Estrutura de Gestão de Riscos

Orientações da Susep ao Mercado

Abril/2020 **Versão 2.0**

Sumário

1. INTRODUÇÃO 3
   1.1. Base Legal 3
   1.2. Abrangência 3
   1.3. Unidades Responsáveis 3
   1.4. Contato para Esclarecimento de Dúvidas 3
   1.5. Contextualização 4
2. CONSIDERAÇÕES GERAIS SOBRE A EGR 4
   2.1. Inter-relação com o Sistema de Controles Internos 5
   2.2. Princípio da Proporcionalidade 6
3. O PROCESSO DE GESTÃO DE RISCOS 7
   3.1. Identificação/Avaliação de Riscos 7
   3.2. Mensuração de Riscos 9
   3.3. Tratamento de Riscos 11
   3.4. Monitoramento de Riscos 12
4. SUPERVISÃO DA GESTÃO DE RISCOS 14
   4.1. O Modelo das 3 Linhas de Defesa 14
   4.2. Gestor de Riscos 15
      4.2.1. Formalização 15
      4.2.2. Âmbito de Atuação 16
      4.2.3. Conflitos de Interesses 19
   4.3. Auditoria Interna 21
   4.4. Diretoria e Conselho de Administração 21
5. POLÍTICAS E DIRETRIZES 22
   5.1. Apetite por Risco 23
   5.2. Políticas 24
      5.2.1. O Conceito de Política 24
      5.2.2. Política de Gestão de Riscos (e outras políticas relacionadas) 26
      5.2.3. Âmbito de Definição das Políticas 28
6. CASOS ESPECIAIS 29
   6.1. Possibilidade de Dispensas (DPVAT e Run-off) 29

6.1.1. Aspectos Gerais 29
6.1.2. Considerações Específicas Sobre a Operação do DPVAT 31
6.1.3. Considerações Específicas Sobre Ramos em Run-off.....32
6.2. Terceirização das Funções do Gestor de Riscos.....32
6.3. Delegação das Funções do Gestor de Riscos para Matriz Estrangeira (Resseguradores) 34

1. INTRODUÇÃO

1.1. BASE LEGAL

Capítulo II do Título II da Circular Susep n° 512, de 2015.

1.2. ABRANGÊNCIA

- Sociedades Seguradoras;
- Entidades Abertas de Previdência Complementar;
- Sociedades de Capitalização; e
- Resseguradores Locais.

1.3. UNIDADES RESPONSÁVEIS

Unidade	Competência
DIR3/CGREP/CORAC corac.rj@susep.gov.br (21) 3233-4065 (ramal: 4236)	Compete à Coordenação de Regulação de Riscos, Ativos e Controles Internos (DIR3/CGREP/CORAC) efetuar a regulação do tema Gestão de Riscos.
DIR3/CGCON cgcon.rj@susep.gov.br (21) 3233-4064 (21) 3233-4065	Compete à Coordenação-Geral de Supervisão Consolidada (DIR3/CGCON) e suas coordenações realizar a fiscalização presencial e à distância das entidades supervisionadas com vistas a verificar o cumprimento de normas e padrões relativos à Gestão de Riscos.

1.4. CONTATO PARA ESCLARECIMENTO DE DÚVIDAS

Este manual tem como principal objetivo servir como um guia para melhor entendimento dos conceitos, exigências e possibilidades contidos na regulação da Estrutura de Gestão de Riscos. Dúvidas que envolvam tais aspectos devem ser endereçadas para a CORAC.

Já dúvidas relativas ao tema Estrutura Gestão de Riscos que envolvam procedimentos ligados às fiscalizações presenciais e à distância, ao envio ou disponibilização de informações e documentos à Susep (ex.: Questionário de Riscos do FIP), às autorizações e permissões (ex.: terceirização do Gestor de Riscos, delegação das funções do Gestor de Riscos de resseguradores para sua matriz estrangeira, utilização de Fatores Reduzidos de Risco, etc.), à comunicação de nomeação ou destituição de Gestor de Riscos, assim como a outras questões mais operacionais da supervisão pela Susep da Estrutura de Gestão de Riscos das supervisionadas, devem ser endereçadas para a CGCON. Os pedidos e comunicações relativos a tais assuntos também deverão ser encaminhados à CGCON.

