



Publicado em Março/2010 e Atualizado em Junho/2018 e em Fevereiro/2021

UM NOVO PARADIGMA PARA AS AUDITORIAS INTERNAS

## Por que sua organização deve implementar a ABR - Auditoria Baseada em Riscos

por Francesco De Cicco<sup>1</sup>

O foco do trabalho dos auditores internos (*de todas as áreas: Finanças, Compliance, Qualidade, Security, Segurança e Saúde, Meio Ambiente, etc.*) tem mudado bastante nas duas últimas décadas. Atualmente, sobretudo por razões de custo e eficácia, a ênfase está na **Auditoria Baseada em Riscos (ABR)**.

*Auditoria Baseada em Riscos* é um termo bastante utilizado no mundo todo, mas ainda muito mal compreendido. Este *paper* visa apresentar a abordagem do QSP para a ABR, bem como fornecer as diretrizes essenciais sobre como entendê-la e colocá-la em prática.

Este trabalho está fundamentado no Manual “[Como implementar a Auditoria Baseada em Riscos nas organizações: uma abordagem inovadora](#)”, que é parte integrante do material didático do tradicional curso do QSP intitulado “[ISO 31000:2018 - Capacitação em Gestão de Riscos e Auditoria Baseada em Riscos](#)”.

### Contexto

A definição de **Auditoria Interna** recomendada pelo IIA - *The Institute of Internal Auditors* (maior associação de Auditores Internos do mundo) - e também adotada pelo QSP - é a seguinte:

***“Auditoria interna é uma atividade independente e objetiva de garantia e aconselhamento, concebida para agregar valor e melhorar as operações de uma organização. Auxilia uma organização a atingir seus objetivos aplicando uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gestão de riscos, controles e governança”.***

---

<sup>1</sup> Diretor Executivo do QSP - Centro da Qualidade, Segurança e Produtividade  
E-mail: [qsp@qsp.org.br](mailto:qsp@qsp.org.br) | [Blog do De Cicco](#) na ISO31000.net

Os auditores internos devem 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 nos processos de **Gestão de Riscos**<sup>2</sup> da organização. Isso possibilita ao auditor evitar a duplicação dos processos já realizados na organização e questionar os processos e as conclusões da direção (ou da gerência) sobre os riscos da empresa (*repetindo: isso vale também para objetivos e áreas específicas da organização como Finanças, Compliance, Qualidade, Segurança, etc.*).

Pode ser que os auditores internos digam que sempre concentraram seus esforços nas áreas e temas de maiores riscos para a organização. Contudo, a experiência mostra que essa abordagem tem sido direcionada pela Avaliação de Riscos efetuada pela própria equipe de auditoria interna da companhia. A **principal diferença** é que o foco da ABR é **entender e analisar a Avaliação de Riscos** efetuada 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 o conselho de administração (e para a alta direção, gerência, etc.) da organização de que:

- Os **processos de Gestão de Riscos** colocados em prática na organização (abrangendo todos os níveis da companhia) estão operando conforme o planejado;
- Tais processos de Gestão de Riscos têm uma sólida **estrutura** (*framework*);
- As **respostas** que a direção tem dado aos riscos são adequadas e eficazes na redução desses riscos a um nível aceitável para o conselho;
- Existe uma estrutura sólida de **controles** para mitigar suficientemente os riscos que a direção deseja tratar.

A ABR começa com os objetivos do negócio e se concentra nos riscos que foram identificados pela direção/gerência e que podem comprometer a consecução desses objetivos.

