

Norma 1007 de Auditoria e Garantia de SI Assertivas

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).

ISACA 2012-2013 Professional Standards and Career Management Committee	
Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaysia
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Norma 1007 de Auditoria e Garantia de SI - Assertivas

Declarações

1007.1 Profissionais de auditoria e garantia de SI deverão revisar as afirmações em relação às quais o assunto será avaliado, para determinar se tais assertivas são capazes de ser auditadas e se são suficientes, válidas e relevantes.

Aspectos principais

Profissionais de auditoria e garantia de SI devem:

- Avaliar os critérios em relação aos quais o tema será avaliado, para garantir que eles apoiem as Assertivas.
 - Determinar se as assertivas são auditáveis e apoiadas por informações confirmadas.
 - Determinar se as assertivas são baseadas em critérios determinados corretamente e sujeitos a análise objetiva e mensurável.
 - Sempre que assertivas forem desenvolvidas pelo gerenciamento, certificar-se de que, quando comparadas a outras normas de pronunciamentos abalizadas, as assertivas sejam suficientes em relação ao que esperaria um leitor ou usuário conhecedor.
 - Quando assertivas forem desenvolvidas por terceiros que operam controles em nome da empresa, certificar-se de que as assertivas sejam verificadas e aceitas pelo gerenciamento.
 - Relatar diretamente em relação ao assunto (relatório direto) ou em relação a uma assertiva sobre o assunto (relatório indireto).
 - Formar uma conclusão sobre cada assertiva, com base no agregado dos resultados em relação a critérios, juntamente com avaliação profissional.
-

Termos

Termo	Definição
Assertiva	Qualquer declaração ou conjunto de declarações formais sobre o assunto, feito pelo gerenciamento. Assertivas devem normalmente ser feitas por escrito e, geralmente, contêm uma lista de atributos específicos sobre o assunto específico ou sobre um processo que envolva o assunto.

Vinculação a diretrizes

Tipo	Título
Diretriz	2007 Assertivas

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.