1.5. CONTEXTUALIZAÇÃO

Em 18 de dezembro de 2015 a Susep publicou a Circular nº 521, que incluiu um novo capítulo sobre a "Estrutura de Gestão de Riscos" na Circular Susep nº 517/2015 (Cap. II do Título II). A vigência desse capítulo iniciou-se em 1º de janeiro de 2016, tendo sido concedidos 2 anos de prazo (até 31 de dezembro de 2017) para que as supervisionadas se adequassem completamente aos seus comandos.

Esta regulamentação foi mais uma importante iniciativa da Susep na direção do chamado Pilar 2 (qualitativo) da Supervisão Baseada em Riscos, vindo complementar o conjunto de normas já existentes neste contexto (ex: Circulares Susep nº 249/2004 e 445/2012).

A Estrutura de Gestão de Riscos foi definida como o *"conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda uma organização"* (Circ. 517, art. 108-B, inciso III). Sendo assim, ela engloba aspectos ligados à estrutura organizacional, funções, políticas, processos, ferramentas, técnicas e qualquer outro componente que vise a garantir:

- Que a gestão de riscos seja efetivamente levada a cabo pela organização, ou seja, que os riscos que podem afetá-la sejam efetivamente identificados, avaliados, mensurados, tratados e monitorados; e
- Que a gestão de riscos seja continuamente supervisionada pela própria organização, visando à identificação e correção de deficiências de forma a promover seu aperfeiçoamento.

Pelo exposto, é possível perceber que o processo de gestão de riscos deve perpassar todos os processos de negócio relevantes de uma companhia e que a Estrutura de Gestão de Riscos (ou, de forma resumida, EGR), que permite que isto seja feito de forma cada vez mais eficaz, pode ser implementada de diversas maneiras, de acordo com as características e a realidade de cada organização.

Sendo assim, a regulamentação da EGR baseia-se em princípios gerais de gestão de riscos e governança corporativa, o que, se por um lado possibilita essa diversidade de implementações (o que é altamente desejável), por outro pode gerar certa insegurança no mercado supervisionado quanto à adequação das soluções adotadas na prática.

Tendo isto em vista, o objetivo deste documento não é definir um *framework*[1] de referência que deve ser seguido pelo mercado segurador, mas sim apresentar alguns conceitos subjacentes à regulamentação da EGR e uma série de interpretações já pacificadas pela Susep quanto aos seus principais requisitos. Com isso, a Susep espera contribuir para um melhor entendimento da regulamentação, possibilitando que as sociedades supervisionadas desenvolvam Estruturas de Gestão de Riscos em conformidade com ela.

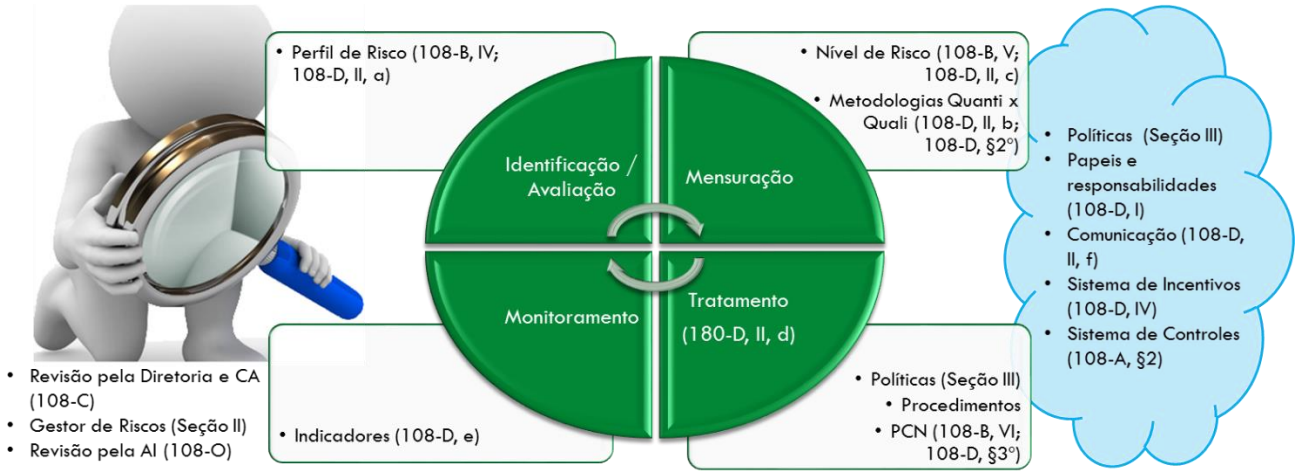
2. CONSIDERAÇÕES GERAIS SOBRE A EGR

A gestão de riscos é um processo, definido na Circular 517/2015 como o conjunto de *"atividades coordenadas para identificar, avaliar, mensurar, tratar e monitorar os riscos de uma organização, tendo por base a adequada compreensão dos tipos de risco, de suas características e*

[1] Alguns frameworks bastante difundidos que podem servir como referências são o COSO ERM e o ISO 31000.

interdependências, das fontes de riscos e de seu potencial impacto sobre o negócio" (art. 108-B, inciso I).

