Norma 1207 de Auditoria e Garantia de SI Irregularidade e Atos Ilegais

A natureza especializada da auditoria e garantia de sistemas de informação (SI) e a capacidade necessária para realizar essas contratações requerem o estabelecimento de normas que se apliquem especificamente à auditoria e garantia de SI. O desenvolvimento e a disseminação das normas de auditoria e garantia de SI são fundamentais como contribuição profissional da ISACA® para a comunidade de auditoria.

As normas de auditoria e garantia de SI definem requisitos obrigatórios para auditoria, emissão de relatórios e orientações sobre:

- Profissionais de auditoria e garantia de SI no nível mínimo de desempenho aceitável exigido para cumprir as responsabilidades profissionais estabelecidas no Código de Ética Profissional da ISACA;
- A gerência e outras partes interessadas sobre as expectativas da profissão no que se refere às atividades daqueles que a exercem;
- Os requisitos necessários para os detentores da certificação Certified Information Systems Auditor® (CISA®) (Auditor Certificado em Sistemas de Informação). A não conformidade com essas normas pode resultar numa investigação da conduta do detentor da CISA pelo Conselho de Administração da ISACA ou pelo comitê apropriado e, finalmente, em ação disciplinar.

Profissionais de auditoria e garantia devem incluir uma declaração em seu trabalho, quando apropriado, de que a contratação foi realizada de acordo com as normas de auditoria e garantia de SI da ISACA ou outras normas profissionais aplicáveis.

A estrutura *ITAF*™ para o profissional de auditoria e garantia de SI apresenta diversos níveis de diretrizes:

- **Normas**, divididas em três categorias:
  - Normas gerais (série 1000) - são os princípios norteadores sob os quais funciona a profissão de auditoria e garantia de SI. As normas se aplicam à realização de todas as tarefas, e lidam com a ética, a independência, a objetividade e o devido cuidado, bem como conhecimento, competência e habilidade do profissional de auditoria e garantia de SI. As declarações de normas (em **negrito**) são obrigatórias.
  - Normas de desempenho (série 1200) – tratam da realização da contratação, por exemplo, planejamento e supervisão, definição de escopo, risco e materialidade, mobilização de recursos, gestão de supervisão e tarefa, evidência de auditoria e garantia, e o exercício de julgamento profissional, bem como o devido cuidado.
  - Normas de relatório (série 1400) - abordam os tipos de relatórios, os meios de comunicação e as informações comunicadas
- **Diretrizes**, em apoio às normas, e também divididas em três categorias:
  - Diretrizes gerais (série 2000)
  - Diretrizes de desempenho (série 2200)
  - Diretrizes de relatório (série 2400)
- **Ferramentas e técnicas**, oferecendo orientação adicional para profissionais de auditoria e garantia de SI, por exemplo, documentos, programas de auditoria/garantia de SI, a família de produtos COBIT® 5

Um glossário on-line de termos usados na ITAF é fornecido em *www.isaca.org/glossary*.

Ressalva: A ISACA desenvolveu este guia visando definir o nível mínimo de desempenho aceitável exigido para dar resposta às responsabilidades profissionais estabelecidas no Código de Ética Profissional da ISACA. A ISACA não oferece qualquer garantia de que o uso deste produto irá assegurar um resultado bem-sucedido. A publicação não deve ser considerada parte integrante de quaisquer procedimentos e testes apropriados, ou de outros procedimentos e testes também voltados para a obtenção dos mesmos resultados. Ao determinar a propriedade de qualquer procedimento ou teste específico, profissionais de controle devem aplicar seu próprio juízo profissional às circunstâncias específicas de controle apresentadas por determinados sistemas ou ambientes de SI.

O ISACA Professional Standards and Career Management Committee (Comitê de Normas Profissionais e Gestão de Carreira, PSCMC) está comprometido em realizar uma ampla consulta na preparação de normas e diretrizes. Antes de divulgar qualquer documento, uma versão preliminar é divulgada internacionalmente para ser submetida à avaliação pública. As avaliações também podem ser enviadas aos cuidados do diretor de desenvolvimento de normas profissionais por e-mail (*standards@isaca.org*), fax (+1.847. 253.1443) ou correio (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

Norma 1207 de Auditoria e Garantia de SI – Irregularidade e Atos Ilegais

Declarações

1207.1 **Profissionais de auditoria e garantia de SI deverão considerar o risco de irregularidades de atos ilegais durante a contratação.**

1207.2 **Profissionais de auditoria e garantia de SI deverão manter uma atitude de ceticismo profissional durante a contratação.**

1207.3 **Profissionais de auditoria e garantia de SI deverão documentar e comunicar qualquer irregularidade material ou atos ilegais à parte adequada de maneira oportuna.**