---

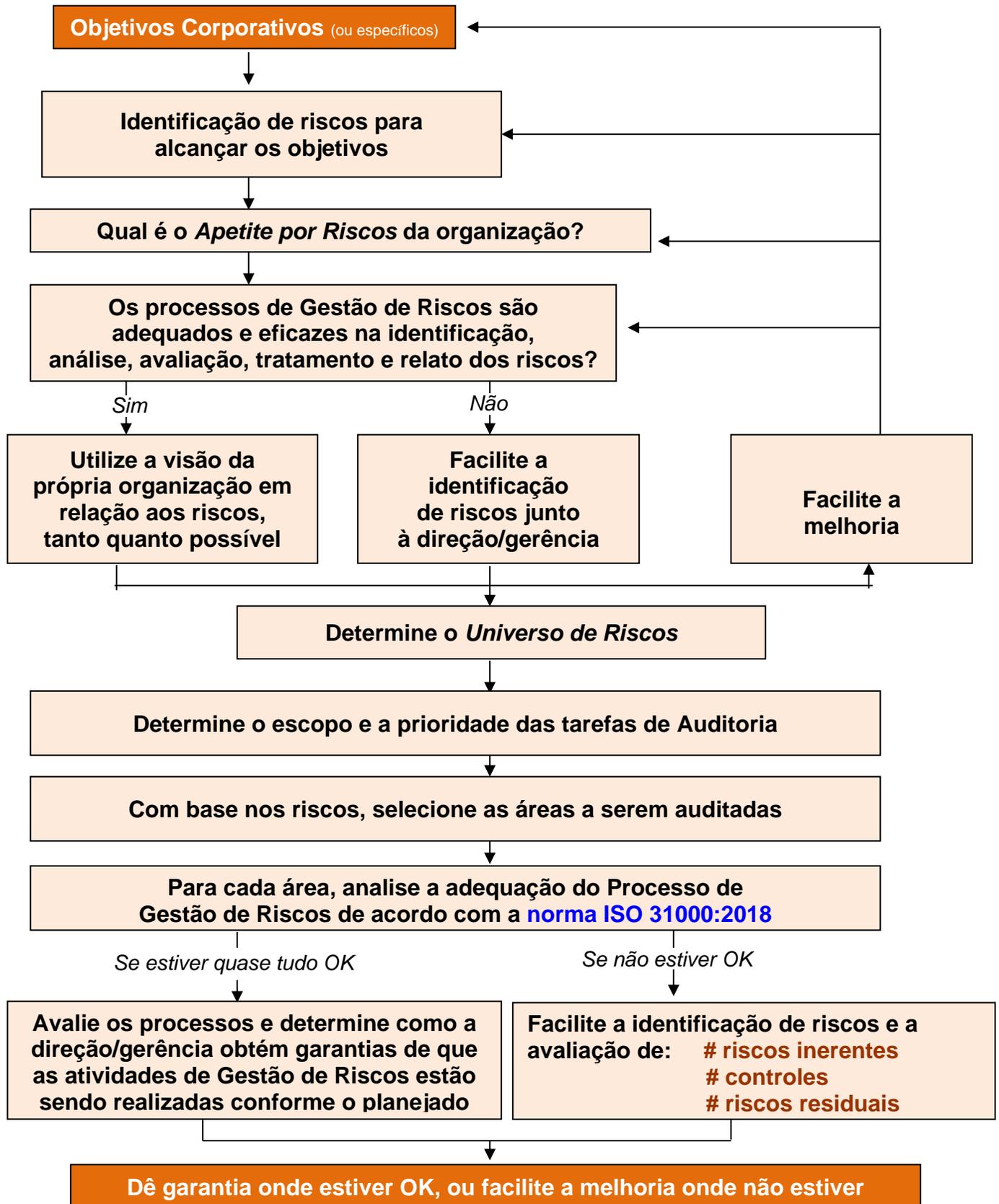
<sup>2</sup> O termo **Risco**, na nova norma internacional ISO 31000:2018, é definido como “*Efeito da incerteza nos objetivos*”. Portanto, os objetivos abrangidos pela Gestão de Riscos incluem tanto os objetivos estratégicos como os objetivos específicos de uma organização (por exemplo: os objetivos da Qualidade, Ambientais, de *Compliance*, etc.). Enfim, a Gestão de Riscos do século XXI engloba a tomada de decisões sobre qualquer tema que afeta/impacta (negativa ou positivamente) os seres humanos, a sociedade, o meio ambiente, as organizações...

O papel da auditoria interna é avaliar até que ponto uma abordagem robusta de Gestão de Riscos é, conforme planejado, adotada e aplicada em toda a organização pela direção, gerência, etc., para reduzir riscos a um nível aceitável (o chamado *Apetite por Riscos* da organização).