De forma geral, como os riscos que podem afetar a organização são dinâmicos, variando de acordo com a evolução dos ambientes interno e externo, é essencial que o processo de gestão de riscos seja realizado de forma recorrente, para garantir que tais riscos continuem a ser adequadamente gerenciados ao longo do tempo. Sendo assim, este processo pode ser representado por um ciclo, tal como demonstrado na figura abaixo:



É importante notar que esta ilustração pode ser dividida em 3 partes:

- O processo de gestão de riscos propriamente dito (no centro), apresentado como um ciclo de 4 etapas (Identificação/Avaliação – Mensuração – Tratamento – Monitoramento) que serão oportunamente discutidas na seção 3;
- A necessidade de uma supervisão contínua da gestão de riscos pela própria organização (boneco que segura a lupa à esquerda) visando à melhoria contínua do processo, o que será tratado na seção 4; e
- O ambiente interno da organização (nuvem à direita), que influencia profundamente não só o processo de gestão de riscos como também a sua supervisão. Neste contexto, destacam-se as políticas e diretrizes organizacionais abordadas na seção 5.

Vale destacar também que a figura faz referência a diversos dispositivos do Título II, Capítulo II da Circular Susep nº 517/2015, buscando situá-los no contexto descrito. Por ora, a intenção não é explorar cada um deles em detalhe (o que será feito mais adiante neste documento), mas apenas demonstrar como esses dispositivos se inter-relacionam para definir o que se espera minimamente da Estrutura de Gestão de Riscos.

2.1. Inter-relação com o Sistema de Controles Internos

A Circular 517 dispõe:

> "A Estrutura de Gestão de Riscos da supervisionada deverá ser alinhada com seu Sistema de Controles Internos, independente da maneira como ambos estejam implementados na estrutura organizacional." (art. 108-A, § 2º)

Este dispositivo reforça a necessidade de alinhamento entre a Estrutura de Gestão de Riscos e o Sistema de Controles Internos (SCI) definido pela Circular Susep nº 249/2004, até porque esta já estabelecia que os controles da supervisionada devem ser consistentes com os riscos de suas operações (art. 1º, parágrafo único). De fato, espera-se que grande parte dos controles de uma supervisionada refira-se diretamente ao tratamento dos riscos que podem afetá-la (por exemplo, impedindo que determinada operação seja realizada ou impondo restrições para tal).

No entanto, é importante esclarecer que o alinhamento da EGR com o SCI refere-se a processos e não à estrutura organizacional. Ou seja, não existe nenhum requisito que imponha que uma área de Controles Internos da empresa tenha que ser necessariamente responsável pela gestão de riscos, podendo a empresa optar por tratar esses dois assuntos em unidades distintas. Independentemente da opção adotada, o que se espera é que o SCI dê ênfase aos principais riscos da companhia, que serão gerenciados de acordo com os preceitos definidos pela EGR.

A título de exemplo, o alinhamento do SCI com a EGR pode se manifestar na definição de níveis de controle mais rigorosos para os negócios que tenham potencial de trazer mais riscos para a empresa, na definição de prioridades da Auditoria Interna, na revisão do SCI face a novos riscos identificados, etc.

2.2. PRINCÍPIO DA PROPORCIONALIDADE

É fato que a estrutura de gestão de Riscos pode fazer uso de uma ampla gama de ferramentas, técnicas, procedimentos e arranjos organizacionais distintos. Entretanto, considerando-se a realidade e as peculiaridades das operações de cada empresa, algumas das opções disponíveis podem se mostrar inadequadas ou desvantajosas em termos de custo x benefício.