Aspectos principais

Profissionais de auditoria e garantia de SI devem:

- Reduzir o risco de auditoria a um nível aceitável no planejamento e na realização da contratação:
  - Estando ciente de que erros materiais, deficiências de controle ou distorções de dados devidos a irregularidades e atos ilegais podem existir, independentemente da avaliação do risco de irregularidades e atos ilegais.
  - Adquirindo um entendimento da empresa e de seu ambiente, incluindo controles internos destinados a impedir ou detectar irregularidades de atos ilegais que sejam relevantes ao assunto, escopo e objetivos da contratação
  - Obtendo evidência suficiente e apropriada para determinar se a gestão ou outras pessoas dentro da empresa têm conhecimento de quaisquer irregularidades ou atos ilegais reais, supostos ou alegados.
- Considerar relacionamentos incomuns ou inesperados que possam indicar um risco de erros materiais, deficiências de controle ou distorções nos dados devidos a irregularidades e atos ilegais ao realizar procedimentos de auditoria,
- Desenvolver e executar procedimentos para testar a adequação de controles internos e o risco de que a gestão se sobreponha a esses controles destinados a impedir ou detectar irregularidades e atos ilegais.
- Avaliar se erros identificados, deficiências de controle ou distorções nos dados podem ser indicativos de uma irregularidade ou ato ilegal. Caso tal indicação exista, considerar as implicações em relação a outros aspectos da contratação e, em particular, às declarações da gestão.
- Obter declarações por escrito da gerência pelo menos uma vez por ano ou com mais frequência, dependendo da contratação, para:
  - Reconhecer a responsabilidade da gerência pelo desenvolvimento e implementação de controles internos para prevenir e detectar irregularidades e atos ilegais.
  - Divulgar os resultados pertinentes de qualquer avaliação de riscos que indique que erros, deficiências de controle ou distorções nos dados possam existir como resultado de uma irregularidade ou ato ilegal.
  - Divulgar o conhecimento de irregularidades e atos ilegais por parte do gerenciamento que afetem a empresa em relação ao gerenciamento e a funcionários que tenham funções significativas no controle interno.
  - Divulgar o conhecimento, por parte do gerenciamento, de quaisquer irregularidades ou atos ilegais supostos ou alegados, que afetam a empresa conforme comunicado por funcionários, ex-funcionários, agências reguladoras e outros.

Aspectos principais

continuação

- Comunicar de maneira oportuna para:
  - O nível apropriado de gerenciamento qualquer informação identificada ou obtida, de que uma irregularidade material ou ato ilegal possa existir
  - Pessoas responsáveis pela governança, qualquer irregularidade material e atos ilegais envolvendo o gerenciamento ou funcionários que tenham funções significativas no controle interno
- Relatar para as pessoas responsáveis pela governança qualquer fraqueza material no desenvolvimento e na implementação de controles internos destinados a impedir e detectar quaisquer irregularidades e atos ilegais identificados durante a contratação, mesmo que estejam fora do escopo.
- Considerar os requisitos de relatório legais e profissionais aplicáveis nas circunstâncias.
- Considerar desistir da contratação se erros materiais, deficiências de controle, distorções nos dados ou atos ilegais afetarem o desempenho contínuo da contratação.
- Documentar todas as comunicações, planejamento, resultados, avaliações e conclusões relacionadas a possíveis irregularidades e atos ilegais que tenham sido relatados à gestão, às pessoas responsáveis pela governança, agências reguladoras e outros

Termos

Termo	Definição
Irregularidade	Violação de uma diretriz do gerenciamento ou requisito regulamentar estabelecido. Pode consistir em distorções deliberadas de dados ou omissão de informações relativas à área sob auditoria, ou negligência grave ou atos ilegais não intencionais da empresa como um todo.
Distorção relevante	Uma declaração inverídica acidental ou intencional, que afeta os resultados de uma auditoria em uma extensão mensurável
Ceticismo profissional	Atitude que inclui uma mente questionadora e uma avaliação crítica da evidência de auditoria. Fonte: American Institute of Certified Public Accountants (Instituto Americano de Contadores Públicos Certificados, AICPA) AU 230.07

Vinculação a normas e diretrizes

Tipo	Título
Norma	1008 - Critérios
Norma	1202 - Avaliação de Risco no Planejamento
Norma	1205 - Evidência
Diretriz	2206 - Uso do Trabalho de Outros Especialistas
Diretriz	2207 Irregularidade e atos ilegais

Data de Vigência

Esta norma da ISACA é válida para todas as contratações de auditoria e garantia de SI a partir de 1º de novembro de 2013.