# 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 Ingles 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 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 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 optimo 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.

---

**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

 

**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.

 

| Titulo 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:<br>• Identificación de la empresa, destinatarios y cualquier restricción al contenido y circulación.<br>• El alcance, objetivos de trabajo, periodo de cobertura y naturaleza, tiempos y alcance de los trabajos realizados<br>• Los hallazgos, conclusiones y recomendaciones<br>• Cualquier cualificación o limitación al alcance que el profesional de auditoría y aseguramiento de SI tiene respecto al trabajo<br>• Firma, fecha y distribución de acuerdo a los términos de la carta de auditoría o carta de compromiso<br><br>Los profesionales de auditoria y aseguramiento de SI se aseguraran que los hallazgos se apoyan en el informe de auditoria por evidencia suficiente, confiable y relevante. |
| 1402 Actividades de seguimiento | Los profesionales de auditoria y aseguramiento de SI monitorizaran 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. |

 

| 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.<br>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.