De forma geral, uma empresa de grande porte, que opera com diversas linhas de negócio, tende a estar exposta a mais riscos do que uma outra de menor porte e com operações mais limitadas. Sendo assim, para a primeira empresa, poderia ser adequado (e factível) adotar ferramentas e técnicas mais sofisticadas de gestão de riscos (ex.: mensuração quantitativa de riscos), bem como implantar uma estrutura organizacional mais robusta (ex.: criação de uma Diretoria de Riscos e *Compliance*). Por outro lado, isso não significa que a segunda empresa não precise implantar uma EGR, mas sim que as soluções adotadas por ela podem ser mais simplificadas ou rudimentares (ex: mensuração qualitativa de riscos e nomeação de um gestor de riscos que acumule outras funções – desde que não haja conflito), embora suficientes frente aos seus riscos.

É por isso que a regulamentação diz:

> "A Estrutura de Gestão de Riscos deverá ser proporcional à exposição da supervisionada a riscos e compatível com a natureza, escala e complexidade de suas operações." (art. 108-A, § 1º)

Este enunciado costuma ser conhecido como "Princípio da Proporcionalidade" e sua aplicação, muitas vezes considerada complexa devido ao alto grau de julgamento envolvido, deve ser exercitada.

Vale ressaltar que não se trata meramente de uma questão de tamanho da empresa (exigir mais porque a empresa é grande), mas sim de ponderar, ante os riscos que podem afetar sua operação, se

a EGR não é excessivamente enxuta ou precária, trazendo vulnerabilidade ao processo de gestão de riscos. Nestes casos, é importante notar que a Susep pode exigir adequações com base no artigo 108-Q da Circular 517, de preferência fundamentada em preocupações concretas oriundas de deficiências que tenham sido constatadas.

3. O PROCESSO DE GESTÃO DE RISCOS

Abaixo destacamos a figura que representa, de forma resumida, o processo de gestão de riscos.

Para fins didáticos, podemos dividi-lo em 4 etapas, a saber:

- Identificação/Avaliação de Riscos;
- Mensuração de Riscos
- Tratamento de Riscos; e
- Monitoramento de Riscos

Antes de abordarmos em detalhe cada uma delas, convém observar que, embora apresentadas de forma lógica e sequencial, na prática as etapas do processo podem apresentar atalhos e sobreposições. Por exemplo, ao se identificar um risco já é possível vislumbrar alternativas de tratamento que seriam interessantes, entretanto, a divisão por etapas é útil não só para facilitar o entendimento conceitual de todo o processo como também para permitir que ele seja implementado de forma organizada pela companhia.

Isto porque, de forma geral, espera-se que os resultados de uma etapa só poderão ser plenamente alcançados se cumpridas as etapas precedentes. Afinal, no exemplo mencionado antes, como seria possível garantir que a estratégia de tratamento pensada inicialmente é de fato a melhor se não houver uma análise adequada do potencial impacto do risco (onde a estratégia pode se mostrar demasiadamente custosa) ou sem serem considerados outros tratamentos alternativos?

Por fim, antes de passarmos a cada uma dessas etapas, é interessante destacar que o artigo 108-D da Circular Susep nº 517/2015 define requisitos a serem observados para sua realização, além de resultados ou documentações que devem ser produzidos.

3.1. IDENTIFICAÇÃO/AVALIAÇÃO DE RISCOS

Esta etapa inicial consiste em relacionar da forma mais abrangente possível os eventos que podem afetar a organização. Este passo é de extrema importância, uma vez que riscos não identificados não poderão ser mensurados, tratados e monitorados.

O reconhecimento de riscos certamente é facilitado pela existência de informações históricas e pelo registro de perdas pela organização (ex.: BDPO[2]), mas também é importante fazer uso da opinião de especialistas, de informações externas entre outros, para permitir identificar riscos emergentes ou que nunca tenham se materializado antes.

Na Circular Susep nº 517/2015, esta lista de riscos recebeu a denominação de Perfil de Risco, termo que foi definido como a *"descrição do conjunto de riscos a que uma organização encontra-se exposta, de acordo com os processos e metodologias empregados para a identificação de riscos"* (art. 108-B, inc. IV). Logo, a supervisionada deverá documentar seu Perfil de Riscos como resultado da etapa de Identificação/Análise de riscos, embora o formato desse documento (planilha, texto, etc.) seja de livre escolha da empresa.

