciones sobre el tema por parte de la dirección. Las afirmaciones, en general, deben ser por escrito y, comúnmente, contienen una lista de atributos específicos sobre el tema específico o sobre un proceso que involucra al tema.

Enlace a los lineamientos

Tipo	Título
Lineamiento	2007 Afirmaciones

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1008 Criterios

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1008 Criterios

Declaraciones

- 1008.1** Los profesionales de auditoría y aseguramiento de SI deben seleccionar criterios con los que será evaluado el tema, que sean objetivos, completos, relevantes, medibles, comprensibles, ampliamente reconocidos, autorizados y comprendidos por, o disponibles para, todos los lectores y usuarios del reporte.
- 1008.2** Los profesionales de auditoría y aseguramiento de SI deben considerar la fuente de los criterios y centrarse en aquellos emitidos por organismos autorizados relevantes antes de aceptar criterios menos reconocidos.
-

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Considerar la selección de Criterios detenidamente y poder justificar su selección.
- Utilizar el buen juicio profesional para asegurar que, si corresponde, el uso de los criterios pueden permitir el desarrollo de una conclusión u opinión objetiva y justa que no ocasione una interpretación errónea por parte del lector o usuario. Hay que admitir que la dirección podría presentar criterios que no cumplan con todos los requerimientos.
- Considerar la idoneidad y disponibilidad de los criterios al determinar los requerimientos de la asignación.
- Cuando los criterios no están fácilmente disponibles, están incompletos o sujetos a interpretación, incluir una descripción y cualquier otra información necesaria para asegurar que el reporte sea justo, objetivo y comprensible, y que se incluya en el reporte el contexto en el que se utilizan los criterios.

Lo adecuado y apropiado de los criterios de evaluación del tema deben ser evaluados en función de los siguientes cinco criterios de idoneidad:

- **Objetividad:** Los criterios no deben tener sesgo que pudiera afectar adversamente los hallazgos y las conclusiones del profesional y, en consecuencia, pudieran ocasionar una interpretación errónea por parte del usuario del reporte.
- **Compleitud:** Los criterios deben ser lo suficientemente completos de modo que se puedan identificar y utilizar todos los criterios que pudieran afectar a las conclusiones de los profesionales cuando se realiza la asignación de auditoría o aseguramiento de SI.
- **Relevancia:** Los criterios deben ser relevantes para el tema y contribuir a los hallazgos y las conclusiones que cumplan con los objetivos de la asignación de auditoría o aseguramiento de SI.
- **Mensurabilidad:** Los criterios deben permitir una medición consistente del tema, así como el desarrollo de conclusiones coherentes cuando sean aplicados por diferentes profesionales en circunstancias similares.
- **Comprensibilidad:** Los criterios deben comunicarse claramente y no ofrecer ocasión a interpretaciones significativamente diferentes a sus usuarios.

La aceptación de los criterios se ve afectada por la disponibilidad de los criterios para los usuarios del reporte de los profesionales, de modo que los usuarios entiendan la base de la actividad de aseguramiento y la relevancia de los hallazgo y las conclusiones. Las fuentes pueden incluir aquellas que son:

- **Reconocidas:** Los criterios deben ser suficientemente bien reconocidos para que su uso no sea cuestionado por los usuarios previstos.

Estándar de auditoría y aseguramiento de SI 1008 Criterios

- | | |
|----------------|--|
| Aspectos clave | <ul style="list-style-type: none">• Autorizadas: Deben buscarse criterios que reflejen pronunciamientos autorizados dentro del área y que sean adecuados para el tema. Por ejemplo, los pronunciamientos autorizados pueden provenir de organismos profesionales, grupos industriales, gobierno y reguladores.• Públicamente disponibles: Los criterios deben estar disponibles para los usuarios del reporte de los profesionales. Los ejemplos incluyen estándares desarrollados por organismos de auditoría y contabilidad profesionales como ISACA, la Federación Internacional de Contadores (IFAC) y otros organismos profesionales o gubernamentales reconocidos.• Disponibles para todos los usuarios: Cuando los criterios no están públicamente disponibles, éstos deben ser comunicados a todos los usuarios mediante afirmaciones que formen parte del reporte de los profesionales. Las afirmaciones consisten en declaraciones sobre el tema que cumplen con los requerimientos de criterios adecuados para que puedan ser auditados. |
| Continúa | |

Además de la idoneidad y la disponibilidad, la selección de criterios de aseguramiento de SI debe considerar la fuente, en términos de su uso y posible audiencia. Por ejemplo, cuando se trata de regulaciones gubernamentales, los criterios basados en las afirmaciones desarrolladas a partir de la legislación y las regulaciones que se aplican al tema pueden ser más apropiados. En otros casos, los criterios de la asociación de comercio o industria pueden ser relevantes. Las posibles fuentes de criterios, enumeradas con el fin de consideración, son:

- **Criterios establecidos por ISACA:** Éstos son criterios públicamente disponibles y estándares que han sido expuestos para revisión por parte de compañeros y un exhaustivo proceso de debida diligencia por expertos internacionales reconocidos en gobierno, control, seguridad y aseguramiento de TI.
- **Criterios establecidos por otros organismos de expertos:** Similares a los criterios y estándares de ISACA, éstos son relevantes para el tema y han sido desarrollados y expuestos para revisión de compañeros y un exhaustivo proceso de debida diligencia por expertos en varios campos.
- **Criterios establecidos por leyes y regulaciones:** Si bien las leyes y regulaciones pueden brindar la base de los criterios, debe tenerse cuidado en su uso. Frecuentemente, la terminología es compleja y acarrea un significado legal específico. En muchos casos, puede ser necesaria para reafirmar los requerimientos como afirmaciones. Además, expresar una opinión sobre la legislación está normalmente restringido a los miembros de la profesión legal.
- **Criterios establecidos por empresas que no respetan el debido proceso:** Éstos incluyen criterios relevantes desarrollados por otras empresas que no respetaron el debido proceso y no han sido sujetos a debate y consulta pública.
- **Criterios desarrollados específicamente para la asignación de auditoría o aseguramiento de SI:** Si bien los criterios desarrollados específicamente para la asignación de auditoría o aseguramiento de SI pueden ser apropiados, debe tenerse especial cuidado para asegurar que estos criterios cumplan con los criterios de idoneidad, completitud particular, mensurabilidad y objetividad. Los criterios desarrollados específicamente para una asignación de auditoría o aseguramiento de SI están en forma de afirmaciones.

Estándar de auditoría y aseguramiento de SI 1008 Criterios

Los criterios de selección deben ser considerados con cuidado. Si bien el cumplimiento con las regulaciones y leyes locales es importante y debe considerarse como un requerimiento obligatorio, se reconoce que muchas asignaciones de auditoría y aseguramiento de SI incluyen áreas, tales como gestión de cambios, controles de acceso y controles generales de TI, no cubiertas por regulaciones o leyes. Además, algunas industrias, como la industria de tarjetas de pagos, han establecido requerimientos obligatorios establecidos que deben cumplirse. Cuando los requerimientos legislativos están basados en principios, el profesional debe asegurar que los criterios seleccionados cumplan con el objetivo de la asignación.

A medida que avanza la asignación, la información adicional puede resultar en ciertos criterios que no son necesarios para cumplir con los objetivos. En esas circunstancias, no es necesario el trabajo adicional relacionado con los criterios.

Términos

Término	Definición
Criterios	Estándares y análisis comparativos (benchmarks) utilizados para medir y presentar el tema y en el que un auditor de SI evalúa el tema. Los criterios deben ser: • Objetivos: Sin sesgo • Completos: Incluyen todos los factores relevantes para llegar a una conclusión • Relevantes: Se relacionan con el tema • Medibles: Brindan medición coherente En una asignación de testación, los análisis comparativos (benchmarks) de acuerdo con los que se puede evaluar la afirmación escrita de la dirección sobre el tema. El profesional formula una conclusión sobre el tema al consultar los criterios adecuados.

Enlace a los lineamientos

Tipo	Título
Lineamiento	2008 Criterios

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1201 Planificación de la asignación

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1201 Planificación de la asignación

Declaraciones

- 1201.1** Los profesionales de auditoría y aseguramiento de SI deben planificar cada asignación de auditoría y aseguramiento de SI para abordar:
- Objetivo(s), alcance, cronograma y productos
 - Cumplimiento con los estándares de auditoría profesional y leyes aplicables
 - Uso de un enfoque basado en riesgo, cuando sea apropiado
 - Problemas específicos a la asignación
 - Requerimientos de reportes y documentación
- 1201.2** Los profesionales de auditoría y aseguramiento de SI deben desarrollar y documentar un plan de proyecto de la asignación de auditoría o aseguramiento de SI, que describa:
- La naturaleza de la asignación, los objetivos, el cronograma y los requerimientos de los recursos
 - Los plazos y el alcance de los procedimientos de auditoría para finalizar la asignación
-

Aspectos clave

- Los profesionales de auditoría y aseguramiento de SI deben:
- Obtener un entendimiento sobre la actividad que se audita. El alcance del conocimiento requerido debe ser determinado por la naturaleza de la empresa, su entorno, las áreas de riesgo y los objetivos de la asignación.
 - Considerar la dirección y orientación del tema, según lo permitido mediante la legislación, las regulaciones, las normas, las directivas y los lineamientos emitidos por el gobierno o la industria.
 - Realizar una evaluación de riesgo que brinde un aseguramiento razonable de que todos los puntos materiales sean cubiertos de manera adecuada durante la asignación. Luego, se pueden desarrollar estrategias de auditoría, niveles de materialidad y requerimientos de los recursos.
 - Desarrollar el plan de proyecto de la asignación utilizando las metodologías de gestión de proyectos adecuadas para asegurar que las actividades se mantengan encaminadas y dentro del presupuesto.
 - Incluir en el plan temas específicos a la asignación, tales como:
 - Disponibilidad de los recursos con la experiencia, las habilidades y el conocimiento apropiados
 - Identificación de las herramientas necesarias para recopilar evidencia, realizando pruebas y preparando/resumiendo información para la generación de los reportes
 - Criterios de evaluación que se utilizan
 - Requerimientos para la generación de reportes y distribución
 - Documentar el plan de proyecto de la asignación de auditoría o aseguramiento de SI para indicar claramente:
 - Objetivo(s), alcance, cronograma y productos
 - Recursos
 - Funciones y responsabilidades
 - Áreas de riesgo identificadas y su impacto en el plan de la asignación
 - Herramientas y técnicas a utilizar
 - Entrevistas de averiguación de datos a realizar
 - Información relevante a obtener

Estándar de auditoría y aseguramiento de SI 1201 Planificación de la asignación

Aspectos
clave
Continúa

- Procedimientos para verificar o validar la información obtenida y su uso como evidencia
- Suposiciones sobre el enfoque, la metodología, los procedimientos y las conclusiones y resultados anticipados
- Programar la asignación en relación al plazo, la disponibilidad y otros compromisos y requerimientos de la dirección y el auditado, en la medida de lo posible.
- Ajustar el plan de proyecto durante la asignación de auditoría o aseguramiento de SI para abordar asuntos que surjan durante la asignación, como nuevos riesgos, suposiciones incorrectas o hallazgos de procedimientos ya realizados.
- Para asignaciones internas:
 - Comunicar el estatuto de la función de auditoría al auditado; cuando sea necesario, utilizar una carta de asignación de auditoría o equivalente para aclarar más o confirmar la participación en asignaciones específicas
 - Comunicar el plan al auditado para que el auditado esté totalmente informado y pueda proporcionar el acceso apropiado a individuos, documentos y otros recursos, cuando se requiera
- Para asignaciones externas:
 - Preparar una carta de asignación de auditoría diferente para cada asignación de auditoría y aseguramiento de SI externa
 - Preparar un plan de proyecto para cada asignación de auditoría y aseguramiento de SI externa. El plan debe, como mínimo, documentar el(los) objetivo(s) y el alcance de la asignación.

Enlace a los
lineamientos

Tipo	Título
Lineamiento	2201 Planificación de la asignación

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1202 Evaluación de riesgo en planificación

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1202 Evaluación de riesgo en planificación

Declaraciones

- 1202.1** La función de auditoría y aseguramiento de SI debe utilizar un enfoque de evaluación de riesgo adecuado y metodología de respaldo para desarrollar el plan completo de auditoría de SI y determinar las prioridades para la asignación efectiva de los recursos de auditoría de SI.
- 1202.2** Los profesionales de auditoría y aseguramiento de SI deben identificar y evaluar el riesgo relevante al área de revisión, cuando planifican asignaciones individuales.
- 1202.3** Los profesionales de auditoría y aseguramiento de SI deben considerar el riesgo del tema, el riesgo de la auditoría y la exposición relativa de la empresa.
-

Aspectos clave

Al planificar las actividades continuas, la función de auditoría y aseguramiento de SI debe:

- Realizar y documentar, al menos una vez al año, una Evaluación de riesgo para facilitar el desarrollo del plan de auditoría de SI.
- Incluir, como parte de la evaluación de riesgo, los objetivos y planes estratégicos organizacionales y las iniciativas y marco de gestión de riesgo empresarial.
- Para cada asignación de auditoría y aseguramiento de SI, cuantificar y justificar la cantidad de recursos de la auditoría de SI necesarios para cumplir con los requerimientos de la asignación.
- Utilizar las evaluaciones de riesgo en la selección de áreas e ítems de interés de la auditoría y las decisiones para diseñar y realizar asignaciones particulares de auditoría y aseguramiento de SI.
- Buscar la aprobación de la evaluación de riesgo por parte de las partes interesadas en la auditoría y otras partes apropiadas.
- Priorizar y programar el trabajo de auditoría y aseguramiento de SI en base a las evaluaciones de riesgo.
- En función a la evaluación de riesgo, desarrollar un plan que:
 - Actúe como marco para las actividades de auditoría y aseguramiento de SI
 - Considere actividades y requerimientos de auditoría y aseguramiento que no sean de SI
 - Sea actualizado al menos una vez al año y aprobado por los órganos de gobierno
 - Aborde responsabilidades establecidas por el Estatuto de la función de auditoría

Al planificar una asignación individual, los profesionales de auditoría y aseguramiento de SI deben:

- Identificar y evaluar el riesgo relevante al área bajo revisión.
- Realizar una evaluación preliminar del riesgo relevante al área bajo revisión para cada asignación. Los objetivos para cada asignación específica deben reflejar los resultados de la evaluación del riesgo preliminar.
- Al considerar las áreas de riesgo y planificar una asignación específica, considerar auditorías anteriores, revisiones y hallazgos, que incluyen cualquier actividad correctiva. También considerar el proceso de evaluación de riesgo de gran alcance del Consejo.
- Intentar reducir el Riesgo de auditoría a un nivel aceptable y cumplir con los

Estándar de auditoría y aseguramiento de SI 1202 Evaluación de riesgo en planificación

objetivos de la auditoría por una evaluación apropiada del tema de SI y controles relacionados, a medida que se planifica y realiza la auditoría de SI.

- Al planificar un procedimiento de auditoría de SI específico, reconocer que mientras más bajo sea el umbral de Materialidad, más precisas son las expectativas de la auditoría y mayor es el riesgo de la auditoría.
- Para reducir el riesgo de mayor materialidad, compensar ampliando las pruebas de controles (reducir el riesgo de control) y/o ampliando los procedimientos de Pruebas sustantivas (reducir el riesgo de detección) para obtener aseguramiento adicional.

Términos

Término	Definición
Estatuto de la función de auditoría	Documento aprobado por los responsables del gobierno que define el propósito, la autoridad y la responsabilidad de la actividad de auditoría interna. El estatuto debe: • Establecer la posición de la función de auditoría interna dentro de la empresa. • Autorizar el acceso a registros, personal y propiedades físicas relevantes para el desempeño de las asignaciones de auditoría y aseguramiento de SI. • Definir el alcance de las actividades de la función de auditoría.
Riesgo de auditoría	El riesgo de alcanzar una conclusión incorrecta en base a los hallazgos de auditoría. Los tres componentes del riesgo de auditoría son: • Riesgo de control • Riesgo de detección • Riesgo inherente
Riesgo del tema de la auditoría	Riesgo relevante al área bajo revisión: • Riesgo de negocio (capacidad del cliente para pagar, solvencia, factores del mercado, etc.) • Riesgo contractual (responsabilidad, precio, tipo, penalizaciones, etc.) • Riesgo del país (político, entorno, seguridad, etc.) • Riesgo del proyecto (recursos, conjunto de habilidades, metodología, estabilidad del producto, etc.) • Riesgo de tecnología (solución, arquitectura, red de infraestructura de hardware y software, canales de entrega, etc.) Ver riesgo inherente.
Riesgo de control	Riesgo de que exista un error material que no sea prevenido o detectado de manera oportuna por el sistema de control interno. (Ver riesgo inherente.)
Riesgo de detección	Riesgo de que los procedimientos sustantivos del profesional de auditoría o aseguramiento de SI no detecten un error que pudiera ser material, individualmente o en combinación con otros

Estándar de auditoría y aseguramiento de SI 1202 Evaluación de riesgo en planificación

	errores. Ver riesgo de auditoría.
Riesgo inherente	Nivel o exposición al riesgo sin tomar en cuenta las acciones que la dirección ha tomado o podría tomar (por ej., implementar controles). Ver riesgo de control.
Materialidad	Un concepto de auditoría sobre la importancia de un ítem de información con respecto a su impacto o efecto en el funcionamiento de la entidad que está siendo auditada. Una expresión de importancia relativa de un tema particular en el contexto de la empresa como un todo.
Evaluación de riesgo	Proceso utilizado para identificar y evaluar los riesgos y sus posibles efectos. Las evaluaciones de riesgo son utilizadas para identificar aquellos ítems o áreas que presentan la exposición, la vulnerabilidad o el riesgo más alto para la empresa para la inclusión en el plan de auditoría anual de SI. Las evaluaciones de riesgo también se utilizan para gestionar el riesgo de beneficios del proyecto y entrega del proyecto.
Pruebas sustantivas	Obtención de evidencia de una auditoría sobre la integridad, precisión o existencia de actividades o transacciones realizadas durante el período de la auditoría.

Enlace a los
lineamientos

Tipo	Título
Lineamiento	2202 Evaluación de riesgo en planificación

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1203 Desempeño y supervisión

Declaraciones

- 1203.1** Los profesionales de auditoría y aseguramiento de SI deben llevar a cabo el trabajo en conformidad con el plan de auditoría de SI aprobado para cubrir el riesgo identificado y dentro del cronograma acordado.
- 1203.2** Los profesionales de auditoría y aseguramiento de SI deben proporcionar supervisión al personal de auditoría de SI sobre quienes tienen responsabilidad de supervisión, para lograr los objetivos de la auditoría y cumplir con los estándares de auditoría profesional aplicables.
- 1203.3** Los profesionales de auditoría y aseguramiento de SI deben aceptar sólo tareas que estén dentro de su conocimiento y habilidades o para las que tengan una expectativa razonable de adquirir las habilidades durante la asignación o lograr la tarea bajo supervisión.
- 1203.4** Los profesionales de auditoría y aseguramiento de SI deben obtener evidencia suficiente y apropiada para lograr los objetivos de la auditoría. Los hallazgos y las conclusiones de la auditoría deben ser respaldados por un análisis e interpretación apropiados de esta evidencia.
- 1203.5** Los profesionales de auditoría y aseguramiento de SI deben documentar el proceso de auditoría, describiendo el trabajo de auditoría y la evidencia de auditoría que respalda los hallazgos y las conclusiones.
- 1203.6** Los profesionales de auditoría y aseguramiento de SI deben identificar y concluir acerca de los hallazgos.
-

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Asignar a miembros del equipo de modo que coincidan sus habilidades y experiencia con las necesidades de la asignación.
- Agregar recursos externos al equipo de auditoría de SI, cuando sea apropiado, y asegurar que su trabajo sea supervisado correctamente.
- Gestionar las funciones y las responsabilidades de los miembros del equipo de auditoría de SI específicos durante la asignación, abordando como mínimo:
 - Las funciones de ejecución y revisión
 - La responsabilidad para designar la metodología y el enfoque
 - Crear programas de auditoría o aseguramiento
 - Realizar el trabajo
 - Enfrentar asuntos, preocupaciones y problemas a medida que surgen
 - Documentar y aclarar los hallazgos
 - Escribir el reporte
- Hacer que cada tarea de la asignación sea ejecutada por un miembro(s) del equipo revisada por otro miembro del equipo apropiado.
- Utilizar la mejor evidencia de auditoría alcanzable. Debe ser consistente con la importancia del objetivo de la auditoría y el tiempo y esfuerzo involucrados para obtener la evidencia.
- Obtener evidencia adicional si, a criterio del profesional, la evidencia obtenida no

Estándar de auditoría y aseguramiento de SI 1203 Desempeño y supervisión

Aspectos clave	cumple con los criterios de ser suficientes y apropiados para formular una opinión o respaldar los hallazgos y las conclusiones.
continúa	• Organizar y documentar el trabajo realizado durante la asignación, después de los procedimientos predefinidos aprobados y documentados. • Incluir en la documentación: - Objetivos de la auditoría y alcance del trabajo, el programa de auditoría, los pasos de auditoría realizados, la evidencia recopilada, los hallazgos, conclusiones y recomendaciones - Detalle suficiente para permitir que una persona informada y prudente vuelvan a realizar las tareas realizadas durante la asignación y alcancen la misma conclusión - Identificación de quién realizó cada tarea y sus funciones al preparar y revisar la documentación - La fecha en que la documentación fue preparada y revisada • Obtener las manifestaciones escritas relevantes del auditado que claramente detallen las áreas críticas de la asignación, los problemas que hayan surgido y su resolución, y las afirmaciones realizadas por el auditado. • Determinar que las manifestaciones del auditado incorporan la firma y la fecha del auditado para indicar el reconocimiento de sus responsabilidades con respecto a la asignación. • Documentar y conservar en los papeles de trabajo cualquier manifestación recibida durante la realización de la asignación, sea escrita u oral.

Enlace a estándares y lineamientos

Tipo	Título
Estándar	1005 Debido cuidado profesional
Estándar	1205 Evidencia
Estándar	1401 Reportes
Lineamiento	2202 Evaluación de riesgo en planificación

Fecha de Vigencia Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1204 Materialidad

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar 1204 Materialidad

Declaraciones

- 1204.1** Los profesionales de auditoría y aseguramiento de SI deben considerar las debilidades potenciales o ausencias de controles mientras planifican una asignación y si esas debilidades o ausencias de controles pudieran resultar en una deficiencia significativa o una debilidad material.
- 1204.2** Los profesionales de auditoría y aseguramiento de SI deben considerar la materialidad de la auditoría y su relación con el riesgo de la auditoría, determinando, a su vez, la naturaleza, los plazos y el alcance de los procedimientos de la auditoría.
- 1204.3** Los profesionales de auditoría y aseguramiento de SI deben considerar el efecto acumulativo de las deficiencias o debilidades menores de control y si la ausencia de controles se traduce en una deficiencia significativa o debilidad material.
- 1204.4** Los profesionales de auditoría y aseguramiento de SI deben divulgar la siguiente información en el reporte:
- Ausencia de controles o controles ineficaces
 - Importancia de las deficiencias de control
 - Probabilidad de que estas debilidades ocasionen una deficiencia significativa o debilidad material
-

Aspectos clave

Al realizar una asignación, los profesionales de auditoría y aseguramiento de SI deben:

- Aplicar el concepto de materialidad al:
 - Planificar y realizar la asignación
 - Evaluar el efecto de elementos, procesos, controles o errores específicos

Cualquier deficiencia, debilidad o falta de políticas, procedimientos y controles apropiados debe determinarse en las circunstancias particulares de la asignación.

- Considerar las definiciones de materialidad cuando son provistas por las autoridades regulatorias o legislativas.
- Observar que la evaluación de la materialidad y el Riesgo de auditoría puede variar de vez en cuando, dependiendo de las circunstancias y el entorno cambiante.
- Intentar reducir el riesgo de auditoría a un nivel aceptable y cumplir con los objetivos mientras planifica y realiza la asignación.
- Considerar la Materialidad al determinar la naturaleza, los plazos y el alcance de procedimientos de la auditoría.
- Reducir el riesgo de auditoría para las áreas relacionadas con mayor materialidad al ampliar la prueba de controles (reducir el riesgo de control) y/o ampliar los procedimientos de pruebas sustantivas (reducir el riesgo de detección).
- Evaluar el efecto de los controles compensatorios y si dichos controles compensatorios son efectivos para determinar si una deficiencia de control o la combinación de las deficiencias de control es una Debilidad material.
- Considerar el efecto acumulativo de múltiples errores o fallas de control al

Estándar 1204 Materialidad

determinar la materialidad.

- Considerar no sólo el tamaño sino también la naturaleza de las deficiencias de control y las circunstancias particulares de cómo han ocurrido al evaluar su efecto general en la opinión o conclusión de la auditoría.

Términos

Término	Definición
Riesgo de auditoría	El riesgo de alcanzar una conclusión incorrecta en base a los hallazgos de auditoría. Los tres componentes del riesgo de auditoría son: • Riesgo de control • Riesgo de detección • Riesgo inherente
Debilidad material	Una deficiencia o una combinación de deficiencias en un control interno, por lo cual exista una posibilidad razonable de que una falsa declaración importante no sea evitada ni detectada de manera oportuna. La debilidad en el control se considera material si la ausencia del mismo ocasiona que no exista una garantía razonable de que se cumplirá con el objetivo de control. Una debilidad clasificada como material implica que: • Los controles no están establecidos y/o los controles no son utilizados y/o los controles son inadecuados. • Se garantiza su escalado. Existe una relación inversa entre la materialidad y el nivel de riesgo de auditoría aceptable para el profesional de auditoría o aseguramiento de SI; es decir, cuanto mayor sea el nivel de materialidad, menor será la capacidad de aceptación del riesgo de auditoría, y <i>viceversa</i>.
Materialidad	Un concepto de auditoría sobre la importancia de un ítem de información con respecto a su impacto o efecto en el funcionamiento de la entidad que está siendo auditada. Una expresión de importancia relativa de un tema particular en el contexto de la empresa como un todo.

Estándar 1204 Materialidad

Enlace a
estándares y
lineamientos

Tipo	Título
Estándar	1201 Planificación de la asignación
Estándar	1202 Evaluación de riesgo en planificación
Estándar	1207 Irregularidades y actos ilegales
Estándar	1401 Reportes
Lineamiento	2202 Evaluación de riesgo en planificación
Lineamiento	2204 Materialidad

Fecha de
Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1205 Evidencia

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1205 Evidencia

Declaraciones

- 1205.1** Los profesionales de auditoría y aseguramiento de SI deben obtener evidencias suficientes y apropiadas para llegar a conclusiones razonables sobre las cuales basar los resultados de la asignación.
- 1205.2** Los profesionales de auditoría y aseguramiento de SI deben evaluar la suficiencia de la evidencia obtenida para respaldar las conclusiones y lograr los objetivos de la asignación.
-

Aspectos clave

Al realizar una asignación, los profesionales de auditoría y aseguramiento de SI deben:

- Obtener Evidencia apropiada y suficiente, que incluye:
 - Los procedimientos realizados
 - Los resultados de los procedimientos realizados
 - Los documentos fuente (en formato electrónico o impresos en papel), registros e información de corroboración utilizados para apoyar la asignación
 - Los hallazgos y resultados de la asignación
 - La documentación de que el trabajo fue realizado y cumple con las leyes, regulaciones y políticas aplicables
- Preparar la documentación, que debe ser:
 - Retenida y estar disponible por un período de tiempo y en un formato que cumpla con las políticas de la organización de auditoría o aseguramiento y estándares, leyes y regulaciones profesionales relevantes
 - Protegida de modificaciones o divulgaciones no autorizadas durante su preparación y retención
 - Eliminada correctamente al final del período de retención
- Considerar la suficiencia de la evidencia para respaldar el nivel evaluado del riesgo de control al obtener evidencia de una prueba de controles.
- Identificar, interrelacionar y catalogar de manera apropiada las evidencias.
- Considerar las propiedades tales como la fuente, la naturaleza (por ejemplo, escrita, oral, visual, electrónica) y la autenticidad (por ejemplo, firmas digitales y manuales, sellos) de la evidencia al evaluar su nivel de fiabilidad.
- Considerar los medios más rápidos y eficientes de costes de recolectar la evidencia necesaria para satisfacer los objetivos y riesgos de la asignación. Sin embargo, la dificultad o costo no es una razón válida para omitir un procedimiento necesario.
- Seleccionar el procedimiento más apropiado para recolectar evidencia según el tema que se está auditando (es decir, su naturaleza, plazos de la auditoría, buen juicio profesional). Los procedimientos utilizados para obtener la evidencia incluyen:
 - Consulta y confirmación
 - Repetición de la ejecución
 - Repetición del cálculo
 - Computación
 - Procedimientos analíticos
 - Inspección
 - Observación

Estándar de auditoría y aseguramiento de SI 1205 Evidencia

Aspectos clave

continúa

- Otros métodos generalmente aceptados
- Considerar la fuente y la naturaleza de cualquier tipo de información obtenida para evaluar su fiabilidad y otros requerimientos de verificación. En términos generales, la fiabilidad de la evidencia es mayor cuando:
 - Aparece en forma escrita, en lugar de presentarse como expresiones orales
 - Es obtenido de fuentes independientes
 - Es obtenida por el profesional en lugar de por la entidad que se está auditando
 - Es certificada por una entidad independiente
 - Es mantenida por una entidad independiente
 - Es el resultado de la inspección
 - Es el resultado de la observación
- Obtener evidencia objetiva que sea suficiente para permitir que una entidad independiente calificada pueda repetir la ejecución de las pruebas y obtener los mismos resultados y conclusiones.
- Obtener evidencia proporcional a la materialidad del elemento y al riesgo involucrado.
- Poner énfasis en la precisión y completitud de la información cuando la información obtenida de la empresa es utilizada por el profesional de auditoría o aseguramiento de SI para realizar los procedimientos de auditoría.
- Divulgar cualquier situación en la que no se pueda obtener Evidencia suficiente de una manera coherente con la comunicación de los resultados de auditoría o aseguramiento de SI.
- Asegurar la evidencia en cuanto al acceso y modificación no autorizado.
- Retener la evidencia después de completarse el trabajo de auditoría o aseguramiento de SI durante el tiempo que resulte necesario para cumplir con todas las leyes, regulaciones y políticas aplicables.

Términos

Término	Definición
Evidencia apropiada	La medida de la calidad de la evidencia.
Evidencia suficiente	La medida de la cantidad de la evidencia; respalda todas las preguntas materiales para el objetivo y el alcance de la auditoría. Ver evidencia.