Embora a principal contribuição da auditoria interna seja dar garantias sobre os controles e tratamentos de riscos existentes numa empresa privada ou instituição pública, a auditoria interna também pode aconselhar sobre outros aspectos de resposta aos riscos como, por exemplo, as decisões de tratar, terminar, transferir ou tolerar os riscos (os chamados “4T”).

A abordagem do QSP para a **Auditoria Baseada em Riscos** está descrita de forma esquemática na página a seguir.

## Abordagem do QSP para a ABR - Auditoria Baseada em Riscos



## A prática da ABR - Auditoria Baseada em Riscos

Pontos importantes:

- O escopo da ABR inclui riscos estratégicos, riscos do negócio e riscos operacionais.
- O ponto de partida é determinar se a organização estabeleceu objetivos apropriados, e então determinar se a companhia tem ou não um processo adequado para identificar, avaliar e manejar os riscos que causam impacto nesses objetivos.
- Em um ambiente maduro de Gestão de Riscos, o foco do trabalho de auditoria pode ser:
  - Auditar a infraestrutura de Gestão de 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 à Gestão de Riscos específicos. Caso vários riscos sejam controlados através de um sistema ou processo comum, talvez seja apropriado realizar uma auditoria combinada desse sistema ou processo.
- Em ambientes menos maduros de Gestão de Riscos, caso as tarefas das auditorias individuais focalizem predominantemente todo um sistema, processo ou unidade de negócio, a auditoria interna deve analisar criticamente os objetivos do negócio e os processos de Gestão de Riscos, dentro de cada uma dessas partes auditáveis.
- Quando os processos de Gestão de Riscos estiverem adequados e enraizados, a auditoria interna, sempre que possível, irá 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 nos processos de Gestão de Riscos, a auditoria interna deve realizar sua própria Avaliação de Riscos (em conjunto com a direção, gerência, etc.), 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 tarefa de auditoria individual deve ser o de assegurar que os riscos estão sendo gerenciados dentro de um nível aceitável (conforme definido no *Apetite por Riscos* da organização), ou facilitar e/ou definir melhorias, conforme necessário.

## Processo Contínuo de Gestão de 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*<sup>3</sup> e a abordagem da auditoria interna que pode ser adotada em cada estágio.

<b>Grau de Maturidade de Riscos</b>	<b>Características Principais</b>	<b>Abordagem da Auditoria Interna</b>
<b>Ingênuo</b>	Nenhuma abordagem formal desenvolvida para a Gestão de Riscos.	Promove a Gestão de Riscos e se baseia na Avaliação de Riscos da própria auditoria.
<b>Consciente</b>	Abordagem para a Gestão de Riscos dispersa em “silos”.	Promove a abordagem corporativa de Gestão de Riscos e se baseia na Avaliação de Riscos realizada pela própria auditoria.
<b>Definido</b>	Estratégia e políticas implementadas e comunicadas, <i>Apetite por Riscos</i> definido.	Facilita a Gestão de Riscos/ Relaciona-se com a Gestão de Riscos, e usa a Avaliação de Riscos pela direção/ gerência quando apropriado.
<b>Gerenciado</b>	Abordagem corporativa para a Gestão de Riscos, desenvolvida e comunicada.	Audita os processos de Gestão de Riscos e utiliza a Avaliação de Riscos pela direção/gerência conforme apropriado.
<b>Habilitado</b>	Gestão de Riscos e controles internos totalmente incorporados às operações.	Audita os processos de Gestão de Riscos e utiliza a Avaliação de Riscos pela direção/gerência, conforme apropriado.

Cada organização deve determinar como pretende implementar/melhorar a Gestão de Riscos (*preferencialmente adotando como referência a [norma ISO 31000:2018](#)*). Isso ajudará a determinar seu *Apetite por Riscos* e o nível de *Maturidade de Riscos* da organização. Por exemplo, nem todas as empresas desejarão atingir completamente o grau de maturidade *Habilitado*, pois talvez tenham que pesar os custos em relação à

<sup>3</sup> Termo simplificado que utilizamos no QSP quando nos referimos à *Maturidade da Gestão de Riscos* de uma organização.

visão que têm dos benefícios potenciais. Cabe à alta direção e à equipe de gerentes determinar até qual ponto desse processo contínuo desejarão chegar.

