# 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 Ingles Certified Information Systems Auditor® (CISA®) la designación de requisitos. El incumplimiento de estos estándares puede dar lugar a una investigación sobre la conducta del poseedor del certificado CISA por la Junta Directiva de ISACA o el comité apropiado y, en última instancia, en una acción disciplinaria.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en sus trabajos, donde sea apropiado, indicando que el trabajo ha sido realizado de acuerdo con los estándares de auditoría y aseguramiento de los SI de ISACA o de otros posibles estándares aplicables.

ITAF™, un marco de trabajo de prácticas profesionales para auditoría y aseguramiento de SI, proporciona múltiples niveles de dirección:

- **Estándares**, divididos en tres categorías:
  - Estándares generales (series 1000)-Son los principios rectores bajo los que opera la profesión de auditoría y aseguramiento de SI. Aplican a la realización de todas las tareas, y hacen frente a la ética, independencia, objetividad y debida diligencia del profesional de auditoría y aseguramiento de SI, así como los conocimientos, competencia y habilidades. Las declaraciones de los estándares (en **negrita**) son obligatorias.
  - Estándares de desempeño(series 1200)-Tienen que ver con la forma en que se conduce la asignación, tales como planificación y supervisión, definición del alcance, riesgos y materialidad, la movilización de recursos, supervisión y administración de asignaciones, evidencias de auditoría y aseguramiento, y el ejercicio de su juicio profesional y debida diligencia.
  - Estándares de presentación de informes (series 1400)-Direccionan los tipos de informes, medios de comunicación y la información comunicada.
- **Guías**, apoyan a los estándares y también se dividen en tres categorías:
  - Guías generales (series 2000).
  - Guías de rendimiento (series 2200).
  - Guías de presentación de informes (series 2400).
- **Herramientas y técnicas**, proporcionan una guía adicional para los profesionales de auditoría y aseguramiento de SI, por ej., documento técnico (white paper), programas de auditoría / aseguramiento de SI, los productos de la familia de COBIT® 5.

Se proporciona un glosario en línea de los términos utilizados en ITAF en *www.isaca.org/glossary*.

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

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

# 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.

**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 irrecuperables, 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

 

**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 proporcional 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

 

**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 (calculo) 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 practicas 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:<br>• La naturaleza, objetivos, línea de tiempo y recursos requeridos del trabajo.<br>• 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.<br><br>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.<br><br>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.<br><br>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.<br><br>Los profesionales de auditoría y aseguramiento revelaran lo |

| Titulo del Estándar | Declaración Estándar Relevante |
|---|---|
| | siguiente en el informe de auditoría:<br>• Ausencia de controles o controles inefectivos.<br>• Importancia de la deficiencia de los controles.<br>• 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.<br><br>Los profesionales de auditoría y aseguramiento de SI deberán mantener una actitud de escepticismo profesional durante el trabajo.<br><br>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. |

 

**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.<br><br>La debilidad en el control se considera material si la ausencia de control resulta en fallo para proporcional seguridad razonable que el objetivo de control se alcanzara. Una debilidad clasificada como material implica:<br>• Los controles no están en su lugar y/o no se usan y/o son inadecuados.<br>• Se garantiza la escalada.<br><br>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.<br><br>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:<br>• Riesgo de control.<br>• Riesgo de detección.<br>• 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.