Enlace a los lineamientos

Tipo	Título
Lineamiento	2205 Evidencia

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1206 Uso del trabajo de otros expertos

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1206 Uso del trabajo de otros expertos

Declaraciones

- 1206.1** Los profesionales de auditoría y aseguramiento de SI deben considerar el uso del trabajo de otros expertos para la asignación, cuando sea apropiado.
- 1206.2** Los profesionales de auditoría y aseguramiento de SI deben evaluar y aprobar la idoneidad de las calificaciones profesionales, competencias, experiencia relevante, recursos, independencia y procesos de control de calidad de otros expertos antes de la asignación.
- 1206.3** Los profesionales de auditoría y aseguramiento de SI deben evaluar, revisar y valorar el trabajo de otros expertos como parte de la asignación, y documentar la conclusión sobre el uso y la confianza en su trabajo.
- 1206.4** Los profesionales de auditoría y aseguramiento de SI deben determinar si el trabajo de otros expertos, que no forman parte del equipo de asignación, es adecuado y completo para concluir acerca de los objetivos de la asignación actual, y documentar con claridad la conclusión.
- 1206.5** Los profesionales de auditoría y aseguramiento de SI deben determinar si se podrá depender del trabajo de otros expertos y se incorporará directamente o se hará referencia al mismo de manera separada en el reporte.
- 1206.6** Los profesionales de auditoría y aseguramiento de SI deben aplicar procedimientos adicionales de prueba para obtener evidencia suficiente y apropiada en los casos en que el trabajo de otros expertos no brinde evidencia suficiente y apropiada.
- 1206.7** Los profesionales de auditoría y aseguramiento de SI deben brindar una opinión o conclusión de la auditoría apropiada e incluir cualquier limitación del alcance cuando no se obtenga la evidencia requerida mediante los procedimientos de prueba adicionales.
-

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Considerar el uso del trabajo de Otros expertos en la asignación cuando existen limitaciones (por ejemplo, conocimiento técnico requerido por la naturaleza de las tareas que deben realizarse, escasos recursos para la auditoría, restricciones de tiempo) que podrían impedir el trabajo que debe realizarse o cuando existen posibles ganancias en la calidad de la asignación.
 - Documentar el impacto en el logro de los objetivos de la asignación, si no se pueden obtener los expertos requeridos, e insertar las tareas específicas en el plan de la asignación para gestionar los requerimientos de evidencia y riesgo.
 - Considerar la independencia de otros expertos al utilizar su trabajo.
 - Tener acceso a todos los papeles de trabajo, documentación de apoyo y reportes de otros expertos, cuando dicho acceso no ocasione problemas legales.
 - Determinar y concluir acerca del alcance del uso y confiabilidad en el trabajo de otros expertos cuando no se haya otorgado a los expertos el acceso a los registros debido a problemas legales.
 - Documentar el uso del trabajo de otros expertos en el reporte.
-

Estándar de auditoría y aseguramiento de SI 1206 Uso del trabajo de otros expertos

Términos	Término	Definición
	Otros expertos	Interno o externo de la empresa, otro experto podría referirse a: • Un auditor de SI de la empresa contable externa. • Un consultor gerencial. • Un experto en el área de la asignación que ha sido asignado por la alta dirección o por el equipo.

Enlace a los lineamientos	Tipo	Título
	Lineamiento	2206 Uso del trabajo de otros expertos

Fecha de Vigencia Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1207 Irregularidades y actos ilegales

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1207 Irregularidades y actos ilegales

Declaraciones

- 1207.1** Los profesionales de auditoría y aseguramiento de SI deben considerar el riesgo de irregularidades y actos ilegales durante la asignación.
- 1207.2** Los profesionales de auditoría y aseguramiento de SI deben mantener una actitud de escepticismo profesional durante la asignación.
- 1207.3** Los profesionales de auditoría y aseguramiento de SI deben documentar y comunicar, de manera oportuna, cualquier acto ilegal o irregularidad material a la parte apropiada.
-

Aspectos clave

Los profesionales de auditoría y aseguramiento de SI deben:

- Reducir el riesgo de auditoría a un nivel aceptable en la planificación y realización de la asignación al:
 - Conocer que podrían existir errores materiales, deficiencias de control o falsas declaraciones debido a irregularidades o actos ilegales, independientemente de la evaluación de riesgo de irregularidades y actos ilegales
 - Obtener un entendimiento de la empresa y su entorno, que incluye controles internos que pretenden evitar o detectar irregularidades y actos ilegales que sean relevantes para el tema, el alcance y los objetivos de la asignación
 - Obtener evidencia suficiente y relevante para determinar si la dirección u otras personas dentro de la empresa poseen conocimientos de cualquier irregularidad y acto ilegal real, sospechado o alegado.
- Considerar relaciones inusuales o inesperadas que pueden indicar un riesgo de errores materiales, deficiencias de control o falsas declaraciones debido a irregularidades y actos ilegales al realizar los procedimientos de la auditoría.
- Diseñar y realizar procedimientos para probar la adecuación de los controles internos y el riesgo de que la dirección no respete los controles que pretenden evitar o detectar irregularidades y actos ilegales.
- Evaluar si los errores identificados, las deficiencias de control o las falsas declaraciones pueden ser indicios de una Irregularidad o acto ilegal. Si existiera dicho indicio, considerar las implicaciones en relación a otros aspectos de la asignación y, en particular, las representaciones de la dirección.
- Obtener manifestaciones escritas de la dirección al menos una vez al año o, más a menudo, según la asignación, para:
 - Reconocer la responsabilidad de la dirección en el diseño y la implementación de controles internos que prevengan y detecten irregularidades o actos ilegales.
 - Divulgar los resultados pertinentes de cualquier evaluación de riesgo que indique que puedan existir errores, deficiencias de control o falsas declaraciones como resultado de una irregularidad o acto ilegal.
 - Divulgar el conocimiento de la dirección sobre irregularidades y actos ilegales que afectan a la empresa en relación a la dirección y los empleados que tienen funciones significativas en el control interno.
 - Divulgar el conocimiento de la dirección sobre cualquier irregularidad y acto ilegal sospechada o alegada que afecte a la empresa según lo comunican los

Estándar de auditoría y aseguramiento de SI 1207 Irregularidades y actos ilegales

Aspectos clave

continúa

- empleados, ex empleados, reguladores y otros.
- Comunicar, de manera oportuna, a:
 - El nivel apropiado de dirección sobre cualquier información identificada u obtenida que pudiera existir una irregularidad material o acto ilegal.
 - Los responsables del gobierno sobre cualquier irregularidad material y actos ilegales que involucren a la dirección o los empleados que tengan funciones significativas en el control interno.
 - Presentar reportes a los responsables del gobierno cualquier sobre cualquier debilidad material en el diseño y la implementación de controles internos que pretenden prevenir y detectar cualquier irregularidad y acto ilegal que sea identificado durante la asignación, incluso si se encuentran fuera del alcance.
 - Considerar los requerimientos de reportes profesionales y legales aplicables en las circunstancias.
 - Considerar retirarse de la asignación si los errores materiales, las deficiencias de control, las falsas declaraciones o los actos ilegales afectan el desempeño continuo de la asignación.
 - Documentar todas las comunicaciones, planificación, resultados, evaluaciones y conclusiones relacionadas con las irregularidades materiales y los actos ilegales que han sido notificadas a la dirección, los responsables del gobierno, reguladores y otros.

Términos

Término	Definición
Irregularidad	Violación de una política de gestión establecida o de los requerimientos regulatorios. Puede constar de falsas declaraciones u omisiones deliberadas de información sobre el área que está siendo auditada o sobre la empresa como un todo, negligencia grave o actos ilegales intencionales.
Falsa declaración material	Declaración accidental o intencional no verdadera que afecta los resultados de una auditoría a un alcance medible.
Escepticismo profesional	Actitud que incluye una mente interrogativa y una evaluación crítica de la evidencia de la auditoría. Fuente: Instituto Americano de Contadores Públicos Certificados (AICPA) AU 230.07

Enlace a estándares y lineamientos

Tipo	Título
Estándar	1008 Criterios
Estándar	1202 Evaluación de riesgo en planificación
Estándar	1205 Evidencia
Lineamiento	2206 Uso del trabajo de otros expertos
Lineamiento	2207 Irregularidades y actos ilegales

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1401 Reportes

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1401 Reportes

Declaraciones

- 1401.1** Los profesionales de auditoría y aseguramiento de SI deben proporcionar un reporte para comunicar los resultados al concluir la asignación, que incluye:
- Identificación de la empresa, los destinatarios previstos y cualquier restricción sobre el contenido y la circulación
 - Alcance, objetivos de la asignación, período de cobertura y la naturaleza, los plazos y el alcance del trabajo realizado
 - Hallazgos, conclusiones y recomendaciones de la auditoría
 - Cualquier calificación o limitación dentro del alcance que el profesional de auditoría y aseguramiento de SI tenga con respecto a la asignación
 - Firma, fecha y distribución según los términos del estatuto de la función de auditoría o carta de asignación de auditoría
- 1401.2** Los profesionales de auditoría y aseguramiento de SI deben asegurar que los hallazgos en el reporte de auditoría estén respaldados por evidencia suficiente y apropiada.
-

Aspectos clave

- Los profesionales de auditoría y aseguramiento de SI deben:
- Obtener las manifestaciones escritas relevantes del auditado que claramente detallen las áreas críticas de la asignación, los problemas que hayan surgido y su resolución, y las afirmaciones realizadas por el auditado.
 - Determinar que las manifestaciones del auditado incorporan la firma y la fecha el auditado para indicar el reconocimiento de las responsabilidades del auditado con respecto a la asignación.
 - Documentar y conservar en el papel de trabajo cualquier manifestación, tanto escrita como oral, recibida durante la realización de la asignación. Para las asignaciones de atestación, las manifestaciones del auditado se deben obtener por escrito para reducir posibles malas interpretaciones.
 - Adaptar la forma y el contenido del reporte para que respalde el tipo de asignación realizada, tales como:
 - Auditoría (dirigir o certificar)
 - Revisión (dirigir o certificar)
 - Procedimientos acordados
 - Describir las debilidades significativas o materiales y su efecto en el logro de los objetivos de la asignación en el reporte.
 - Discutir el contenido del borrador del reporte con la dirección en el área antes de la finalización y divulgación, e incluir la respuesta de la dirección a hallazgos, conclusiones y recomendaciones en el reporte final, cuando corresponda.
 - Comunicar las deficiencias significativas y debilidades materiales en el ambiente de control a los responsables del gobierno y, cuando corresponda, a la autoridad responsable, y divulgar en el reporte que éstas han sido comunicadas.
 - Hacer referencia a cualquier reporte diferente en el reporte final.
 - Comunicar a la dirección del auditado sobre las deficiencias del control interno que sean menos que significativas pero más que irrelevantes. En esos casos, los responsables del gobierno o la autoridad responsable deben ser notificadas que dichas deficiencias del control interno han sido comunicadas a la dirección del auditado.
 - Identificar los estándares aplicados en la realización de la asignación y comunicar cualquier incumplimiento de estos estándares, según corresponda.

Estándar de auditoría y aseguramiento de SI 1401 Reportes

Términos

Término	Definición
Información relevante	Relacionada con controles, le indica al evaluador algo significativo sobre la operación de los controles subyacentes o componente de control. La información que directamente confirma la operación de los controles es la más relevante. La información que se relaciona indirectamente a la operación de los controles también puede ser relevante pero menos relevante que la información directa. Consultar las metas de calidad de información COBIT 5.
Información confiable	Información que es precisa, verificable y de una fuente objetiva. Consultar las metas de calidad de información COBIT 5.
Información suficiente	La información es suficiente cuando los evaluadores han recolectado suficiente información para formular una conclusión razonable. Sin embargo, para que la información sea suficiente, primero debe ser adecuada. Consultar las metas de calidad de información COBIT 5.
Información adecuada	Información relevante (es decir, se adapta para su propósito previsto), confiable (es decir, precisa, verificable y de una fuente objetiva) y oportuna (es decir, producida y utilizada en un marco de tiempo apropiado). Consultar las metas de calidad de información COBIT 5.
Información oportuna	Producida y utilizada en un marco de tiempo que permite prevenir o detectar las deficiencias de control antes de que sean materiales en una empresa. Consultar las metas de calidad de información COBIT 5.

Enlace a estándares y lineamientos

Tipo	Título
Lineamiento	2401 Reportes

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

Estándar de auditoría y aseguramiento de SI 1402 Actividades de seguimiento

La naturaleza especializada de la auditoría y el aseguramiento de los sistemas de información (SI), así como las habilidades necesarias para llevarlos a cabo, requieren de estándares que sean específicamente aplicables a la auditoría y el aseguramiento de SI. El desarrollo y la difusión de los estándares de auditoría y aseguramiento de SI son una piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen los requerimientos obligatorios para la auditoría, el reporte e informe de SI:

- Profesionales de auditoría y aseguramiento de SI con el nivel mínimo de desempeño aceptable exigido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) de los requerimientos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación sobre la conducta del poseedor del certificado CISA por parte del Consejo de dirección de ISACA o del comité apropiado y, en última instancia, en sanciones disciplinarias.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en su trabajo, cuando corresponda, de que la asignación se ha llevado a cabo en conformidad con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables.

La estructura de ITAF™ para el profesional de auditoría y aseguramiento de SI brinda múltiples niveles de orientación:

- **Estándares**, divididos en tres categorías:
 - **Estándares generales (serie 1000)**: Los principios de orientación según los cuales operan los profesionales de auditoría y aseguramiento de SI. Se refieren a la realización de todas las asignaciones y se ocupan de la ética, independencia, objetividad, debido cuidado, conocimiento, competencia y habilidad de los profesionales de auditoría y aseguramiento de SI. Las declaraciones de los estándares (en **negrita**) son obligatorias.
 - **Estándares de desempeño (serie 1200)**: Se refieren a la realización de la asignación; es decir, planificación y supervisión, alcance, riesgo e importancia, movilización de recursos, gestión de supervisión y asignaciones, evidencia de auditoría y aseguramiento, y la puesta en práctica del juicio profesional y debido cuidado.
 - **Estándares de reportes (serie 1400)**: Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada.
- **Lineamientos**, que respaldan los estándares y también están divididos en tres categorías:
 - Lineamientos generales (serie 2000)
 - Lineamientos de desempeño (serie 2200)
 - Lineamientos de reportes (serie 2400)
- **Herramientas y técnicas**, que brindan orientación adicional para los profesionales de auditoría y aseguramiento de SI; por ejemplo, libros blancos, programas de auditoría/aseguramiento de SI, la familia de productos de COBIT® 5

Se proporciona un glosario de términos en línea utilizado en ITAF en www.isaca.org/glossary.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, los profesionales de control deben utilizar su propio juicio profesional para las circunstancias de control específicas presentadas por el entorno particular de sistemas o de SI.

El Comité de Gestión de Carreras y Estándares Profesionales (PSCMC) de ISACA está comprometido a realizar consultas extensas en la preparación de estándares y orientación. Antes de emitir cualquier documento, se emite un borrador del mismo y se expone a nivel internacional para recibir comentarios del público en general. También se pueden enviar comentarios en atención del director del desarrollo de los estándares profesionales por correo electrónico (standards@isaca.org), fax (+1.847. 253.1443) o correo postal (Oficina Central Internacional de ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, EE.UU.).

Comité de Gestión de Carreras y Estándares Profesionales de ISACA 2012-2013

Steven E. Sizemore, CISA, CIA, CGAP, Presidente	Comisión de Servicios Humanos y Salud de Texas, EE.UU.
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	Servicios de Seguridad de Empresas de HP, Reino Unido
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, EE.UU.
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	Servicios de TI Británico Americano, Malasia
Alisdair McKenzie, CISA, CISSP, ITCP	Servicios de Aseguramiento de SI, Nueva Zelanda
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japón
Ian Sanderson, CISA, CRISC, FCA	OTAN, Bélgica
Timothy Smith, CISA, CISSP, CPA	LPL Financial, EE.UU.
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Estándar de auditoría y aseguramiento de SI 1402 Actividades de seguimiento

Declaraciones

1402.1 Los profesionales de auditoría y aseguramiento de SI deben monitorear información relevante para concluir si la dirección ha planeado/tomado la acción oportuna y apropiada para abordar los hallazgos y las recomendaciones de la auditoría reportados.

Aspectos clave

La función interna de auditoría de SI debe establecer un proceso de seguimiento para monitorear y asegurar que las acciones de la dirección han sido implementadas de manera efectiva o que la alta dirección ha aceptado el riesgo de no tomar ninguna acción.

Los profesionales de auditoría o aseguramiento de SI externos pueden confiar en una función de auditoría de SI interna para realizar el seguimiento en sus recomendaciones acordadas, según el alcance y los términos de la asignación.

Enlace a los lineamientos

Tipo	Título
Lineamiento	2402 Actividades de seguimiento

Fecha de Vigencia

Este estándar de ISACA entrará en vigencia para todas las asignaciones de auditoría y aseguramiento de SI a partir del 1 de noviembre de 2013.

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 disseminación 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®) 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 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 2001 Estatuto de Auditoría

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

Guía de Auditoría y Aseguramiento de SI 2001 Estatuto de Auditoría

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.

Guía de Auditoría y Aseguramiento de SI 2001 Estatuto de Auditoría

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: Habilidad 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.

Guía de Auditoría y Aseguramiento de SI 2001 Estatuto de Auditoría

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.



Guía de Auditoría y Aseguramiento de SI 2002 Independencia Organizacional

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 disseminación 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	The Weinman Group, USA

Guía de Auditoría y Aseguramiento de SI 2002 Independencia Organizacional

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 direccionar la [independencia](#) de la función de auditoría y aseguramiento de SI en la empresa. Se consideran tres aspectos importantes:
- La posición de la función de auditoría y aseguramiento de SI dentro de la empresa.
 - El nivel al que reporta la función de auditoría y aseguramiento de SI dentro de la empresa.
 - El desempeño de servicios distintos de auditoría dentro de la empresa por la gerencia y profesionales de auditoría y aseguramiento de SI.
- 1.1.2** Esta guía ofrece orientación sobre la evaluación de la independencia organizacional y detalla la relación entre la independencia organizacional y la carta y plan de auditoría.
- 1.1.3** Los profesionales de auditoría y aseguramiento de SI deben considerar esta guía para determinar cómo implementar el estándar, usar su juicio profesional en su aplicación, estar preparado para justificar cualquier desviación y buscar orientación adicional si lo 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.
- 1.2.4** Estándar 1004 Expectativa razonable.
- 1.2.5** Estándar 1006 Competencia.

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 Posición en la empresa. 2.2 Nivel de presentación de informes. 2.3 Servicios distintos de auditoría. 2.4 Evaluación de la independencia. 2.5 Carta y plan de auditoría.
2.1 Posición en la Empresa	2.1.1 Para permitir la independencia organizacional, la función de auditoría necesita tener una posición en la empresa que le permita realizar sus responsabilidades sin interferencia. Esto se puede lograr a través de: • Establecer la función de auditoría en el Estatuto de Auditoría como una función o departamento independiente, fuera del departamento operacional. La función de auditoría no debe ser asignada a ninguna responsabilidad o actividad operacional. • Asegurar que la función de auditoría informa a un nivel dentro de la empresa que le permita lograr la independencia organizacional. Informar a la gerencia de un departamento operacional podría comprometer la independencia organizacional, como se describe en más detalle en la sección 2.2. 2.1.2 La función de auditoría debe evitar realizar roles distintos de auditoría en las iniciativas que requieran la asunción de responsabilidades de administración, debido a que estos roles podrían poner en peligro la independencia futura. La independencia y responsabilidad final de la función de auditoría debe ser direccionada en el Estatuto de Auditoría como se describe en el Estándar 1001 Estatuto de Auditoría.
2.2 Nivel de Presentación de Informes	2.2.1 La función de auditoría debe reportar a un nivel dentro de la empresa que le permita actuar con independencia organizacional total. La independencia debe estar definida en la Estatuto de Auditoría y confirmada por la función de auditoría a la junta directiva y aquellos encargados del Gobierno de forma regular, al menos anualmente. 2.2.2 Para asegurar la independencia organizacional de la función de auditoría, se debe informar de lo siguiente a aquellos encargados del Gobierno (ejemplo, consejo de administración) para su entrada y/o aprobación: • Plan y presupuesto de recursos de auditoría. • El plan de auditoría (basado en riesgos). • Desempeño de seguimiento realizado por la función de auditoría sobre la actividad de auditoría de SI. • Seguimiento del alcance significativo o limitaciones de recursos. 2.2.3 Para asegurar la independencia organizacional de la función de auditoría, se necesita soporte explícito tanto de la junta directiva como de la gerencia ejecutiva.

Guía de Auditoría y Aseguramiento de SI 2002 Independencia Organizacional

2.3 Servicios Distintos de Auditoría

- 2.3.1** En muchas empresas, la expectativa de la gerencia y personal de SI es que la función de auditoría puede estar involucrada en la prestación de servicios distintos de auditoría. Esto implica, tiempo completo o parcial, participación de los profesionales en iniciativas de SI y equipos de proyecto de SI para proporcionar funciones de asesoramiento o consultivas.
- 2.3.2** Las actividades rutinarias y administrativas o que involucren cuestiones que son generalmente insignificantes se consideran sin responsabilidad de administración y, por tanto, no podrían perjudicar su independencia. Los servicios distintos de auditoría que tampoco podrían perjudicar la independencia o la [objetividad](#), si se aplican las salvaguardas adecuadas, incluyen la prestación de asesoramiento rutinario en controles y riesgos de tecnologías de la información.
- 2.3.3** Los siguientes servicios distintos de auditoría se consideran que atentan contra la independencia y objetividad, porque las amenazas creadas podrían ser tan significantes que ninguna salvaguarda podría reducirlas a un nivel aceptable:
- Asumir responsabilidades de gerencia o realizar actividades de gerencia.
 - Participación material de los profesionales en la supervisión o desempeño de diseño, desarrollo, pruebas, instalación, configuración o la operativa de sistemas de la información que son materiales o significativos para el objeto de la auditoría o aseguramiento.
 - Diseñar controles para sistemas de la información que sean materiales o significativos para el objeto de los compromisos de auditoría actuales o planificados para el futuro.
 - Servir en un rol de Gobierno donde los profesionales son responsables de forma independiente o en conjunto de la toma de decisiones de gerencia o aprobación de políticas y estándares.
 - Proporcionar asesoramiento que forma la base principal de las decisiones de gerencia.
- 2.3.4** Prestar servicios distintos de auditoría en áreas que son actualmente, o en el futuro, el sujeto de un trabajo de auditoría también crea amenazas a la independencia que puede ser difícil de superar con salvaguardas. En esta situación, la percepción puede ser que tanto la independencia y objetividad de la función de auditoría y profesionales han sido dañados por la realización de servicios distintos de auditoría en esa área específica. La función de auditoría y los profesionales deben determinar si las salvaguardas adecuadas se pueden implementar para mitigar suficientemente estas amenazas reales o percibidas a la independencia.
- 2.3.5** Se puede encontrar una guía más detallada sobre el tratamiento de estas amenazas a la independencia en el Estándar 1003 Independencia Profesional y la Guía relacionada 2003.
-

Guía de Auditoría y Aseguramiento de SI 2002 Independencia Organizacional

2.4 Evaluación de la Independencia	2.4.1	La independencia debe ser evaluada regularmente por la función de auditoría y los profesionales. Esta evaluación debe hacerse de forma anual para la función de auditoría y antes de cada compromiso con los profesionales, como se describe en el Estándar 1003 Independencia Profesional. La evaluación debe considerar factores tales como: • Cambios en relaciones personales. • Intereses financieros. • Asignaciones de trabajo y responsabilidades anteriores.
	2.4.2	La función de auditoría necesita revelar los posibles problemas relacionados con la independencia organizacional y discutirlos con el consejo de administración o los encargados del Gobierno. Se necesita encontrar una resolución y confirmarla en la carta o plan de auditoría.
2.5 Carta y Plan de Auditoría	2.5.1	La Estatuto de Auditoría debe detallar, en virtud de la ‘responsabilidad’, la implementación de independencia organizacional de la función de auditoría. Además de detallar la independencia, el Estatuto de Auditoría debe también incluir posibles impedimentos a la independencia.
	2.5.2	La independencia organizacional debe estar reflejada en el plan de auditoría. La función de auditoría tiene que ser capaz de determinar el alcance del plan independientemente, sin restricciones impuestas por la gerencia ejecutiva.

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.

Guía de Auditoría y Aseguramiento de SI 2002 Independencia Organizacional

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.
1004 Expectativa Razonable	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.
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.

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.
APO01 Gestionar el marco de gerencia de TI.	Proporcionar un enfoque de gerencia consistente que permita conseguir los requerimientos de Gobierno de la empresa, que abarca los procesos de gerencia, estructuras organizacionales, roles y responsabilidades, actividades confiables y repetibles y las habilidades y competencias.

Guía de Auditoría y Aseguramiento de SI 2002 Independencia Organizacional

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 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) de áreas de auditoría de SI y aseguramiento.

4. Terminología

Término	Definición
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.
Objetividad	La capacidad de ejercer un juicio, expresar opiniones y presentar recomendaciones imparcialmente.

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para toda asignación de auditoría y aseguramiento de SI de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.

Guía de Auditoría y Aseguramiento de SI 2003 Independencia 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 disseminación 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 Gestión 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 2003 Independencia Profesional

La guía se presenta en las siguientes secciones:

1. Propósito de la guía y vinculación con estándares.
 2. Contenido de la guía.
 3. Referencias y mapeo.
 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 proporcionar un marco que permita a los profesionales de auditoría y aseguramiento de SI a:
 - Establecer cuándo la [independencia](#) puede ser o parecer ser dañada.
 - Considerar posibles alternativas potenciales al proceso de auditoría cuando la independencia es, o parece ser dañada.
 - Reducir o eliminar el impacto o independencia de los profesionales de auditoría y aseguramiento de SI al realizar roles, funciones y servicios distintos de auditoría.
 - Determinar los requisitos de divulgación cuando la independencia requerida es, o puede ser, dañada.
 - 1.1.2** Los profesionales de auditoría y aseguramiento deben considerar esta guía para determinar cómo implementar el estándar, usar su [juicio profesional](#) en su aplicación, estar preparado para justificar cualquier desviación y buscar orientación 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.
-

1.3 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 Marco conceptual.
 - 2.2 Amenazas y salvaguardas.
 - 2.3 Gestión de amenazas.
 - 2.4 Servicios o Roles distintos de auditoría.
 - 2.5 Servicios o Roles distintos de auditoría que no dañan la independencia.
 - 2.6 Servicios o Roles distintos de auditoría que dañan la independencia.
 - 2.7 Relevancia de la independencia en la prestación de servicios o roles distintos de auditoría.
 - 2.8 Gobernar la admisibilidad de servicios o roles distintos de auditoría.
 - 2.9 Presentación de informes.
-

2.1 Marco Conceptual

- 2.1.1** Muchas circunstancias diferentes o combinaciones de circunstancias pueden ser relevantes en la evaluación de amenazas a la independencia. Es posible definir cada situación que crea una amenaza a la independencia y especificar la acción apropiada. Por lo tanto, esta guía establece un marco conceptual que requiere que el profesional identifique, evalúe y aborde las amenazas a la independencia. El enfoque del marco conceptual ayuda a cumplir con los estándares de independencia, y se acomoda a muchas variaciones en circunstancias que crean amenazas a la independencia.
- 2.1.2** El enfoque del marco conceptual se debe aplicar por los profesionales para:
- Identificar amenazas a la independencia.
 - Evaluar la importancia de las amenazas identificadas.
 - Aplicar salvaguardas, cuando sea necesario, para eliminar amenazas o reducirlas a niveles aceptables.
- 2.1.3** Cuando los profesionales determinen que las salvaguardas apropiadas no están disponibles o no se pueden aplicar para eliminar las amenazas o reducirlas a niveles aceptables, los profesionales deben eliminar la circunstancia o relación que crea la amenaza, o rechazar o terminar el compromiso. Si los profesionales no pueden rechazar o terminar el compromiso, se debe hacer divulgación adecuada de la [discapacidad](#) a la independencia a los encargados del Gobierno y en cualquier informe resultante de la contratación.
- 2.1.4** Los profesionales deben usar juicio profesional en la aplicación de este marco conceptual.
- 2.1.5** Un importante aspecto cuando se aplica el marco es la consulta. El profesional de auditoría y aseguramiento de SI debe buscar asesoramiento, cuando lo considere necesario, de:
- Colegas dentro de la empresa.
 - Administración.
 - Encargados del Gobierno.
 - Organizaciones profesionales relevantes.

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.1 Marco Conceptual cont.

2.1.6 Aunque no existe ningún requerimiento para los profesionales ser independientes para realizar servicios o roles distintos de la auditoría, la [objetividad](#) sigue siendo un requisito profesional cuando ellos lo realizan. Los profesionales deben considerar aplicar este marco conceptual para identificar amenazas a la objetividad, evaluar la importancia de las amenazas e implementar salvaguardas apropiadas cuando realizan servicios o roles distintos de auditoría.

2.2 Amenazas y Salvaguardas

- 2.2.1** Las amenazas se pueden crear por una amplia gama de relaciones y circunstancias. Cuando una relación o circunstancia crea una amenaza, tal amenaza podría perjudicar, o podría ser percibida como perjudicial, a la independencia profesional. Una circunstancia o relación puede crear más de una amenaza a la independencia. Las amenazas caen en una o más de las siguientes categorías:
- **Interés propio**—La amenaza de que un interés financiero u otro influirá en el juicio o comportamiento profesional de forma inadecuada.
 - **Auto-examen**—La amenaza de que los profesionales no evalúen apropiadamente los resultados de un juicio previo o servicio realizado por ellos o por otro individuo dentro de la función de auditoría, en la que los profesionales se basarán para formar un juicio como parte de la realización del trabajo actual.
 - **Defensa**—La amenaza de que los profesionales promuevan la posición de un auditado al punto en el que la objetividad profesional esté comprometida.
 - **Familiaridad**—La amenaza de que debido a una relación larga o estrecha con el auditado, los profesionales sean demasiado favorables a los intereses del auditado o que acepten fácilmente el trabajo, opiniones o argumentos del auditado.
 - **Intimidación**—La amenaza de que a los profesionales se les impida actuar con [integridad](#) u objetividad debido a las presiones actuales o percibidas, incluidos intentos de ejercitar influencia indebida sobre los profesionales.
 - **Parcialidad**—La amenaza de que los profesionales pudieran tomar una posición que no es objetiva, como resultado de política, ideología, social, psicología u otras convicciones.
 - **Participación de la gerencia**—La amenaza de que los resultados de los profesionales asuman el rol de la gerencia o realización de otras funciones de gerencia en nombre de la entidad que se somete a un trabajo de auditoría o compromiso de aseguramiento.
- 2.2.2** Las salvaguardas son controles diseñados para eliminar las amenazas a la independencia o para reducirlas a un nivel aceptable. En el marco conceptual, los profesionales aplican salvaguardas que se ocupan de hechos y circunstancias concretas en las que existan amenazas a la independencia. En algunos casos, pueden ser necesarias múltiples salvaguardas para hacer frente a una amenaza.

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.2 Amenazas y Salvaguardas cont.

Los profesionales pueden considerar los siguientes ejemplos de salvaguardas, en respuesta a amenazas identificadas:

- Una estructura de Gobierno en la empresa y la función de auditoría que proporcionan control y comunicaciones apropiados respecto a los servicios de auditoría y aseguramiento de SI a realizar.
- Asegurar que los profesionales (y gerentes de auditoría de SI) informan al nivel jerárquico adecuado dentro de la empresa, preferiblemente a los encargados del Gobierno.
- Los procedimientos internos en la empresa y la función de auditoría que garantizan las decisiones objetivas en la asignación de compromisos, por ejemplo, requisitos de formación, entrenamiento y experiencia adecuadas, requisitos de desarrollo profesional continuo.
- Asignación de gerencia y plantilla externa a la función de auditoría, tales como uso de personal de otra función, división, organización externa, para complementar a los profesionales.
- Un sistema adecuado de incentivos (premios y penalizaciones) que premie a los profesionales por pensamientos críticos y objetivos y penalice la parcialidad o el prejuicio.
- Una rotación periódica en la asignación de profesionales en auditoría de SI reduciendo el grado de familiaridad y auto revisión.
- Prácticas de contratación adecuadas, como selección e investigación de antecedentes, que podrían mejorar las probabilidades de que los profesionales estén libres de prejuicios o intereses propios.
- Quitar a un individuo de un equipo de auditoría de SI cuando el interés o relación de ese individuo represente una amenaza a la independencia.
- Requisitos de documentación y de información adecuados que aseguren que la evaluación de la independencia profesional está documentada en los papeles de trabajo y reportada consistentemente en los entregables.
- Tener un individuo o gestor de la plantilla profesional dentro de la función de auditoría que no fue parte del equipo de auditoría de SI que revise esmeradamente el trabajo realizado.
- Asignación de un recurso independiente, desde la función de auditoría o de otras fuentes referenciadas previamente, para llevar a cabo una revisión de pares o para actuar como observador independiente durante la planificación, trabajo de campo y presentación de informes.
- Tener una revisión externa de los informes, comunicaciones o información producida por los profesionales por un tercero reconocido, por ejemplo, autoridad aceptada en el campo o especialista independiente.
- La externalización de la asignación de auditoría y aseguramiento de SI a un proveedor de servicios externos.

