Norma 1401 de Auditoria e Garantia de SI Relatórios

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 1401 de Auditoria e Garantia de SI - Relatórios

Declarações

1401.1 **Profissionais de auditoria e garantia de SI deverão fornecer um relatório para comunicar os resultados na conclusão da contratação, incluindo:**

- **Identificação da empresa, os destinatários pretendidos e todas as restrições de conteúdo e circulação**
- **O escopo, objetivos da contratação, período de cobertura, e a natureza, cronograma e extensão do trabalho executado**
- **Os resultados, as conclusões e as recomendações**
- **Qualquer qualificação ou limitação no escopo que o profissional de auditoria e garantia de SI tenha em relação à contratação**
- **Assinatura, data e distribuição, de acordo com os termos da carta de auditoria ou carta de contratação**

1401.2 **Profissionais de auditoria e garantia de SI deverão garantir que resultados no relatório de auditoria sejam apoiados por uma evidência suficiente e apropriada.**

Aspectos principais

Profissionais de auditoria e garantia de SI devem:

- Obter declarações por escrito relevantes do auditado, que detalhem claramente as áreas críticas da contratação, questões que surgiram e sua solução, e declarações feitas pelo auditado.
- Determinar que as declarações do auditado foram assinadas e datadas pelo próprio, para indicar conhecimento de suas responsabilidades em relação à contratação.
- Documentar e reter no papel de trabalho qualquer declaração, seja por escrito ou oral, recebida no decorrer da realização da contratação. Para contratações de certificação, as declarações do auditado devem ser obtidas por escrito, para reduzir possíveis mal-entendidos.
- Personalizar a forma e o conteúdo do relatório para apoiar o tipo de contratação realizada, como:
  - Auditoria (diretamente ou como testemunha)
  - Revisão (diretamente ou como testemunha)
  - Procedimentos concordados
- Descrever fraquezas materiais ou significativas e seu efeito na concretização dos objetivos da contratação no relatório.
- Discutir o conteúdo do rascunho do relatório com a gerência na área de assunto apropriada, antes de ser finalizado e publicado, e incluir a resposta da gerência para resultados, conclusões e recomendações no relatório final, quando aplicável.
- Comunicar deficiências significativas e fraquezas materiais no ambiente de controle às pessoas responsáveis pela governança e, quando aplicável, à autoridade responsável, e divulgar no relatório que essas partes foram comunicadas.
- Mencionar qualquer relatório separado no relatório final.
- Comunicar ao auditado as deficiências de controle interno do gerenciamento que sejam menos significativas, porém mais do que irrelevantes. Em tais casos, pessoas responsáveis pela governança ou a autoridade responsável deve ser notificada de que tais deficiências de controle interno foram comunicadas ao gerenciamento do auditado.
- Identificar padrões aplicados na condução da contratação, e comunicar qualquer não conformidade com esses padrões, conforme aplicável.

Termos

Termo	Definição
Informações relevantes	Relaciona-se a controles, informa o avaliador algo significativo sobre a operação dos controles subjacentes ou componente de controle. Informações que confirmam diretamente que a operação de controles é mais relevante. Informações que se relacionam indiretamente à operação de controles também podem ser relevantes, mas são menos relevantes do que informações diretas. Consulte os objetivos de qualidade de informações do COBIT 5
Informação confiável	Informação que seja precisa, verificável e proveniente de uma fonte objetiva. Consulte os objetivos de qualidade de informações do COBIT 5
Informação suficiente	A informação é suficiente quando os avaliadores já coletaram o suficiente para formar uma conclusão razoável. Para a informação ser suficiente, no entanto, primeiramente ela deve ser adequada. Consulte os objetivos de qualidade de informações do COBIT 5
Informação adequada	Informação relevante (ou seja, adequada para seu objetivo pretendido), confiável (ou seja, precisa, verificável e proveniente de uma fonte objetiva) e oportuna (ou seja, produzida e utilizada em um período adequado). Consulte os objetivos de qualidade de informações do COBIT 5
Informação oportuna	Produzida e utilizada em um período que possibilita impedir ou detectar deficiências de controle antes que se tornem materiais para uma empresa. Consulte os objetivos de qualidade de informações do COBIT 5

Vinculação a normas e diretrizes

Tipo	Título
Diretriz	2401 - Relatórios

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.