Norma 1205 de Auditoria e Garantia de SI Evidência

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 1205 de Auditoria e Garantia de SI – Evidência

Declarações

1205.1 **Profissionais de auditoria e garantia de SI deverão obter evidência suficiente e apropriada para tirar conclusões razoáveis sobre em que basear os resultados de contratação.**

1205.2 **Profissionais de auditoria e garantia de SI deverão avaliar a suficiência de evidência obtida para apoiar conclusões e alcançar objetivos de contratação.**

Aspectos principais

Na realização de uma contratação, profissionais de auditoria e garantia de SI devem:

- Obter evidência suficiente e apropriada, incluindo:
  - Os procedimentos como são realizados
  - Os resultados de procedimentos realizados
  - Documentos de origem (em formato eletrônico ou em papel), registros e informações confirmadas utilizadas para dar suporte à contratação
  - Descobertas e resultados da contratação
  - Documentação de que o trabalho foi realizado e obedece às leis, regulamentos e diretrizes aplicáveis.
- Preparar a documentação, que deve ser:
  - Mantida e estar disponível por um período e em um formato compatível com as diretrizes e normas, leis e regulamentações profissionais relevantes da organização de auditoria ou garantia
  - Protegida contra divulgação ou modificação não autorizada ao longo de toda sua preparação e retenção
  - Corretamente descartada no final do período de retenção
- Considerar a suficiência da evidência para apoiar o nível de risco de controle avaliado ao obter evidência de um teste de controles.
- Identificar, cruzar referências e catalogar evidências corretamente.
- Considerar propriedades como origem, natureza (p. ex.: escrita, oral, visual, eletrônica) e autenticidade (p. ex.: assinaturas digitais e manuais, carimbos) da evidência ao avaliar sua confiabilidade.
- Considerar os meios mais eficazes e oportunos de coletar a evidência necessária para satisfazer aos objetivos e risco da contratação. Contudo, a dificuldade ou o custo não são bases válidas para a omissão de um procedimento necessário.
- Selecione o procedimento mais apropriado para reunir evidência, dependendo do tema que está sendo auditado (ou seja, sua natureza, época da auditoria, julgamento profissional). Procedimentos usados para obter a evidência incluem:
  - Investigação e confirmação
  - Reexecução
  - Recálculo
  - Cálculo
  - Procedimentos analíticos
  - Inspeção
  - Observação
  - Outros métodos geralmente aceitos

Aspectos principais

continuação

- Considerar a origem e natureza de qualquer informação obtida para avaliar a sua confiabilidade e os requisitos de verificação adicionais. Em termos gerais, a confiabilidade da evidência é maior quando:
  - Está em formato escrito, em vez de manifestações orais;
  - É obtida de fontes independentes
  - É obtida pelo profissional em vez da entidade que está sendo auditada
  - É certificada por uma parte independente
  - É guardada por uma parte independente
  - O resultado da inspeção
  - O resultado da observação
- Obter evidência objetiva que seja suficiente para permitir que uma parte independente qualificada reexecute os testes e obtenha os mesmos resultados e conclusões.
- Obter evidência proporcional à materialidade do item e ao risco envolvido.
- Aplicar a devida ênfase na precisão e na totalidade da informação quando a informação obtida da empresa for usada pelo profissional de auditoria ou garantia de SI para realizar procedimentos de auditoria.
- Divulgar qualquer situação na qual evidência suficiente não possa ser obtida de maneira consistente com a comunicação dos resultados da contratação de auditoria ou garantia de SI.
- Assegurar a evidência contra acesso e modificação não autorizados.
- Reter a evidência após a conclusão do trabalho de auditoria ou garantia de SI, enquanto for necessário para obedecer a todas as leis, regulamentos e diretrizes aplicáveis.

Termos

Termo	Definição
Evidência Apropriada	A medida da qualidade da evidência
Evidência Suficiente	A medida da quantidade de evidência; apoia todas as questões materiais para o objetivo e escopo da auditoria. Consulte evidência.

Vinculação a diretrizes

Tipo	Título
Diretriz	2205 - Evidência

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.