2.3 Gestión de amenazas

2.3.1 Los hechos o circunstancias que crean amenazas a la independencia pueden resultar de eventos tales como el inicio de una nueva auditoría, asignación de nuevo personal a una auditoría en curso y aceptación de un

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.3 Gestión de amenazas cont.

servicio distinto de auditoría en una entidad auditada. Otros muchos eventos pueden resultar en amenazas a la independencia. Siempre que la nueva información relevante acerca de la amenaza a la independencia llegue a la atención del profesional durante un encargo de auditoría o aseguramiento, deberán volver a evaluar la importancia de la amenaza de acuerdo con el marco conceptual.

2.3.2 Los profesionales deben evaluar las amenazas:

- A la independencia, empleando el marco conceptual cuando los hechos y circunstancias en las que los profesionales realizan su trabajo pueda crear nuevas amenazas, o aumentar la importancia de las amenazas existentes a la independencia.
- Tanto individualmente como en su conjunto, porque las amenazas pueden tener un efecto acumulativo sobre la independencia profesional.
- Tanto cualitativa como cuantitativamente cuando se determina la importancia de una amenaza.

2.3.3 La función de auditoría y profesionales deben determinar cuando las amenazas a la independencia identificadas están en un nivel aceptable o han sido eliminadas o reducidas a un nivel aceptable. Una amenaza a la independencia no es aceptable si puede:

- Impactar en la capacidad de un profesional para realizar un trabajo de auditoría o compromiso de aseguramiento sin verse afectado por influencias que comprometan su juicio profesional.
- Exponer a los profesionales, a la función de auditoría, o a la organización de auditoría a circunstancias que podrían causar que un tercero razonable y bien informado concluya que la integridad, objetividad o [escepticismo profesional](#) de la organización auditada, o un empleado del equipo de auditoría y aseguramiento, había sido comprometido.

2.3.4 Cuando la función de auditoría y profesionales identifican amenazas a la independencia y, basándose en una evaluación de esas amenazas, determinan que las amenazas no están a un nivel aceptable, deben:

- Determinar cuándo las salvaguardas apropiadas están disponibles y se pueden aplicar para eliminar las amenazas o reducirlas a niveles aceptables.
- Ejercer juicio profesional en la toma de esa determinación, y debe tener en cuenta si tanto la [independencia de la mente](#) y la [independencia de apariencia](#) se mantienen.
- Buscar orientación de las partes apropiadas, como se describe en 2.1.5, para identificar y aplicar salvaguardas apropiadas.

2.3.5 La documentación proporciona evidencia de los juicios profesionales en formar conclusiones de acuerdo con el cumplimiento de los requerimientos de independencia.

2.3.6 Los profesionales deben documentar las conclusiones sobre el cumplimiento con los requerimientos de independencia y la esencia de cualquier discusión relevante con la gerencia de auditoría y, si es necesario, los encargados del Gobierno, que apoyen estas conclusiones, incluyendo:

- Los pasos que se realizaron para analizar la naturaleza de la

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.3 Gestión de amenazas cont.

independencia.

- La naturaleza actual de la cuestión de la independencia
 - Lista y descripción de las amenazas.
 - La conclusión final alcanzada.
 - Las salvaguardas para eliminar o reducir las amenazas a un nivel aceptable.
-

2.4 Servicios o roles distintos de auditoría

- 2.4.1** En muchas empresas, la expectativa de la gerencia, plantilla de SI y auditores internos es que los profesionales pueden estar involucrados en proporcionar servicios o roles distintos a la auditoría como:
- Definir las estrategias de SI relacionadas a áreas como tecnología, aplicaciones y recursos.
 - Evaluar, seleccionar e implementar tecnologías.
 - Evaluar, seleccionar, personalizar e implementar aplicaciones y soluciones de SI de terceras partes.
 - Diseñar, desarrollar e implementar aplicaciones y soluciones de SI a medida.
 - Establecer buenas prácticas, políticas y procedimientos relacionados a distintas funciones de TI.
 - Diseñar, desarrollar, probar e implementar seguridad y controles de TI
 - Gestión de proyectos de TI.
- 2.4.2** Proporcionar servicios o roles distintos de la auditoría, en general, involucra participación de tiempo completo o parcial en las iniciativas y proyectos de TI para proporcionar capacidades de asesoramiento o consultoría. Los profesionales de auditoría y aseguramiento pueden cumplir una función distinta de la auditoría en actividades como:
- Asignación o cesión temporal a tiempo completo de personal de auditoría y aseguramiento de SI a un equipo de proyectos de TI.
 - Asignación a tiempo parcial de un individuo de la plantilla de auditoría y aseguramiento de SI como personal de la estructura de proyectos diferentes de TI, como el grupo de dirección del proyecto, grupo de trabajo del proyecto, equipo de evaluación, equipo de negociación y contratación, equipo de implementación, equipo de aseguramiento de la calidad y equipo de solución de problemas.
 - Actuar como asesor o revisor de proyectos de TI o controles de TI según necesidades.
- 2.4.3** La prestación de servicios o roles distintos de la auditoría puede crear amenazas a la independencia profesional en actitud o apariencia que pueden ser particularmente difícil de superar con aseguramiento si el área en la que los servicios o roles distintos de auditoría es actualmente, o lo será en el futuro, el sujeto de un encargo de auditoría o aseguramiento. En esta situación, la percepción puede ser que tanto la independencia como la objetividad de los profesionales han sido dañadas por la realización de los servicios o roles distintos de la auditoría.
- 2.4.4** Los profesionales que prestan servicios o roles distintos de auditoría deben evaluar, el uso del marco conceptual, si los servicios o roles distintos de auditoría generan un daño a la independencia, ya sea en actitud o en

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.4 Servicios o roles distintos de auditoría cont.

apariencia para el encargo de auditoría o aseguramiento actual o futuro. Esto aplica a encargos donde el área donde se realiza el servicio o rol distinto de la auditoría es significativa o [materialidad](#) para la materia o interesados de esos encargos. Los profesionales deben buscar asesoramiento de colegas y gestores en auditoría y aseguramiento de SI cuando sea necesario, y también, si es necesario, de aquellos encargados del Gobierno, para determinar si las salvaguardas adecuadas se pueden implementar para mitigar adecuadamente cualquier amenaza a la independencia real o percibida.

- 2.4.5** Antes de iniciar los servicios o roles distintos de la auditoría, los profesionales deben establecer y documentar su entendimiento con la gerencia de auditoría de SI y/o de los encargados del Gobierno, según proceda, en relación a:
- Los objetivos de los servicios o roles distintos de auditoría.
 - La naturaleza de los servicios o roles distintos de auditoría a realizar.
 - La aceptación de las responsabilidades de la entidad auditada relacionadas con los servicios o roles distintos de auditoría.
 - Responsabilidades profesionales relacionadas con los servicios o roles distintos de auditoría.
 - Cualquier limitación de los servicios o roles distintos de auditoría.
 - Cualquier limitación al alcance de los servicios de auditoría futuro que los profesionales puedan proporcionar.
- 2.4.6** En el caso de un encargo de auditoría o de aseguramiento de SI donde existe la posibilidad de dañar la independencia en actitud o apariencia debido a los servicios o roles distintos de auditoría realizados, la dirección de auditoría y aseguramiento de SI debe implementar salvaguardas como:
- Seguimiento de cerca de la realización de la auditoría.
 - Evaluar cualquier indicio de daño a la independencia en actitud o apariencia que surja de los servicios o roles realizados distintos de la auditoría y el inicio de las salvaguardas necesarias.
 - Informar a los encargados del Gobierno del daño potencial de la independencia en la actitud o apariencia y las salvaguardas implementadas.

2.5 Servicios o Roles Distintos de la Auditoría que No Dañan la Independencia

- 2.5.1** Las actividades rutinarias y administrativas o que involucran materias que son insignificantes generalmente se consideran que no son responsabilidad de la gerencia y por lo tanto no dañan la independencia. Además, la prestación de asesoramiento y recomendaciones para ayudar a la gerencia en el ejercicio de sus responsabilidades no se considera como un supuesto de responsabilidad de gerencia.
- 2.5.2** Los servicios o roles distintos de la auditoría que tampoco podrían dañar la independencia o la objetividad si se implementan las salvaguardas adecuadas incluye el asesoramiento rutinario sobre riesgo y controles de TI.
- 2.5.3** Para evitar el riesgo de asumir una responsabilidad gerencial cuando se proporcionan servicios o roles distintos de la auditoría en un área que es, o podría ser, sujeto de un encargo de auditoría o de aseguramiento, los profesionales deben proporcionar únicamente los servicios o roles distintos

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.5 Servicios o Roles Distintos de la Auditoría que No Dañan la Independencia cont.

de auditoría si satisfacen que la gerencia realiza o realizará las siguientes funciones en conexión con los servicios o roles distintos de la auditoría:

- Asumir todas las responsabilidades gerenciales.
- Supervisar los servicios designando a un individuo, preferiblemente dentro de la alta dirección, que posea la capacidad, conocimiento o experiencia adecuada.
- Evaluar la adecuación y resultados de los servicios realizados.
- Aceptar la responsabilidad de los resultados de los servicios.

Los profesionales deben documentar la consideración de la capacidad de la gerencia para supervisar los servicios o roles distintos de auditoría que se deben realizar.

2.6 Servicios o Roles Distintos de Auditoría que Dañan la Independencia

2.6.1 Si los profesionales debían asumir responsabilidades de gerencia o realizar actividades de gerencia, las amenazas a la independencia podrían ser tan significativos que ninguna salvaguarda podría reducirlas a un nivel aceptable. Si una actividad es responsabilidad de la gerencia depende de las circunstancias y requiere el ejercicio de juicio profesional. Ejemplos de actividades que podrían ser consideradas generalmente como responsabilidad de la gerencia son:

- Establecer las políticas y la dirección estratégica.
- Dirigiendo y asumiendo la responsabilidad de las acciones de los empleados de la entidad.
- Autorización de transacciones.
- Decidiendo qué recomendaciones de la función de auditoría, auditoría interna, organización, firma o de otras terceras partes han de ser implementadas.
- Asumiendo la responsabilidad de diseñar, implementar o mantener el control interno.
- Aceptando la responsabilidad para la gerencia de un proyecto o iniciativa de TI.

2.6.2 Además de asumir las responsabilidades de la gerencia, los siguientes servicios o roles distintos de la auditoría se consideran perjudiciales para la independencia y la objetividad:

- Participación material de profesionales en la supervisión o realización de diseño, desarrollo, pruebas, instalación, configuración u operación de sistemas de la información que son importantes o significativos para el sujeto de la auditoría o aseguramiento encargados.
 - Diseñar controles para los sistemas de la información que son importantes o significativos para el sujeto de la auditoría o compromiso de aseguramiento contratados.
 - Servir en un rol de Gobierno donde los profesionales son responsables de forma independiente o en conjunto de la toma de decisiones de gerencia o aprobación de políticas y estándares.
 - Proporcionar asesoramiento que forme la base principal de las decisiones de gerencia /administración o realizar funciones de gerencia / administración.
-

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.7 Relevancia de la Independencia Cuando se Proporcionan Servicios o Roles Distintos de la Auditoría

2.7.1 A menos que esté prohibido por estándares externos o por legislación, no hay requerimientos para los profesionales para ser, o ser visto, independientes cuando se realizan tareas relacionadas con el desarrollo de servicios o roles distintos de la auditoría; la objetividad sigue siendo un requerimiento profesional. De acuerdo con ello, los profesionales deben llevar a cabo tareas relativas a los servicios o roles distintos de la auditoría de una forma objetiva y profesional.

2.7.2 A pesar de que no existe ningún requerimiento a los profesionales para ser independientes mientras realizan servicios o roles distintos de auditoría, los profesionales deben considerar si la independencia podría dañarse si se les asigna a realizar un encargo de auditoría o de aseguramiento en el área donde se están ofreciendo o fueron ofrecidos los servicios o roles distintos de la auditoría es importante para el sujeto del encargo. Cuando tal daño potencial es previsible (ejemplo, cuando se requerirá un auditor independiente y sólo hay un profesional con las habilidades requeridas para realizar tanto los servicios o roles distintos de la auditoría como la auditoría posterior), el profesional debe buscar asesoramiento de la gerencia de auditoría y, si es necesario, de los encargados del Gobierno, antes de aceptar o realizar los servicios o roles distintos de la auditoría.

2.7.3 Determinar si los profesionales deben realizar servicios o roles distintos de la auditoría, cuando se ha planificado o realizado un encargo de auditoría o aseguramiento actual o posterior del área donde los servicios o roles distintos de la auditoría por el mismo profesional, debe ser decisión de la gerencia de auditoría de SI y de los encargados del Gobierno. La gerencia de auditoría de SI debe aplicar el marco conceptual cuando realice una decisión, y los siguientes factores también pueden influenciar en la decisión:

- Los profesionales no deben ser colocados en una situación para auditar su propio trabajo u ofrecer servicios o roles distintos de la auditoría en áreas que se sabe o se cree importantes o materiales al sujeto del encargo de auditoría o aseguramiento de SI en los que ellos están o estarán involucrados.
 - Si existen recursos disponibles para realizar de forma separada tanto la función distinta de auditoría como la función de auditoría y aseguramiento independiente.
 - La percepción de la gerencia de SI y de los encargados del Gobierno del valor o importancia de los servicios o roles distintos de la auditoría relativa al encargo de auditoría y aseguramiento.
 - Nivel de riesgo a la función de auditoría asociada con los servicios o roles distintos de la auditoría.
 - Efecto de la decisión sobre los requerimientos de auditores o reguladores externos, si existen.
 - Las disposiciones del Estatuto de Auditoría de SI.
-

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

2.8 Admisibilidad de Servicios o Roles Distintos de la Auditoría

- 2.8.1** El Estatuto de Auditoría de SI debe establecer cuándo se permite a los profesionales involucrarse en realizar servicios o roles distintos de la auditoría y el carácter general, tiempo y extensión de tales servicios o roles, para asegurar que la independencia no se dañe respecto a los sistemas que ellos puedan auditar. Esto podría eliminar o minimizar la necesidad de obtener mandatos específicos para cada servicio o rol distinto de la auditoría para cada caso.
- 2.8.2** Los profesionales deben proporcionar aseguramiento razonable de que los términos de referencia (TOR) de los servicios o roles específicos distintos de la auditoría están en conformidad con el Estatuto de Auditoría. Cuando hay desviaciones, las mismas deben ser indicadas expresamente en el TOR y aprobadas por la gerencia de auditoría y aseguramiento de SI y/o de los encargados del Gobierno.
- 2.8.3** Cuando el Estatuto de Auditoría no especifique los servicios o funciones o cuando no haya Estatuto de Auditoría, los profesionales deben informar de la naturaleza de su participación en los servicios o roles distintos de la auditoría a la gerencia de auditoría y aseguramiento de SI y a los encargados del Gobierno. El tiempo y extensión de la participación de los profesionales en los servicios o roles distintos de la auditoría deben estar sujetos a TOR individuales firmados por la gerencia de la función donde los servicios o roles serán desarrollados y aprobados por los encargados del Gobierno.
-

2.9 Presentación de informes

- 2.9.1** Cuando la independencia de los profesionales, con referencia a un encargo de auditoría o aseguramiento de SI, pueda ser o parecer dañada, y los encargados del Gobierno han tomado la decisión de continuar el encargo, el informe del encargo de auditoría y aseguramiento de SI debe incluir información suficiente que permita a los usuarios del informe comprender la naturaleza del daño potencial. La información que los profesionales deben considerar revelar en un informe de encargo de auditoría y aseguramiento de SI incluye:
- Los nombres y antigüedad de los profesionales involucrados en el encargo de auditoría y aseguramiento de SI que pueden tener o parecer, un impedimento a su independencia.
 - Análisis y descripción de las amenazas a la independencia.
 - Salvaguardas implementadas para eliminar o mitigar las diferentes amenazas a la independencia y objetividad durante el curso del encargo de trabajo y los procesos de presentación de informes.
 - El hecho que el impedimento potencial de la independencia ha sido revelado a los encargados del Gobierno y su aprobación a la realización o continuación del encargo de aseguramiento y/o los servicios o roles distintos de 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.

Para los estándares sólo se muestran las cláusulas más relevantes.

- 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.
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.

- 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*.

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

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.
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 de Gobierno dentro de la empresa, ejemplo, comité de auditoría de áreas de auditoría de SI y aseguramiento.

4. Terminología

Término	Definición
Discapacidad	Una condición que causa una debilidad o disminución de la capacidad para ejecutar los objetivos de la auditoría. La discapacidad para la independencia organizacional y la objetividad individual pueden incluir conflictos o intereses personales; limitaciones al alcance; restricciones de acceso a registros, personal, equipamiento o locales, y limitaciones de recursos (tales como financiación o dotación de personal).
Escepticismo profesional	Una actitud que incluye una mente inquisitiva y una evaluación crítica de la evidencia de auditoría. Fuente: American Institute of Certified Public Accountants (AICPA) AU 230.07.
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.
Independencia de mente	El estado de la mente que permita la expresión de una conclusión sin verse afectado por influencias que comprometan el juicio profesional, lo que permite a un individuo actuar con integridad, ejercer objetivamente y con escepticismo profesional.
Independencia en apariencia	Evitar hechos y circunstancias que son tan significativos que una tercera parte razonable e informada podría concluir, sopesando todos los hechos y circunstancias específicos, que se ha comprometido un equipo de auditoría de SI, o individuo del equipo de auditoría de SI, la integridad, objetividad o escepticismo profesional.

Guía de Auditoría y Aseguramiento de SI 2003 Independencia Profesional

Término	Definición
Integridad	La custodia contra la modificación o destrucción de información inadecuada, que incluye garantizar el no repudio y la autenticidad de la información.
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.
Objetividad	La capacidad de ejercer un juicio, expresar opiniones y presentar recomendaciones imparcialmente.

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.
------------------------------	--

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.

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 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

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 Estándares y reglamentos. 2.2 Alcance. 2.3 Limitaciones del alcance. 2.4 Información. 2.5 Aceptación de un cambio en los términos de compromiso.
2.1 Estándares y Reglamentos	2.1.1 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. 2.1.2 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. 2.1.3 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: • 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. • Proponer un cambio en los términos del trabajo o que el trabajo propuesto no se acepta.
2.2 Alcance	2.2.1 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. 2.2.2 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. 2.2.3 En caso de que los profesionales determinen que el ámbito del trabajo de auditoría no les permite expresar una opinión o conclusión profesional, deben: • Informar a la gerencia de auditoría y aseguramiento y a los encargados del Gobierno de los asuntos identificados en el alcance. • Proponer un cambio en los términos del encargo o no aceptar el trabajo de auditoría propuesto.

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.

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 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
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
(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.

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).

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 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.

Guía de Auditoría y Aseguramiento de SI 2005 Debido Cuidado Profesional

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.

Guía de Auditoría y Aseguramiento de SI 2005 Debido Cuidado Profesional

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.

Título 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.

Guía de Auditoría y Aseguramiento de SI 2005 Debido Cuidado Profesional

Título 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.

Guía de Auditoría y Aseguramiento de SI 2005 Debido Cuidado Profesional

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 crítica 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.

Guía de Auditoría y Aseguramiento de SI 2006 Competencia

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	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.
1201 Planificación de la Asignación	Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir: • 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. 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: • 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
	Tiempos y grado de los procedimientos de auditoría para completar el trabajo.
1203 Desempeño y Supervisión	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. 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.

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 optima, 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.
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

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.
------------------------------	--

Guía de Auditoría y Aseguramiento de SI 2007 Afirmaciones

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 2007 Afirmaciones

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 detallar las diferentes afirmaciones, guiar a los profesionales de auditoría y aseguramiento de SI en asegurar que el criterio, contra los que se evalúa la materia, es compatible con las afirmaciones y proporcionan orientación para formular una conclusión y redacción de un informe sobre las afirmaciones.
 - 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 preparado para justificar cualquier desvío y buscar guías adicionales si se considera necesario.
-

1.2 Vinculación con Estándares

- 1.2.1** Estándar 1007 Afirmaciones.
 - 1.2.2** Estándar 1008 Criterios.
 - 1.2.3** Estándar 1204 Materialidad.
 - 1.2.4** Estándar 1206 Uso del Trabajo de Otros Expertos.
 - 1.2.5** Estándar 1401 Reportes.
-

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 Afirmaciones.
- 2.2 Materia y criterios.
- 2.3 Afirmaciones desarrolladas por terceros.

2.1 Afirmaciones

- 2.1.1** Las [afirmaciones](#) son toda declaración o conjunto de declaraciones si la [materia](#) se basa en la conformidad con los [criterios](#) seleccionados. Los profesionales deben tener en cuenta estas afirmaciones durante la ejecución de un trabajo de auditoría, obtener aseguramiento de su logro y expresarlas en un informe de auditoría.
- 2.1.2** Las afirmaciones comunes que se pueden considerar son:
- **Confidencialidad**—Preservar las restricciones autorizadas al acceso y divulgación, así como medios para proteger la privacidad y la propiedad de la información.
 - **Compleitud**—Todas las actividades, información y otros datos que deberían haberse registrado están registrados, por ejemplo, todos los cambios a los sistemas de TI promovidos a producción se registran en la aplicación de seguimiento de gerencia del cambio.
 - **Precisión**—Los importes, fechas y otros datos relacionados con las actividades registradas se han registrado adecuadamente, por ejemplo, datos relacionados a la promoción de cambios en los sistemas de TI en producción se muestran correctamente en los registros de cambios de la aplicación de seguimiento de gerencia del cambio.
 - **Integridad**—La información, evidencias y otros datos recibidos provienen de fuentes confiables, por ejemplo, los registros de cambios solicitados por los profesionales se reciben desde el gerente de cumplimiento, una fuente de confianza y fiable dentro de la empresa.
 - **Disponibilidad**—La información, evidencias y otros datos requeridos para el trabajo de auditoría existen y son accesibles, por ejemplo, los registros de solicitud de cambios existen y son de fácil acceso en la aplicación de seguimiento de gerencia del cambio.
 - **Cumplimiento**—La información, evidencias y otros datos han sido grabados de acuerdo a la empresa, regulaciones o de otras estipulaciones aplicables, por ejemplo, los campos necesarios, de acuerdo a las estipulaciones aplicables, están presentes en los registros de cambios de la aplicación de seguimiento de gerencia del cambio.
- 2.1.3** La gerencia es responsable de definir y aprobar la materia y afirmaciones relacionadas. Los profesionales deben asegurarse que cualquier afirmación desarrollada por la gerencia es lo que un lector o usuario experto podrían esperar comparado a los estándares de pronunciamientos autorizados.
- 2.1.4** Una precondition previa para que el profesional acepte el trabajo de auditoría debe ser la confirmación de la gerencia que comprende completamente su responsabilidad de proporcionar toda la información necesaria respecto a la materia y las afirmaciones de los profesionales. Si los profesionales creen que la gerencia no será capaz de cumplir esta responsabilidad, deben:
- Informar a la gerencia de auditoría y aseguramiento de SI y a los encargados del Gobierno de las cuestiones identificadas.
 - No aceptar el trabajo de auditoría propuesto.

Guía de Auditoría y Aseguramiento de SI 2007 Afirmaciones

2.1 Afirmaciones cont.	2.1.5 Los profesionales deben revisar las afirmaciones seleccionadas para el trabajo de auditoría y asegurar que son: • Suficientes—Para cumplir el propósito del trabajo de auditoría, que está expresando una opinión o conclusión de la materia en el alcance. • Validas—Capaz de ser probadas, dada la materia en el alcance. • Relevante—Tener una conexión directa a la materia en el alcance y contribuir al cumplimiento de la finalidad del trabajo de auditoría.
2.2 Materia y Criterios	2.2.1 La materia de un trabajo de auditoría está determinada por la gerencia y los encargados del Gobierno. Normalmente, la materia del trabajo de auditoría de SI no será definida con tanta precisión como lo es en los trabajos de auditoría financiera. Por ejemplo, la materia de la asignación de auditoría y aseguramiento de SI puede variar de un sistema y sus interfaces, a los procesos (cubriendo múltiples sistemas e interfaces), o incluso todas las operaciones relativas a SI de un cierto departamento. 2.2.2 Los profesionales deben evaluar la materia del trabajo de auditoría contra los criterios predeterminados para expresar una opinión o conclusión sobre la materia. Los profesionales deben evaluar estos criterios para asegurar que respaldan las afirmaciones relevantes. 2.2.3 Un criterio puede vincular a múltiples afirmaciones. Por otra parte, una afirmación puede también ser apoyada por múltiples criterios que todos proporcionan una parte de la seguridad en la consecución de la afirmación. 2.2.4 En caso que los profesionales concluyan que los criterios no soportan completamente todas las afirmaciones relevantes, deben hacer sugerencias para modificar los criterios existentes o para añadir criterios adicionales. La gerencia de auditoría y aseguramiento de SI revisa y aprueba o rechaza los criterios nuevos o modificados. 2.2.5 Tras evaluar que los criterios soportan totalmente las afirmaciones relevantes, los profesionales deben evaluar que los criterios pueden ser sujeto de aun análisis objetivo y medible, como se detalla en el Estándar 1008 Criterios.
2.3 Afirmaciones Desarrolladas por Terceros	2.3.1 Las empresas que externalizan operaciones a terceros recibirán informes sobre el entorno de control de las operaciones externalizadas. La gerencia revisara cada informe para determinar si: • El informe es emitido por una entidad profesional independiente relevante. • La opinión de auditoría es calificada o no calificada. • El alcance de los objetivos de control cubre adecuadamente los controles requeridos por la empresa. • El periodo auditado este en línea con las expectativas de la empresa. • Las deficiencias de controles específicos (que no conducen a una calificación global del informe) son relevantes para la empresa. • Las afirmaciones utilizadas están en línea con las afirmaciones requeridas.

Guía de Auditoría y Aseguramiento de SI 2007 Afirmaciones

2.3 Afirmaciones Desarrolladas por Terceros cont.

La gerencia de auditoría y aseguramiento de SI debe documentar el análisis realizado y las conclusiones alcanzadas. Los profesionales deben asegurarse que las afirmaciones están verificadas y aprobadas formalmente por la gerencia, como parte de un trabajo de auditoría que tiene en el alcance las operaciones externalizadas. El estándar 1206 Uso del Trabajo de Otros Expertos proporciona mas orientación sobre este tema.

2.4 Conclusión e Informe

- 2.4.1** Después de evaluar la materia del trabajo de auditoría contra los criterios, los profesionales deben formar una conclusión sobre cada afirmación, basada en la suma de los hallazgos contra los criterios relacionados, junto con el [juicio profesional](#).
- 2.4.2** Tras formar una conclusión, los profesionales deben emitir un informe indirecto o directo sobre la materia:
- **Informe indirecto**—En las afirmaciones sobre la materia. Por ejemplo, en la afirmación ‘completitud’, para un componente en la materia: ‘Basado en nuestras pruebas de efectividad operativa, en nuestra opinión los cambios de sistemas de TI promocionan a producción, en todos los aspectos materiales de acuerdo a los criterios seleccionados, han sido completamente registrados en la aplicación de seguimiento de gerencia del cambio’.
 - **Informe directo**—En la materia en sí misma. Por ejemplo, sobre la materia entera: ‘Basado en nuestras pruebas, en nuestra opinión los cambios en los sistemas de TI están siguiendo, en todos los aspectos materiales de acuerdo a los criterios seleccionados, los procedimientos de gerencia del cambio requeridos’.

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
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.

Guía de Auditoría y Aseguramiento de SI 2007 Afirmaciones

Titulo del Estándar	Declaración Estándar Relevante
1008 Criterios	Los profesionales de auditoría y aseguramiento seleccionaran criterios, contra los que se evaluara 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.
1204 Materialidad	Los profesionales de auditoría y aseguramiento revelaran lo siguiente en el informe de auditoría: • Ausencia de controles o controles inefectivos. • Importancia de la deficiencia de los controles. • Probabilidad de que estas debilidades resulten en una deficiencia significativa o material.
1206 Uso del Trabajo de Otros Expertos	Los profesionales de auditoría y aseguramiento deberán asesorar, revisar y evaluar el trabajo de otros expertos como parte del trabajo, y documentar la conclusión sobre el grado de uso y confianza en su trabajo.
1401 Reportes	Los profesionales de auditoría y aseguramiento de SI deberán presentar un informe para comunicar los resultados una vez finalizado el trabajo, incluyendo: • Identificación de la empresa, destinatarios y cualquier restricción al contenido y circulación. • El alcance, objetivos de trabajo, periodo de cobertura y naturaleza, tiempos y alcance de los trabajos realizados. • Los hallazgos, conclusiones y recomendaciones. • Cualquier cualificación o limitación al alcance que el profesional de auditoría y aseguramiento de SI tiene respecto al trabajo. • Firma, fecha y distribución de acuerdo a los términos de la Estatuto de Auditoría o carta de compromiso.

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 del Gobierno de los miembros del consejo.

Guía de Auditoría y Aseguramiento de SI 2007 Afirmaciones

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 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).

4. Terminología

Término	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.
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 prácticas de privacidad, estándares, legislación y regulaciones específicas (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.

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 Inglés 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 específico 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 Comité de Estándares Profesionales y Gestión 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 2008 Criterios

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.
-

Guía de Auditoría y Aseguramiento de SI 2008 Criterios

2.1 Selección y Uso de Criterios

- 2.1.1** Los profesionales deberán seleccionar [criterios](#), contra los que se evaluará 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 embargo 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 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. Es 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.

Guía de Auditoría y Aseguramiento de SI 2008 Criterios

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 medible 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 específica) 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.
-

Guía de Auditoría y Aseguramiento de SI 2008 Criterios

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.

Guía de Auditoría y Aseguramiento de SI 2008 Criterios

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. En 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*.

Guía de Auditoría y Aseguramiento de SI 2008 Criterios

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.

Guía de Auditoría y Aseguramiento de SI 2008 Criterios

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 específicas (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.
------------------------------	--

Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la Asignación

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®) 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

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 2201 Planificación de la Asignación

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 proporciona ayuda a los profesionales de auditoría y aseguramiento de SI. La planificación adecuada ayuda a garantizar que se dedica la atención adecuada a las áreas importantes de la auditoría, se identifican y resuelven los problemas potenciales de manera oportuna, y que el trabajo de auditoría está organizado adecuadamente, gestionado y realizado de una forma efectiva y eficaz.
 - 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 1201 Planificación de la asignación
 - 1.2.2** Estándar 1202 Evaluación de Riesgos en la Planificación de Auditoría
 - 1.2.3** Estándar 1203 Desempeño y Supervisión
 - 1.2.4** Estándar 1204 Materialidad
-

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 Plan de auditoría de SI

Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la Asignación

- 2.2 Objetivos
- 2.3 Alcance y conocimiento del negocio
- 2.4 Planteamiento basado en el riesgo
- 2.5 Documentar el plan de proyecto del trabajo de auditoría
- 2.6 Cambios durante el transcurso de la auditoría

2.1 Plan de Auditoría de SI

- 2.1.1 Para una función de auditoría, se debe desarrollar y actualizar [plan de auditoría](#) basada en riesgos, al menos anualmente. Se debe establecer un horizonte temporal multi anual (tres a cinco años) e incorporar en el plan anual. Los planes multi anual y anual deben actuar como marco de las actividades de auditoría y aseguramiento de SI y servir para hacer frente a las responsabilidades establecidas por el Estatuto de Auditoría.
- 2.1.2 El plan de auditoría de SI debe estar preparado para que este en cumplimiento con cualquier requerimiento externo adecuado, además de los actuales estándares de ISACA.
- 2.1.3 En cada trabajo de auditoría debe estar referenciado o el plan de auditoría de SI o el estado del mandato específico, objetivos y otros aspectos relevantes del trabajo a realizar.

2.2 Objetivos

- 2.2.1 Los profesionales deben definir los objetivos del trabajo de auditoría y documentarlos en el plan de proyecto del trabajo de auditoría, con el fin de realizarse de forma efectiva. Los objetivos del trabajo deberán establecerse para hacer frente al riesgo asociado con la actividad bajo revisión.
- 2.2.2 Los profesionales deberán desarrollar un plan de proyecto del trabajo de auditoría que tenga en cuenta los objetivos del trabajo de auditoría. Estos objetivos podrían influir en el trabajo de auditoría, por ejemplo, recursos necesarios, plazos y entregables.