Vale ressaltar que a regulamentação também estabelece algumas informações básicas que deverão constar no Perfil de Risco, que resultam de uma avaliação das características de cada risco identificado. No texto da norma:

> "Elaboração e manutenção de um Perfil de Risco que descreva cada risco identificado, indique sua categoria e suas causas e possibilite atribuir responsabilidades em relação à sua gestão." (art. 108-D, inc. II, alínea "a")

Verifica-se, portanto, a necessidade de identificar as causas de cada risco e as possíveis pessoas ou áreas responsáveis pelo seu controle direto (1ª Linha de Defesa - ver seção 4.1). Além disso, a norma exige que a cada risco seja atribuída uma "categoria", sendo que, para os riscos que se enquadrem nas definições já adotadas pelo CNSP nas regulamentações dos Capitais de Risco de Subscrição[3], de Crédito[4], de Mercado[5] ou Operacional[6], as respectivas categorias utilizadas deverão ser obrigatoriamente "Risco de Subscrição", "Risco de Crédito", "Risco de Mercado" e "Risco Operacional" (Circ. Susep nº 517/2015, art. 108-D, §1º, inc. I).

Por exemplo, o risco de longevidade, por se tratar de uma "possibilidade de ocorrência de perdas que contrariem as expectativas da supervisionada, associadas, diretamente ou indiretamente, às bases técnicas utilizadas para cálculo de prêmios, contribuições, quotas e provisões técnicas" (Res. CNSP nº 321/2015, art. 35, inc. I), deverá ser categorizado no Perfil de Risco como um "Risco de Subscrição",

[2] Banco de Dados de Perdas Operacionais – para maiores detalhes consultar a Circular Susep nº 517/2015, Título I, Capítulo IV, Seção II.

[3] Possibilidade de ocorrência de perdas que contrariem as expectativas da supervisionada, associadas, diretamente ou indiretamente, às bases técnicas utilizadas para cálculo de prêmios, contribuições, quotas e provisões técnicas (Res. CNSP nº 321/2015, art. 35, inc. I).

[4] Possibilidade de ocorrência de perdas associadas ao não cumprimento, pelo tomador ou contraparte, das suas respectivas obrigações financeiras nos termos pactuados, e/ou da desvalorização dos recebíveis decorrente da redução na classificação de risco do tomador ou contraparte (Res. CNSP nº 321/2015, art. 35, inc. III).

[5] Possibilidade de ocorrência de perdas resultantes de flutuações dos mercados financeiros, que causam mudanças na avaliação econômica de ativos e passivos das supervisionadas (Res. CNSP nº 321/2015, art. 35, inc. IX).

[6] Possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou decorrentes de fraudes ou eventos externos, incluindo-se o risco legal e excluindo-se os riscos decorrentes de decisões estratégicas e à reputação da instituição (Res. CNSP nº 321/2015, art. 35, inc. V).

sendo vedado o uso de denominações alternativas, tais como "Riscos - Vida", "Riscos Biométricos" ou quaisquer outras que a imaginação seja capaz de produzir.

Observa-se, no entanto, que pode haver riscos que não se enquadrem nas definições dos capitais já regulamentados pelo CNSP, notadamente riscos políticos, estratégicos, reputacionais, de liquidez, etc. Neste caso, a supervisionada fica livre para definir categorias adicionais às 4 obrigatórias da maneira que melhor lhe aprouver (Circ. Susep nº 517/2015, art. 108-D, §1º, inc. II). Vale destacar que essas definições devem ser documentadas pela companhia, de preferência na Política de Gestão de Riscos, de modo a permitir sua aplicação de forma consistente.

A Susep entende que o uso de categorias de risco facilita a organização racional e lógica do processo de gestão de riscos, contribuindo para a concepção da EGR. Além disso, a definição de categorias de uso obrigatório contribui para a adoção de uma terminologia comum no mercado segurador, facilitando a comunicação entre este e a Autarquia.

Outro ponto que merece ser destacado diz respeito à "manutenção do Perfil de Risco", conforme expresso no art. 108-D, inc. II, alínea "a" da Circular 517/2015. Este trecho deixa claro o caráter cíclico do processo de gestão de riscos, dado que, em função da evolução da própria organização e do meio em que ela se encontra inserida, espera-se que os riscos que a afetam variem ao longo do tempo. Conforme destacaremos mais adiante, é importante que a companhia monitore esta evolução do Perfil de Riscos e estabeleça critérios que disparem outros tipos de ações, como por exemplo uma reavaliação extraordinária da EGR por parte da Diretoria, também prevista na regulamentação (art. 108-C, §1º). É essencial que critérios deste tipo, que requerem a adoção de outras ações, estejam definidos na Política de Gestão de Riscos.

Ainda com relação ao Perfil de Riscos, a Susep considera uma boa prática que sua elaboração e, posteriormente, suas revisões, sejam realizados de forma abrangente, com envolvimento e participação das diversas unidades operacionais da companhia. O papel do Gestor de Riscos neste contexto deve ser o de facilitador, auxiliando as diversas áreas na identificação/avaliação de seus riscos e consolidando os resultados de forma a garantir sua consistência.

