Francesco De Cicco

AUDITORIA BASEADA EM RISCOS APLICADA A SISTEMAS DE GESTÃO

Março/2014

Março de 2014

UM NOVO DESAFIO PARA OS
AUDITORES INTERNOS DE SISTEMAS DE GESTÃO

Auditoria Baseada em Riscos Aplicada a Sistemas de Gestão

(E alinhada às novas ISO 9001:2015, ISO 14001:2015, ISO 45000:2016, etc.)

por ***Francesco De Cicco***[1]

O foco do trabalho dos auditores internos de sistemas de gestão pode mudar consideravelmente com a publicação das novas normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2016, entre outras. Por causa dos novos requisitos dessas normas e por razões de custo e eficácia, espera-se que seja dada especial ênfase à **Auditoria Baseada em Riscos** (ABR).

Auditoria Baseada em Riscos é um termo bastante utilizado no mundo todo, mas ainda muito mal compreendido. Este *paper* tem por objetivo apresentar a abordagem do QSP para a **ABR Aplicada a Sistemas de Gestão**, bem como visa fornecer diretrizes básicas sobre como abordá-la e colocá-la em prática.

Este trabalho foi inspirado no Manual "*Como implementar a Auditoria Baseada em Riscos nas organizações: uma abordagem inovadora*", lançado em 2007 pelo QSP.

Contexto

Conforme o Anexo SL das novas Diretivas ISO, todas as normas ISO de sistemas de gestão, publicadas a partir de 2012, deverão trazer a seguinte definição de **Auditoria**:

"Processo sistemático, independente e documentado, para obter evidência de auditoria e avaliá-la objetivamente, para determinar a extensão na qual os critérios de auditoria são atendidos.

NOTA 1 Uma auditoria pode ser uma auditoria interna (de primeira parte) ou uma auditoria externa (de segunda parte ou de terceira parte), e pode ser uma auditoria combinada (combinação de duas ou mais disciplinas).

[1] Diretor executivo do **QSP - *Centro da Qualidade, Segurança e Produtividade***.
E-mail: qsp@qsp.org.br. Telefone: (11) 3704-3200.

NOTA 2 A "evidência de auditoria" e os "critérios de auditoria" são definidos na ABNT NBR ISO 19011:2012."

Por sua vez, a **NBR ISO 19011:2012** - *Diretrizes para auditoria de sistemas de gestão* - introduziu o conceito de **risco** para essas auditorias. O enfoque adotado se relaciona com o risco do processo de auditoria em não atingir seus objetivos e com o risco da auditoria interferir com os processos e atividades da organização auditada.

A nova NBR ISO 19011 não fornece diretrizes específicas sobre o **Processo de Gestão de Riscos** da organização (nem sobre Auditoria Baseada em Riscos), mas reconhece que as organizações podem focar o esforço da auditoria em assuntos de importância para o sistema de gestão.

Existem muitos riscos diferentes associados ao estabelecimento, implementação, monitoramento, análise crítica e melhoria de um programa de auditoria que podem afetar o alcance dos seus objetivos. A NBR ISO 19011:2012 recomenda que a pessoa que gerencia o programa de auditoria considere esses riscos no seu desenvolvimento.

Tais riscos podem estar relacionados a:

- *planejamento* (por exemplo, falha em estabelecer os objetivos pertinentes da auditoria e determinar a abrangência do programa de auditoria);

- *recursos* (por exemplo, tempo insuficiente para desenvolver o programa de auditoria ou para realizar a auditoria);

- *seleção da equipe de auditoria* (por exemplo, a equipe não tem a competência coletiva para realizar auditorias de forma eficaz);

- *implementação* (por exemplo, comunicação ineficaz do programa de auditoria);

- *registros e seus controles* (por exemplo, falha em proteger de forma adequada os registros de auditoria para demonstrar a eficácia do programa de auditoria);

- *monitoramento, análise crítica e melhoria do programa de auditoria* (por exemplo, monitoramento ineficaz dos resultados do programa de auditoria).