2.3 Alcance y Conocimiento del Negocio

- 2.3.1 Antes de empezar un trabajo de auditoría, el trabajo de los profesionales debe ser planificado adecuadamente para el cumplimiento de los objetivos de auditoría. Como parte del proceso de planificación, los profesionales deberán obtener una comprensión de la empresa y sus procesos. Esto les ayudara a determinar la importancia de los recursos que están siendo revisados en relación con los objetivos de la empresa. De esta forma, los profesionales pueden enfocarse en las áreas más sensitivas al fraude o practicas inadecuadas. Deben establecer el alcance del trabajo de auditoría y también realizar un análisis preliminar de los controles internos sobre la función a revisar.
- 2.3.2 Los profesionales deben obtener una comprensión de los tipos de personal, eventos, transacciones y prácticas que pueden tener un efecto significativo sobre la empresa, función, proceso o datos específicos que es la materia del trabajo de auditoría. El conocimiento de la empresa debe incluir el riesgo de negocios y financiero frente a la empresa así como las condiciones en el mercado de la empresa y el grado en que la empresa se basa en externalizar para cumplir sus objetivos. Los profesionales deben utilizar esta información

Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la Asignación

2.3 Alcance y Conocimiento del Negocio cont.	para identificar problemas potenciales, formular los objetivos y alcance del trabajo, realizar el trabajo y considerar acciones de gerencia de las que deben estar alerta.
2.4 Planteamiento Basado en el Riesgo	2.4.1 Los profesionales deben desarrollar un plan de proyecto del trabajo de auditoría para reducir el riesgo de auditoría a un nivel aceptable. 2.4.2 Se debe realizar un análisis de riesgos para proporcionar aseguramiento razonable de que todos los elementos materiales serán cubiertos adecuadamente durante el trabajo de auditoría y que los profesionales serán capaces de llegar a una conclusión. Este análisis debe identificar las áreas con alta probabilidad relativa de problemas materiales. 2.4.3 Se debe llevar a cabo un análisis de riesgos y priorización de los riesgos identificados para el área bajo revisión y el entorno de SI de la empresa en la medida necesaria. 2.4.4 Normalmente en el proceso de planificación, los profesionales deben establecer niveles de planificación de materialidad tales que el trabajo de auditoría será suficiente para conseguir los objetivos de auditoría y usara los recursos de auditoría eficientemente. Por ejemplo, en la revisión de un sistema existente, los profesionales deben evaluar la materialidad de los distintos componentes del sistema en la planificación del trabajo de auditoría para el trabajo a realizar. Tanto los aspectos cualitativos como cuantitativos se deben considerar en la determinación de la materialidad. 2.4.5 Antes de empezar un trabajo de auditoría y en el transcurso de la auditoría, el profesional deberá considerar el cumplimiento con leyes aplicables y estándares de auditoría profesionales. 2.4.6 Cuando los profesionales evalúen los controles internos a efectos de dar confianza en los procedimientos de control en apoyo a la información que se reúne como parte de un ejercicio de auditoría mayor (como auditoría de información financiera historia), deben, como norma, hacer una evaluación preliminar de los controles y desarrollar el plan de proyecto del trabajo de auditoría en base a esta evaluación.
2.5 Documentar el Plan de Proyecto del Trabajo de Auditoría	2.5.1 Los papeles de trabajo de los profesionales deben incluir el plan de proyecto del trabajo de auditoría. 2.5.2 Una definición clara del proyecto es un factor de éxito crítico para asegurar la efectividad y eficiencia del proyecto. Un plan de proyecto del trabajo de auditoría debe incluir en los términos de referencia elementos como: • Áreas a auditar • Tipo de trabajo planificado • Objetivos de alto nivel y alcance del trabajo • Entrevistas a realizar para descubrir hechos • Información relevante a obtener • Procedimientos para verificar o validar la información obtenida y su uso como evidencia de auditoría • Temas generales, ejemplo: – Presupuesto

Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la

Asignación

2.5 Documentar el Plan de Proyecto del Trabajo de Auditoría cont.

- Disponibilidad y asignación de recursos
- Fechas planificadas
- Tipo de informe
- A quien va dirigido
- Entregables
- Temas específicos, ejemplo:
 - Identificación de las herramientas necesarias para obtener las evidencias, pruebas realizadas y preparación / resumen de la información para el informe
 - Criterios de evaluación a utilizar
 - Requisitos y distribución de los informes
- Otros aspectos generales del trabajo, cuando sea aplicable

2.5.3 El plan de proyecto debe incluir los requerimientos relacionados con la línea de tiempo del trabajo de auditoría, tales como el periodo cubierto y las distintas fechas de terminación, para realizar el trabajo de auditoría dentro de las fechas acordadas. Esto también incluye el gasto presupuestario.

2.5.4 Los profesionales deben garantizar una cobertura completa de las competencias requeridas por los recursos del trabajo de auditoría. Ellos deben crear un equipo de trabajo de auditoría que tenga las habilidades, conocimiento y experiencia adecuados para completar con éxito el trabajo de auditoría. Los profesionales deben asegurarse de asignar los diferentes roles y responsabilidades a los miembros del equipo de auditoría de SI que mejor encajen con sus competencias. Para más información, consultar el Estándar 1203 Desempeño y Supervisión.

2.5.5 El plan de proyecto del trabajo de auditoría deberá listar todos los entregables vinculados al trabajo de auditoría.

2.5.6 El plan de proyecto del trabajo de auditoría y cualquier cambio posterior a este plan deben ser aprobados por la gerencia de auditoría y aseguramiento de SI.

2.5.7 Tras la aprobación por la gerencia de auditoría y aseguramiento de SI, partes del plan de proyecto del trabajo de auditoría (ejemplo, alcance, tiempos, requerimientos de documentación, planificación de entrevistas) deben ser comunicadas oportunamente a los auditados para brindar acceso apropiado y completo y disponibilidad de los documentos y recursos necesarios.

2.6 Cambios Durante el Transcurso de la Auditoría

2.6.1 El plan de proyecto del trabajo de auditoría debe ser actualizado y cambiado según sea necesario durante el curso del trabajo de auditoría.

2.6.2 Planificar un trabajo de auditoría es un proceso continuo e iterativo. Como resultado de eventos no esperados, cambios en las condiciones o evidencias de auditoría obtenidas, los profesionales pueden necesitar modificar la naturaleza, tiempos y extensión planificada de los procedimientos adicionales de auditoría.

2.6.3 El plan de auditoría debe considerar la posibilidad de eventos imprevistos que impliquen riesgo para la empresa. En consecuencia, el plan de proyecto del trabajo de auditoría debe ser capaz de priorizar tales eventos dentro del proceso de auditoría y aseguramiento basado en el riesgo.

Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la Asignación

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
1201 Planificación de la asignación	Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir: • 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. 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: • La naturaleza, objetivos, línea de tiempo y recursos requeridos del trabajo • Tiempos y grado de los procedimientos de auditoría para completar el trabajo
1202 Evaluación de Riesgos en la Planificación de Auditoría	La función de auditoría y aseguramiento de SI deberá utilizar un enfoque apropiado y el apoyo de metodología de análisis de riesgos para desarrollar el plan de auditoría de SI general y determinar las prioridades para la asignación efectiva de recursos de auditoría de SI. Los profesionales de auditoría y aseguramiento de SI deberán identificar y analizar los riesgos relevantes al área bajo revisión, en la planificación de trabajos individuales.
1203 Desempeño y Supervisión	Los profesionales de auditoría y aseguramiento de SI deberán conducir el trabajo de acuerdo al plan de auditoría de SI aprobado para cubrir los riesgos identificados y dentro del plan acordado.
1204 Materialidad	Los profesionales de auditoría y aseguramiento de SI deberán considerar las debilidades o ausencias de controles potenciales mientras planifican un trabajo, y si tal debilidad o ausencia de control podría resultar en una deficiencia significativa o debilidad material.

Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la Asignación

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: Habilidad de Procesos*.

Procesos de COBIT 5	Propósito de los Procesos
MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	Proporcionar transparencia del desarrollo, cumplimiento y dirigir el logro de los objetivos.
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 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
Análisis de riesgos	Un proceso utilizado para identificar y evaluar riesgos y sus efectos potenciales. Los análisis de riesgos se utilizan para identificar aquellos elementos o áreas que presentan el riesgo, vulnerabilidad o exposición más altos para la empresa para incluirlos en el plan de auditoría anual de SI. Los análisis de riesgos se utilizan también para gestionar la ejecución de los proyectos y el riesgo en beneficio del proyecto.
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.

Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la Asignación

Termino	Definición
Plan de auditoría	1. Un plan que contiene la naturaleza, plazos y alcance de los procedimientos de auditoría a realizar por los miembros del equipo de trabajo con el fin de obtener evidencias apropiadas de auditoría suficientes para formar una opinión. Notas del alcance: Incluyen las áreas a auditar, el tipo de trabajo planificado, los objetivos de alto nivel, y alcance del trabajo, y temas como el presupuesto, asignación de recursos, fechas planificadas, tipo de informe, publico objetivo y otros aspectos generales del trabajo. 2. Una descripción de alto nivel del trabajo de auditoría a realizar en un cierto periodo de tiempo.
Riesgo de Auditoría	El riesgo de llegar a una conclusión incorrecta basada en los resultados de la auditoría. Los tres componentes de riesgo de auditoría son: • Riesgo de control • Riesgo de detección • Riesgo inherente

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.
------------------------------	--



Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

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®) 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 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 2202 Análisis de Riesgos en la Planificación

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 nivel de trabajo de auditoría requerido para conseguir los objetivos de auditoría es una decisión subjetiva realizada por los profesionales de auditoría y aseguramiento de SI. El propósito de esta guía es reducir el riesgo de alcanzar una conclusión incorrecta basada en los hallazgos de auditoría y reducir la existencia de errores en el área auditada. 1.1.2 La guía proporciona ayuda en aplicar una aproximación de análisis de riesgos para desarrollar: • Plan de auditoría de SI que cubre todos los trabajos de auditoría anuales. • Plan de proyecto del trabajo de auditoría que se enfoca en un trabajo de auditoría específico. 1.1.3 La guía proporciona los detalles de los diferentes tipos de riesgo que se encuentran los profesionales de auditoría y aseguramiento de SI se encontrara. 1.1.4 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 1201 Planificación de la asignación. 1.2.2 Estándar 1202 Evaluación de riesgo en planificación. 1.2.3 Estándar 1203 Desempeño y supervisión. 1.2.4 Estándar 1204 Materialidad. 1.2.5 Estándar 1207 Irregularidades y actos ilegales.
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'.

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

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: 1.1 Análisis de riesgos del plan de auditoría de SI. 1.2 Metodología de análisis de riesgos. 1.3 Análisis de riesgos de trabajos de auditoría individuales. 1.4 Riesgo de auditoría. 1.5 Riesgo inherente. 1.6 Riesgo de control. 1.7 Riesgo de detección.
2.1 Análisis de Riesgos del Plan de Auditoría de SI	2.1.1 Al desarrollar un plan de auditoría de SI completo, se debe seguir un enfoque de análisis de riesgos adecuado. Se debe realizar y documentar un análisis de riesgos al menos una vez al año para facilitar el proceso de desarrollo del plan de auditoría de SI. Debe tener en cuenta los planes y objetivos estratégicos organizacionales y el marco e iniciativas de gerencia del riesgo de la empresa. 2.1.2 Para evaluar correcta y completamente que el riesgo está relacionado al alcance del área de auditoría de SI, los profesionales deben considerar los siguientes elementos al desarrollar el plan de auditoría de SI: • Cubrir completamente todas las áreas del alcance del universo de auditoría de SI, que representa el rango de toda posible actividad de auditoría. • Fiabilidad y adecuación del análisis de riesgos proporcionado por la gerencia. • Los procesos seguidos por la gerencia para supervisar, examinar e informar posibles riesgos o problemas. • Cubrir el riesgo en actividades conexas relacionadas a las actividades bajo revisión. 2.1.3 El enfoque de análisis de riesgos aplicado debe ayudar a priorizar y planificar los procesos de auditoría de SI y el trabajo de aseguramiento. Debe apoyar la selección de áreas y temas de interés para la auditoría y la decisión del proceso para diseñar y llevar a cabo los trabajos de auditoría de SI particulares. 2.1.4 Los profesionales deben asegurarse que el enfoque de análisis de riesgos aplicado está aprobado por los encargados del Gobierno y distribuido a los diferentes interesados del trabajo. 2.1.5 Los profesionales deben usar el análisis de riesgos para cuantificar y justificar la cantidad de recursos de auditoría de SI necesarios para completar el plan de auditoría de SI y los requerimientos para los trabajos específicos. 2.1.6 Basándose en el análisis de riesgos, los profesionales deben desarrollar un plan de auditoría de SI que actúe como marco de trabajo para las actividades de auditoría y aseguramiento de SI. Debe:

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

2.1 Análisis de Riesgos del Plan de Auditoría de SI cont.

- Considerar requerimientos y actividades distintos de auditoría y aseguramiento.
- Actualizarse al menos anualmente.
- Estar aprobado por los encargados del Gobierno.
- Direccionar las responsabilidades establecidas por la [carta de auditoría](#).

Para más información referirse al Estándar 1201 Planificación de la asignación.

2.2 Metodología de Análisis de Riesgos

- 2.2.1** Los profesionales deben considerar la metodología de análisis de riesgos apropiada para asegurar que se cubre completa y exactamente los trabajos de auditoría en el plan de auditoría de SI.
- 2.2.2** Los profesionales deben al menos incluir un análisis, dentro de la metodología, del riesgo para la empresa relacionado con la disponibilidad de los sistemas, integridad de los datos y confidencialidad de la información del negocio.
- 2.2.3** Existen muchas metodologías de análisis de riesgos que apoyan el proceso de análisis de riesgos. Estas van desde simples clasificaciones de alto, medio y bajo, basadas en juicio profesional, a cálculos más cuantitativos y científicos proporcionando una clasificación de riesgo numérico, y otras que son una combinación de ambas. Los profesionales deben considerar el nivel de complejidad y detalle apropiado para la empresa o materia auditada. Se puede encontrar ayuda específica en el desarrollo del análisis de riesgos en la publicación de ISACA *COBIT 5 para el Riesgo*.
- 2.2.4** Todas las metodologías de análisis de riesgos se basan en juicios subjetivos en algún punto del proceso (ejemplo, para asignar pesos a los diferentes parámetros). Los profesionales deben identificar la decisión subjetiva requerida para utilizar una metodología particular y considerar si estos juicios pueden hacerse y validarse en un nivel adecuado de precisión.
- 2.2.5** Para decidir cuál es la metodología de análisis de riesgos más adecuada, los profesionales deben considerar:
 - Tipo de información requerida a recoger (algunos sistemas utilizan efectos financieros como la única medida – esto no siempre es adecuado para los trabajos de auditoría de SI).
 - Coste del software o de otras licencias requeridas para utilizar la metodología.
 - Grado en que la información requerida esta siempre disponible.
 - Cantidad de información adicional requerida para recoger antes de que se pueda obtener una salida confiable, y los costes de recoger esta información (incluyendo el tiempo necesario a invertir en el ejercicio de recopilación).
 - Opiniones de otros usuarios de la metodología, y su visión de cómo les ha ayudado en la mejora de la eficiencia y/o efectividad de sus auditorías.
 - Disposición de los encargados del Gobierno del área de auditoría de SI para aceptar la metodología como los medios para determinar el tipo y

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

2.2 Metodología de Análisis de Riesgos cont.

- nivel del trabajo de auditoría llevado a cabo.
- 2.2.6** No existe una metodología única de análisis de riesgos que sea apropiada para todas las situaciones. Las condiciones que afectan a la auditoría pueden cambiar en el tiempo. Periódicamente, los profesionales deben reevaluar la adecuación de la metodología de análisis de riesgos elegida.
- 2.2.7** Los profesionales deben utilizar las técnicas de análisis de riesgos seleccionadas en el desarrollo del plan de auditoría de SI completo y en la planificación de los trabajos de auditoría específicos. El análisis de riesgos, en combinación con otras técnicas de auditoría, debe ser considerado en la toma de decisiones de planificación como:
- Áreas o funciones de negocio a auditar.
 - Cantidad de tiempo y recursos a asignar a una auditoría.
 - Naturaleza, alcance y tiempos de los procedimientos de auditoría.
- 2.2.8** La metodología de análisis de riesgos adoptada debe producir resultados consistentes, validos, comparables y repetibles. El análisis de riesgos que surge de la metodología debe ser coherente (durante un periodo), valida, comparable (con evaluaciones anteriores / posteriores usando la misma metodología de análisis) y repetible (dado un conjunto de hechos similar, utilizando la misma metodología de análisis producirá una salida similar).
-

2.3 Análisis de Riesgos de Trabajos de Auditoría Individuales

- 2.3.1** Cuando se planifica un trabajo individual, los profesionales deben identificar y analizar el riesgo relevante para el área bajo revisión. Los resultados de este análisis de riesgos deben estar reflejados en los objetivos del trabajo de auditoría. Durante el análisis de riesgos, los profesionales deben considerar:
1. Los resultados de un trabajo de auditoría anterior, las revisiones y hallazgos, incluyendo cualquier actividad correctiva.
 2. El proceso de análisis de riesgos global de la empresa.
 3. La probabilidad de suceso de un riesgo particular.
 4. El impacto de un riesgo particular (en medida monetaria u otro valor) si ocurre.
- 2.3.2** Los profesionales deben garantizar la comprensión completa de las actividades en el alcance antes del análisis de riesgos. Deben solicitar comentarios y sugerencias de interesados y otras partes adecuadas. Es necesario determinar y examinar correctamente el impacto del posible riesgo en los trabajos de auditoría.
- 2.3.3** El objetivo del análisis de riesgos es la reducción del [riesgo de auditoría](#) a un nivel bajo aceptable, e identificar esas partes de una actividad que deben recibir más foco de auditoría. Esto necesita realizarse por un análisis adecuado de la materia de SI y controles relacionados, mientras que se planifica y realiza la auditoría de SI.
- 2.3.4** Cuando se planifica un procedimiento de auditoría y aseguramiento de SI específica, los profesionales deben reconocer el hecho que cuando menor es el nivel de la [materialidad](#), las expectativas de la auditoría serán más precisas y mayor el riesgo de auditoría.

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

- | | |
|--|---|
| 2.3 Análisis de Riesgos de Trabajos de Auditoría Individuales cont. | 2.3.5 Cuando se planifica un procedimiento de auditoría y aseguramiento de SI específico, los profesionales deben considerar los posibles actos ilegales que pueden requerir una modificación de la naturaleza, tiempos o extensión de los procedimientos existentes. Para más información, consulte el Estándar 1207 Irregularidades y actos ilegales y la Guía 2207. |
| | 2.3.6 Para tener seguridad adicional en los casos donde hay elevado riesgo de auditoría o un umbral de materialidad menor, los profesionales deben compensar por cualquier extensión al alcance o naturaleza de las pruebas de auditoría de SI o incrementar o extender las pruebas sustantivas . |
-

- | | |
|--------------------------------|---|
| 2.4 Riesgo de Auditoría | 2.4.1 El riesgo de auditoría se refiere al riesgo de alcanzar una conclusión incorrecta basada en los resultados de la auditoría. Los tres componentes del riesgo de auditoría son: <ul style="list-style-type: none">• Riesgo de Control.• Riesgo de Detección.• Riesgo Inherente. |
| | 2.4.2 Los profesionales deben considerar cada componente del riesgo para determinar el nivel de riesgo general. Esto incluye el riesgo de la materia, que incluye el riesgo inherente y el riesgo de control; juntos con el riesgo de detección se referencian como riesgo de auditoría. Puede encontrar más información de los diferentes componentes del riesgo de auditoría en las secciones 2.5 a 2.7. |
-

- | | |
|-----------------------------|--|
| 2.5 Riesgo Inherente | 2.5.1 El riesgo inherente es la susceptibilidad de errar un área de auditoría de forma que puede ser importante, individual o en combinación con otros errores, asumiendo que no hubo controles internos relacionados. Por ejemplo, el riesgo inherente asociado con sistemas operativos sin controles apropiados es generalmente alto, ya que los cambios, o incluso la divulgación, de datos o programas a través de los fallos de seguridad del sistema operativo podrían llevar a información de administración falsa o desventaja competitiva. Por contraste, el riesgo inherente asociado con la seguridad para un PC independiente sin controles es bajo generalmente, cuando un análisis adecuado demuestra que no se usa para fines de negocio críticos. |
| | 2.5.2 Los riesgos inherentes para la mayoría de las áreas de auditoría es alto ya que los efectos potenciales de errores generalmente abarca varios sistemas de negocio y muchos usuarios. |
-

- | | |
|------------------------------|--|
| 2.6 Riesgo de Control | 2.6.1 El riesgo de control es el riesgo que pueda suceder un error en un área de auditoría y podría ser material, individual o una combinación con otros errores, no será prevenido, detectado ni corregido oportunamente por el sistema de control interno. Por ejemplo, el riesgo de control asociado con |
|------------------------------|--|

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

2.6 Riesgo de Control cont.

revisiones manuales de logs de ordenador puede ser alto por el volumen de la información de log. El riesgo de control asociado con los procedimientos de validación de datos por ordenador generalmente es bajo porque los procesos se aplican coherentemente.

2.6.2 Los profesionales deberán evaluar el riesgo de control como alto a menos existan controles internos relevantes:

- Identificados.
- Evaluados como efectivos.
- Se prueba y demuestra que funcionan adecuadamente.

2.6.3 Los profesionales deben considerar tanto los controles de SI generalizados como los [controles de SI detallados](#):

- [Controles de SI generalizados](#) considerados un subconjunto de controles generales; son controles que se centran en la gerencia y monitorización del entorno de SI. Por lo tanto afectan a todas las actividades relacionadas con SI. El efecto de los controles de SI generalizados en el trabajo de los profesionales no se limita a la fiabilidad de los controles de aplicación en el sistema de proceso del negocio. También afectan a la fiabilidad de los controles de SI detallados sobre, por ejemplo, desarrollo de programas, implementación de sistemas, administración de seguridad y procedimientos de backup. Los controles de SI generalizados débiles, y por lo tanto la gerencia y monitorización débil del entorno de SI, debe alertar a los profesionales a la posibilidad de un alto riesgo que los controles diseñados a operar en el nivel detallado pueden ser inefectivos.
- Los controles de SI detallados se componen de los controles de aplicación más aquellos controles generales no incluidos en los generalizados. Siguiendo el marco de trabajo COBIT, son los controles sobre los sistemas y servicios de SI de adquisición, implementación, entrega y soporte.

2.6.4 Un riesgo que deben considerar los profesionales es la limitaciones y deficiencias en los controles de SI detallados que son inducidos por insuficiencias de los controles de SI generalistas.

2.7 Riesgo de Detección

2.7.1 El riesgo de detección es el riesgo de que los procedimientos sustantivos de los profesionales no detecten un error que podría ser material, individual o una combinación con otros errores. Por ejemplo, el riesgo de detección asociado con la identificación de brechas de seguridad en una aplicación generalmente es alto porque los logs para el periodo completo de la auditoría no están disponibles en el momento de la auditoría. El riesgo de detección asociado con la identificación de la falta de planes de recuperación de desastres generalmente es bajo, ya que se comprueba fácilmente.

2.7.2 Para determinar el nivel de pruebas sustantivas requeridas, los profesionales deben considerar:

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

2.7 Riesgo de Detección cont.

- Análisis del riesgo inherente.
- Conclusiones sobre el riesgo de control tras las pruebas de cumplimiento.

2.7.3 Cuando mayor sea la evaluación del riesgo inherente y de control, el profesional deberá obtener normalmente mas evidencia de auditoría de la realización de los procedimientos de auditoría sustantivos.

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 ISACA que están directamente soportados por esta guía.
- Las declaraciones estándar más relevantes para esta guía.

Nota: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Titulo del Estándar	Declaración Estándar Relevante
1201 Planificación de la asignación.	Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir: • 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.
1202 Evaluación de Riesgos en la Planificación de Auditoría.	La función de auditoría y aseguramiento de SI deberá utilizar un enfoque apropiado y el apoyo de metodología de análisis de riesgos para desarrollar el plan de auditoría de SI general y determinar las prioridades para la asignación efectiva de recursos de auditoría de SI. Los profesionales de auditoría y aseguramiento de SI deberán identificar y analizar los riesgos relevantes al área bajo revisión, en la planificación de trabajos individuales. Los profesionales de auditoría y aseguramiento deberán considerar el riesgo de la materia, riesgo de auditoría y exposiciones relacionadas con la empresa.

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

Título del Estándar	Declaración Estándar Relevante
1203 Desempeño y Supervisión.	Los profesionales de auditoría y aseguramiento de SI deberán conducir el trabajo de acuerdo al plan de auditoría de SI aprobado para cubrir los riesgos identificados y dentro del plan acordado.
1204 Materialidad.	Los profesionales de auditoría y aseguramiento de SI deberán considerar las debilidades o ausencias de controles potenciales mientras planifican un trabajo, y si tal debilidad o ausencia de control podría resultar en una deficiencia significativa o debilidad material. Los profesionales de auditoría y aseguramiento de SI deberán considerar la materialidad y su relación con el riesgo de auditoría mientras determinan la naturaleza, tiempos y extensión de los procedimientos de auditoría. Los profesionales de auditoría y aseguramiento de SI deberán considerar el efecto acumulativo de las deficiencias o debilidades de control menor y si la ausencia de controles se traduce en una deficiencia significativa o debilidad material. Los profesionales de auditoría y aseguramiento revelaran lo siguiente en el informe de auditoría: • Ausencia de controles o controles inefectivos. • Importancia de la deficiencia de los controles. • Probabilidad de estas debilidades resulten en una deficiencia significativa o debilidad material.
1207 Irregularidades y actos ilegales.	Los profesionales de auditoría y aseguramiento de SI deberán considerar el riesgo de actos irregulares e ilegales durante el 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: Habilidad 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

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

Procesos de COBIT 5	Propósito de los Procesos
	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.
EDM03 Asegurar la optimización del riesgo.	Asegurar que el riesgo empresarial relacionado con TI no excede el riesgo aceptado y la tolerancia de riesgo, el impacto de riesgo de TI al valor de la empresa está identificado y gestionado, y la posibilidad de fallos de cumplimiento esta minimizada.
APO12 Gestionar el riesgo.	Integrar la gerencia de riesgos empresariales relacionados con TI con el ERM en general, y el balance de costes y beneficios de la gerencia de riesgos empresariales relacionados con TI.
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 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
Análisis de Riesgos	Un proceso utilizado para identificar y evaluar riesgos y sus efectos potenciales. Los análisis de riesgos se utilizan para identificar aquellos elementos o áreas que presentan el riesgo, vulnerabilidad o exposición más altos para la empresa para incluirlos en el plan de auditoría anual de SI. Los análisis de riesgos se utilizan también para gestionar la ejecución de los proyectos y el riesgo en beneficio del proyecto.

Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

Término	Definición
Carta de Auditoría	Un documento aprobado por los encargados de 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.
Controles de SI Detallados	Controles sobre las adquisición, implementación, entrega y soporte de sistemas y servicios de SI formado por los controles de aplicación más aquellos controles generales no incluidos en los controles generales.
Controles de SI Generalizados	Controles generales diseñados para gestionar y monitorear el entorno de SI y que, por tanto, afecta a todas las actividades relacionadas con 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.
Prueba Sustantiva	La obtención de evidencia de auditoría sobre la integridad, exactitud o existencia de actividades o transacciones durante el periodo de la auditoría.
Riesgo de Auditoría	El riesgo de llegar a una conclusión incorrecta basada en los resultados de la auditoría. Los tres componentes de riesgo de auditoría son: • Riesgo de control. • Riesgo de detección. • Riesgo inherente.
Riesgo de Control	El riesgo que exista un error material que no se evite o detectado de forma oportuna por el sistema de control interno. Ver riesgo inherente.
Riesgo de Detección	El riesgo que los procedimientos sustantivos del profesional de auditoría y aseguramiento de SI no detectara un error que podría ser material, individual o en combinación con otros errores. Ver riesgo de auditoría.
Riesgo Inherente	El nivel de riesgo o exposición sin tener en cuenta las acciones que la gerencia ha tomado o ha podido tomar (ejemplo, implementar controles). Ver riesgo de control.

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.



Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

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®) 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 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 2203 Rendimiento y Supervisión

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 proporciona ayuda a los profesionales de auditoría y aseguramiento de SI en la realización del trabajo de auditoría y supervisor los miembros de los equipos de auditoría de SI. Cubre:
 - Realizar un trabajo de auditoría.
 - Roles y responsabilidades, conocimiento requerido y habilidades para realizar trabajos de auditoría.
 - Aspectos claves de la supervisión
 - Obtener evidencias
 - Documentar el trabajo realizado
 - Formular hallazgos y conclusiones
 - 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 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
 - 1.2.5** Estándar 1205 Evidencia
 - 1.2.6** Estándar 1401 Reportes
-

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:

- 1.1 Realizar el trabajo
 - 1.2 Roles y responsabilidades, conocimiento y habilidades
 - 1.3 Supervisión
 - 1.4 Evidencia
 - 1.5 Documentación
 - 1.6 Hallazgos y conclusiones.
-

2.1 Realizar el Trabajo

- 2.1.1** Los profesionales planificarán y realizarán cada trabajo de auditoría de acuerdo con el plan de auditoría de SI aprobado. Establecerán un plan de proyecto del trabajo de auditoría, como se detalla en el Estándar 1201 Planificación de la asignación, permitiendo a los profesionales comprender todos los elementos en el alcance, las habilidades y conocimientos requeridos para realizar el trabajo de auditoría dentro de la planificación acordada, mientras se cubren todos los riesgos identificados.
- 2.1.2** Las principales tareas en la realización de un trabajo de auditoría incluyen:
- **Planificación y análisis de riesgos**—Los profesionales deben realizar estas actividades alineadas con el estándar 1201 Planificación de la asignación y 1202 Planificación del Análisis de Riesgos.
 - **Identificar los controles**—Basado en el alcance, objetivos de auditoría y áreas principales de los riesgos identificados en el plan de auditoría de SI, los profesionales deben identificar los controles en el alcance del trabajo de auditoría.
 - **Evaluar controles y obtener evidencias**—Los profesionales deben evaluar los controles en el alcance obteniendo y analizando la información y evidencias sobre el [diseño efectivo](#) and [desempeño efectivo](#) de los controles, como se describe en el Estándar 1205 Evidencia.
 - **Documentar el trabajo realizado y los hallazgos identificados**—Los profesionales deben documentar el trabajo realizado, registrar la información y evidencias obtenidas y documentar cualquier hallazgo identificado.
 - **Confirmar hallazgos y las siguientes acciones correctivas**—Los profesionales deben confirmar sus hallazgos con el auditado. El auditado debe realizar acciones correctivas sobre los hallazgos antes del final del trabajo de auditoría, los profesionales deben incluir las acciones tomadas en la documentación (y conclusión), pero también deben siempre mencionar los hallazgos originales.
 - **Describir las conclusiones y el informe**—Los profesionales deben describir las conclusiones e informar sobre el impacto de los hallazgos para conseguir los objetivos de la auditoría, como se detalla en el Estándar 1401 Informe. Enfocarse solo sobre los controles hallados, sin evaluar el impacto sobre los objetivos de la auditoría, es insuficiente.
-

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

2.2 Roles y Responsabilidades, Conocimiento y Habilidades

- 2.2.1** Los profesionales a cargo del trabajo de auditoría deben definir y gestionar los roles y responsabilidades de los miembros del equipo de auditoría de SI durante el trabajo, abordando como mínimo:
- Diseñar la metodología y enfoque
 - Creando de programas de trabajo de auditoría
 - Definir los roles de ejecución y revisión
 - Tratar las cuestiones, preocupaciones y problemas que surjan
 - Documentar y aclarar las conclusiones
 - Escribir el informe
- 2.2.2** En base a las necesidades del trabajo, los profesionales a cargo deben considerar las competencias requeridas para el trabajo de auditoría específico. Deben establecer un equipo del trabajo que tenga habilidades, conocimiento y experiencia combinados para completar el trabajo de auditoría con éxito. Los profesionales deben asegurarse de asignar estos roles y responsabilidades a los miembros del equipo de auditoría de SI que mejor se ajusten a sus competencias.
- 2.2.3** Los profesionales solo deben aceptar roles, responsabilidades y tareas asociadas que estén dentro de sus conocimientos y habilidades. Cuestiones de tiempo y dinero podrían prohibir a los profesionales adquirir todo el conocimiento y habilidades necesarias antes de comenzar el trabajo de auditoría; Por lo tanto, se permite a los profesionales aceptar roles, responsabilidades y tareas asociadas si tienen expectativas razonables de que se tomaran las medidas adecuadas durante el trabajo de auditoría para asegurar la terminación exitosa. Las siguientes medidas podrían permitir una expectativa razonable:
- **Aprender en el trabajo**—En ciertas circunstancias, será posible que los profesionales adquieran las habilidades y conocimiento necesario durante el trabajo de auditoría.
 - **Supervisión**—Los profesionales a cargo podrían organizar una supervisión adecuada de los miembros del equipo de auditoría de SI, permitiéndoles conseguir la tarea bajo supervisión exitosamente.
 - **Recursos externos**—Los profesionales a cargo podrían considerar contratar expertos externos para aquellas áreas del trabajo de auditoría que carecen de conocimiento y habilidades internas adecuadas. Los profesionales a cargo deben considerar promocionar el desarrollo de los miembros del equipo de auditoría de SI interna teniéndoles trabajando junto a los expertos externos para asegurar una transferencia al equipo de conocimiento y habilidades.
- 2.2.4** Se detalla la orientación sobre adquisición, mantenimiento y monitorización de las competencias requeridas en el Estándar 1006 Competencia
-

2.3 Supervisión

- 2.3.1** Cada tarea ejecutada durante un trabajo de auditoría por los miembros del equipo de auditoría debe ser supervisada por los profesionales que tienen responsabilidades de supervisión sobre ellos, para asegurar que los objetivos de auditoría y estándares de auditoría profesional aplicables se cumplen. El alcance de la supervisión requerida dependerá altamente de sus habilidades,

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

2.3 Supervisión cont.

conocimiento y experiencia de los profesionales ejecutando la tarea bajo revisión y sobre la complejidad del trabajo de auditoría.