Além da *Maturidade de Riscos* da organização, a extensão da Avaliação de Riscos que a própria auditoria interna deve realizar (em conjunto com a direção/gerências) também depende do grau e da velocidade das mudanças estratégicas e organizacionais.

## Conclusão

A Auditoria Baseada em Riscos pode fornecer maior eficácia às auditorias internas, incluindo as [auditorias de sistemas de gestão](#), conforme as circunstâncias exigiam. É, porém, uma abordagem que focaliza as **questões que realmente interessam** à organização (em qualquer área: Controladoria, Finanças, *Compliance*, Qualidade, *Security*, *Segurança e Saúde*, Meio Ambiente, etc.).

A ABR fornece garantias em relação à estrutura para gerenciar riscos de uma organização. A Auditoria Baseada em Riscos possibilita que a auditoria interna se ligue diretamente a essa estrutura, alavancando dessa forma as sinergias.

---

### Conheça também:

- ✓ **Manual:** [Gestão de Riscos - Diretrizes para a Implementação da ISO 31000:2018](#)
- ✓ **Curso:** [Administração Pública - Capacitação em Gestão de Riscos e Auditoria Baseada em Riscos - ISO 31000:2018](#)

## Principais termos e definições da ABR<sup>4</sup>

**Análise de Riscos:** uso sistemático das informações disponíveis para determinar a probabilidade de que ocorram eventos especificados e a magnitude de suas consequências, isto é, seu impacto.

**Apetite por Riscos:** nível de risco considerado aceitável pelo conselho ou direção, que pode ser estabelecido em relação à organização como um todo, para grupos diferentes de riscos ou em termos de riscos individuais.

**Arcabouço (ou Estrutura ou *Framework*) de Gestão de Riscos:** totalidade de estruturas, metodologia, procedimentos e definições que uma organização decidiu utilizar para implementar seus processos de gestão de riscos.

**Auditoria Baseada em Riscos:** metodologia que fornece garantia de que o arcabouço de Gestão de Riscos está operando conforme requerido pelo conselho.

**Avaliação de Riscos:** processo utilizado para determinar as prioridades da Gestão de Riscos através da comparação do nível de risco com padrões, níveis-alvo de risco ou outros critérios pré-determinados.

**Cadastro de Riscos:** lista completa, identificada pela direção, dos riscos que ameaçam os objetivos da organização.

**Conselho:** grupo diretivo de uma organização, como o conselho de administração, conselho de diretores, chefe de uma agência ou órgão legislativo, conselho de governantes ou curadores de uma organização sem fins lucrativos.

**Controle:** qualquer ação tomada pela direção, pelo conselho e por outras partes para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam atingidos. A direção planeja, organiza e dirige o desempenho das ações necessárias para manter os riscos em um nível aceitável, ou para aumentar a probabilidade do resultado desejado.

**Corporação:** qualquer organização estabelecida para atingir um conjunto de objetivos.

**Diretor:** membro de um conselho de comando, como o diretor da organização, curador, conselheiro ou governante.

**Facilitação:** trabalho com um grupo (ou indivíduo) para tornar mais fácil para o grupo (ou indivíduo) atingir os objetivos que o grupo tenha estabelecido para a reunião ou atividade. Isso envolve ouvir, observar, questionar e apoiar o grupo e seus membros. Não envolve realizar o trabalho nem tomar decisões.

**Garantia:** apresentação de uma opinião ou conclusão em relação à credibilidade das informações divulgadas e ao processo que fornece tais informações, ou em relação à

---

<sup>4</sup> Este glossário foi produzido originalmente em 2007 e aplica-se à abordagem do QSP para a ABR - *Auditoria Baseada em Riscos*. Ele é coerente e está alinhado à nova terminologia internacional de Gestão de Riscos, igualmente adotada pelo QSP. Para uma melhor compreensão de conceitos, recomendamos consultar também o **ISO Guia 73**.

confiabilidade dos processos de acordo com sua conformidade com certos critérios. O receptor da opinião pode ficar seguro ou não, dependendo de outras influências por ele sofridas.

