

## 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](http://www.isaca.org/glossary).

**Aclaración:** ISACA ha diseñado esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado exitoso. La publicación no debe considerarse como incluyente de cualquier procedimiento y pruebas o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a obtener los mismos resultados. Para determinar la conveniencia de cualquier procedimiento o prueba específica, los profesionales de controles deben aplicar su propio juicio profesional a las circunstancias de control específicas presentadas por los sistemas particulares o entorno de SI.

El Comité de Estándares Profesionales y Administración de Carreras de ISACA, en Inglés "ISACA Professional Standards and Career Management Committee" (PSCMC) se ha comprometido a una amplia consulta en la preparación de estándares y guías. Antes de emitir cualquier documento, se emite internacionalmente un borrador de la norma para comentar por el público general. Los comentarios pueden también presentarse a la atención del director de desarrollo de estándares profesionales por correo electrónico ([standards@isaca.org](mailto:standards@isaca.org)), fax (+1.847. 253.1443) o correo postal (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

### ISACA 2013-2014 Professional Standards and Career Management Committee

Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP	University of North Texas, USA
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Todd Weinman	TheWeinman Group, USA

# Guía de Auditoría y Aseguramiento de SI 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.

Título del Estándar	Declaración Estándar Relevante
1201 Planificación de la asignación	<p>Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir:</p> <ul style="list-style-type: none"> <li>• Objetivo(s), alcance, línea de tiempo y entregables</li> <li>• Cumplimiento con leyes aplicables y estándares de auditoría profesionales</li> <li>• Uso de enfoque basado en riesgos, cuando sea adecuado</li> <li>• Cuestiones específicas del trabajo</li> <li>• Requisitos de documentación y presentación de informes.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>• La naturaleza, objetivos, línea de tiempo y recursos requeridos del trabajo</li> <li>• Tiempos y grado de los procedimientos de auditoría para completar el trabajo</li> </ul>
1202 Evaluación de Riesgos en la Planificación de Auditoría	<p>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.</p> <p>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.</p>
1203 Desempeño y Supervisión	<p>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.</p>
1204 Materialidad	<p>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.</p>

# 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	<p>Un proceso utilizado para identificar y evaluar riesgos y sus efectos potenciales.</p> <p>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.</p> <p>Los análisis de riesgos se utilizan también para gestionar la ejecución de los proyectos y el riesgo en beneficio del proyecto.</p>
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	<ol style="list-style-type: none"><li data-bbox="370 205 1425 449">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.</li><li data-bbox="370 449 1425 512">2. Una descripción de alto nivel del trabajo de auditoría a realizar en un cierto periodo de tiempo.</li></ol>
Riesgo de Auditoría	<p data-bbox="370 529 1425 562">El riesgo de llegar a una conclusión incorrecta basada en los resultados de la auditoría.</p> <p data-bbox="370 562 1425 596">Los tres componentes de riesgo de auditoría son:</p> <ul data-bbox="370 596 1425 693" style="list-style-type: none"><li data-bbox="370 596 1425 630">• Riesgo de control</li><li data-bbox="370 630 1425 663">• Riesgo de detección</li><li data-bbox="370 663 1425 693">• Riesgo inherente</li></ul>

## 5. Fecha de Vigencia

<b>5.1 Fecha de Vigencia</b>	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.
------------------------------	--