2.3.2 La supervisión es un proceso que está presente en todo paso del trabajo de auditoría. Esto incluye:

- Asegurar que los miembros del equipo de auditoría tienen las habilidades, conocimiento y experiencia combinados para completar el trabajo de auditoría con éxito.
- Asegurar que se ha establecido y aprobado un plan de proyecto del trabajo de auditoría y un programa de trabajo de auditoría.
- Revisar los papeles de trabajo de la auditoría
- Asegurar que la comunicación del trabajo de auditoría hacia los auditados y otros interesados relevantes es exacta, clara, concisa, objetiva, constructiva y oportuna.
- Asegurar que el programa de trabajo de auditoría aprobado se completa al final del trabajo de auditoría, a menos que los cambios estén justificados y aprobados antemano, y los objetivos del trabajo de auditoría se cumplen.
- Proporcionar oportunidades a los miembros del equipo de auditoría de SI para desarrollar sus habilidades y conocimiento.

2.3.3 Se requiere la revisión de los papeles de trabajo para asegurar que todos los procedimientos de auditoría necesarios se llevan a cabo, las pruebas reunidas son suficientes y adecuadas y las conclusiones apoyan adecuadamente los objetivos y conclusión u opinión del trabajo. Considerando el objetivo de la revisión, se debe realizar por los miembros del equipo de auditoría de SI teniendo responsabilidades de supervisión sobre los profesionales que crearon los papeles de trabajo de la auditoría.

2.3.4 Durante el proceso de revisión, los revisores deben registrar las cuestiones que puedan surgir. Cuando los profesionales proporcionan una respuesta o solución a las cuestiones planteadas, deben tener cuidado de asegurar que se tiene la evidencia suficiente y adecuada para demostrar que las cuestiones fueron planteadas, tratadas y contestadas.

2.3.5 Se debe documentar y retener las evidencias adecuadas de revisión. Opciones para documentar evidencia de realización de entrevistas consiste, aunque no se limita a:

- Firmar y fechar cada papel de trabajo de la auditoría tras su revisión.
- Completar una lista de comprobación de la revisión del trabajo de auditoría.
- Preparar un documento firmado que proporcione referencia a los papeles de trabajo de la auditoría bajo revisión y detallando la naturaleza, tiempos, alcance y resultado de la revisión.

Todas estas opciones son validas tanto electrónicamente como en papel.

2.3.6 La supervisión permite el desarrollo y supervisión de los profesionales. Los revisores tienen una vista privilegiada del trabajo realizado por otros miembros del equipo de auditoría de SI, lo que permite una evaluación detallada y adecuada de su trabajo. Los revisores deben señalar las áreas de desarrollo y asesorar las formas para mejorar habilidades y conocimientos.

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

2.4 Evidencia

- 2.4.1** Los profesionales deben obtener evidencia que es suficiente y adecuada para formar una opinión o soportar las conclusiones y lograr los objetivos de auditoría. Determinar si la evidencia es suficiente y adecuada debe basarse en la importancia del objetivo de auditoría y el esfuerzo que implica obtener las evidencias.
- 2.4.2** Los profesionales deben obtener evidencia adicional si, en su juicio, la evidencia obtenida no cumple con los criterios de ser suficiente y apropiada para formar una opinión o apoyar las conclusiones y lograr los objetivos de auditoría.
- 2.4.3** Los profesionales deben seleccionar el procedimiento más apropiado para reunir pruebas, dependiendo de la materia a auditar.
- 2.4.4** Los profesionales deben considerar la fuente y naturaleza de la evidencia obtenida para evaluar su fiabilidad y la necesidad de más verificaciones.
- 2.4.5** Se debe realizar el análisis e interpretación adecuado por los profesionales para apoyar los hallazgos de auditoría y formar conclusiones. La evidencia e información recibida debe compararse con expectativas identificadas o desarrolladas por profesionales. Los profesionales deben tener en cuenta:
- Diferencias inesperadas
 - La ausencia de diferencias cuando las esperaban
 - Errores potenciales
 - Actos fraudulentos o ilegales
 - Incumplimiento con leyes o regulaciones
 - Actividades inusuales o no recurrentes
- 2.4.6** Deben identificar las desviaciones de las expectativas, los profesionales deben preguntar a la gerencia sobre las razones de la diferencia. Las explicaciones de gerencia deben ser adecuadas, de acuerdo al juicio profesional, los profesionales deben modificar sus expectativas y volver a analizar la evidencia e información.
- 2.4.7** Desviaciones significativas no explicadas adecuadamente por el auditor deben resultar en hallazgos de auditoría y ser comunicados a la gerencia ejecutiva o a los encargados del Gobierno. Dependiendo de las circunstancias, los profesionales podrían recomendar las acciones apropiadas que deben tomarse.
- 2.4.8** Orientación detallada de las diferentes clases de evidencia, procedimientos para recolectar evidencias, fuentes pertinentes, formas de evaluar las pruebas, etc., se puede encontrar en la guía Estándar 1205 Evidencia
-

2.5 Documentación

- 2.5.1** Los profesionales deben preparar la documentación suficiente, apropiada y relevante puntualmente que proporciona una base para la conclusión y contiene evidencia de la revisión realizada. Suficiente, apropiada y relevante documentación debe permitir a una persona prudente e informada, sin conexión previa con el trabajo de auditoría, volver a realizar las tareas realizadas durante el trabajo de auditoría y alcanzar la misma conclusión. La documentación debe incluir:
- Objetivos y alcance del trabajo de auditoría
 - Plan del proyecto del trabajo de auditoría
 - Programa de trabajo de auditoría

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

2.5

Documentación cont.

- Pasos de auditoría realizados
- Evidencia obtenida
- Conclusiones y recomendaciones

- 2.5.2** La documentación ayuda en la planificación, ejecución y revisión de los trabajos de auditoría ya que:
- Identifica quien de los miembros del equipo de auditoría de SI realice cada tarea de auditoría y su role en la preparación y revisión de la documentación.
 - Registra las pruebas requeridas
 - Apoya la exactitud, integridad y validez del trabajo realizado
 - Proporciona soporte para las conclusiones alcanzadas
 - Facilita el proceso de revisión
 - Documenta si se alcanzaron los objetivos del trabajo
 - Proporciona la base para los programas de mejora de la calidad
- 2.5.3** Por lo general, antes de empezar el trabajo los profesionales deben establecer un programa preliminar para la revisión. Este programa de auditoría debe estar documentado de forma que permita a los profesionales registrar la finalización de los trabajos de auditoría e identificar el trabajo que queda por hacer. Conforme progresa el trabajo, los profesionales evaluarán la adecuación del programa de auditoría basándose en la información obtenida durante el trabajo de auditoría. Cuando los profesionales determinen que los procedimientos planeados no son suficientes, deben modificar el programa de auditoría en consecuencia.
- 2.5.4** Se deben documentar las actividades de desempeño y supervisión en los papeles de trabajo de auditoría. El diseño y contenido de los papeles de trabajo de auditoría varía dependiendo de las circunstancias del trabajo de auditoría particular. La gerencia de auditoría y aseguramiento de SI, sin embargo, debe detallar un número limitado de plantillas estándar como papel de trabajo para los diferentes tipos de trabajos de auditoría. Los papeles de trabajo estándar mejoran la eficiencia del trabajo de auditoría y facilitan la supervisión. La gerencia de auditoría y aseguramiento de SI debe también determinar los portadores de los medios a emplear y los procedimientos de almacenaje y retención para los papeles de trabajo.
- 2.5.5** Los profesionales deben asegurar que la documentación del trabajo realizado esta completa de manera oportuna. Toda la información y evidencia requerida para formar una conclusión u opinión debe ser obtenida antes de la fecha de emisión del informe de auditoría. Los papeles de trabajo de auditoría deben incluir la fecha en que se prepararon y revisaron.
- 2.5.6** Los papeles de trabajo de la auditoría son propiedad de la empresa. La gerencia de auditoría y aseguramiento de SI controla los papeles de trabajo y proporciona acceso al personal autorizado. Las solicitudes de acceso a los papeles de trabajo de la auditoría por los auditores externos deben ser aprobadas por la gerencia ejecutiva y los encargados del Gobierno. Las peticiones de acceso por externos, distintos de los auditores externos, debe ser aprobada por la gerencia ejecutiva y los encargados del Gobierno y asesorados por un abogado.
-

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

2.6 Hallazgos y Conclusiones

- 2.6.1** Los profesionales deben analizar la evidencia e información recogida, como se describe en la sección 2.4.5. Las desviaciones significativas de las expectativas deberían dar lugar a conclusiones. Los profesionales deben confirmar estos hallazgos con el auditado, así como el impacto de estos hallazgos sobre otros aspectos del [entorno de control](#).
- 2.6.2** Los profesionales pueden proponer acciones correctivas a realizar, pero nunca las ejecutaran. El auditado debe realizar las acciones correctivas que remedian el hallazgo original, antes de finalizar el trabajo de auditoría, los profesionales deben incluir las acciones correctivas tomadas en la documentación.
- 2.6.3** Los profesionales deben concluir sobre los hallazgos identificados y evaluar su impacto sobre los objetivos de auditoría. Las conclusiones deben realizarse sobre los hallazgos originales. Si se han tomado acciones correctivas, se puede formular un anexo a la conclusión explicando la acción correctiva y el impacto de la acción correctiva sobre la conclusión original.
- 2.6.4** Toda conclusión formulada y tanto si los objetivos de auditoría han sido alcanzados como si no, se debe documentar en el informe de trabajo de auditoría. Se pueden encontrar directrices detalladas sobre la documentación en el Estándar 1401 Informe y en la Guía 2401 Informe.
-

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 ISACA que están directamente soportados por esta guía.
- Las declaraciones estándar más relevantes para esta guía.

Nota: Solo 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.

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

Título del Estándar	Declaración Estándar Relevante
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.
1201 Planificación de la Asignación	Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir: • 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. 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: • La naturaleza, objetivos, línea de tiempo y recursos requeridos del trabajo • Tiempos y grado de los procedimientos de auditoría para completar el trabajo
1203 Desempeño y Supervisión	Los profesionales de auditoría y aseguramiento de SI deberán conducir el trabajo de acuerdo al plan de auditoría de SI aprobado para cubrir los riesgos identificados y dentro del plan acordado. 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. 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. Los profesionales de auditoría y aseguramiento de SI deberán obtener evidencias suficientes, confiables, relevantes y a tiempo para conseguir los objetivos de auditoría. Los hallazgos y conclusiones de auditoría deben

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

Título del Estándar	Declaración Estándar Relevante
	estar soportados por análisis e interpretación apropiados de estas evidencias. Los profesionales de auditoría y aseguramiento deberán documentar el proceso de auditoría, describiendo el trabajo de auditoría y la evidencia de auditoría que soporta los hallazgos y conclusiones. Los profesionales de auditoría y aseguramiento de SI deberán identificar y concluir sobre los hallazgos.
1205 Evidencia de Auditoría	Los profesionales de auditoría y aseguramiento deberán obtener evidencia suficiente y adecuada para llegar a conclusiones razonables sobre las que 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..
1401 Reportes	Los profesionales de auditoría y aseguramiento de SI deberán presentar un informe para comunicar los resultados una vez finalizado el trabajo, incluyendo: • Identificación de la empresa, destinatarios y cualquier restricción al contenido y circulación. • El alcance, objetivos de trabajo, periodo de cobertura y naturaleza, tiempos y alcance de los trabajos realizados • Los hallazgos, conclusiones y recomendaciones • Cualquier cualificación o limitación al alcance que el profesional de auditoría y aseguramiento de SI tiene respecto al trabajo • Firma, fecha y distribución de acuerdo a los términos de la Estatuto de Auditoría o carta de compromiso Los profesionales de auditoría y aseguramiento de SI velaran por que los hallazgos del informe de auditoría estén soportados por evidencias de auditoría suficientes y adecuadas.

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*.

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

Procesos de COBIT 5	Propósito de los Procesos
APO07 Administración de recursos humanos.	Optimizar las capacidades de los recursos humanos para cumplir los objetivos empresariales.
APO08 Administración de relaciones.	Crear mejores resultados, aumentar la confidencialidad, confianza en TI y uso efectivo de los recursos.
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

Término	Definición
Diseño Efectivo	Si se operan los controles de la compañía según lo prescrito por las personas con la autoridad y competencia necesaria para realizar el control efectivo, satisfacer los objetivos de control de la compañía y poder prevenir efectivamente o detectar errores o fraudes que pueden dar lugar a errores materiales en las declaraciones financieras, se considera que están diseñados efectivamente. Fuente: PCAOB, Estándar de Auditoría No. 5, 2007
Entorno de control	La actitud y las acciones de la junta directiva y la administración respecto de la importancia del control dentro de la organización. El entorno del control proporciona disciplina y estructura para conseguir los objetivos primarios del sistema de control interno. El entorno del control incluye los siguientes elementos: • Integridad y valores éticos • Filosofía de gerencia y estilo operativo • Estructura organizacional • Asignación de autoridad y responsabilidad • Políticas y prácticas de recursos humanos • Competencia del personal Fuente: Estándares Internacionales para la Práctica Profesional de Auditoría Interna, 2010

Guía de Auditoría y Aseguramiento de SI 2203 Rendimiento y Supervisión

Término	Definición
Desempeño efectivo	Si un control es operado como está diseñado y la persona que realiza el control posee la autoridad y competencia necesaria para realizar el control de forma efectiva, se considera que el control está funcionando de forma efectiva. Fuente: PCAOB, Estándar de Auditoría No. 5, 2007

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.



Guía de Auditoría y Aseguramiento de SI 2204 Materialidad

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®) 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 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 2204 Materialidad

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 definir claramente el concepto de 'materialidad' para los profesionales de auditoría y aseguramiento de SI y hacer una clara distinción con el concepto de materialidad utilizado por los profesionales de auditoría y aseguramiento financiera.
 - 1.1.2** La guía ayuda al profesional de auditoría y aseguramiento de SI a evaluar la materialidad del sujeto y considerar materialidad en relación con los controles y cuestiones reportables.
 - 1.1.3** 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 1201 Planificación de la asignación.
 - 1.2.2** Estándar 1202 Evaluación de riesgo en planificación.
 - 1.2.3** Estándar 1204 Materialidad.
 - 1.2.4** Estándar 1207 Irregularidades y actos ilegales.
-

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 2204 Materialidad

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:

- 1.1 Trabajos de auditoría de SI vs. financieros.
 - 1.2 Evaluación de la materialidad del sujeto.
 - 1.3 Materialidad y controles.
 - 1.4 Materialidad y cuestiones reportables.
-

2.1 Trabajos de Auditoría de SI vs. Financieros

2.1.1 Los profesionales de SI requieren un criterio diferente para medir la [materialidad](#), en comparación a sus colegas trabajando en auditoría financiera. Los profesionales financieros normalmente miden la materialidad en términos monetarios, porque lo que ellos auditan se mide y reporta en términos monetarios. Los profesionales de SI normalmente realizan auditorías de elementos no financieros, por ejemplo, controles de desarrollo de programas, controles de cambio de programas, controles de acceso físico, controles de acceso lógico y controles de operación del ordenador sobre una variedad de sistemas. Por tanto, los profesionales de SI pueden necesitar orientación sobre como la materialidad debe ser evaluada para planificar sus trabajos de auditoría de forma efectiva, como enfocar sus esfuerzos en las áreas de mayor riesgo y como evaluar la gravedad de los errores o debilidades encontrados.

2.2 Evaluación de la Materialidad del Sujeto

2.2.1 La evaluación de lo que es material es una materia de juicio profesional. Incluye la consideración de los efectos y/o efectos potenciales sobre la capacidad de la empresa para cumplir sus objetivos de negocio en caso de errores, omisiones, irregularidades y actos ilegales que pueden surgir como resultado de una debilidad de control en el área auditada. Cuando los objetivos de auditoría de SI se refieren a sistemas u operaciones que procesan transacciones financieras, la medida adoptada por el profesional de la materialidad debe ser considerada mientras se realiza la auditoría de SI.

2.2.2 Para evaluar la materialidad, los profesionales deben establecer una clasificación de los activos de la información en términos de:

- Confidencialidad, disponibilidad e integridad.
- Reglas de control de acceso sobre la administración de privilegios.
- Grado de criticidad y riesgo al negocio.
- Cumplimiento con leyes y reglamentos.

La evaluación debe incluir la consideración de:

- La naturaleza de los datos y la información procesada y almacenada.
- Hardware de SI.
- Arquitectura de SI y software (aplicaciones y sistema operativo).
- Infraestructura de red de SI.
- Operaciones de SI.
- Entornos de producción, desarrollo y pruebas.
- Leyes y reglamentos aplicables.

Guía de Auditoría y Aseguramiento de SI 2204 Materialidad

2.2 Evaluación de la Materialidad del Sujeto cont.

2.2.3 Mas ejemplos detallados de factores que podrían considerarse para evaluar la materialidad son:

- Criticidad de los procesos de negocio soportados por los sistemas u operación.
- Criticidad de las bases de datos de información soportada por los sistemas u operación.
- Número y tipo de aplicaciones desarrolladas.
- Número de usuarios que utilizan los sistemas de información.
- Numero de gerentes y directores que trabajan con los sistemas de información clasificados por privilegios.
- Criticidad de las redes de comunicaciones soportadas por el sistema o operación.
- Coste de los sistemas o operación (hardware, software, personal, servicios de terceros, gastos generales o combinación de estos).
- Coste potencial de errores (posibilidad en términos de pérdida de ventas, reclamaciones de aseguramiento, costes de desarrollo irre recuperables, coste de publicidad requerida para advertencias, costes de rectificación, costes de salud y seguridad, costes de producción altos innecesariamente, desperdicio alto, etc.).
- Coste de pérdida de información crítica y vital en términos monetarios y tiempo para reproducir, pero también pérdida de reputación e imagen.
- Numero de accesos/transacciones/consultas procesadas por periodo
- Naturaleza, tiempos y alcance de los informes preparados y ficheros mantenidos.
- Naturaleza y cantidades de materiales manejados (ejemplo, donde los movimientos de inventario se registran sin valores).
- Requerimientos del acuerdo de nivel de servicio y coste de posibles sanciones.
- Sanciones por fallo en el cumplimiento de requerimientos legales, reglamentarios y contractuales.
- Sanciones por fallo en el cumplimiento de requerimientos de salud, seguridad y de entorno.
- Definiciones específicas o consideraciones sobre, la materialidad proporcionada por autoridades legislativas o regulatorias.
- Transferir operaciones de TI a terceras partes, que causa un cambio significativo en el cumplimiento de requerimientos regulatorios, ejemplo, privacidad y protección de datos, reglas de control del comercio, requerimientos financieros.

2.2.4 La indicación de áreas de mayor importancia debe usarse para reducir el [riesgo de auditoría](#) apropiadamente por extender las pruebas de control (reduce el riesgo de control) y/o extender los procedimientos de pruebas sustantivas (reduce el riesgo de detección).

2.2.5 Los profesionales deben re evaluar la materialidad establecida cuando lleguen a su conocimiento cambios en circunstancias particulares o información adicional que pueda influenciar la materialidad de los sistemas u operaciones. La situación más común en que esto puede suceder incluye:

1. La materialidad se estableció inicialmente sobre estimaciones o información preliminar que se diferencia significativamente de la situación

Guía de Auditoría y Aseguramiento de SI 2204 Materialidad

2.2 Evaluación de la Materialidad del Sujeto cont.

actual.

2. Los eventos o cambios en las condiciones desde que se estableció la materialidad tienen un impacto significativo sobre la capacidad de la empresa para cumplir con los objetivos de negocio.

2.3 Materialidad y Controles

- 2.3.1** Para cumplir con los objetivos de auditoría, los profesionales deben identificar los objetivos de control relevantes y, en base al nivel de tolerancia de riesgo, determinar que debe examinarse. Con respecto a objetivos de control específicos, un control o grupo de controles es material si la ausencia de control resulta en fallo para proporcionar aseguramiento razonable que el objetivo de control se cumpla.
- 2.3.2** Los profesionales deben considerar la materialidad cuando determinan la naturaleza, tiempos y extensión de los procedimientos de auditoría a aplicar para probar un control o grupo de controles. Los controles materiales deben probarse más a fondo, frecuentemente y de forma extensiva comparados a los controles no materiales para reducir el riesgo de auditoría.
- 2.3.3** Mientras evalúan la materialidad, los profesionales deben considerar:
- El nivel de error aceptable para gerencia, los profesionales, organismos regulatorios apropiados y otros interesados.
 - Posibilidad de que el efecto acumulativo de múltiples pequeños errores o debilidades se haga material.
- 2.3.4** Antes del inicio del trabajo de campo de la auditoría, los profesionales deben considerar obtener la aprobación de los interesados apropiados que reconocen que cualquier [debilidad material](#) existente que conocen ha sido resuelta.
- 2.3.5** Cuando los profesionales descubren deficiencias de control, deben evaluar el efecto sobre la opinión o conclusión general de auditoría. Cuando evalúan el efecto, los profesionales deben tener en cuenta diferentes aspectos de la aparición de las deficiencias de control, incluyendo:
- Tamaño.
 - Naturaleza.
 - Circunstancias particulares.
- 2.3.6** Al probar controles materiales, los profesionales deben evaluar el efecto de controles compensatorios para mitigar el riesgo asociado con una deficiencia de control descubierta. La deficiencia de control debe ser clasificada como:
- Debilidad material, cuando el control compensatorio no es efectivo.
 - [Deficiencia significativa](#), cuando el control compensatorio es efectivo parcialmente.
 - Una deficiencia intrascendente, cuando los controles compensatorios reducen el riesgo a un nivel aceptable.
- 2.3.7** Múltiples errores o fallos de control pueden causar un efecto acumulativo, que deben considerar los profesionales en la determinación de la materialidad general de las deficiencias de control.
- 2.3.8** Los profesionales deben determinar cuándo cualquier deficiencia de control general de TI es material. La importancia de tal deficiencia de controles generales de TI debe ser evaluada en relación a sus efectos sobre los controles

Guía de Auditoría y Aseguramiento de SI 2204 Materialidad

2.3 Materialidad y Controles cont.

de aplicación, por ejemplo, cuando los controles de la aplicación asociados son inefectivos. Si la deficiencia de la aplicación está causada por el control general de TI, entonces es material. Por ejemplo, si una aplicación basada en el cálculo de impuestos es materialmente incorrecta y fue causada por controles de cambio pobres a las tablas de impuestos, entonces el control basado en la aplicación (cálculo) y el control general (cambios) son materialmente débiles.

- 2.3.9** Los profesionales deben evaluar la deficiencia de un control general de TI en relación a su efecto sobre los controles de aplicaciones y cuando se agrega con otras deficiencias de control. Por ejemplo, la gerencia decide no corregir una deficiencia de control general de TI y su reflejo asociado sobre el control de entorno podría convertirse en material cuando se agrega a otras deficiencias de control que afectan el entorno de control.
 - 2.3.10** Los profesionales deben también tener en cuenta que el fallo para remediar una deficiencia podría convertirse en material, por ejemplo, tras que la gerencia y los encargados del Gobierno han sido alertados de la deficiencia.
 - 2.3.11** Las deficiencias de control son siempre materiales en áreas donde se han anulado como resultado de fraude o actos ilegales.
-

2.4 Materialidad y Cuestiones Reportables

- 2.4.1** Al determinar los hallazgos, conclusiones y recomendaciones a reportar, los profesionales deben considerar tanto la materialidad de cualquier error encontrado como la materialidad de los errores que puedan surgir como resultado de las deficiencias de control.
 - 2.4.2** Cuando el trabajo de auditoría se usa por la gerencia para obtener una declaración de aseguramiento de los controles de SI, una opinión incondicional sobre la adecuación de los controles debe entender que los controles establecidos son de conformidad con las prácticas de control de aceptación general para cumplir los objetivos de control, carente de cualquier debilidad de control material.
 - 2.4.3** Se debe considerar material una debilidad de control y, por tanto, reportable, si la ausencia del control resulta en fallo para proporcionar aseguramiento razonable que el objetivo de control se cumplirá. El trabajo de auditoría identifica debilidades de control material, los profesionales deben considerar emitir una opinión calificada o adversa sobre el objetivo de auditoría.
 - 2.4.4** Dependiendo de los objetivos del trabajo de auditoría, los profesionales deben considerar informar a la gerencia de las debilidades que no son materiales, particularmente cuando el coste de reforzar los controles es bajo. Además, los profesionales pueden aconsejar sobre resoluciones de las debilidades identificadas.
-

Guía de Auditoría y Aseguramiento de SI 2204 Materialidad

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 ISACA que están directamente soportados por esta guía.
 - Las declaraciones estándar más relevantes para esta guía.

Nota: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Titulo del Estándar	Declaración Estándar Relevante
1201 Planificación de la Asignación	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: • La naturaleza, objetivos, línea de tiempo y recursos requeridos del trabajo. • Tiempos y grado de los procedimientos de auditoría para completar el trabajo.
1202 Evaluación de Riesgos en la Planificación de Auditoría	Los profesionales de auditoría y aseguramiento de SI deberán identificar y analizar los riesgos relevantes al área bajo revisión, en la planificación de trabajos individuales. Los profesionales de auditoría y aseguramiento deberán considerar el riesgo de la materia, riesgo de auditoría y exposiciones relacionadas con la empresa.
1204 Materialidad	Los profesionales de auditoría y aseguramiento de SI deberán considerar las debilidades o ausencias de controles potenciales mientras planifican un trabajo, y si tal debilidad o ausencia de control podría resultar en una deficiencia significativa o debilidad material. Los profesionales de auditoría y aseguramiento de SI deberán considerar la materialidad y su relación con el riesgo de auditoría mientras determinan la naturaleza, tiempos y extensión de los procedimientos de auditoría. Los profesionales de auditoría y aseguramiento de SI deberán considerar el efecto acumulativo de las deficiencias o debilidades de control menor y si la ausencia de controles se traduce en una deficiencia significativa o debilidad material. Los profesionales de auditoría y aseguramiento revelaran lo

Guía de Auditoría y Aseguramiento de SI 2204 Materialidad

Título del Estándar	Declaración Estándar Relevante
	siguiente en el informe de auditoría: • Ausencia de controles o controles inefectivos. • Importancia de la deficiencia de los controles. • Probabilidad de estas debilidades resulten en una deficiencia significativa o debilidad material.
1207 Irregularidades y actos ilegales	Los profesionales de auditoría y aseguramiento de SI deberán considerar el riesgo de actos irregulares e ilegales durante el trabajo. Los profesionales de auditoría y aseguramiento de SI deberán mantener una actitud de escepticismo profesional durante el trabajo. Los profesionales de auditoría y aseguramiento de SI deberán documentar y comunicar cualquier irregularidad material o acto ilegal a las partes adecuadas de forma oportuna.

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
EDM03 Asegurar la optimización del riesgo.	Asegurar que el riesgo empresarial relacionado con TI no excede el riesgo aceptado y la tolerancia de riesgo, el impacto de riesgo de TI al valor de la empresa está identificado y gestionado, y la posibilidad de fallos de cumplimiento esta minimizada.
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.

Guía de Auditoría y Aseguramiento de SI 2204 Materialidad

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
Debilidad material	Una deficiencia o combinación de deficiencias en controles internos, como que hay una posibilidad razonable de un error material, no sea prevenido o detectado de forma oportuna. La debilidad en el control se considera material si la ausencia de control resulta en fallo para proporcionar seguridad razonable que el objetivo de control se alcanzara. Una debilidad clasificada como material implica: • Los controles no están en su lugar y/o no se usan y/o son inadecuados. • Se garantiza la escalada. Existe una relación inversa entre materialidad y nivel de riesgo de auditoría aceptable para el profesional de auditoría o aseguramiento de SI, ejemplo, a mayor nivel de materialidad, menor la aceptabilidad del riesgo de auditoría y viceversa.
Deficiencia significativa	Una deficiencia o combinación de deficiencias, en control internos, que es menos severa que una debilidad material, pero lo suficiente importante para merecer atención de los responsables de supervisión. Nota: Una debilidad material es una deficiencia significativa o combinación de deficiencias significativas que resulta en una probabilidad más que remota de un evento indeseable no previsto o detectado.
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.
Riesgo de Auditoría	El riesgo de llegar a una conclusión incorrecta basada en los resultados de la auditoría. Los tres componentes de riesgo de auditoría son: • Riesgo de control. • Riesgo de detección. • Riesgo inherente.

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.

