Norma 1201 de Auditoria e Garantia de SI Planejamento de Contratação

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 1201 de Auditoria e Garantia de SI – Planejamento de Contratação

Declarações

1201.1 **Profissionais de auditoria e garantia de SI deverão planejar cada contratação de auditoria e garantia de SI para abordar:**

- **Objetivo(s), escopo, cronograma e resultados tangíveis**
- **Conformidade com leis e normas de auditoria profissional aplicáveis**
- **O uso de uma abordagem baseada no risco, quando apropriado**
- **Questões específicas da contratação**
- **Requisitos de documentação e relatório**

1201.2 **Profissionais de auditoria e garantia de SI deverão desenvolver e documentar um plano de projeto de contratação de auditoria e garantia de SI, descrevendo:**

- **Natureza, objetivos, cronograma e requisitos de recursos da contratação**
- **Época e extensão de procedimentos de auditoria para conclusão da contratação**

Aspectos principais

Profissionais de auditoria e garantia de SI devem:

- Obter uma compreensão da atividade a ser auditada. A extensão do conhecimento requerido deve ser determinada pela natureza da empresa, seu ambiente, suas áreas de risco e os objetivos da contratação.
- Considerar a orientação ou direção do assunto, conforme garantido por meio de legislação, regulamentos, leis, diretivas e diretrizes emitidas pelo governo ou indústria.
- Realizar uma avaliação de risco para fornecer garantia razoável de que todos os itens materiais serão cobertos de maneira adequada durante a contratação. As estratégias, os níveis de materialidade e os requisitos de recursos da auditoria podem, então, ser desenvolvidos.
- Desenvolver o plano de projeto de contratação usando metodologias de gestão de projeto adequadas para garantir que as atividades permaneçam no lugar certo e dentro do orçamento.
- Incluir no plano questões específicas da contratação, como:
  - Disponibilidade de recursos com conhecimento, habilidades e experiência apropriados
  - Identificação de ferramentas necessárias para coletar evidências, realizar testes e preparar/resumir informações para relatórios
  - Critérios de avaliação a serem usados
  - Requisitos e distribuição de relatório
- Documentar o plano de projeto da contratação de auditoria ou garantia de SI, para indicar claramente:
  - Objetivo(s), escopo e cronograma
  - Recursos
  - Funções e responsabilidades
  - Áreas de risco identificadas e seu impacto no plano de contratação
  - Ferramentas e técnicas a serem empegadas
  - Entrevistas de investigação dos fatos a serem conduzidas
  - Informações relevantes a serem obtidas
  - Procedimentos para verificar ou validar as informações obtidas e seu uso como evidência
  - Suposições em relação à abordagem, metodologia, procedimentos e resultados e conclusões antecipadas

Aspectos principais Continuação

- Programar a contratação em relação ao cronograma, disponibilidade e outros compromissos e exigências do gerenciamento e do auditado, na medida do possível.
- Ajustar o plano de projeto no decorrer da contratação de auditoria ou garantia de SI, para resolver problemas que surjam durante a contratação, como novo risco, suposições incorretas ou resultados dos procedimentos já realizados.
- Para contratações internas:
  - Comunicar a carta de auditoria ao auditado; quando necessário, usar uma carta de contratação ou equivalente para esclarecer mais ou confirmar o envolvimento em contratações específicas.
  - Comunicar o plano ao auditado, para que ele fique totalmente informado e possa fornecer acesso adequado a indivíduos, documentos e outros recursos, quando necessário.
- Para contratações externas:
  - Preparar uma carta de contratação separada para cada contratação de auditoria e garantia de SI.
  - Preparar um plano de projeto para cada contratação de auditoria e garantia de SI externa. O plano deve, no mínimo, documentar o(s) objetivo(s) e o escopo da contratação.

Vinculação a diretrizes

Tipo	Título
Diretriz	2201 - Planejamento de Contratação

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.