Na futura **ISO 9001:2015** - *Sistemas de gestão da qualidade - Requisitos*, por exemplo, o conceito de **risco** no contexto da nova norma irá se referir à **incerteza** da organização em alcançar os seguintes **objetivos**:

- proporcionar confiança na sua capacidade de fornecer consistentemente aos clientes bens e serviços conformes;

- aumentar a satisfação dos clientes.

Os auditores internos podem implementar uma abordagem baseada em riscos compatível com a abordagem adotada por suas organizações. Há muitos enfoques que podem ser utilizados, dependendo de quanto a auditoria interna é capaz de se apoiar no **Processo de Gestão de Riscos**[2] da organização. Isso possibilita ao auditor evitar a duplicação dos processos já realizados pela organização e questionar os processos e as conclusões da direção/gerência sobre os riscos que podem afetar (positiva ou negativamente) os objetivos do sistema de gestão.

Pode ser que os auditores internos digam que sempre concentraram seus esforços nas áreas e temas de maiores riscos para o sistema de gestão e para a organização. Contudo, a experiência mostra que essa abordagem tem sido direcionada pela Avaliação de Riscos efetuada pela própria equipe de auditoria. A principal diferença é que o foco da ABR é entender e analisar a Avaliação de Riscos realizada pela direção/gerência e basear os esforços de auditoria em torno dessa avaliação.

Os objetivos da ABR - *Auditoria Baseada em Riscos*

O principal objetivo da ABR é fornecer **garantia independente** para a direção/gerência da organização de que:

- O **Processo de Gestão de Riscos** relacionado aos sistemas de gestão (da Qualidade, Ambiental, da Segurança e Saúde no Trabalho, etc.) está operando conforme o planejado;

- O **tratamento** que a direção/gerência tem dado aos riscos é adequado e eficaz em tornar os níveis de risco aceitáveis ou toleráveis para a organização;

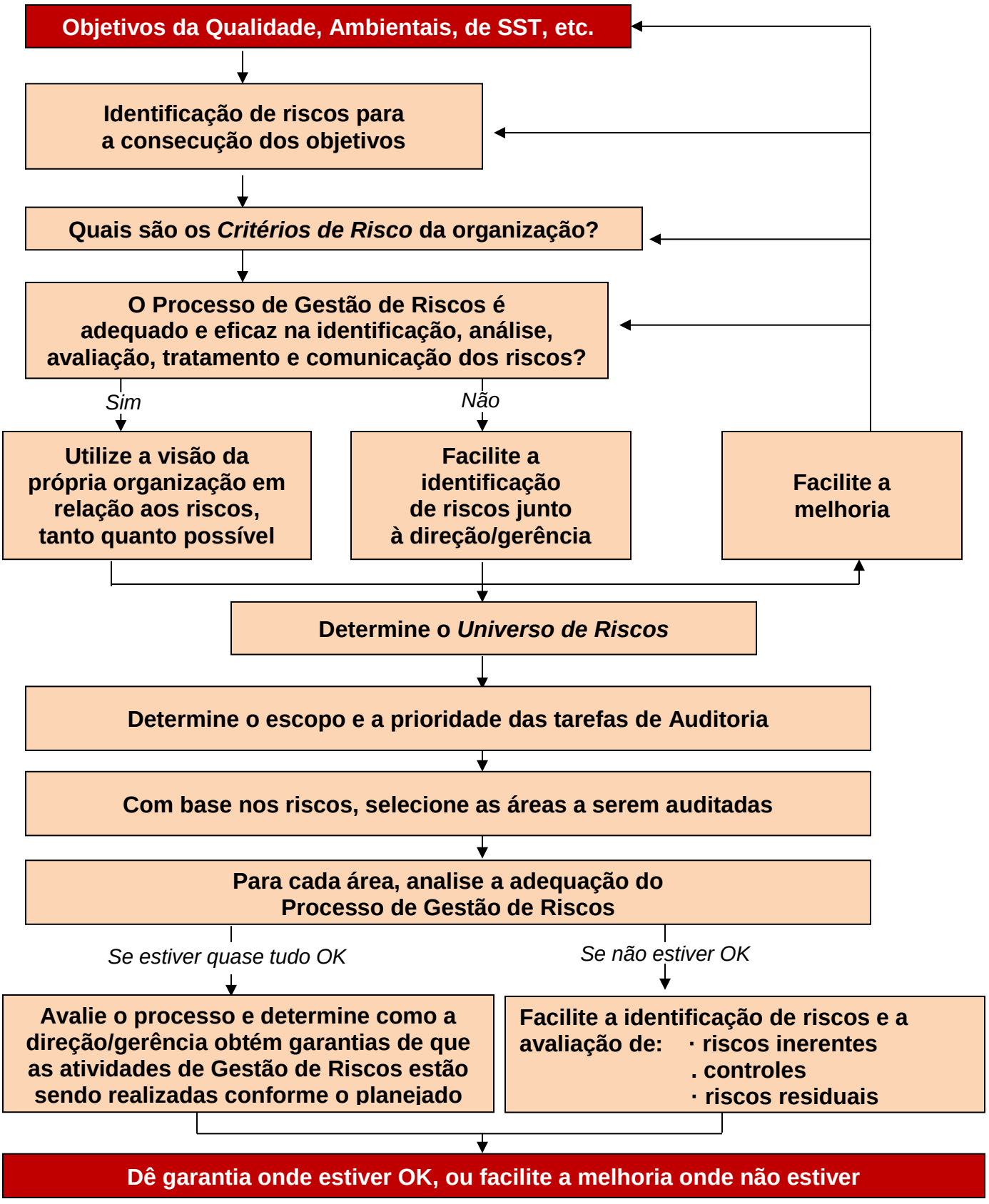
- Existe uma estrutura sólida de **controles** para modificar suficientemente os riscos que a direção/gerência deseja tratar.