3.2. MENSURAÇÃO DE RISCOS

Esta é a etapa que se segue à identificação e análise inicial dos riscos e seu objetivo é começar a segregá-los em níveis de relevância para que, mais à frente, se definam as prioridades e estratégias de tratamento mais adequadas para cada caso. Para auxiliar nesse sentido a Circular 517/2015 trouxe o conceito de Nível de Risco, definido como a *"magnitude de um risco, expressa em termos da combinação de sua probabilidade e impacto"* (art. 108-B, inc. V).

Sendo assim, a Circular 517/2015 requer:

> "Estimação do Nível de Risco, com base nas metodologias requeridas pela alínea "b", para cada um dos riscos identificados;
> (art. 108-D, inc. II, alínea "c")

Por sua vez, a alínea "b" mencionada no dispositivo acima transcrito admite que as metodologias utilizadas para definição do Nível de Risco podem ser qualitativas ou quantitativas.

De forma geral, a Susep encara que o desenvolvimento de metodologias quantitativas, com base em técnicas como VaR (*Value at Risk*) ou outros modelos estatísticos aplicados aos dados operacionais da companhia é uma boa prática, porém, frisa-se que, como regra geral, isto não é obrigatório. O importante é que, de alguma forma, a companhia busque mensurar, mesmo que de forma qualitativa, os Níveis de Risco, o que pode ser feito de maneira empírica, com base na experiência e opinião de profissionais da empresa e outros especialistas. No entanto, a norma impõe que pelo menos dois aspectos devem ser considerados na definição do Nível de Risco: a probabilidade de ocorrência do risco e o potencial impacto de sua materialização.

Especialmente no tocante aos processos de mensuração qualitativos, destacamos novamente a necessidade de envolvimento das diversas unidades operacionais da companhia, sendo de suma importância que se definam critérios que visem a reduzir a subjetividade da avaliação e garantir sua consistência e homogeneidade. Por exemplo, se o impacto de cada risco tiver que ser descrito como "Alto", "Médio" ou "Baixo", pode-se definir "Alto" como "acima de R$ X", onde X é um valor financeiro que guarda alguma relação com o Apetite por Risco da organização. Este tipo de critério deve ser documentado pela supervisionada, de preferência em sua Política de Gestão de Riscos. Convém que o Gestor de Riscos atue como facilitador de todo o processo.

Quando da utilização de metodologias qualitativas, dada a necessidade desse esforço concentrado de diversas áreas da empresa e a relativa simplicidade das técnicas de mensuração empregadas, pode ser interessante para a empresa realizar simultaneamente as etapas de Identificação/Análise e Mensuração, possivelmente com algum refinamento da mensuração *a posteriori* (ex: revisão por comitê, opinião de especialistas, etc.).

Já quanto à mensuração quantitativa, o mais desejável seria que as unidades responsáveis por cada risco pudessem desenvolver suas metodologias de mensuração com base em diretrizes gerais definidas na Política de Gestão de Riscos (ex. nível de confiança, medida de risco, etc.). Entretanto, como isso requer grande maturidade em termos de gestão de riscos, inicialmente pode ser mais adequado concentrar a mensuração quantitativa de todos os riscos em uma única área (possivelmente a área responsável pela supervisão da EGR), cabendo às demais unidades disponibilizar as informações necessárias. De qualquer forma, assim como para a mensuração qualitativa, se requer que as metodologias estejam documentadas. No caso de mensuração quantitativa, deve-se definir explicitamente as fontes dos dados utilizados.

Metodologias qualitativas e quantitativas podem (e em muitos casos devem) ser utilizadas em conjunto, devendo a empresa estabelecer em sua Política de Gestão de Riscos como os resultados de ambas são levados em consideração.

Como resultado da etapa de Mensuração, a empresa deve documentar o Nível de Risco para cada risco identificado, sendo que a norma não estabelece nomenclatura específica para tais níveis. A empresa pode, portanto, adotar uma classificação do tipo "Alto / Médio / Baixo" ou "Prioridade 1 / Prioridade 2 / Prioridade 3 / Prioridade 4", devendo tais níveis ser claramente definidos em termos da combinação de probabilidade e impacto de cada risco (art. 108-B, inc. V).

