Norma 1001 de Auditoria e Garantia de SI
Carta de auditoria

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 1001 de Auditoria e Garantia de SI – Carta de auditoria

Declarações

1001.1 **A função de auditoria e garantia de SI deverá documentar a função de auditoria corretamente em uma carta de auditoria, indicando objetivo, responsabilidade, autoridade e responsabilização.**

1001.2 **A função de auditoria e garantia de SI deverá ter uma carta de auditoria acordada e aprovada em um nível apropriado na empresa.**

Aspectos principais

A função de auditoria e garantia de SI deverá:

- Preparar uma Carta de Auditoria para definir as atividades da função de auditoria e garantia de SI interna, com detalhes suficientes para comunicar:
  - a autoridade, o objetivo, as responsabilidades e limitações da função de auditoria e garantia de SI
  - A Independência e a responsabilidade da função de auditoria e garantia de SI
  - As funções e responsabilidades da entidade auditada durante a Contratação de auditoria de SI ou Contratação de garantia
  - Normas profissionais que o profissional de auditoria e garantia de SI seguirão na realização dos contratações de auditoria e garantia de SI
- Revisar a carta de auditoria, pelo menos anualmente, ou com mais frequência, se as responsabilidades mudarem.
- Atualizar a carta de auditoria conforme necessário para garantir que o objetivo e as responsabilidades tenham sido e permaneçam documentados adequadamente.
- Comunicar formalmente a carta de auditoria para o auditado a cada contratação de auditoria ou garantia de SI.

Termos

Termo	Definição
Contratação de garantia	Uma análise de evidência objetiva com o fim de fornecer uma avaliação sobre gestão de riscos, controle ou processos de governança da empresa. Observação sobre o escopo: exemplos podem incluir contratações financeiras, de desempenho, de conformidade e segurança de sistema
Carta de Auditoria	Um documento aprovado pelas pessoas encarregadas da governança, que define o objetivo, a autoridade e a responsabilidade da atividade de auditoria interna A carta deve: • Estabelecer a posição da função de auditoria interna na empresa • Autorizar o acesso a registros, pessoal e propriedades físicas relevantes para o desempenho de contratação de auditoria e garantia de SI • Definir o escopo das atividades da função de auditoria

Contratação de auditoria	Uma atividade de contratação de auditoria, tarefa ou revisão específica, como uma auditoria, revisão de auto-avaliação de controle, consultoria ou teste de fraude. Uma contratação de auditoria pode incluir várias tarefas ou atividades desenvolvidas para a realização de um conjunto específico de objetivos relacionados.
Independência	A liberdade de condições que ameaçam a objetividade ou a aparência da objetividade. Tais ameaças à objetividade devem ser gerenciadas nos níveis individuais de auditor, contratação, funcional e organizacional. Independência inclui a independência de pensamento e de aparência.

Vinculação a diretrizes

Tipo	Título
Diretriz	2001 - Carta de auditoria

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.