A ABR começa com os objetivos do negócio, passando pelos objetivos da Qualidade, Ambientais, etc., e se concentra nos riscos que foram identificados pela direção/gerência e que podem afetar, positiva ou negativamente, a consecução desses objetivos.

O papel da auditoria interna é avaliar até que ponto uma abordagem planejada e robusta de Gestão de Riscos é adotada e aplicada em toda a organização pela direção/gerência, para tornar os níveis de risco aceitáveis ou toleráveis (conforme os *Critérios de Risco* da organização). A **abordagem do QSP** para a Auditoria Baseada em Riscos Aplicada a Sistemas de Gestão está descrita de forma esquemática na página a seguir.

[2] O termo **Risco**, na norma NBR ISO 31000:2009, é definido como "*Efeito da incerteza nos objetivos*". Portanto, os objetivos abrangidos pela Gestão de Riscos incluem tanto os objetivos estratégicos como os objetivos específicos de uma organização (por exemplo: os objetivos da Qualidade, Ambientais, de Responsabilidade Social, de *Compliance*, etc.).

Abordagem do QSP para a ABR Aplicada a Sistemas de Gestão



A prática da ABR - *Auditoria Baseada em Riscos*

Aspectos gerais importantes a serem considerados:

- O escopo da ABR pode incluir riscos estratégicos, riscos do negócio e riscos operacionais, incluindo os relacionados aos sistemas de gestão da organização.

- O ponto de partida é determinar se a organização estabeleceu objetivos apropriados, e então determinar se a empresa tem ou não um processo adequado para identificar, analisar, avaliar, tratar e comunicar os riscos que afetam, positiva ou negativamente, esses objetivos.

- Em um ambiente maduro de Gestão de Riscos, o foco da auditoria interna pode ser:

    - Auditar a estrutura para gerenciar riscos como, por exemplo, recursos, documentação, métodos e relatórios;
    - Auditar o sistema de controles de toda a organização e de cada área, divisão, departamento ou processo;
    - Realizar auditorias individuais que visem predominantemente o gerenciamento de riscos específicos. Caso vários riscos sejam controlados através de um Sistema Integrado de Gestão ou processo comum, talvez seja apropriado realizar uma auditoria combinada desse sistema ou processo.

- Em ambientes menos maduros de Gestão de Riscos, caso as auditorias individuais focalizem predominantemente todo um sistema, processo ou unidade de negócio, a auditoria interna deve analisar criticamente os objetivos estabelecidos e o Processo de Gestão de Riscos, dentro de cada uma dessas partes auditáveis.

