



Norma 1203 de Auditoria e Garantia de SI Desempenho e Supervisão

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 1203 de Auditoria e Garantia de SI – Desempenho e Supervisão

Declarações

- 1203.1** Profissionais de auditoria e garantia de SI deverão realizar o trabalho de acordo com o plano de auditoria de SI aprovado, para cobrir riscos identificados e dentro da programação acordada.
- 1203.2** Profissionais de auditoria e garantia de SI devem fornecer supervisão à equipe de auditoria de SI por quem tenham responsabilidade de supervisão, para cumprir com objetivos de auditoria e atender a normas profissionais de auditoria aplicáveis.
- 1203.3** Profissionais de auditoria e garantia de SI deverão aceitar apenas tarefas que estejam dentro de seus conhecimentos e habilidades, ou para as quais eles tenham uma expectativa razoável de aquisição de habilidades durante a contratação ou realização da tarefa sob supervisão.
- 1203.4** Profissionais de auditoria e garantia de SI devem obter evidência suficiente e adequada para alcançar os objetivos de auditoria. Os resultados e as conclusões da auditoria deverão ser suportados pela análise e interpretação apropriadas dessa evidência.
- 1203.5** Profissionais de auditoria e garantia de SI deverão documentar o processo de auditoria, descrevendo o trabalho e a evidência de auditoria que suporte resultados e conclusões.
- 1203.6** Profissionais de auditoria e garantia de SI deverão identificar e emitir parecer sobre resultados.
-

Aspectos principais

Profissionais de auditoria e garantia de SI devem:

- Designar membros para a equipe que possuam habilidades e experiência que atendam às necessidades da contratação.
- Adicionar recursos externos à equipe de auditoria de SI, quando apropriado, e garantir que seu trabalho seja supervisionado corretamente.
- Gerenciar as funções e responsabilidades dos membros específicos da equipe de auditoria de SI por toda a contratação, abordando, no mínimo:
 - Funções de execução e análise
 - Responsabilidade pelo desenvolvimento da metodologia e da abordagem
 - Criação de programas de auditoria ou garantia
 - Realização do trabalho
 - Trato com questões, preocupações e problemas conforme eles surgem
 - Documentação e justificativa dos resultados
 - Redação do relatório
- Ter cada tarefa da contratação realizada por um membro da equipe, revisada por outro membro adequado da equipe.
- Usar a melhor evidência possível. A evidência deve ser consistente com a importância do objetivo da auditoria e com o tempo e esforço envolvidos na obtenção da evidência.
- Obter evidência adicional se, no julgamento do profissional, a evidência obtida não atender ao critério de ser suficiente e apropriada para formar uma opinião ou suportar os resultados e as conclusões.

Norma 1203 de Auditoria e Garantia de SI – Desempenho e Supervisão

- Aspectos principais
- continuação
- Organizar e documentar o trabalho realizado durante a contratação, seguindo procedimentos predefinidos documentados e aprovados.
 - Incluir na documentação:
 - Objetivos da auditoria e escopo do trabalho, programa da auditoria, etapas de auditoria executadas, evidência coletada, resultados, conclusões e recomendações.
 - Detalhes suficientes para permitir que uma pessoa prudente e informada execute novamente as tarefas realizadas durante a contratação e chegue à mesma conclusão.
 - Identificação de quem realizou cada tarefa e suas funções na preparação e revisão da documentação.
 - A data em que a documentação foi preparada e revisada
 - 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 papéis de trabalho com qualquer declaração recebida no decorrer da realização da contratação, seja por escrito ou oral.
-

Vinculação a normas e diretrizes

Tipo	Título
Norma	1005 - Devido cuidado profissional
Norma	1205 - Evidência
Norma	1401 - Relatório
Diretriz	2202 - Avaliação de Risco no Planejamento

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.