**Gestão Corporativa de Riscos (*Gestão Total de Riscos*):** processo estruturado, consistente e contínuo em toda a organização, para identificar, avaliar, estabelecer respostas e relatar oportunidades e ameaças que afetam a consecução de seus objetivos.

**Identificação de Riscos:** processo para determinar quais eventos podem ocorrer e afetar os objetivos da organização, e quais são suas causas-raízes.

**Manejo de Riscos:** implementação das respostas a riscos, que reduzem suas ameaças para abaixo do nível do apetite por riscos. Quando isso não for possível, deve-se relatar o risco ao conselho.

**Maturidade de Riscos:** grau de adoção e aplicação, por parte da direção, de uma abordagem de Gestão de Riscos robusta, conforme planejada, em toda a organização, a fim de identificar, avaliar, decidir sobre respostas e relatar oportunidades e ameaças que afetam a consecução dos objetivos da organização.

**Monitoramento:** processos que relatam à direção, em intervalos apropriados, o sucesso, ou não, das respostas a riscos.

**Plano de Auditorias Periódicas:** lista de auditorias a serem conduzidas em um período de tempo especificado.

**Pontuação de Controle:** diferença entre a pontuação do risco inerente e a pontuação do risco residual em um sistema quantitativo. Quanto maior for o valor, maior será a importância da gama de respostas que criarão a diferença. Também conhecida como 'pontuação de resposta'.

**Processo de Avaliação de Riscos:** processo completo de identificação, análise e avaliação de riscos.

**Processos de Gestão de Riscos:** processos para identificar, analisar, avaliar, manejar e controlar eventos ou situações potenciais, a fim de fornecer garantia adequada em relação à consecução dos objetivos da organização.

**Respostas a Riscos:** meios através dos quais uma organização decide gerenciar cada risco. As principais categorias são: eliminar a atividade geradora do risco; tolerar o risco; transferi-lo para outra organização; ou tratá-lo, reduzindo seu impacto ou probabilidade. Controles internos são uma forma de tratar um risco.

**Risco:** possibilidade de ocorrência de um evento que terá um impacto na consecução dos objetivos. O risco é mensurado em termos de consequência e probabilidade

**Risco Inerente (ou Bruto):** situação de um risco (mensurado em termos de impacto e probabilidade) sem levar em consideração qualquer resposta ao risco que a organização possa já ter adotado.

**Risco Residual (ou Líquido):** situação de um risco (mensurado em termos de impacto e probabilidade) após levar em consideração qualquer resposta de Gestão de Riscos que a organização possa já ter adotado.

**Serviços de Consultoria:** atividades de aconselhamento e outras relacionadas a serviços a clientes, cuja natureza e escopo são acordados com o cliente e cuja finalidade é agregar valor e melhorar os processos da organização de governança, Gestão de Riscos e os de controle, sem que o auditor interno assuma responsabilidades gerenciais. São exemplos: pareceres, conselhos, facilitação e treinamento.

**Serviços de Garantia:** exame objetivo de evidências com o propósito de fornecer à organização uma avaliação independente dos processos de gestão de riscos, processos de controle ou processos de governança. São exemplos: exames financeiros, de desempenho, de conformidade legal, de segurança e *due diligence*.

**Universo de Auditorias:** lista de auditorias que mostra os processos por elas cobertos e a importância ou prioridade desses processos.

## **Certificação Profissional Internacional**

Participe do **Exame Nacional** para a obtenção da Certificação Internacional **C31000 - Certified ISO 31000 Risk Management Professional**.  
Agregue este importante diferencial ao seu currículo!

**Como sua Empresa pode Obter a Certificação / Declaração de Conformidade em Gestão de Riscos (baseada na norma ISO 31000)**

**[Assista a este Vídeo...](#)**