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

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®) 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 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 2205 Evidencia

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 proporcionar ayuda a los profesionales de auditoría y aseguramiento de SI a obtener evidencia suficiente y apropiada, evaluar la evidencia recibida y preparar la documentación de auditoría apropiada.
 - 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 1203 Desempeño y supervisión
 - 1.2.2** Estándar 1205 Evidencia
 - 1.2.3** Estándar 1206 Uso del Trabajo de Otros Expertos
-

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:

- 1.1 Tipos de evidencia
 - 1.2 Obtener evidencia
 - 1.3 Evaluar la evidencia
 - 1.4 Preparar documentación de auditoría
-

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

2.1 Tipos de Evidencia

- 2.1.1** Cuando se planifica y desarrolla un trabajo, los profesionales deben considerar los tipos de evidencia a obtener, su uso para cumplir los objetivos del trabajo y sus diferentes niveles de confiabilidad. Los diferentes tipos de evidencia que los profesionales deben considerar usar se incluyen:
- Procesos observados y existencia de elementos físicos
 - Evidencia documental
 - [Representaciones](#)
 - Análisis
- 2.1.2** Los procesos observados y la existencia de elementos físicos puede incluir observaciones de actividades, propiedad y funciones de SI, como:
- Un sistema de monitoreo de la seguridad de la red en desempeño
 - Un inventario de medios en un lugar de almacenamiento externo
- 2.1.3** Evidencia documental, grabada en papel u otro medio, puede incluir:
- Políticas y procedimientos escritos
 - Resultados de extracciones de datos
 - Registros de transacciones
 - Listados de programas
 - Otros documentos y registros producidos en el curso del negocio ordinario
- 2.1.4** Representaciones escritas y orales de los auditados que pueden incluir:
- Declaración por escrito por la gerencia, ejemplo, representaciones acerca de la existencia y efectividad de controles internos o planes para la implementación de un nuevo sistema financiero.
 - Representación oral de cosas tales como el desempeño de un proceso o un plan de seguimiento para la gerencia de acciones relacionadas con el programa de concienciación de la seguridad
- 2.1.5** Los resultados de analizar la información a través de comparaciones, simulaciones, cálculos y razonamiento que pueden también ser usadas como evidencia. Algunos ejemplos:
- Comparación de rendimiento de SI con otras empresas o periodos pasados
 - Comparación de ratios de error entre aplicaciones, transacciones y usuarios
 - Repetición de los procesos o controles
-

2.2 Obtener Evidencia

- 2.2.1** Los profesionales deben obtener [evidencia suficiente](#) y [apropiada](#) para permitirles definir conclusiones de auditoría razonable. Esta evidencia incluye:
- Procedimientos realizados
 - Resultados de los procedimientos realizados
 - Documentos fuente (en formato electrónico o papel), registros e información utilizada para apoyar el trabajo de auditoría.
 - Documentación de que se realizó el trabajo y cumple con leyes aplicables, regulaciones y políticas.
- 2.2.2** Cuando la evidencia obtenida en forma de representación oral es crítica para la opinión o conclusión de auditoría, los profesionales deben considerar obtener la confirmación de las representaciones, por escrito o

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

2.2 Obtener Evidencia cont.

electrónicamente (por ejemplo por correo electrónico). Los profesionales deben considerar también evidencia alternativa para corroborar estas representaciones para asegurar su fiabilidad.

2.2.3 Cuando obtiene las evidencias, el profesional debe considerar:

- El tiempo, nivel de esfuerzo y coste de obtener la evidencia comparado a la suficiencia de evidencia en la reducción de riesgo de auditoría.
- Importancia de la materia evaluada y del procedimiento de auditoría que requiere la evidencia en el logro de los objetivos de auditoría y reducir el riesgo de auditoría.
- Evidencia electrónica que no puede ser recuperable en su totalidad o parte después del paso del tiempo

2.2.4 Los Procedimientos utilizados para obtener evidencias varían dependiendo de las características de los SI auditados, tiempos de la auditoría, alcance y objetivos de la auditoría, y juicio profesional. La evidencia puede ser obtenida a traves del so de procedimientos de auditoría manual, técnicas de auditoría asistidas por ordenador (CAATs) o una combinación de ambos. Los profesionales deben seleccionar el procedimiento más apropiado en relación al objetivo de auditoría de SI. Se deben considerar los siguientes procedimientos:

- **Investigación y confirmación**—El proceso de búsqueda de información de personas con experiencia que están familiarizados con la materia. Las personas experimentadas no necesitan ser miembros de la empresa auditada. Este procedimiento puede ir desde investigaciones formales por escrito a orales informales.
- **Observación**—La observación de un procedimiento o proceso realizado por los individuos que típicamente son responsables de su realización, u observar elementos físicos como locales, ordenadores o ajustes o configuraciones de SI. Este tipo de evidencia está limitado al punto de tiempo en que se llevo a cabo. Los profesionales deben tener en cuenta que observar la realización de un proceso o procedimiento puede afectar a como se realiza ese procedimiento o proceso.
- **Inspección**—Examen de documentos y registros internos o externos. Los elementos a inspeccionar pueden suministrarse en papel o formato electrónico. La inspección puede también incluir examen de activos físicos.
- **Procedimientos analíticos**—Evaluar datos (financieros o no) mediante examen de las posibles relaciones entre los datos o entre los datos y otra información importante. Esto también incluye el examen de fluctuaciones, tendencias y relaciones inconsistentes.
- **Nuevo cálculo / computación**—El proceso de comprobar la exactitud aritmética y matemática de los documentos o registros. Puede realizarse manualmente o a través del uso de CAATs.
- **Realización de nuevo**—Realización independiente de procedimientos y / o controles que fueron ejecutados originalmente por los SI o por la propia empresa.
- **Otros métodos aceptados generalmente**—Otros procedimientos aceptados generalmente que pueden seguir los profesionales para obtener evidencias suficientes y apropiadas. Por ejemplo, pueden

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

2.2 Obtener Evidencia cont.

realizar ingeniería social, actuar como un invitado misterioso o realizar pruebas éticas de intrusión.

- 2.2.5** Cuando obtienen evidencias, los profesionales deben considerar la independencia y competencia del proveedor de la evidencia de auditoría. Por ejemplo, la evidencia de auditoría corroborativa de un tercero independiente puede ser más confiable que la evidencia de auditoría obtenida de la empresa auditada. La evidencia de auditoría física generalmente es más confiable que las representaciones de un individuo.
- 2.2.6** Si hay una posibilidad que la evidencia obtenida forme parte de un procedimiento legal, los profesionales deben consultar con el consultor legal apropiado para determinar si existen requisitos especiales que afectaran en la forma en que la evidencia necesita ser obtenida, presentada y revelada.
- 2.2.7** En situaciones donde los profesionales no son capaces de obtener suficiente evidencia de auditoría, como cuando los individuos o la gerencia rehúsan a proporcionar evidencia suficiente y apropiada necesaria para conseguir los objetivos de auditoría de SI, los profesionales deben revelar la situación a los gerentes de auditoría, y si es necesario a los encargados del Gobierno. Los profesionales deben revelar este hecho también de acuerdo con los procedimientos de auditoría establecidos en la organización. Las restricciones o limitaciones del alcance de la auditoría y el logro de los objetivos de auditoría deben darse a conocer en el comunicado de los resultados de la auditoría.
- 2.2.8** Los profesionales deben conservar las evidencias después de completar el trabajo de auditoría para asegurar que la evidencia es:
 - Disponible para un periodo de tiempo y en un formato que cumple con las políticas de auditoría de la organización y estándares, leyes y regulaciones profesionales relevantes,
 - Protección contra la divulgación o modificación no autorizada durante su preparación y retención
 - Correctamente eliminados al final del periodo de retención

2.3 Evaluar Evidencia

- 2.3.1** La evidencia es suficiente y apropiada cuando proporciona una base razonable para apoyar los hallazgos o conclusiones dentro del contexto de los objetivos de auditoría. Si, en juicio de los profesionales, la evidencia no cumple esos criterios, deben obtener evidencia adicional o realizar procedimientos adicionales para reducir las limitaciones o incertidumbres relacionadas con la evidencia. Por ejemplo, un listado fuente del programa no puede ser evidencia adecuada hasta que se obtiene otra evidencia que verifique que representa el programa actual utilizado en el proceso de producción.
- 2.3.2** Al evaluar la fiabilidad de las evidencias obtenidas durante la auditoría, los profesionales deben considerar las características y propiedades de la evidencia, como su origen, naturaleza (escrita, oral, visual o electrónica), autenticidad (presencia de firma digital o manual, sellado de fecha / hora), y relaciones entre la evidencia que proporciona la evidencia corroborativa de

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

2.3 Evaluar Evidencia cont.

múltiples fuentes. En general, la confiabilidad de la evidencia se categoriza de baja a alta basándose en los procedimientos utilizados para obtener la evidencia como sigue:

- Investigación y confirmación
- Observación
- Inspección
- Procedimientos analíticos
- Repetir el cálculo o computación
- Repetir la realización

Para cada procedimiento anterior, la confiabilidad de la evidencia es mayor generalmente cuando:

- Forma escrita, en lugar de obtenerse de representaciones orales
- Obtenida directamente por los profesionales en lugar de indirectamente por la entidad auditada
- Obtenida de fuentes independientes
- Certificada por un tercero independiente
- Mantenido por un tercero independiente

2.3.3 Los profesionales deben considerar el periodo de tiempo durante el que existe o está disponible la información para determinar la naturaleza, tiempos y alcance de las pruebas sustantivas y, si es aplicable, pruebas de cumplimiento. Por ejemplo, la evidencia procesada por intercambio electrónico de datos (EDI), procesamiento de documentos de imágenes (DIP) y sistemas dinámicos como hojas de cálculo puede no ser recuperable tras un periodo de tiempo específico si los cambios a los ficheros no están controlados o no los archivos no están respaldados. La disponibilidad de la documentación puede verse impactada por las políticas de retención de documentos de la empresa.

2.3.4 Si hay un tercero auditor independiente, los profesionales deben considerar si las pruebas de controles relevantes para el sujeto de la auditoría fueron realizadas y si se puede confiar en los resultados de las pruebas.

2.3.5 Los profesionales deben obtener evidencia suficiente y apropiada para permitir a un tercero independiente cualificado realizar las pruebas y obtener el mismo resultado y conclusiones.

2.4 Preparar Documentación de Auditoría

2.4.1 Durante la realización de la auditoría, los profesionales deben preparar documentación de la evidencia obtenida para retener y estar disponible durante un periodo de tiempo predefinido y en un formato que cumple las políticas de la empresa y estándares, leyes y regulaciones profesionales relevantes.

2.4.2 La evidencia obtenida durante el desarrollo de la auditoría debe ser adecuadamente identificada, con referencias cruzadas, y catálogos para facilitar la determinación de la suficiencia global y adecuación de la evidencia para apoyar de forma razonable los hallazgos y conclusiones dentro del contexto de los objetivos de la auditoría y permitir fácilmente la recuperación por otros miembros del equipo de auditoría de SI o terceros independientes.

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

2.4 Preparar Documentación de Auditoría cont.

- 2.4.3** Los profesionales deben asegurarse que la documentación de la evidencia está protegida de acceso, divulgación o modificación no autorizados durante su preparación y retención.
- 2.4.4** Los profesionales deben disponer de documentación de la evidencia al final del periodo de retención establecido.

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 ISACA que están directamente soportados por esta guía
- Las declaraciones estándar más relevantes para esta guía

Nota: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Título del Estándar	Declaración Estándar Relevante
1203 Desempeño y Supervisión	Los profesionales de auditoría y aseguramiento de SI deberán obtener evidencias suficientes, confiables, relevantes y a tiempo para conseguir los objetivos de auditoría. Los hallazgos y conclusiones de auditoría deben estar soportados por análisis e interpretación apropiados de estas evidencias. Los profesionales de auditoría y aseguramiento deberán documentar el proceso de auditoría, describiendo el trabajo de auditoría y la evidencia de auditoría que soporta los hallazgos y conclusiones.
1205 Evidencia de Auditoría	Los profesionales de auditoría y aseguramiento deberán obtener evidencia suficiente y adecuada para llegar a conclusiones razonables sobre las que 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.
1206 Uso del Trabajo de Otros Expertos	Los profesionales de auditoría y aseguramiento de SI deberán aplicar procedimientos de pruebas adicionales para obtener evidencia suficiente y adecuada en las circunstancias donde el trabajo de otros expertos no provea evidencia suficiente y adecuada.

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

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 desde auditoría y aseguramiento de SI:

- Colegas dentro de la empresa
- Gerentes
- Órganos de Gobierno dentro de la empresa, ejemplo, comité de auditoría
- Organizaciones profesionales o grupos de redes sociales profesionales
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías)

4. Terminología

Término	Definición
Evidencia apropiada	La medida de calidad de la evidencia
Evidencia suficiente	La medida de la cantidad de evidencia; apoya todas las cuestiones materiales al objetivo y alcance de la auditoría. Ver evidencia.
Representación	Una declaración firmada u oral emitida por la gerencia a los profesionales, donde la gerencia declara que un hecho actual o futuro (por ejemplo, proceso, sistema, procedimiento, política) esta o estará en cierto estado, para el mejor conocimiento de la gerencia

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.

Guía de Auditoría y Aseguramiento de SI 2206 Uso del Trabajo de Otros Expertos

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 disseminación 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®) 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 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 2206 Uso del Trabajo de Otros Expertos

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 proporciona asesoramiento a los profesionales de auditoría y garantía de SI cuando consideren el uso del trabajo de otros expertos. La guía ayuda a evaluar la adecuación de los expertos, revisiones y evaluaciones del trabajo de otros expertos, evaluar las necesidades para realizar procedimientos de pruebas adicionales y expresar una opinión para el trabajo de auditoría, mientras se tiene en cuenta el trabajo realizado por otros expertos.
 - 1.1.2** Los profesionales de auditoría y garantía 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 1007 Afirmaciones
 - 1.2.2** Estándar 1203 Desempeño y supervisión
 - 1.2.3** Estándar 1206 Uso del Trabajo de Otros Expertos
-

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 2206 Uso del Trabajo de Otros Expertos

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 garantía:	
	2.1	Considerar el uso del trabajo de otros expertos
	2.2	Evaluar la adecuación de otros expertos
	2.3	Planificar y revisar el trabajo de otros expertos
	2.4	Evaluar el trabajo de otros expertos que no son parte del equipo de trabajo de auditoría
	2.5	Procedimientos de prueba adicionales
	2.6	Opinión o conclusión de auditoría
2.1 Considerar el Uso del Trabajo de Otros Expertos	2.1.1	Cuando los profesionales no tienen las competencias requeridas para realizar el trabajo de auditoría (parte), deben considerar buscar ayuda de otros expertos con las habilidades requeridas.
	2.1.2	El uso del trabajo de otros expertos debe ser considerado cuando hay limitaciones que pueden afectar a realizar el trabajo de auditoría, por ejemplo, conocimiento técnico requerido por la naturaleza de las tareas a realizar, recursos de auditoría escasos, limitaciones de tiempo y para hacer frente a posibles problemas de independencia. El uso de otros expertos debe ser considerado si esto se traduce en mejora de la calidad del trabajo.
	2.1.3	Los profesionales deben tener suficiente conocimiento del trabajo a realizar para orientar y revisar el trabajo, pero no se espera que tengan un nivel de conocimiento equivalente a los expertos.
	2.1.4	Los profesionales deben basar la elección de los expertos específicos y el uso del trabajo de otros expertos en criterios objetivos.
	2.1.5	Los profesionales deben comunicar y documentar los requisitos de rendimiento para otros expertos en un contrato o acuerdo antes de que los expertos comiencen el trabajo.
	2.1.6	Cuando está prohibido por las políticas internas de la empresa el acceso a registros o sistemas de otros expertos, los profesionales deben determinar la extensión apropiada del uso y dependencia del trabajo de otro experto.
	2.1.7	Si no se pueden obtener los expertos necesarios, los profesionales deben documentar el impacto en el logro de los objetivos de auditoría e incluir tareas específicas en el plan de auditoría para gestionar el riesgo de auditoría resultante. Si el riesgo de auditoría resultante no se puede gestionar, los profesionales podrían tener que rechazar el trabajo de auditoría.
2.2 Evaluar la Adecuación de Otros Expertos	2.2.1	Cuando un trabajo de auditoría implica el uso del trabajo de otros expertos, los profesionales deben considerar la adecuación de los otros expertos mientras planean el trabajo de auditoría de SI. Incluye: • Evaluar la independencia y objetividad de los otros expertos • Evaluar sus cualificaciones profesionales, experiencia relevante, recursos y uso de procesos de control de la calidad

Guía de Auditoría y Aseguramiento de SI 2206 Uso del Trabajo de Otros Expertos

2.2 Evaluar la Adecuación de Otros Expertos cont.

2.2.2 Los profesionales deben considerar cuidadosamente la independencia y objetividad de otros expertos cuando usen su trabajo. El proceso de selección y nombramiento, su posición en la organización, la línea de reporte y el efecto de sus recomendaciones sobre prácticas de gerencia son indicadores típicos de la independencia y objetividad de otros expertos.

2.3 Planificar y Revisar el Trabajo de Otros Expertos

2.3.1 Los profesionales deben considerarlas actividades de otros expertos y su efecto en los objetivos de auditoría de SI mientras planifican el trabajo de auditoría de SI. Incluye:

- Obtener una comprensión del alcance del trabajo, enfoque, tiempos y uso de procesos de control de la calidad
- Determinar el nivel de revisión requerido

2.3.2 Los profesionales deben verificar que la carta o carta de compromiso especifica sus derechos de acceso al trabajo de otros expertos. Los profesionales deben tener acceso a todos los papeles de trabajo, documentación de soporte e informes creados por otros expertos, cuando dicho acceso no cree problemas legales.

2.3.3 La naturaleza, tiempos y alcance de la evidencia de auditoría requerida dependerá de la importancia y alcance del trabajo de otros expertos. Durante el proceso de planificación, los profesionales deben identificar el nivel de revisión que se requiere para proporcionar evidencia de auditoría suficiente y adecuada para lograr los objetivos totales de auditoría de SI efectivamente. Los profesionales deben revisar el informe final, metodología o programas de auditoría y otros papeles de trabajo de otros expertos.

2.3.4 En la revisión de los papeles de trabajo de otros expertos, los profesionales deben evaluar si el trabajo de otros expertos fue planificado, supervisado, documentado y revisado apropiadamente, para considerar la idoneidad y suficiencia de la evidencia de auditoría que proporcionan, y determinar el grado de uso y confianza del trabajo de los expertos. Esta evaluación puede incluir realizar de nuevo la prueba del trabajo de los otros expertos. El cumplimiento con los estándares profesionales relevantes debe evaluarse también. En general, los profesionales deben evaluar si el trabajo de otro experto es adecuado y completo para permitirles concluir sobre los objetivos de auditoría de SI actuales y documentar una conclusión.

2.3.5 Los profesionales deben realizar revisiones suficientes del informe final de otros expertos para confirmar:

- Se ha cumplido el alcance especificado en la carta de auditoría, términos de referencia o carta de compromiso.
 - Se ha identificado cualquier hipótesis importante utilizada por otros expertos.
 - La evidencia soporta adecuadamente los hallazgos y conclusiones reportados.
-

Guía de Auditoría y Aseguramiento de SI 2206 Uso del Trabajo de Otros Expertos

2.4 Evaluar el Trabajo de Otros Expertos Que No Son Parte del Equipo de Auditoría

- 2.4.1** Las dependencias actuales entre clientes y proveedores en relación al procesamiento y externalización de actividades no esenciales conduce a un entorno de auditoría más complejo. Partes del entorno auditado pueden ser controlados y auditados por otras funciones u organizaciones independientes. Como resultado, la organización externalizada recibirá informes de los terceros sobre el entorno de control de las operaciones externalizadas. En algunos casos esto puede disminuir la necesidad de cobertura de la auditoría de SI a pesar que los profesionales no tengan acceso a documentación de apoyo y papeles de trabajo. Los profesionales deben ser cautos en proporcionar una opinión en estos casos.
- 2.4.2** Los profesionales deben evaluar la utilidad y pertinencia de los reportes emitidos por otros expertos, y deben considerar cualquier hallazgo reportado por los otros expertos. Es la responsabilidad de los profesionales determinar si se basara en el trabajo de los otros expertos y se incorporara directamente o será referenciado por separado en el informe. Los profesionales deben también evaluar el efecto de los hallazgos y conclusiones de otros expertos sobre el objetivo general de auditoría de SI, y verificar que cualquier trabajo adicional requerido para lograr el objetivo general de auditoría de SI se realiza. Todas las afirmaciones hechas por otros expertos deben ser verificadas y aprobadas formalmente por la gerencia; se puede encontrar guía detallada sobre este tema en el Estándar 1007 Afirmaciones.
-

2.5 Procedimientos de Pruebas Adicionales

- 2.5.1** Basado en la evaluación del trabajo de otros expertos, los profesionales deben aplicar procedimientos de pruebas adicionales para obtener evidencia de auditoría suficiente y adecuada en las circunstancias donde el trabajo de otros expertos no proporciona tal evidencia.
- 2.5.2** Los profesionales deben considerar si se requiere prueba complementaria del trabajo de otros expertos.
-

2.6 Opinión o Conclusión de Auditoría

- 2.6.1** Los profesionales tienen la última responsabilidad para formular una opinión o conclusión de auditoría. Los profesionales necesitan determinar si el trabajo realizado por otros expertos fue suficiente para llegar a la opinión o conclusión de auditoría.
- 2.6.2** Si las pruebas adicionales realizadas no ofrecen evidencia de auditoría suficiente y adecuada, los profesionales deben ofrecer una opinión o conclusión de auditoría adecuada e incluir la limitación al alcance cuando se requiera.
- 2.6.3** Las opiniones y comentarios de los profesionales sobre poder adoptar y la relevancia de los informes de otros expertos debe formar parte del informe del trabajo de auditoría si se usa el informe de los expertos en formar la opinión de los profesionales.

Guía de Auditoría y Aseguramiento de SI 2206 Uso del Trabajo de Otros Expertos

2.6 Opinión o Conclusión de Auditoría cont.

2.6.4 Cuando corresponda, los profesionales deben considerar el grado en que la gerencia ha implementado cualquier recomendación de otros expertos. Esto debe incluir la evaluación de si la gerencia se ha comprometido a remediar los problemas identificados por otros expertos dentro de los plazos adecuados y la situación actual de remediación.

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: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Título 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.
1203 Desempeño y Supervisión	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. Los profesionales de auditoría y garantía de SI deberán obtener evidencias suficientes, confiables, relevantes y a tiempo para conseguir los objetivos de auditoría. Los hallazgos y conclusiones de auditoría deben estar soportados por análisis e interpretación apropiados de estas evidencias.
1206 Uso del Trabajo de Otros Expertos	Los profesionales de auditoría y garantía de SI deberán considerar usar el trabajo de otros expertos para el trabajo, cuando sea apropiado. Los profesionales de auditoría y garantía de SI deberán evaluar y aprobar la adecuación de las cualificaciones,

Guía de Auditoría y Aseguramiento de SI 2206 Uso del Trabajo de Otros Expertos

Título del Estándar	Declaración Estándar Relevante
	competencias, experiencia relevante, recursos, independencia y procesos de calidad del control de los otros expertos antes del trabajo. Los profesionales de auditoría y aseguramiento deberán asesorar, revisar y evaluar el trabajo de otros expertos como parte del trabajo, y documentar la conclusión sobre el grado de uso y confianza en su trabajo. Los profesionales de auditoría y garantía de SI deberán determinar cuando el trabajo de otros expertos, que no son parte del equipo de trabajo, es adecuado y completo para concluir sobre los objetivos del trabajo actual, y claramente documentar la conclusión. Los profesionales de auditoría y garantía de SI deberán determinar cuándo se han basado en el trabajo de otros expertos y se incorpora directamente o se hace referencia por separado en el informe. Los profesionales de auditoría y aseguramiento de SI deberán aplicar procedimientos de pruebas adicionales para obtener evidencia suficiente y adecuada en las circunstancias donde el trabajo de otros expertos no provea evidencia suficiente y adecuada. Los profesionales de auditoría y garantía de SI deberán proporcionar una opinión o conclusión de auditoría apropiada, e incluir cualquier limitación al alcance cuando la evidencia requerida no se obtenga por los procedimientos de prueba adicionales.

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.

Guía de Auditoría y Aseguramiento de SI 2206 Uso del Trabajo de Otros Expertos

- 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 garantía de SI:
- Colegas dentro de la empresa
 - Gerentes
 - Órganos de gobierno dentro de la empresa, ejemplo, comité de auditoría
 - Organizaciones profesionales o grupos de redes sociales profesionales
 - Otras guías profesionales (por ejemplo, libros, papeles, otras guías)
-

4. Terminología

Término	Definición
Otro experto	Interno o externo a una empresa, otro experto puede referirse a: • Un auditor de SI de la empresa de auditoría externa • Un consultor de gestión • Un experto en el área del trabajo que ha sido designado por la dirección o por el equipo

5. Fecha de Vigencia

- 5.1 Fecha de Vigencia** Esta guía revisada es efectiva para todo compromiso de auditoría y garantía de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

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®) 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 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 2207 Actos Irregulares e Ilegales

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 proporcionar ayuda a los profesionales de auditoría y aseguramiento de SI de cómo manejar las irregularidades y actos ilegales.
 - 1.1.2** La guía detalla las responsabilidades tanto de la gerencia como de los profesionales de auditoría y aseguramiento de SI respecto a las irregularidades y actos ilegales. Asimismo proporciona ayuda de cómo manejar las irregularidades y actos ilegales durante la planificación y realización del trabajo de auditoría. Finalmente, la guía sugiere buenas prácticas para reporte interno y externo sobre las irregularidades y actos ilegales.
 - 1.1.3** 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 1005 Debido Cuidado Profesional
 - 1.2.2** Estándar 1201 Planificación de la asignación
 - 1.2.3** Estándar 1202 Evaluación de riesgo en planificación
 - 1.2.4** Estándar 1207 Irregularidades y Actos Ilegales
 - 1.2.5** Estándar 1401 Reportes
-

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 2207 Actos Irregulares e Ilegales

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 Irregularidades y actos ilegales 2.2 Responsabilidades de la gerencia 2.3 Responsabilidades de los profesionales 2.4 Irregularidades y actos ilegales durante la planificación del trabajo 2.5 Diseñar y revisar procedimientos de trabajo 2.6 Responder a irregularidades y actos ilegales 2.7 Informes internos 2.8 Informes externos
2.1 Irregularidades y Actos Ilegales	2.1.1 Las irregularidades y los actos ilegales pueden impactar directamente a una empresa de muchas (negativas) formas, afectando a las finanzas y reputación, así como indirectamente afectando a la productividad y retención de empleados. Por lo tanto, es importante que las empresas tengan mecanismos de sensibilización, prevención y detección para identificar irregularidades y actos ilegales rápidamente. Las irregularidades y los actos ilegales ocurrirán con más probabilidad en las áreas que los controles no existen, están mal diseñados o funcionan mal. 2.1.2 Las irregularidades y los actos ilegales pueden ser cometidos por un empleado en cualquier nivel de la empresa y pueden incluir actividades como: • Fraude, que es cualquier acto que implique el uso de engaño para obtener una ventaja ilegal • Tergiversación deliberada de hechos con el fin de obtener ventaja ilegal u ocultar irregularidades o actos ilegales. • Los actos que involucran no cumplir con leyes y regulaciones, incluyendo el fallo de sistemas de TI para cumplir con leyes y regulaciones aplicables. • Divulgación no autorizada de datos sujetos a leyes de privacidad • Actos que impliquen no cumplir los convenios y contratos de la empresa con terceros, como bancos, proveedores, vendedores, proveedores de servicios y partes interesadas. • Manipulación, falsificación o alteración de registros o documentos (en formato electrónico o papel) • Supresión u omisión de los efectos de las transacciones de registros o documentos (en formato electrónico o papel) • Fugas inapropiadas o deliberadas de información confidencial • Registro de transacciones en registros financieros u otros (en formato electrónico o papel) que carecen de enjundia y se sabe que son falsas (ej.: falso desembolso, fraude de nomina, evasión de impuestos) • Apropiación indebida y mal uso de los activos • Robo de tarjetas o desfalco, que es la apropiación indebida de dinero efectivo antes de registrarse en los registros financieros de una

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

2.1 Irregularidades y Actos Ilegales cont.		empresa.
		• Actos, intencionales o no, que violan los derechos de propiedad intelectual (IP), como derechos de autor, marca registrada o patentes. • Permitir el acceso no autorizado a información y sistemas • Errores en registros financieros u otros que surjan por el acceso no autorizado a datos y sistemas
	2.1.3	La determinación de si un acto particular es ilegal por lo general se basa en el asesoramiento de un calificado experto informado para ejercer la abogacía o puede tener que esperar a la determinación final de un tribunal de justicia. Los profesionales deben preocuparse principalmente del efecto o efecto potencial de la acción irregular, con independencia de si el acto es una sospecha o se ha demostrado ilegal.
	2.1.4	No todas las irregularidades se deben considerar actividades fraudulentas. La determinación de actividad fraudulenta depende de la definición legal de fraude en la jurisdicción respectiva. Las irregularidades fraudulentas incluyen: • Elusión deliberada de controles con la intención de ocultar la perpetuación de fraude • Uso no autorizado de activos o servicios • Complicidad o ayuda a ocultar este tipo de actividades Las irregularidades no fraudulentas pueden incluir: • Violación intencionada de políticas de gerencia establecidas • Violación intencionada de requerimientos regulatorios • Errores deliberados u omisiones de información sobre el área bajo auditoría o la empresa en su conjunto • Negligencia grave • Actos ilegales no intencionados
2.2 Responsabilidades de la Gerencia	2.2.1	Es principalmente responsabilidad de la gerencia y de la junta proporcionar los controles para disuadir, prevenir y detectar irregularidades y actos ilegales.
	2.2.2	La gerencia usa típicamente los siguientes medios para obtener aseguramiento razonable que las irregularidades y actos ilegales se disuaden, previenen o detentan de forma oportuna: • Diseño, implementación y mantenimiento de sistemas de control interno para prevenir y detectar irregularidades o actos ilegales. Los controles internos incluyen la revisión y aprobación de transacciones y procedimientos de revisión de gerencia. • Políticas y procedimientos que rigen la conducta de los empleados • Procedimientos de validación de cumplimiento y monitorización • Diseño, implementación y mantenimiento de sistemas adecuados para el reporte, registro y gerencia de incidentes relacionados con irregularidades o actos ilegales • Políticas y procedimientos que rigen los requerimientos de cumplimiento y regulatorios

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

2.2 Responsabilidades de la Gerencia cont.	2.2.3	La gerencia debe divulgar a los profesionales su conocimiento de cualquier irregularidad o acto ilegal y las áreas afectadas, supuestas, presuntas o comprobadas, y la acción tomada por la gerencia, si la hay.
	2.2.4	Cuando se alegue un acto de irregularidad o ilegalidad, sospechado o detectado, la gerencia debe ayudar al proceso de investigación y consulta.
2.3 Responsabilidades de los Profesionales	2.3.1	Los profesionales deben considerar definir las responsabilidades la gerencia y la gerencia de auditoría y aseguramiento de SI en la carta de auditoría respecto a la prevención, detección y reporte de irregularidades, para que sean entendidos claramente en todo el trabajo de auditoría. Si estas responsabilidades están ya documentadas en la política o documento similar en la empresa, se debe incluir una declaración en ese sentido en la carta de auditoría.
	2.3.2	Los profesionales deben comprender que los mecanismos de control no pueden eliminar completamente la posibilidad de suceder irregularidades o actos ilegales. Los profesionales son responsables de evaluar de que sucedan irregularidades o actos ilegales, evaluar el impacto de irregularidades identificadas, y diseñar y realizar pruebas que son apropiadas para la naturaleza de la tarea de auditoría
	2.3.3	Los profesionales no son responsables de la prevención o detección de irregularidades o actos ilegales. Un trabajo de auditoría no puede garantizar que se detectaran las irregularidades. Incluso cuando una auditoría se planifico y realizo adecuadamente, las irregularidades podrían no ser detectadas, ejemplo, si hay confabulación entre empleados, confabulación entre empleados y externos, o la gerencia está involucrada en las irregularidades. El objetivo es determinar que el control está en su lugar, adecuado, efectivo y cumple.
	2.3.4	Cuando los profesionales tienen información específica sobre la existencia de una irregularidad o acto ilegal, tienen la obligación de informarlo.
	2.3.5	Los profesionales deben informar a la gerencia y encargados del Gobierno cuando identifiquen situaciones donde exista un alto nivel de riesgo de irregularidad o acto ilegal potencial, aunque no se detecte ninguno.
	2.3.6	Los profesionales deben estar familiarizados razonablemente con el área bajo revisión para ser capaces de identificar factores de riesgo que puedan contribuir al suceso de irregularidades o actos ilegales.
2.4 Irregularidades y Actos Ilegales Durante la Planificación del Trabajo	2.4.1	Los profesionales deben evaluar el riesgo de aparición de irregularidades o actos ilegales relacionados con el área auditada siguiendo el uso de la metodología apropiada. En la preparación de esta evaluación, los profesionales deben considerar factores como: • Características organizacionales, ej.: ética empresarial, estructura empresarial, adecuación de las estructuras de supervisión, compensación y gratificación, las medidas de extensiones de presión de rendimiento corporativo, dirección de la empresa • La historia de la empresa, apariciones de irregularidades anteriores, y

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

2.4

Irregularidades y Actos Ilegales Durante la Planificación del Trabajo cont.

las actividades tomadas posteriormente para mitigar o minimizar los hallazgos relacionados con las irregularidades.