- Se o Processo de Gestão de Riscos estiver adequado e enraizado, a auditoria interna, sempre que possível, deve se apoiar na própria visão da organização com relação aos riscos, a fim de determinar o trabalho de auditoria que ela necessita conduzir.

- Quando ela não puder se basear no Processo de Gestão de Riscos, a auditoria interna deve realizar sua própria Avaliação de Riscos (*em conjunto com a direção, gerência, etc., e preferencialmente utilizando como referência a norma internacional e brasileira NBR ISO/IEC 31010 - Gestão de riscos - Técnicas para o processo de avaliação de riscos*), para determinar o nível preciso do trabalho necessário, e então focalizar a maneira como a direção/gerência se assegura de que as atividades de Gestão de Riscos estão sendo praticadas conforme o planejado.

- O resultado final de cada auditoria individual deve ser o de assegurar que os riscos estão sendo gerenciados dentro de um nível aceitável ou tolerável

(conforme definido nos *Critérios de Risco* da organização), ou facilitar e/ou definir melhorias conforme necessário.

Processo contínuo de administração dos riscos

É óbvio, mas é importante enfatizar, que nem todas as organizações estão no mesmo estágio de implementação da Gestão de Riscos. O quadro a seguir estabelece os graus de *Maturidade de Riscos*[3] e a abordagem da auditoria interna que pode ser adotada em cada estágio.

Grau de Maturidade de Riscos	Características Principais	Abordagem da Auditoria Interna
Ingênuo	Nenhuma abordagem formal desenvolvida para a Gestão de Riscos.	Promove a Gestão de Riscos e se baseia na Avaliação de Riscos da própria auditoria.
Consciente	Abordagem para a Gestão de Riscos dispersa em "silos".	Promove a abordagem corporativa da Gestão de Riscos e se baseia na Avaliação de Riscos realizada pela própria auditoria.
Definido	Estratégia e políticas implementadas e comunicadas, *Critérios de Risco* definidos.	Facilita a Gestão de Riscos/ Relaciona-se com a Gestão de Riscos, e usa a Avaliação de Riscos realizada pela direção/ gerência quando apropriado.
Gerenciado	Abordagem corporativa para a Gestão de Riscos, desenvolvida e comunicada.	Audita o Processo de Gestão de Riscos e utiliza a Avaliação de Riscos realizada pela direção/gerência conforme apropriado.
Habilitado	Gestão de Riscos e controles internos totalmente incorporados às operações.	Audita o Processo de Gestão de Riscos e utiliza a Avaliação de Riscos realizada pela direção/gerência conforme apropriado.

Cada organização deve determinar como pretende implementar/melhorar a Gestão de Riscos (*preferencialmente adotando como referência a norma internacional e brasileira NBR ISO 31000:2009 - Gestão de riscos - Princípios e diretrizes*). Isso ajudará a determinar os *Critérios de Risco* e o nível de *Maturidade de Riscos* da organização. Por exemplo, nem todas as empresas desejarão atingir completamente o grau de

[3] Termo simplificado que utilizamos no QSP quando nos referimos à *Maturidade da Gestão de Riscos* de uma organização.

maturidade *Habilitado*, pois talvez tenham que pesar os custos em relação à visão que têm dos benefícios potenciais. Cabe à alta direção e à equipe de gerentes determinarem até que ponto desse processo contínuo desejarão chegar.

Além da *Maturidade de Riscos* da organização, a extensão da Avaliação de Riscos que a própria auditoria interna irá realizar, se for o caso, também depende do grau e da velocidade das mudanças estratégicas e organizacionais.

Conclusão

A Auditoria Baseada em Riscos é uma abordagem que focaliza as **questões que realmente importam** para a organização, em qualquer área: Finanças, Qualidade, Meio Ambiente, Segurança e Saúde no Trabalho, Responsabilidade Social, *Compliance*, etc.

A ABR **fornece garantias** em relação à estrutura para gerenciar riscos da empresa, possibilitando que a auditoria interna se ligue diretamente a essa estrutura e, dessa forma, potencialize as sinergias.

Capacite-se no QSP (clique na figura acima para conhecer nosso Curso de Capacitação e Certificação em Gestão de Riscos - ISO 31000)