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 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 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'.

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

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

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

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 critica 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

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 explicita 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

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

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

2.8 Informes Externos cont.

información reportada, a menos que se prevenga por regulaciones aplicables o circunstancias especificas del contrato de auditoría. Ejemplos de circunstancias especificas 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 haces 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 especificas 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.

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)

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.