Cumpre ainda observar que, apesar dos conceitos de Perfil de Riscos e de Nível de Risco serem distintos, nada impede que ambas as informações constem do mesmo documento (ex.: uma tabela). Opcionalmente, a empresa pode optar por representar os Níveis de Risco através de uma Matriz de Riscos, onde cada risco tem um código que o identifica em uma lista que contém as informações

requeridas em termos de Perfil de Riscos (ex.: Dicionário de Riscos). Aliás, nada impede que as próprias informações do Perfil de Riscos estejam dispersas em mais de um documento.

Entretanto, apesar de toda essa flexibilidade, é essencial que todas as informações requeridas pela norma estejam acessíveis para serem utilizadas internamente e que possam ser facilmente apresentadas à Susep mediante solicitação.

3.3. TRATAMENTO DE RISCOS

A etapa de tratamento dos riscos consiste em definir que ações a organização irá adotar em relação a eles. As estratégias normalmente consideradas são (art. 108-B, inc. II):

- Evitar: geralmente consiste em não realizar uma operação e pode ser adequada quando a organização conclui que determinado risco possui um Nível de Risco muito elevado (ex: probabilidade e impacto muito altos). Entretanto, antes de se adotar esta alternativa, pode ser conveniente avaliar outras, pois ela implica também em abrir mão de potenciais ganhos. Como exemplo dessa estratégia, uma seguradora pode evitar certos riscos de subscrição não subscrevendo apólices com determinadas coberturas.
- Mitigar: significa agir para reduzir a probabilidade e/ou o impacto de um risco, trazendo seu Nível de Risco para um patamar considerado aceitável[7]. O interessante dessa estratégia é que ela permite que a organização se proteja de efeitos negativos dos riscos de uma determinada operação sem ter que desistir dela, podendo assim obter ganhos. Alguns riscos de Mercado, por exemplo, podem ser mitigados através do uso de derivativos financeiros (*hedge*).
- Compartilhar[8]: ocorre quando uma organização repassa parte de um risco para outra, que, mediante contrato, se obriga a indenizá-la caso o risco se materialize. O próprio seguro é um mecanismo de compartilhamento de riscos do segurado com a seguradora. Já no contexto do mercado supervisionado pela Susep, a principal ferramenta de compartilhamento de riscos é o resseguro[9].
- Aceitar: é o que acontece quando não se adota nenhuma ação em relação ao risco. Normalmente a organização adota esta estratégia para riscos que apresentam baixo Nível de Risco. É importante deixar claro que a aceitação é uma opção consciente, definida pela organização após uma análise criteriosa (aceitar o risco é diferente de ignora-lo). Portanto, mesmo os riscos 'aceitos' devem constar do Perfil de Riscos da organização e possuir um Nível de Risco associado.

A Circular 517/2015 aborda esses conceitos relativos ao tratamento de riscos quando exige:

[7] Muitas vezes se fala de "risco bruto", que seria o risco na ausência de qualquer mecanismo de mitigação, e de "risco líquido", sendo este o risco residual que permanece após a adoção de tais mecanismos. Estes conceitos podem ser utilizados para avaliar a eficiência dos controles adotados para mitigação de riscos.

[8] Também é comum o termo "Transferir", embora "Compartilhar" tenha se popularizado recentemente diante do entendimento de que é praticamente impossível se eximir por completo de todos os potenciais efeitos negativos de um risco.

[9] Em especial com relação ao resseguro, embora o ressegurador suporte parte do risco de subscrição da cedente, esta fica exposta a uma outra gama de riscos, como por exemplo, de crédito (incerteza sobre a capacidade do ressegurador honrar seus compromissos), operacional (possíveis problemas no contrato de resseguro), de liquidez (caso o ressarcimento ocorra após a liquidação do sinistro junto ao segurado), etc.

> "Adoção de tratamentos e controles, compatíveis com cada Nível de Risco e com as prioridades estabelecidas pela supervisionada, visando a manter as exposições a riscos dentro dos limites definidos em suas políticas e procedimentos, além de mecanismos para avaliação da efetividade de tais medidas." (art. 108-D, inc. II, alínea "d")

Cabe observar que, para cada risco, a companhia deve definir controles específicos que são reflexos da estratégia de tratamento adotada. Esta definição deve levar em conta o Nível de Risco e as diretrizes internas estabelecidas na Política de Gestão de Riscos.