- Los cambios recientes en la gerencia, operaciones o SI y la dirección estratégica actual de la empresa.
- Impactos resultantes de las nuevas asociaciones estratégicas
- Los tipos de activos utilizados o servicios ofrecidos y su susceptibilidad a irregularidades
- Evaluación de la resistencia de controles y vulnerabilidades relevantes a salvar o burlar controles establecidos
- Requisitos regulatorios o legales aplicables
- Políticas internas como una política de denuncia, política de uso de información privilegiada, y código de ética del empleado y la gerencia
- Relación entre interesados y mercados financieros
- Capacidades de recursos humanos
- Confidencialidad e integridad de la información crítica de mercado
- Hallazgos de auditoría de auditorías previas
- Industria y entorno competitivo en el que opera la empresa
- Hallazgos de revisiones realizadas fuera del alcance de la auditoría, como hallazgos de consultores, equipos de control de la calidad o investigaciones de administración específicas.
- Hallazgos presentados durante el curso del día a día del negocio.
- Existencia de documentación de procesos y/o sistemas de gerencia de la calidad
- La sofisticación y complejidad técnica de los SI de apoyo al área auditada
- Existencia de sistemas de aplicación de desarrollo/mantenimiento internos para los sistemas de negocio centrales comparados con paquetes de software
- Efecto de insatisfacción de empleados
- Potenciales despidos, subcontratación, cesión o reestructuración
- Existencia de activos susceptibles fácilmente de apropiación indebida
- Desempeño financiero y/o operacional de la organización pobre
- Actitud de la gerencia respecto a la ética
- Irregularidades y actos ilícitos que son comunes a una industria particular o suceden en organizaciones similares

2.4.2 Como parte del proceso de planificación y realización del análisis de riesgos, los profesionales deben preguntar a la gerencia, y obtener representación escrita si aplica, respecto a:

- Su comprensión respecto al nivel de riesgo de las irregularidades y actos ilegales en la organización
- Si tienen conocimiento de irregularidades y actos ilegales que han o puedan ocurrir contra o dentro de la empresa
- Responsabilidad de la gerencia para diseñar e implementar controles internos para prevenir irregularidades y actos ilegales
- Como se monitoriza o gestiona el riesgo de irregularidades o actos ilegales
- Que procesos se han establecido para comunicar irregularidades o actos

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

2.4 Irregularidades y Actos Ilegales Durante la Planificación del Trabajo cont.	ilegales presuntos, sospechosos o existentes a los interesados adecuados • Legislación nacional y regional aplicable en la jurisdicción en que opera la empresa y grado de coordinación que tiene el departamento legal con el comité de riesgos y/o auditoría
2.5 Diseño y Revisión de Procedimientos de Trabajo	2.5.1 Aunque los profesionales no tienen responsabilidad explícita para detectar o prevenir actos ilegales o irregularidades, deben diseñar procedimientos para el trabajo de auditoría que tengan en cuenta el nivel de riesgo de las irregularidades y actos ilegales identificados. 2.5.2 Los profesionales deben usar los resultados del análisis de riesgo para determinar la naturaleza, oportunidad y grado de las pruebas requeridas para obtener evidencia de auditoría suficiente de aseguramiento razonable que se identificara lo siguiente: • Irregularidades que pueden tener un efecto material sobre el área auditada o sobre la empresa en conjunto • Debilidades de control que podrían fallar en prevenir o detectar irregularidades materiales • Toda deficiencia significativa en el diseño u operación de los controles internos que podría afectar potencialmente la posibilidad de registrar, procesar, resumir y reportar datos de negocio del emisor. 2.5.3 Los profesionales deben revisar el resultado de los procedimientos de trabajo para determinar si hay indicios de que puedan haber sucedido irregularidades o actos ilegales. El uso de técnicas de auditoría asistidas por ordenador (CAATs) podría ayudar significativamente en la detección efectiva y eficiente de irregularidades o actos ilegales. 2.5.4 Cuando se realiza esta evaluación, los factores de riesgo identificados en 2.4.1 se deben revisar contra los procedimientos actuales desarrollados para ofrecer aseguramiento razonable que todo riesgo identificado ha sido direccionado.
2.6 Responder a Irregularidades y Actos Ilegales	2.6.1 Durante un trabajo de auditoría, las indicaciones de existencia de irregularidades o actos ilegales pueden llegar a la atención de los profesionales. Ellos deben considerar el efecto potencial de las irregularidades o actos ilegales sobre la materia del trabajo, los objetivos de auditoría, el informe del trabajo de auditoría y la empresa. 2.6.2 Los profesionales deben demostrar una actitud de escepticismo profesional. Indicadores (a veces llamados ‘Fraude o Banderas Rojas’) se personas cometiendo irregularidades o actos ilegales son: • Anulaciones de controles por la gerencia • Asuntos de la gerencia explicados de forma irregular o pobre • Consistente en el rendimiento, comparado con objetivos establecidos

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

2.6 Responder a Irregularidades y Actos Ilegales cont.

- Problemas, o retrasos, con la recepción de información solicitada o evidencias
- Transacciones que no siguen el ciclo de aprobación normal
- Incremento en una actividad de un cierto cliente
- Incremento de quejas de los clientes
- Desvío de los controles de acceso de algunas aplicaciones o usuarios

Los profesionales deben prestar mucha atención cuando noten estos asuntos.

- 2.6.3** Cuando los profesionales se preocupan de información concerniente a posibles irregularidades o actos ilegales, deben considerar tomar los siguientes pasos tras dirección de la autoridad legal adecuada:
- Comprender la naturaleza del acto
 - Comprender las circunstancias en las que ha ocurrido el acto
 - Obtener evidencia de la aparición del hecho (ej.: carta, registro del sistema, archivo informático, log de seguridad, información de cliente)
 - Identificar todas las personas involucradas en cometer el acto
 - Obtener información suficiente de soporte a evaluar el efecto del acto
 - Realizar procedimientos adicionales limitados para determinar el efecto del acto y si existen actos adicionales
 - Documentar y preservar toda evidencia y trabajo realizado
- 2.6.4** Los profesionales deben entonces consultar con la gerencia de auditoría para determinar sus próximas acciones que puede involucrar reportar el 'evento' a la gerencia de la empresa, dando más acción a los investigadores de fraude interno, y/o informar a las autoridades policiales o reguladores.
- 2.6.5** Cuando una irregularidad involucre a un miembro de la gerencia, los profesionales deben reconsiderar la confiabilidad de las representaciones realizadas por la gerencia. Típicamente, los profesionales deben trabajar con un nivel de gerencia adecuado sobre el asociado con la irregularidad o acto ilegal.

2.7 Informes Internos

- 2.7.1** La detección de irregularidades y actos ilegales debe ser comunicada (por escrito u oral) a las personas apropiadas en la empresa de forma oportuna por los profesionales. La notificación debe ser dirigida a un nivel de gerencia sobre el que se sospecha ha ocurrido la irregularidad o acto ilegal. Además, las irregularidades y actos ilegales debe ser informado a los encargados del Gobierno en la empresa, como el comité ejecutivo, fideicomisarios, comité de auditoría o cuerpo equivalente, excepto para materias que son claramente insignificantes en términos tanto de efecto financieros como indicaciones de debilidad del control.

Si los profesionales sospechan que todos los niveles de la gerencia están involucrados, entonces los hallazgos, deben ser confidencialmente informados directamente a los encargados del Gobierno, como el comité ejecutivo, fideicomisarios, comité de auditoría o cuerpo equivalente, de acuerdo a las leyes y regulaciones locales aplicables. Las leyes y

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

2.7 Informes Internos cont.

- regulaciones locales pueden prohibiré informar a otras partes que las prescritas como autoridad legal.
- 2.7.2** Los profesionales deben usar juicio profesional cuando informen una irregularidad o acto ilegal. Deben discutir los hallazgos y la naturaleza, oportunidad y grado de cualquier otro procedimiento a ser realizado con un nivel apropiado de gerencia que sea al menos un nivel sobre las personas que aparecen estar involucradas. En estas circunstancias, es particularmente importante que los profesionales mantengan su independencia.
- 2.7.3** Las personas incluidas en la distribución interna del informe de irregularidades o actos ilegales debe ser considerado cuidadoso. La aparición y efecto de irregularidades o actos ilegales es una cuestión sensitiva y la distribución del informe lleva su propio riesgo, incluyendo:
- Mas abuso de la debilidad del control como resultado de publicar detalles de ellos
 - Pérdida de clientes, proveedores e inversores cuando se difunde (autorizado o no) fuera de la empresa
 - Perdida de personal y gerencia clave, incluyendo a los no involucrados en la irregularidad o acto ilegal, porque se reduce la confianza en la gerencia y el futuro de la empresa
- 2.7.4** Los profesionales deben considerar informar las irregularidades o actos ilegales de forma separada a otras cuestiones de auditoría si esto puede ayudar en el control de la distribución del informe.
- 2.7.5** Los profesionales deben tratar de evitar alertar a cualquier persona que pueda estar implicada o involucrada en la irregularidad o acto ilegal, para reducir la probabilidad de destruir o eliminar evidencias por esas personas.
- 2.7.6** La carta de auditoría debe definir las responsabilidades profesionales respecto a informar irregularidades o actos ilegales.
-

2.8 Informes Externos

- 2.8.1** Informar externamente de fraudes, irregularidades o actos ilegales puede ser una obligación legal o regulatoria. La obligación puede aplicar a la gerencia empresarial o a las personas involucradas en detectar las irregularidades, o ambas. Los requerimientos de informe legal para el auditor están sujetos a jurisdicción local y sustitución de política interna y/o acuerdos contractuales. Otras situaciones que pueden requerir informar externamente son:
- Cumplimiento con requerimientos legales o regulatorios
 - Orden judicial
 - Agencia financiera o de Gobierno de acuerdo con los requerimientos de los auditores de entidades que reciben asistencia financiera gubernamental
 - Petición de auditores externos
- 2.8.2** Cuando se requiere informar externamente, antes del envío externo se debe aprobar por un nivel de gerencia de auditoría y aseguramiento de SI y revisar con el comité ejecutivo de auditoría la forma y contenido de la

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

2.8 Informes Externos cont.

información reportada, a menos que se prevenga por regulaciones aplicables o circunstancias específicas del contrato de auditoría. Ejemplos de circunstancias específicas que pueden prevenir obtener acuerdo de la gerencia ejecutiva del auditado son:

- Involucración activa de la gerencia ejecutiva del auditado en la irregularidad o acto ilegal
- Consentimiento pasivo de la gerencia ejecutiva del auditado en la irregularidad o acto ilegal

2.8.3 Si la gerencia ejecutiva del auditado no acepta el envío externo del informe, y el envío externo es una obligación estatutaria o regulatoria, entonces los profesionales deben considerar consultar al comité de auditoría y consejo legal sobre el asesoramiento y riesgo de informar de los hallazgos fuera de la empresa. Aun en situaciones donde los profesionales estén protegidos por privilegios, deben buscar asesoramiento legal y consejo antes de hacer este tipo de entrega para asegurar que están de hecho protegidos por este privilegio.

2.8.4 Los profesionales, con la aprobación de la gerencia de auditoría y aseguramiento de SI, deben informar las irregularidades o actos ilegales a los reguladores adecuados de forma oportuna. Si la empresa no da a conocer una conocida irregularidad o acto ilegal o solicita a los profesionales eliminar estos hallazgos, los profesionales deben buscar asesoramiento y consejo legal.

2.8.5 Si se ha detectado una irregularidad o acto ilegal por los profesionales, ellos deben informar a los auditores externos de forma oportuna.

2.8.6 Cuando los profesionales son conscientes que la gerencia requiere informar de actividades fraudulentas fuera de la organización, los profesionales deben formalmente asesorar a la gerencia de esta responsabilidad.

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: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

Titulo 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.
1201 Planificación de la Asignación	Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir: • 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.
1202 Evaluación de Riesgos en la Planificación de Auditoría	La función de auditoría y aseguramiento de SI deberá utilizar un enfoque apropiado y el apoyo de metodología de análisis de riesgos para desarrollar el plan de auditoría de SI general y determinar las prioridades para la asignación efectiva de recursos de auditoría de SI. Los profesionales de auditoría y aseguramiento de SI deberán identificar y analizar los riesgos relevantes al área bajo revisión, en la planificación de trabajos individuales. Los profesionales de auditoría y aseguramiento deberán considerar el riesgo de la materia, riesgo de auditoría y exposiciones relacionadas con la empresa.
1207 Irregularidades y actos ilegales	Los profesionales de auditoría y aseguramiento de SI deberán considerar el riesgo de actos irregulares e ilegales durante el trabajo. Los profesionales de auditoría y aseguramiento de SI deberán mantener una actitud de escepticismo profesional durante el trabajo. Los profesionales de auditoría y aseguramiento de SI deberán documentar y comunicar cualquier irregularidad material o acto ilegal a las partes adecuadas de forma oportuna.
1401 Reportes	Los profesionales de auditoría y aseguramiento de SI se aseguraran que los hallazgos se apoyan en el informe de auditoría por evidencia suficiente, confiable y relevante.

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

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
EDM03 Asegurar la optimización del riesgo.	Asegurar que el riesgo empresarial relacionado con TI no excede el riesgo aceptado y la tolerancia de riesgo, el impacto de riesgo de TI al valor de la empresa está identificado y gestionado, y la posibilidad de fallos de cumplimiento esta minimizada.
APO12 Gestionar el riesgo.	Integrar la gerencia de riesgos empresariales relacionados con TI con el ERM en general, y el balance de costes y beneficios de la gerencia de riesgos empresariales relacionados con TI.
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 desde auditoría y aseguramiento de SI:

- Colegas dentro de la empresa
- Gerentes
- Órganos de Gobierno dentro de la empresa, ejemplo, comité de auditoría
- Organizaciones profesionales
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías)

Guía de Auditoría y Aseguramiento de SI 2207 Actos Irregulares e Ilegales

4. Terminología

Término	Definición
Escepticismo profesional	Una actitud que incluye una mente inquisitiva y una evaluación crítica de la evidencia de auditoría. Fuente: American Institute of Certified Public Accountants (AICPA) AU 230.07
Irregularidad	La violación de una política de gerencia o requerimiento regulatorio establecido. Puede consistir en errores deliberados u omisión de información concerniente al área auditada o la empresa completa, negligencia grave o actos ilegales no intencionados.

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

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®) 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 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 2208 Muestreo

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 proporcionar asesoramiento a los profesionales de auditoría y aseguramiento de SI diseñar y seleccionar una muestra de auditoría y evaluación de los resultados de la muestra. Un muestreo y evaluación apropiados ayudara a lograr los requerimientos de evidencia suficiente y apropiada. 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 1006 Competencia 1.2.2 Estándar 1202 Evaluación de riesgo en planificación 1.2.3 Estándar 1203 Desempeño y supervisión 1.2.4 Estándar 1205 Evidencia
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: 2.1 Muestreo 2.2 Diseño de la muestra 2.3 Selección de la muestra 2.4 Evaluación de los resultados de la muestra 2.5 Documentación
-------------------------	--

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

2.1 Muestreo

- 2.1.1** Al formar una opinión o conclusión, frecuentemente los profesionales no examinan toda la información disponible porque puede ser poco práctico (ejemplo requiere demasiado tiempo tanto para el auditado como para los profesionales investigar toda la información) y se pueden alcanzar conclusiones validas usando el [muestreo de auditoría](#).
- 2.1.2** Cuando se usa el método de [muestreo estadístico](#) o [no estadístico](#), los profesionales deben diseñar y seleccionar un muestreo de auditoría, procedimientos de realización de la auditoría y evaluación de los resultados del muestreo para obtener evidencias suficientes y apropiadas para formar una conclusión. Al usar métodos de muestreo para extraer una conclusión sobre la [población](#) completa, los profesionales deben usar muestreo estadístico.
-

2.2 Diseño de la Muestra

- 2.2.1** Al diseñar el tamaño y estructura de un muestreo de auditoría, los profesionales deben considerar los objetivos de auditoría de SI específicos, los objetivos de auditoría específicos, los procedimientos de auditoría que tienen más probabilidades de lograr esos objetivos, la naturaleza de la población, subgrupos relevantes dentro de la población, y los métodos de muestreo y selección. Además, cuando el muestreo de auditoría es adecuado, se debe considerar la naturaleza de las evidencias solicitadas, posibles condiciones de error y posibles causas raíz.
- 2.2.2** Al diseñar el muestreo de auditoría, teniendo en cuenta los objetivos de la auditoría de SI, los profesionales deben considerar:
- Propósito de la muestra
 - Unidad de muestreo
 - Población
 - [Riesgo del muestreo](#) y tamaño de la muestra
 - [Error tolerable](#)
 - Distribución esperada subyacente (por ejemplo, Poisson, binomial, normal, exponencial)
 - Comportamiento en el tiempo (ejemplo, por estación, disminución en el rendimiento)
 - Sub poblaciones o subgrupos que son de origen natural y deben ser considerados para determinar la relevancia operativa
 - Valores atípicos
 - Poblaciones pequeñas de eventos adversos o inusuales
 - Datos de herramientas de apoyo externo, usadas para confirmar o complementar los resultados del muestreo
- 2.2.3** Los profesionales deben considerar el propósito de la muestra:
- **Pruebas de cumplimiento/pruebas de controles**—Un procedimiento de auditoría diseñado para evaluar la efectividad operativa de los controles en la prevención o detección y corrección de las debilidades materiales. Ejemplos de pruebas de cumplimiento de los controles, en las que las muestras pudieran ser consideradas, incluyen los derechos de acceso de los usuarios, procedimientos de control de cambio a programas, documentación del procedimiento, documentación del programa, seguimiento de las excepciones, revisión de logs y auditorías de licencias de software.

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

2.2 Diseño de la Muestra cont.

- **Pruebas sustantivas/pruebas de detalles**—Un procedimiento de auditoría diseñado para detectar las debilidades materiales a nivel afirmativo. Ejemplos de pruebas sustantivas, donde se podría considerar el muestreo, incluyen la repetición de cálculos complejos (ejemplo intereses) sobre una muestra de cuentas, una muestra de transacciones para dar fe a la documentación de soporte, etc.

- 2.2.4** La unidad de muestreo depende del propósito de la muestra. Para muestreos de cumplimiento de los controles, donde la unidad de muestreo es un evento o transacción (por ejemplo, un control de autorización de un recibo), el [muestreo de atributos](#) se aplica típicamente para determinar las características de una población. Para las pruebas sustantivas, donde la muestra unitaria a menudo es monetaria, el [muestreo de variables](#) se aplica frecuentemente porque se usa para determinar el impacto monetario o volumétrico de características de una población.
- 2.2.5** La población es el conjunto de datos completo del que los profesionales desean muestrear para llegar a una conclusión. Por lo tanto, la población de la que se extrae la muestra debe ser adecuada para probar el diseño y/o operatividad de la efectividad de los controles, y verificada como completa para el objetivo y alcance de la auditoría de SI específica.
- 2.2.6** Para ayudar en el diseño eficiente y efectivo de la muestra, puede ser adecuado la [estratificación de la muestra](#). La estratificación es el proceso de dividir una población en sub poblaciones con características similares explícitamente definidas, de forma que cada unidad de la muestra puede pertenecer a un solo estrato.
- 2.2.7** Cuando se determina el tamaño de la muestra, los profesionales deben considerar el riesgo de muestreo, la cantidad de los errores que podría ser aceptable y el grado que se espera de los errores. El riesgo de muestreo surge de la posibilidad que la conclusión de los profesionales pueda ser diferente de la conclusión que se alcanzaría si se sometiera a la población entera al mismo procedimiento de auditoría. Hay dos tipos de riesgo de muestreo:
- **El riesgo de aceptación incorrecta**—Se evalúa como poco probable una debilidad material cuando, de hecho, la población es incorrecta materialmente.
 - **El riesgo de rechazo incorrecto**—Se evalúa como probable una debilidad material cuando, de hecho, la población no es incorrecta materialmente.
- 2.2.8** El tamaño de la muestra se ve afectado por el nivel de riesgo de la muestra que el profesional está dispuesto a aceptar. El riesgo de muestreo debe ser considerado también en relación al modelo de riesgo de auditoría y sus componentes, riesgo inherente, riesgo de control y riesgo de detección, como se detalla en el Estándar 2202 Evaluación de riesgo en planificación.
- 2.2.9** El error tolerable es el error máximo que los profesionales están dispuestos a aceptar en la población y aun concluir que el objetivo de la prueba se ha logrado. Para pruebas sustantivas, el error tolerable está relacionado con el juicio de los profesionales sobre materialidad. En las pruebas de cumplimiento, es el porcentaje máximo de desviación de un procedimiento de control prescrito que los profesionales están dispuestos a aceptar.

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

2.2 Diseño de la Muestra cont.

- 2.2.10** Si los profesionales esperan que se presenten errores en la población, se debe examinar una muestra mayor que cuando no se esperan errores para concluir que el error actual en la población no es mayor que el error tolerable esperado. Se justifican tamaños de muestra más pequeños cuando la población se espera libre de errores. Al estimar el error esperado en una población, los profesionales deben considerar cuestiones como:
- Niveles de error identificados en auditorías previas
 - Cambios en los procedimientos de la empresa
 - Evidencia disponible de una evaluación del sistema de control interno, resultados de procedimientos de revisión analíticos, y/o resultados de pruebas preliminares de la población.
- 2.2.11** Los profesionales deben considerar, si es adecuado, la necesidad para involucrar especialistas en el diseño y análisis enfoques de muestreo complejos, como muestras aleatorias estratificadas que deben tener validez estadística, o muestreo basado en métodos de control de calidad establecidos (ejemplo Six Sigma).
- 2.2.12** Los profesionales deberán concluir que el muestreo no permite lograr los objetivos de auditoría de SI y se requiere una prueba de la población entera, deben considerar aplicar un aseguramiento continuo porque permite probar la población entera de forma oportuna y rentable. Se puede encontrar orientación detallada sobre este tema en la Guía 2211 Aseguramiento Continua.
-

2.3 Selección de la Muestra

- 2.3.1** Los profesionales deben asegurar que la población es completa y controla la selección de la muestra, para mantener independencia de auditoría. Los profesionales deben seleccionar elementos de muestra de forma que la muestra se espere representativa de la población cuanto a las características que se están probando.
- 2.3.2** Para que una muestra sea representativa de la población entera, todas las unidades del muestreo en la población deben tener igual o conocida, probabilidad no nula de ser seleccionada. Esto implica el uso de métodos de muestreo estadístico, porque implican el uso de técnicas el uso de técnicas de las que se pueden extraer conclusiones construidas matemáticamente. Los profesionales deben validar la completitud de la población para asegurar que la muestra se selecciona de un conjunto de datos adecuado.
- 2.3.3** El muestreo no estadístico es una aproximación utilizada por profesionales que quieren usar su propia experiencia, conocimiento y juicio profesional para determinar una muestra. Este método implica un sesgo humano porque no está basado estadísticamente, no asegura que toda unidad de muestreo tenga una conocida, probabilidad no nula de ser elegida, por lo que los resultados no pueden ser extrapolados sobre la población porque la muestra es poco probable de ser representativa para toda la población. El muestreo estadístico puede utilizarse cuando los resultados se necesitan rápidamente para confirmar una proposición y no deben usarse para confirmar una conclusión construida matemáticamente sobre la población entera.

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

2.3 Selección de la Muestra cont.

2.3.4 Hay cinco métodos de muestreo usados comúnmente, divididos en métodos de muestreo estadísticos y no estadísticos:

- Métodos de muestreo estadísticos:
 - **Muestreo aleatorio simple**—Asegura que todas las combinaciones de las unidades del muestreo en la población tienen la misma probabilidad de selección.
 - **Muestreo sistemático**—Involucra la selección de unidades de muestreo usando un intervalo fijo entre las selecciones, el primer intervalo tiene un inicio aleatorio. Los ejemplos incluyen selección de Muestreo de Unidad Monetaria o Valores Ponderados donde cada valor monetario individual (ejemplo \$1000) en la población tiene la misma oportunidad de selección. Debido a que normalmente la unidad monetaria individual no puede ser examinada por separado, el elemento que incluye esa unidad monetaria se selecciona para su examen. Este método pesa sistemáticamente la selección a favor de las mayores cantidades. Otro ejemplo incluye la selección de cada unidad de muestreo enésima.
 - **Muestreo aleatorio estratificado**—Asegura que toda unidad de muestreo en cada grupo tiene una posibilidad de selección no nula. Los profesionales deben considerar el uso estadístico de software para calcular desviaciones estándar y otros resúmenes estadísticos para resultados de muestreo estadístico
- Métodos de muestreo no estadístico:
 - **Muestreo arbitrario**—Los profesionales seleccionan la muestra sin seguir una técnica estructurada, evitando a la vez cualquier sesgo consciente o previsible. Sin embargo, el análisis de un muestreo arbitrario no debe ser tomado como base para concluir sobre la población.
 - **Muestreo prejuicioso**—Los profesionales ponen un sesgo en la muestra (ejemplo, todas las unidades del muestreo sobre un cierto valor, todo por un típico de excepción específico, todos negativos). Cabe señalar que una muestra de juicio no se basa estadísticamente y los resultados no deben ser extrapolados sobre la población porque la muestra es poco probable de ser representativa de la población completa.

2.3.5 Hay dos métodos de selección usados comúnmente:

- Selección de registros y subgrupos de población; métodos comunes son:
 - Muestreo aleatorio simple
 - Muestreo aleatorio estratificado
 - Muestreo arbitrario
 - Muestreo prejuicioso
- Selección de campos cuantitativos (ej.: unidades monetarias); métodos comunes son:
 - Muestreo aleatorio simple
 - Muestreo sistemático

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

2.4 Evaluación de Resultados de la Muestra

- 2.4.1** Habiendo realizado los procedimientos de auditoría apropiados para el objetivo de auditoría de SI sobre cada elemento de la muestra, los profesionales deben analizar cualquier error posible detectado en la muestra para determinar si hay errores actualmente y, en su caso, la naturaleza y la causa de los errores. Para los que sean evaluados como errores actualmente, los errores deben ser proyectados como apropiados para la población, pero solo si el método de muestreo usado se basa estadísticamente.
- 2.4.2** Cualquier error posible detectado en la muestra debe ser revisado para determinar si hay errores actualmente. Los profesionales deben considerar los aspectos cualitativos de los errores. Incluyendo la naturaleza y causa del error y los posibles efectos del error en las otras fases de la auditoría. Por ejemplo, errores que son resultado de un desajuste en un proceso automático tienen mayor implicación que errores humanos.
- 2.4.3** Cuando la evidencia de auditoría esperada respecto a una unidad de la muestra específica no se puede obtener, los profesionales deben considerar si son capaces de obtener evidencia de auditoría suficiente y adecuada realizando procedimientos alternativos sobre el elemento seleccionado, o seleccionando y probando otra una unidad de muestra.
- 2.4.4** Los profesionales deben considerar la proyección de los resultados de la muestra a la población con un método de proyección consistente con el método empleado para seleccionar la unidad de muestreo. La proyección de la muestra puede implicar estimar el error probable en la población y estimar cualquier error que pueda no haber sido detectado por la imprecisión de la técnica, junto con los aspectos cualitativos de cualquier error encontrado.
- 2.4.5** Se debe limitar la discusión de los resultados de muestreos no estadísticos (arbitrario o juicioso) a una descripción de los resultados de analizar la muestra, en un contexto de la población como un todo.
- 2.4.6** Los profesionales deben considerar si los errores en la población pueden exceder el error tolerable comparando el error de la población proyectada con el error tolerable estimado o definido, teniendo en cuenta los resultados de otros procedimientos de auditoría relevantes para el objetivo de auditoría. El error tolerable puede estimarse o definirse por criterios de auditoría, estándares de la industria, requerimientos contractuales, especificaciones del software, etc. Cuando el error de la población proyectada excede el error tolerable, los profesionales deben reevaluar el riesgo de muestreo y, si no es aceptable ese riesgo, considerar extender el procedimiento de auditoría, recalcular el tamaño de la muestra usando el error tolerable refinado y probar las unidades de muestra adicionales, o realizar procedimientos de auditoría alternativos.
-

2.5 Documentación

- 2.5.1** Los papeles de trabajo deben incluir detalle suficiente para describir claramente el objetivo del muestreo y el proceso de muestreo usado. Los papeles de trabajo deben incluir.
- Propósito de la muestra, incluyendo unidad de muestra
 - Fuente y definición de la población y relación con el alcance de auditoría.

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

2.5

Documentación cont.

- Parámetros de muestreo, ejemplo, tamaño de muestra (incluyendo cualquier consideración sobre el riesgo de muestreo), inicio aleatorio o semilla numérica o método como se obtiene el inicio aleatorio, intervalo de muestreo.
- Método de muestreo
- Elementos seleccionados y, si se emplea método no estadístico, justificación de los elementos seleccionados
- Detalle de las pruebas de auditoría realizadas, incluyendo evaluación de errores y, si aplica, procedimientos de auditoría alternativos
- Conclusiones

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: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Titulo del Estándar	Declaración Estándar Relevante
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.
1202 Evaluación de Riesgos en la Planificación de Auditoría	Los profesionales de auditoría y aseguramiento deberán considerar el riesgo de la materia, riesgo de auditoría y exposiciones relacionadas con la empresa.
1203 Desempeño y Supervisión	Los profesionales de auditoría y aseguramiento de SI deberán obtener evidencias suficientes, confiables, relevantes y a tiempo para conseguir los objetivos de auditoría. Los hallazgos y conclusiones de auditoría deben estar soportados por análisis e interpretación apropiados de estas evidencias. Los profesionales de auditoría y aseguramiento deberán documentar el proceso de auditoría, describiendo el trabajo de auditoría y la evidencia de auditoría que soporta los

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

Título del Estándar	Declaración Estándar Relevante
	hallazgos y conclusiones. Los profesionales de auditoría y aseguramiento de SI deberán identificar y concluir sobre los hallazgos.
1205 Evidencia de Auditoría	Los profesionales de auditoría y aseguramiento deberán obtener evidencia suficiente y adecuada para llegar a conclusiones razonables sobre las que 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
APO12 Gestionar el riesgo.	Integrar la gerencia de riesgos empresariales relacionados con TI con el ERM en general, y el balance de costes y beneficios de la gerencia de riesgos empresariales relacionados con TI.
MEA02 Monitorizar 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 desde auditoría y aseguramiento de SI:

- Colegas dentro de la empresa
- Gerentes
- Órganos de Gobierno dentro de la empresa, ejemplo, comité de auditoría
- Organizaciones profesionales o grupos de redes sociales profesionales
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías)

Guía de Auditoría y Aseguramiento de SI 2208 Muestreo

4. Terminología

Término	Definición
Error tolerable	El error máximo en la población que los profesionales están dispuestos a aceptar y concluir que se ha logrado el objetivo de la prueba. Para pruebas sustantivas, el error tolerable está relacionado al juicio de los profesionales sobre la materialidad. En las pruebas de cumplimiento, es el ratio máximo de desviación de un procedimiento de control prescrito que los profesionales están dispuestos a aceptar.
Estratificación de muestreo	El proceso de dividir una población en grupos con características similares definidas explícitamente, de forma que cada unidad de muestra solo puede pertenecer a un estrato.
Muestreo de auditoría	La aplicación de procedimientos de auditoría a menos del 100% de los elementos dentro de la población para obtener evidencia de auditoría sobre una característica particular de la población
Muestreo estadístico	Método de seleccionar una porción de la población, por medio de cálculos y probabilidades matemáticas, con el propósito de hacer sondeos científicos y matemáticos respecto de las características de la población entera.
Muestreo no estadístico	Método de selección de una porción de la población, por medios de juicio propio y experiencia, con la intención de confirmar rápidamente una proposición. Este método no permite obtener conclusiones matemáticas sobre la población entera.
Muestreo por atributos	Método para seleccionar una parte de la población basada en la presencia o ausencia de una cierta característica
Muestreo variable	Una técnica de muestreo usada para estimar el valor medio o total de la población basándose en una muestra; un modelo estadístico usado para proyectar una característica cuantitativa, como una cantidad monetaria.
Población	El conjunto entero de datos del que se selecciona una muestra y del que un auditor de SI desea obtener conclusiones.
Riesgo de Muestreo	La probabilidad que un auditor de SI alcance una conclusión incorrecta por probar una muestra de auditoría, en lugar de toda la población. Ámbito de las notas: Mientras el riesgo de muestreo puede reducirse a un nivel bajo aceptable usando un tamaño de muestra apropiado y un método de selección, nunca puede ser eliminado.

