Norma 1008 de Auditoria e Garantia de SI Critérios

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 1008 de Auditoria e Garantia de SI - Critérios

Declarações

1008.1 **Profissionais de auditoria e garantia de SI deverão selecionar os critérios em relação aos quais o assunto será avaliado, que são: ser objetivos, completos, relevantes, mensuráveis, compreensíveis, amplamente reconhecidos, confiáveis e compreensíveis, ou disponíveis, a todos os leitores e usuários do relatório.**

1008.2 **Profissionais de auditoria e garantia de SI deverão considerar a fonte dos critérios e se concentrar nos critérios emitidos por órgãos autorizados relevantes antes de aceitar critérios menos conhecidos.**

Aspectos principais

Profissionais de auditoria e garantia de SI devem:

- Considerar a seleção de Critérios cuidadosamente, e ser capazes de justificar a seleção.
- Usar avaliação profissional para garantir que, se aplicado, o uso dos critérios permitirá o desenvolvimento de uma opinião ou conclusão justa e objetiva, que não induzirá a erro o leitor nem o usuário. É sabido que a gestão pode colocar em evidência critérios que não atendam a todos os requisitos.
- Considerar a adequação e disponibilidade de critérios na determinação dos requisitos de contratação.
- Quando critérios não estiverem prontamente disponíveis, estiverem incompletos ou sujeitos a interpretação, inclua uma descrição e qualquer outra informação necessária para garantir que o relatório seja justo, objetivo e compreensível, e que o contexto no qual os critérios são usados seja incluído no relatório.

A adequação e conveniência dos critérios de avaliação do assunto devem ser avaliados em relação aos cinco critérios de adequação seguintes:

- **Objetividade -** os critérios devem ser livres de tendências que possam afetar adversamente os resultados e as conclusões do profissional e, dessa forma, possam induzir a erro o usuário do relatório.
- **Totalidade -** os critérios devem ser suficientemente completos, para que todos os critérios que possam afetar as conclusões do profissional sobre o assunto sejam identificados e usados na condução da contratação da auditoria ou garantia de SI.
- **Relevância -** os critérios devem ser relevantes para o assunto, e contribuir com resultados e conclusões que atendam aos objetivos da contratação da auditoria ou garantia de SI.
- **Mensurabilidade -** os critérios devem permitir a mensuração consistente do assunto, e o desenvolvimento de conclusões consistentes quando aplicados por diferentes profissionais em circunstâncias semelhantes.
- **Compreensibilidade -** os critérios devem ser comunicados de forma clara, e não devem estar sujeitos às interpretações significativamente diferentes por usuários aos quais se destinam.

© ISACA 2013 Todos os direitos reservados.

Aspectos principais Continuação

A aceitabilidade dos critérios é afetada pela disponibilidade dos critérios para usuários do relatório do profissional, de modo que os usuários compreendam a base da atividade de garantia e a relevância dos resultados e conclusões. As fontes podem incluir fontes que sejam:

- **Reconhecidas -** os critérios devem ser suficientemente bem reconhecidos para que seu uso não seja questionado por usuários a que se destinam.
- **Confiáveis -** devem ser buscados critérios que reflitam pronunciamentos abalizados na área, e que sejam apropriados para o assunto. Por exemplo, pronunciamentos abalizados podem ser provenientes de órgãos profissionais, grupos do setor, governo e agências reguladoras.
- **Publicamente disponíveis -** os critérios devem estar disponíveis para os usuários do relatório do profissional. Exemplos incluem normas desenvolvidas por órgãos profissionais contábeis e de auditoria, como a ISACA, a Federação Internacional de Contabilistas (IFAC) ou outros órgãos governamentais ou profissionais reconhecidos.
- **Disponível para todos os usuários -** quando critérios não estiverem publicamente disponíveis, deverão ser comunicados a todos os usuários por meio de afirmações que façam parte do relatório do profissional. Afirmações consistem em declarações sobre o assunto que atendam aos requisitos de critérios adequados, de modo que elas possam ser auditadas.

Além de adequação e disponibilidade, a seleção dos critérios de garantia de SI também deve considerar a fonte - em termos de seu uso e do público potencial. Por exemplo, ao lidar com regulamentos governamentais, critérios baseados em afirmações desenvolvidas a partir da legislação e de regulamentos que se aplicam ao assunto podem ser o mais apropriado. Em outros casos, critérios do setor ou da associação comercial podem ser relevantes. Possíveis fontes de critérios, listadas por ordem de consideração são:

- **Critérios estabelecidos pela ISACA -** são critérios e normas publicamente disponíveis, que foram expostos a revisão por pares e a um processo meticuloso de devido empenho por especialistas internacionais reconhecidos em governança, controle, segurança e garantia de TI.
- **Critérios estabelecidos por outros órgãos de especialistas -** semelhantes a normas e critérios da ISACA, esses critérios são relevantes para o assunto, e foram desenvolvidos e expostos a revisão por pares e a um processo meticuloso de devido empenho por especialistas em vários campos.
- **Critérios estabelecidos por leis e regulamentos -** embora leis e regulamentos possam fornecer a base de critérios, é preciso ter cuidado com sua utilização. Frequentemente, o texto é complexo e carrega um significado legal específico. Em muitos casos, pode ser necessário reafirmar os requisitos como declarações. Além disso, expressar uma opinião sobre a legislação geralmente é restrito a membros profissionais do direito.
- **Critérios estabelecidos por empresas que não seguem o devido processo -** inclui critérios relevantes desenvolvidos por outras empresas que não seguiram o devido processo e não foram submetidas a consulta pública e debate.
- **Critérios desenvolvidos especificamente para a contratação da auditoria e garantia de SI** - embora critérios desenvolvidos especificamente para o contratação da auditoria e garantia de SI sejam apropriados, é preciso ter cuidado específico para garantir que esses critérios atendam aos critérios de adequação, especificamente totalidade, mensurabilidade e objetividade. Critérios desenvolvidos especificamente para uma contratação da auditoria ou garantia de SI estão na forma de afirmações.

© ISACA 2013 Todos os direitos reservados.

Os critérios de seleção devem ser considerados atentamente. Embora seguir as leis e regulamentos locais seja importante e deva ser considerado um requisito obrigatório, é reconhecido que muitas contratações de auditoria e garantia de SI incluem áreas como a gestão de mudanças, controles gerais de TI e controles de acesso, não cobertos por leis ou regulamentos. Além disso, alguns setores, como o de cartão de pagamento, estabeleceram requisitos obrigatórios que devem ser atendidos. Quando requisitos legislativos forem baseados em princípios, o profissional deverá garantir que critérios selecionados atendam ao objetivo da contratação.

Conforme a contratação progride, informações adicionais podem resultar em determinados critérios não serem necessários para alcançar os objetivos. Nessas circunstâncias, trabalho adicional relacionado aos critérios não é necessário.

Termos

Termo	Definição
Critérios	As normas e referências usadas para medir e apresentar o assunto, e em relação aos quais um auditor de SI avalia o assunto. Os critérios devem ser: • Objetivos - livres de tendências • Completos - incluir todos os fatores relevantes para chegar a uma conclusão • Relevantes - relacionados ao assunto • Mensuráveis - fornecer avaliação consistente Em uma contratação de Ateste (ou Certificação), referências em relações às quais a afirmação por escrito da gestão sobre o assunto possam ser avaliadas. O profissional chega uma conclusão sobre o assunto consultando os critérios adequados.

Vinculação a diretrizes

Tipo	Título
Diretriz	2008 - Critérios

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.

© ISACA 2013 Todos os direitos reservados.