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.



Guía de Auditoría y Aseguramiento de SI 2401 Reportes

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	The Weinman Group, USA

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

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 ayuda a los profesionales de auditoría y aseguramiento de SI sobre los diferentes tipos de trabajo de auditoría de SI e informes relacionados.
 - 1.1.2** La guía detalla todos los aspectos que se deben incluir en un informe de trabajo de auditoría y proporciona a los profesionales de auditoría y aseguramiento de SI con las consideraciones a realizar cuando se redacta y termina un informe de trabajo de auditoría.
 - 1.1.3** 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 1007 Afirmaciones
 - 1.2.2** Estándar 1205 Evidencia
 - 1.2.3** Estándar 1401 Reportes
 - 1.2.4** Estándar 1402 Actividades de seguimiento
-

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 2401 Reportes

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 Tipos de trabajo

2.2 Contenidos requeridos del informe de trabajo de auditoría

2.3 Eventos posteriores

2.4 Comunicación adicional

2.1 Tipos de Trabajo

2.1.1 Los profesionales pueden realizar cualquiera de los siguientes tipos de trabajo de auditoría:

- Examen
- Revisión
- Conformidad Sobre Procedimientos

Nota: Estos términos están definidos en ITAF, 2ª Edición.

2.1.2 Tanto el examen como la revisión involucran:

- Planificación del trabajo
- Evaluar el diseño efectivo de procedimientos de control
- Probar la operatividad efectiva de los procedimientos de control (la naturaleza, oportunidad y grado de prueba puede variar entre ambos tipos de trabajo)
- Formar una conclusión, e informar, sobre el diseño y/o efectividad operativa de los procedimientos de control basándose en criterios identificados:
 - La conclusión para un trabajo de aseguramiento razonable se expresa como opinión positiva y ofrece un alto nivel de aseguramiento.
 - La conclusión para un trabajo de aseguramiento limitada se expresa como opinión negativa y ofrece solo un nivel moderado de aseguramiento.

2.1.3 Un trabajo de 'conformidad sobre procedimientos' no dan lugar a la expresión de aseguramiento de los profesionales. Los profesionales se encargan de llevar a cabo procedimientos específicos para lograr las necesidades de la información de las partes que han aprobado realizar los procedimientos (ej.: gerencia ejecutiva, comité o encargados del Gobierno). Los profesionales emiten un informe de hallazgos verdaderos a las partes que han aprobado los procedimientos. Los destinatarios forman sus propias conclusiones de este informe por la naturaleza, oportunidad y grado de los procedimientos que no permiten a los profesionales expresar ninguna aseguramiento. El informe está restringido a las partes que han aprobado realizar los procedimientos porque otros no son conscientes de las razones de los procedimientos y pueden mal interpretar el resultado.

2.1.4 Un informe de conformidad sobre los procedimientos puede también ser distribuido a terceros (ej.: órgano regulatorio) cuando sea predeterminado y aprobado por las partes que aprobaron los procedimientos antes del inicio del trabajo actual. Los profesionales deben considerar esto, usando su juicio profesional, basado en el riesgo de mal interpretación del trabajo a realizar.

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

- 2.1.5** Los profesionales, antes de completar el trabajo de auditoría, se les solicita cambiar el trabajo de auditoría de examen o revisión a conformidad sobre procedimientos, necesitan considerar la adecuación de hacerlo y no pueden aceptar un cambio cuando no hay justificación razonable para el cambio. Por ejemplo, un cambio no es adecuado para evitar un informe cualificado.

2.2 Contenidos Requeridos del Informe de Trabajo de Auditoría

- 2.2.1** Al desarrollar un informe de trabajo de auditoría, se debe considerar toda evidencia relevante obtenida, independientemente si aparecen corroborando o contradiciendo la materia. Cuando haya una opinión, debe ser apoyada por los resultados de los procedimientos de control basados en los criterios identificados. Los profesionales deben concluir si se ha obtenido [evidencia suficiente](#) y [apropiada](#) para apoyar las conclusiones en el informe de trabajo de auditoría. Se puede encontrar más ayuda detallada en el Estándar 1205 Evidencia.
- 2.2.2** Cuando se concluya en un trabajo de examen o revisión, los profesionales deben llegar a una expresión de opinión sobre si, en todos los aspectos materiales, el diseño y/o operación de los procedimientos de control en relación al área de actividad fueron efectivos. Esta opinión puede ser:
- **No cualificada**—Los profesionales deben expresar una opinión no cualificada cuando concluyan que, en todos los aspectos materiales, el diseño y/o operación de los procedimientos de control en relación al área de actividad fueron efectivos, de acuerdo con los criterios aplicables.
 - **Cualificada**—Los profesionales deben expresar una opinión cualificada cuando:
 - Hayan obtenido evidencia suficiente y apropiada, concluyan que la debilidad del control, individualmente o en grupo, son materiales, pero no predominante en los objetivos de auditoría de SI
 - No son capaces de obtener evidencia suficiente y apropiada en que basar la opinión, pero concluyen que los efectos posibles sobre los objetivos de auditoría de SI de debilidades no detectadas, si hay, podrían ser materiales pero no predominantes
 - **Adversa**— Los profesionales deben expresar una opinión adversa cuando una o más deficiencias significativas se une a una debilidad material y predominante
 - **Renuncia**—Los profesionales deben renunciar una opinión cuando no son capaces de obtener evidencia suficiente y apropiada en que basar la opinión, y concluyen que el posible efecto sobre los objetivos de auditoría de las debilidades no detectadas, si hay, podría ser tanto material como predominante.
- 2.2.3** El informe de examen o revisión de los profesionales sobre la efectividad de procedimientos de control debe incluir los siguientes elementos:
- Un título apropiado y distintivo, claramente distinguir el informe de cualquier otro tipo de informe no sujeto a estándares de auditoría
 - Identificar los destinatarios a quien se dirige el informe, de acuerdo a los términos en la carta de auditoría o carta de encargo.

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

2.2 Contenidos Requeridos del Informe de Trabajo de Auditoría cont.

- Identificar la parte responsable, incluyendo una declaración de la parte responsable para la materia.
- Descripción del alcance del trabajo de auditoría, el nombre de la entidad o componente de la entidad que relata la materia, incluyendo:
 - Identificación o descripción del área de actividad
 - Criterios usados como base para la conclusión de los profesionales
 - Fecha o periodo de tiempo en que el trabajo, evaluación o medida relata la materia
 - Declaración que el mantenimiento de una estructura de control interno efectiva, incluyendo procedimientos de control para el área de actividad, es responsabilidad de la gerencia
- Declaración identificando la fuente de la representación de la gerencia sobre la efectividad de los procedimientos de control
- Declaración que los profesionales han realizado el trabajo de auditoría para expresar una opinión sobre la efectividad de los procedimientos de control
- Identificación del propósito (ej.: Objetivos de auditoría de SI) para lo que se han preparado los informes de los profesionales y titulados para confiar en él, y una renuncia de responsabilidad para su uso para cualquier otro propósito o por cualquier otra persona
- Descripción del criterio o rechazo de la fuente del criterio. Además, los profesionales deben considerar revelar:
 - Cualquier interpretación significativa hecha para aplicar el criterio
 - Métodos de medición utilizados cuando el criterio permite una elección entre un número de métodos de medición.
 - Cambios en los métodos de medición estándar utilizados
- Declaración del trabajo de auditoría ha sido realizado de acuerdo con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables. Cualquier no cumplimiento con estos estándares debe ser mencionado explícitamente en el informe.
- Además detalles explicativos sobre las variables que afectan a la aseguramiento proporcionada y otra información como adecuada
- Hallazgos, conclusiones y recomendaciones para las acciones correctivas e incluir la respuesta de la gerencia. Para cada respuesta de la gerencia, los profesionales deben obtener información sobre las acciones propuestas para implementar o direccionar las recomendaciones informadas y la implementación planificada o fechas de acción.
 - La gerencia responsable puede decidir aceptar el riesgo de no corregir una condición informada por coste, complejidad de la acción correctiva o de otras consideraciones. El comité de directores (o los encargados del Gobierno) deben estar informados de las recomendaciones por las que la gerencia acepta el riesgo de no corregir la situación informada.
 - Si los profesionales y el auditado no están de acuerdo sobre una recomendación particular o comentario de auditoría, las comunicaciones del trabajo pueden mostrar ambas posiciones y las razones del desacuerdo. Los comentarios escritos del auditado

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

2.2 Contenidos Requeridos del Informe de Trabajo de Auditoría cont.

pueden ser incluidos como un anexo al informe del trabajo. Alternativamente, la visión del auditado se puede presentar en el cuerpo del informe o en una carta de introducción. La gerencia ejecutiva, o los encargados del Gobierno, deben tomar una decisión sobre qué punto de vista apoyan.

- Un párrafo indicando que debido a las limitaciones inherentes de cualquier control interno, pueden ocurrir y no ser detectadas declaraciones erróneas debido a errores o fraude. Además, el párrafo debe indicar que las proyecciones de cualquier evaluación de los controles internos sobre los informes financieros a periodos futuros está sujeto al riesgo que los controles internos puedan volverse inadecuados por los cambios en las condiciones, o que el nivel de cumplimiento con las políticas o procedimientos podría deteriorar. Un trabajo de auditoría no está diseñado para detectar toda debilidad en los procedimientos de control porque no se realiza continuamente durante el periodo y las pruebas realizadas sobre los procedimientos de control son en base a muestras.
- Un resumen del trabajo realizado, que ayudara a los usuarios del informe a comprender mejor la naturaleza de la aseguramiento comunicada
- Una expresión de opinión acerca de si, en todos los aspectos materiales, el diseño y/o operación de los procedimientos de control en relación al área de actividad fueron efectivos. Cuando la opinión de los profesionales es cualificada, se debe incluir un párrafo describiendo las razones de la cualificación.
- Cuando sea apropiado, referenciar cualquier otro informe separado que deba ser considerado, como un informe separado que comunique las vulnerabilidades de seguridad que está protegido frente a difusión y debe ser distribuido a listas restrictas de destinatarios.
- Fecha de emisión del informe del trabajo de auditoría. En muchos casos la fecha del informe se basa en la fecha del evento. Es recomendable mencionar también las fechas en que fue realizado el trabajo de auditoría, si no se menciona ya en el resumen del trabajo realizado.
- Nombres de las personas o entidad responsable del informe, firmas adecuadas y lugares.

- 2.2.4** Los informes de conformidad sobre procedimientos debe ser en forma de procedimientos y hallazgos. El informe debe contener los siguientes elementos:
- Título adecuado y distintivo, distinguir claramente el informe de cualquier otro tipo de informe no sujeto a estándares de auditoría.
 - Identificar la parte responsable, incluyendo una declaración de la parte responsable de la materia
 - Declarar que el trabajo de auditoría se ha realizado de acuerdo con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables. Cualquier no cumplimiento con estos estándares debe ser mencionado explícitamente en el informe.
 - Identificación de la materia (o la afirmación escrita relacionada al mismo) y el propósito (ej.: objetivos de auditoría de SI) del trabajo de auditoría.

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

2.2 Contenidos Requeridos del Informe de Trabajo de Auditoría cont.

- Declarar que los procedimientos realizados fueron los acordados por las partes responsables identificadas en el informe
- Declarar que la suficiencia de los procedimientos es responsabilidad única de las partes responsables y un rechazo de responsabilidad de la suficiencia de esos procedimientos
- Una lista de procedimientos realizados (o referencia a los mismos)
- Una descripción de los hallazgos, incluyendo suficiente detalle de errores y excepciones encontrados
- Declarar que los profesionales solo realizaron la conformidad sobre procedimientos y, por tanto, no se expresa aseguramiento
- Declarar que si los profesionales hubieran realizado procedimientos adicionales, podrían haber surgido otras materias a la atención de los profesionales y hubiera sido reportada
- Declarar las restricciones sobre el uso del informe ya que es de uso único por las partes específicas
- Declarar que el informe solo se refiere a los elementos específicos y que no se extiende mas allá de ellos
- Referencias a cualquier otro informe separado que se pueda considerar
- Fecha de realización del informe del trabajo de auditoría. En muchas instancias, la fecha del informe se basa en la fecha del evento. Se recomienda mencionar también las fechas en que se realizó el trabajo de auditoría, si no se menciona ya en el resumen del trabajo realizado.
- Nombres de personas o entidad responsable del informe, firmas adecuadas y locales.

2.2.5 Hay dos tipos de reporte de examen:

- **Informes directos**—Sobre la materia en lugar de sobre una aserción. El informe deberá hacer referencia solo al sujeto del trabajo y no debe hacer ninguna referencia a la aserción de la gerencia sobre la materia.
- **Informes indirectos**—Basados en aserciones de la gerencia sobre la materia.

Se puede encontrar más ayuda detallada sobre la diferencia entre informe directo e indirecto en el Estándar 1007 Afirmaciones.

2.3 Eventos Posteriores

- 2.3.1** A veces los eventos suceden, tras el momento o periodo de tiempo en que la materia fue probada pero antes de la fecha del informe de los profesionales, que tiene un efecto material sobre la materia y por tanto requiere ajustes o revelación en la presentación de la materia o en las afirmaciones. Estos sucesos se referencian como eventos posteriores. En la realización de un trabajo de auditoría, los profesionales deben considerar la información sobre eventos posteriores que llegan a su atención. Sin embargo los profesionales no tienen responsabilidad de detectar los eventos posteriores.
- 2.3.2** Los profesionales deben consultar con la gerencia a si son conscientes de los eventos posteriores, tras la fecha del informe de los profesionales, que podría tener un efecto material sobre la materia o afirmaciones.
-

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

2.4 Comunicación adicional

- 2.4.1** Los profesionales deben discutir los contenidos del borrador del informe con la gerencia en el área antes de finalizar y entregar, e incluir la respuesta a los hallazgos, conclusiones y recomendaciones de la gerencia en el informe final, si es aplicable.
- 2.4.2** Los profesionales deben comunicar deficiencias significativas y debilidades materiales en el entorno de control a los encargados del Gobierno y, si es aplicable, a la autoridad responsable. También deben concluir en el informe que han sido comunicados.
- 2.4.3** Los profesionales deben comunicar a la gerencia las deficiencias de control interno que son menos significativas pero más que [inconsecuentes](#). En esos casos, los encargados del Gobierno o la autoridad responsable deben ser notificados por los profesionales que tales deficiencias de control interno se han comunicado a la gerencia.
- 2.4.4** Los profesionales deben obtener representación escrita de la gerencia reconociendo, al menos, las siguientes afirmaciones:
- La responsabilidad de la gerencia para establecer y mantener los controles internos adecuados y efectivos, incluyendo sistemas de finanza interna y controles administrativos sobre actividades operativas y SI bajo revisión, y las actividades para identificar todas las leyes, reglas y regulaciones, que gobiernan el área del sujeto bajo revisión, y para asegurar el cumplimiento con ellos.
 - Toda información solicitada relevante para los objetivos de trabajo fue proporcionada al equipo de trabajo incluyendo, pero sin limitar:
 - Registros, datos relacionados, ficheros electrónicos e informes
 - Políticas y procedimientos
 - Personal pertinente
 - Resultados de auditorías, revisiones y asignaciones de SI internos y externos relevantes
 - No ha sucedido ningún evento o se ha descubierto ninguna materia desde el final del trabajo de campo que pudiera tener un efecto material sobre el trabajo
 - La gerencia no tiene conocimiento de ningún fraude o sospecha de fraude, irregularidad o acto ilegal relacionado al área bajo revisión, incluyendo gerencia y empleados con responsabilidad en el control interno aun no divulgado.
 - La gerencia no tiene conocimiento de ninguna alegación de fraude o sospecha de fraude, irregularidades y actos ilegales que afecten el área bajo revisión recibida en comunicación por empleados, clientes, contratistas u otros aun no concluidos
 - Conocimiento de responsabilidad del diseño e implementación de programas y controles para prevenir y detectar fraude, irregularidades y actos ilegales.
-

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

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: Solo 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.
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.
1401 Reportes	Los profesionales de auditoría y aseguramiento de SI deberán presentar un informe para comunicar los resultados una vez finalizado el trabajo, incluyendo: • Identificación de la empresa, destinatarios y cualquier restricción al contenido y circulación. • El alcance, objetivos de trabajo, periodo de cobertura y naturaleza, tiempos y alcance de los trabajos realizados • Los hallazgos, conclusiones y recomendaciones • Cualquier cualificación o limitación al alcance que el profesional de auditoría y aseguramiento de SI tiene respecto al trabajo • Firma, fecha y distribución de acuerdo a los términos de la Estatuto de Auditoría o carta de compromiso Los profesionales de auditoría y aseguramiento de SI velaran por que los hallazgos del informe de auditoría estén soportados por evidencias de auditoría suficientes y adecuadas.

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

Título del Estándar	Declaración Estándar Relevante
1402 Seguimiento	Los profesionales de auditoría y aseguramiento de SI monitorearán la información relevante para concluir si la gerencia ha planeado/tomado apropiadamente, acciones oportunas para direccionar los hallazgos y recomendaciones reportados.

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
EDM05 Asegurar la transparencia hacia las partes interesadas.	Estar seguro que la comunicación a los interesados es efectiva y a tiempo, y la base para el informe se ha establecido para aumentar el rendimiento, identificar áreas para mejorar y confirmar que los objetivos y estrategias relacionados con TI están en línea con la estrategia de la empresa.
MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad.	Proporcionar transparencia del desarrollo, cumplimiento y dirigir el logro de los objetivos.
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 desde auditoría y aseguramiento de SI:

- Colegas dentro de la empresa
- Gerentes
- Órganos de Gobierno dentro de la empresa, ejemplo, comité de auditoría
- Organizaciones profesionales
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías)

Guía de Auditoría y Aseguramiento de SI 2401 Reportes

4. Terminología

Término	Definición
Deficiencia inconsecuente	Una deficiencia es inconsecuente si una persona razonable podría concluir, tras considerar la posibilidad de mas deficiencias no detectadas, que las deficiencias, ya sean individuales o en conjunto con otras deficiencias, podrían ser claramente triviales a la material. Si una persona razonable pudiera no alcanzar tal conclusión respecto a una deficiencia particular, esa deficiencia es más que intrascendente.
Evidencia apropiada	La medida de calidad de la evidencia
Evidencia suficiente	La medida de la cantidad de evidencia; apoya todas las cuestiones materiales al objetivo y alcance de la auditoría. Ver evidencia.

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

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	The Weinman Group, USA

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

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 proporcionar ayuda al profesional de auditoría y aseguramiento de SI a monitorizar si la gerencia ha tomado las acciones apropiadas y oportunas sobre las recomendaciones reportadas y hallazgos de auditoría. 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 1401 Reportes 1.2.2 Estándar 1402 Actividades de seguimiento
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 Proceso de seguimiento 2.2 Acciones propuestas de la Gerencia 2.3 Asumir los riesgos de no tomar acciones correctivas 2.4 Procedimientos de seguimiento 2.5 Tiempos y planificación de las actividades de seguimiento 2.6 Naturaleza y oportunidad de las actividades de seguimiento 2.7 Aplazar las actividades de seguimiento
-------------------------	--

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

2.8 Formas de respuestas de seguimiento

2.9 Seguimiento de los profesionales sobre recomendaciones de auditoría externas

2.10 Informe de actividades de seguimiento

2.1 Proceso de Seguimiento

- 2.1.1** Las [actividades de seguimiento](#) realizadas por los profesionales es un proceso que ellos determinan la adecuación, efectividad y tiempos de las acciones tomadas por la gerencia sobre las observaciones y recomendaciones informadas, incluyendo las realizadas por auditores externos y otros.
- 2.1.2** Se debe establecer un proceso de seguimiento para ayudar a proporcionar garantía razonable de que cada revisión realizada por los profesionales proporciona beneficio óptimo a la empresa, requiriendo que los acuerdos sobre las conclusiones de las revisiones se implementan de acuerdo con los compromisos de la gerencia o la gerencia (ejecutiva) y reconoce y comprende el riesgo de retrasar o no implementar los resultados y /o recomendaciones propuestas.
-

2.2 Acciones Propuestas de la Gerencia

- 2.2.1** Como parte de sus discusiones con el auditado, los profesionales deben obtener un acuerdo sobre los resultados del trabajo de auditoría y sobre un plan de acción para mejorar las operaciones, como se requiera.
- 2.2.2** Los profesionales deben discutir con la gerencia las acciones propuestas para implementar o direccionar las recomendaciones informadas y comentarios de auditoría. Estas acciones propuestas deben ser proporcionadas a los profesionales y deben ser registradas como una respuesta de la gerencia en el informe final con una implementación comprometida y/o fecha de acción.
- 2.2.3** Si los profesionales y el auditado llegan a un acuerdo sobre las acciones propuestas, los profesionales deben iniciar los procedimientos para las actividades de seguimiento, como se detalla en la sección 2.4.
-

2.3 Asumir los Riesgos de No Tomar Acciones Correctivas

- 2.3.1** La gerencia (Ejecutiva) puede decidir aceptar el riesgo de no corregir la condición informada por coste, complejidad de la acción correctiva o por otras consideraciones. El comité (o los encargados del gobierno) deben ser informados de la decisión de la gerencia (ejecutiva) sobre todas las observaciones y recomendaciones del trabajo significantes para los que la gerencia acepta el riesgo de no corregir la situación informada.
- 2.3.2** Cuando los profesionales creen que el auditado ha aceptado un nivel de riesgo residual que es inapropiado para la empresa, deben discutir la materia con la gerencia de auditoría y aseguramiento de SI y la gerencia ejecutiva. Si los profesionales permanecen en desacuerdo con la decisión respecto al riesgo residual, Junto con la gerencia ejecutiva, deben informar la materia al comité (o encargados del gobierno) para su resolución.
- 2.3.3** La aceptación de riesgo se debe documentar y aprobar formalmente por la gerencia ejecutiva y comunicada a los encargados del gobierno.
-

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

2.4 Procedimientos de Seguimiento	2.4.1 Los procedimientos de actividades de seguimiento deben establecerse e incluir: • El registro de un rango de tiempo en que la gerencia debe responder a las recomendaciones acordadas • Una evaluación de las respuestas de la gerencia • Una verificación de la respuesta, si es adecuada (referirse a la sección 2.6) • Seguimiento del trabajo, si es adecuado • Procedimiento de comunicación que escale respuestas excepcionales y no satisfactorias y/o acciones para el nivel adecuado de la gerencia y encargados del gobierno • Proceso para obtener asunción de la gerencia del riesgo asociado, en el caso que la acción correctiva se retrase o no se proponga para implementar. 2.4.2 Un sistema de rastreo automatizado o base de datos puede ayudar a llevar a cabo las actividades de seguimiento. 2.4.3 Los factores que se deben considerar al determinar los procedimientos adecuados de seguimiento son: • La importancia y el impacto de los hallazgos y recomendaciones • Cualquier cambio en el entorno de SI que pueda afectar la importancia y el impacto de los hallazgos y recomendaciones • La complejidad de corregir la situación reportada • Tiempo, coste y esfuerzo necesario para corregir la situación reportada • El efecto si corregir la situación reportada fallase. 2.4.4 La responsabilidad de las acciones de seguimiento, informar y escalar debe ser definido en la carta de auditoría.
2.5 Tiempos y Planificación de las Actividades de Seguimiento	2.5.1 La planificación de las actividades de seguimiento debe tener en cuenta la importancia de los hallazgos informados y el efecto se no tomar las acciones correctivas. La planificación de las actividades de seguimiento en relación al informe original es una materia de juicio profesional dependiente de un número de consideraciones, como la naturaleza o magnitud de riesgos asociados y costes para la empresa. 2.5.2 Porque son parte integral del proceso de auditoría de SI, las actividades de seguimiento deben ser planificadas, junto con otros pasos necesarios para realizar cada revisión. Actividades de seguimiento específicas y la planificación de tales actividades puede estar influenciada por el grado de dificultad, el riesgo y exposición involucrada, los resultados de la revisión, el tiempo necesario para implementar acciones correctivas, etc., y puede establecerse en consulta con la gerencia. 2.5.3 Los acuerdos sobre los resultados relacionados con cuestiones de alto riesgo debe ser seguido tan pronto tras la fecha debida para la acción y puede ser monitoreada progresivamente. 2.5.4 La implementación de todas las repuestas de gerencia puede ser seguida de forma regular (ej.: cada cuatrimestre) para diferentes trabajos de auditoría juntos, aunque la implementación de fechas comprometidas por la gerencia puede ser diferente. Otra aproximación es seguir respuestas de la gerencia individuales de acuerdo a la fecha debida acordada con la gerencia.

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

2.6 Naturaleza y Oportunidad de las Actividades de Seguimiento	2.6.1	Se data un rango de tiempo al auditado normalmente dentro del cual responder con los detalles de las acciones tomadas para implementar las recomendaciones.
	2.6.2	Se debe evaluar la respuesta de la gerencia detallando las acciones tomadas, si es posible, por los profesionales que realizaron la revisión original. Cuando sea posible, se debe obtener la evidencia de auditoría de las acciones tomadas.
	2.6.3	Cuando la gerencia proporciona información sobre las acciones tomadas para implementar las recomendaciones y los profesionales tengan dudas sobre la información proporcionada o la efectividad de la acción tomada, se deben llevar a cabo pruebas adecuadas u otros procedimientos de auditoría para confirmar la posición o estado certero antes de concluir además de las actividades de seguimiento.
	2.6.4	Como parte de las actividades de seguimiento, los profesionales deben evaluar si las recomendaciones no implementadas siguen siendo relevantes o tienen mayor importancia. Los profesionales pueden decidir que la implementación de una recomendación particular ya no es apropiada. Esto podría suceder cuando cambian los sistemas de aplicación, donde los controles compensatorios se han implementado o donde los objetivos o prioridades del negocio han cambiado de forma que se eliminan o se reducen significativamente el riesgo original. De la misma forma, un cambio en el entorno de SI puede aumentar la importancia del efecto de una observación previa y la necesidad de su resolución.
	2.6.5	Podría ser necesario planificar un trabajo de seguimiento para verificar la implementación de acciones críticas y/o importantes.
	2.6.6	La opinión de los profesionales sobre respuestas o acciones de la gerencia no satisfactorias se debe comunicar al nivel adecuado de la gerencia.
2.7 Posponer las Actividades de Seguimiento	2.7.1	Los profesionales son responsables de planificar las actividades de seguimiento como parte de la planificación del trabajo a desarrollar. La planificación de seguimientos debe basarse en el riesgo y exposición en cuestión, así como al grado de dificultad y tiempo necesarios para implementar las acciones correctivas.
	2.7.2	También pueden haber casos donde los profesionales juzgan las respuestas orales o por escrito de la gerencia mostrando que la acción tomada es suficiente cuando se compara con la importancia relativa de la observación o recomendación del trabajo. En esos casos, las actividades de verificación de seguimiento actual pueden realizarse como parte del próximo trabajo que se realice con el sistema o tema relevante.
2.8 Formas de Respuesta de Seguimiento	2.8.1	La manera más efectiva de recibir respuestas del seguimiento por la gerencia es por escrito, porque ayuda a reforzar y confirmar la responsabilidad de la gerencia de la acción de seguimiento y progresos realizados. Además, las respuestas escritas garantizan un registro preciso de acciones, responsabilidades y estado actual. Las respuestas orales pueden recibirse también y registrarse por los profesionales y, cuando sea posible, aprobadas por la gerencia. También se puede suministrar con la respuesta la

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

2.8 Formas de Respuesta de Seguimiento cont.	prueba de la acción o implementación de las recomendaciones. 2.8.2 Los profesionales deben pedir y/o recibir actualizaciones periódicas de la gerencia responsable de implementar las acciones acordadas para evaluar el progreso que la gerencia ha realizado, particularmente en relación con cuestiones de alto riesgo y acciones correctivas con largos plazos de entrega.
2.9 Seguimiento de los Profesionales Sobre Recomendaciones de Auditoría Externas	2.9.1 Dependiendo del alcance y términos del trabajo de auditoría y de acuerdo con los estándares de auditoría de SI relevantes, los profesionales externos pueden contar con los profesionales internos para el seguimiento en sus recomendaciones acordadas. Las responsabilidades en relación a este seguimiento pueden determinarse en la carta de auditoría o carta de compromiso.
2.10 Informe de Actividades de Seguimiento	2.10.1 Se debe presentar al nivel adecuado de la gerencia y a los encargados del gobierno un informe sobre el estado de las acciones correctivas acordadas que aparecen en los informes del trabajo de auditoría, incluyendo las recomendaciones acordadas no implementadas. (ej.: comité de auditoría). 2.10.2 Si, durante un trabajo de auditoría posterior, los profesionales encuentran que las acciones correctivas que la gerencia había informado como 'implementadas' no fueron implementadas, deben comunicar esto al nivel adecuado de la gerencia y a los encargados del gobierno. Si es apropiado, el profesional debe obtener un plan de acción correctivo actual y fecha de implementación planificada. 2.10.3 Cuando todas las acciones correctivas acordadas se han implementado, se puede enviar un informe detallando todas las acciones implementadas y/o completadas a la gerencia ejecutiva y a los encargados del gobierno.

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 ISACA que están directamente soportados por esta guía • Las declaraciones estándar más relevantes para esta guía

Nota: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

Título del Estándar	Declaración Estándar Relevante
1401 Reportes	Los profesionales de auditoría y aseguramiento de SI deberán presentar un informe para comunicar los resultados una vez finalizado el trabajo, incluyendo: • Identificación de la empresa, destinatarios y cualquier restricción al contenido y circulación. • El alcance, objetivos de trabajo, periodo de cobertura y naturaleza, tiempos y alcance de los trabajos realizados • Los hallazgos, conclusiones y recomendaciones • Cualquier cualificación o limitación al alcance que el profesional de auditoría y aseguramiento de SI tiene respecto al trabajo • Firma, fecha y distribución de acuerdo a los términos de la carta de auditoría o carta de compromiso Los profesionales de auditoría y aseguramiento de SI se aseguran que los hallazgos se apoyan en el informe de auditoría por evidencia suficiente, confiable y relevante.
1402 Actividades de seguimiento	Los profesionales de auditoría y aseguramiento de SI monitorizarán la información relevante para concluir si la gerencia ha planeado/tomado apropiadamente, acciones oportunas para direccionar los hallazgos y recomendaciones reportados.

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.
EDM02 Asegurar la entrega de beneficios.	Asegurar el valor óptimo de iniciativas, servicios y activos habilitados de TI; Entrega de soluciones y servicios eficientes en costes; y una imagen de costes fiable y precisa y beneficios probables para que las necesidades del negocio estén soportadas efectiva y eficientemente.

Guía de Auditoría y Aseguramiento de SI 2402 Actividades de Seguimiento

Procesos de COBIT 5	Propósito de los Procesos
EDM03 Asegurar la optimización del riesgo.	Asegurar que el riesgo empresarial relacionado con TI no excede el riesgo aceptado y la tolerancia de riesgo, el impacto de riesgo de TI al valor de la empresa está identificado y gestionado, y la posibilidad de fallos de cumplimiento esta minimizada.
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 desde auditoría y aseguramiento de SI:

- Colegas dentro de la empresa
- Gerentes
- Órganos de gobierno dentro de la empresa, ejemplo, comité de auditoría
- Organizaciones profesionales
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías)

4. Terminología

Termino	Definición
Actividad de seguimiento	Un proceso por el cual los auditores internos evalúan la adecuación, efectividad y oportunidad de las acciones tomadas por la gerencia sobre las observaciones y recomendaciones reportadas, incluyendo las realizadas por los auditores externos y otros. Fuente: Instituto de Auditores Internos—Practice Advisory 2500.A1-1; Copyright © por The Institute of Internal Auditors, Inc. Todos los derechos reservados.
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 todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.