É importante notar que a norma pede explicitamente que a Política de Gestão de Riscos contenha indicativos de "estratégias e diretrizes para a gestão dos riscos mais relevantes, ou considerados prioritários" (art. 108-L, § 1º), o que significa que essas diretrizes deverão ser validadas também pelo Conselho de Administração, quando esse existir, no contexto de aprovação da própria política (art. 108-L, § 4º).

Quanto ao critério de relevância, espera-se que a supervisionada o associe à sua classificação interna de Níveis de Risco. Os tratamentos e controles para níveis menos prioritários poderão estar definidos em procedimentos operacionais e outros tipos de documentos que não necessitem de aprovação da Diretoria e do Conselho de Administração.

Em suma, todas as estratégias e controles utilizados para o tratamento de riscos deverão ser documentados pela supervisionada. Para os riscos mais relevantes, isso deve ser feito na Política de Gestão de Riscos (ou outras políticas, conforme detalhado na seção 5.2.2), enquanto que, para os demais riscos, esses assuntos poderão ser tratados a nível de procedimentos.

Como a definição de estratégias de tratamento, seja a nível de política ou procedimento, pode envolver a consideração de diversas alternativas, não se requer que a companhia seja capaz de demonstrar à Susep todo o processo que o embasou (ex.: todas as alternativas consideradas e porque algumas delas foram rejeitadas.). Por outro lado, ela deve ser capaz de justificar porque considera que um determinado tratamento adotado é considerado apropriado.

Por fim, vale a pena mencionar que a Circular 517/2015 introduziu o conceito de Plano de Continuidade de Negócios – PCN (art. 108-B, inc. VI) – e estabeleceu alguns requisitos básicos para o mesmo (art. 108-D, §3º). Embora muitas vezes, em termos conceituais, o PCN seja considerado dentro de um contexto de "Sistema de Gestão de Continuidade de Negócios" (SGCN) que é mais amplo que o plano em si[10], para fins da norma optou-se por fazer referência a tal plano apenas na medida em que o mesmo também se relaciona com a gestão de riscos. Além disso, é importante notar que alguns requisitos mínimos para a continuidade de negócios deverão ser estabelecidos em política (art. 108-L, §1º, inc. V, alínea "g").

3.4. MONITORAMENTO DE RISCOS

Muitas vezes, nos textos que tratam de gestão de riscos, a palavra "monitoramento" se refere à avaliação crítica do processo como um todo, que retroalimenta o ciclo de melhoria contínua. No entanto, neste documento, quando tratamos do processo de gestão de riscos em si o termo

[10] Para maiores referências consultar ISO 22301.

"monitoramento" é utilizado com um significado mais estrito, de acompanhamento e reporte das exposições a riscos. Por outro lado, para nos referirmos à avaliação crítica mencionada anteriormente temos utilizado o termo "supervisão".

Em que pese esta distinção, é inegável que o monitoramento contínuo das exposições da organização a riscos também contribui de forma muito relevante para o aperfeiçoamento da gestão de riscos, e é por isso que a Circular 517/2015 requer:

> "Definição de indicadores ou variáveis para o monitoramento dos níveis de exposição aos principais riscos."
> (art. 108-D, inc. II, alínea "e")

O objetivo deste dispositivo é que a companhia defina parâmetros (indicadores ou variáveis) que lhe permitam aferir periodicamente sua exposição a riscos, para que ela possa se certificar de que permanece dentro dos limites estabelecidos em seu Apetite por Risco e em sua Política de Gestão de Riscos. Nota-se que o texto faz referência aos principais riscos da companhia, ou seja, no mínimo aqueles definidos como prioritários em função de seu Nível de Risco.

Este acompanhamento é considerado vital apesar da existência de controles para os riscos (definidos na etapa de tratamento), pois, além de tais controles poderem eventualmente apresentar falhas, muitas vezes eles se referem a riscos individuais, sendo difícil implementar controles efetivos para a exposição agregada.

A norma impõe ainda que os níveis de exposição sejam monitorados de tempos em tempos pelo Gestor de Riscos (art. 108-E, inc. I) e pela Diretoria (art. 108-C, §1º), frisando ainda a necessidade de mecanismos de comunicação adequados para o seu reporte (art. 108-D, inc. II, alínea "f").

O relatório anual do Gestor de Riscos, que deve trazer informações sobre novos riscos e violações ao Apetite por Risco e a outros limites de exposição definidos (art. 108-E, § 4º, inciso II) é uma importante ferramenta para essa comunicação, mas não deve ser a única. Especialmente no caso de eventual desenquadramento das exposições em relação aos limites, onde a comunicação é particularmente crítica, pois deve possibilitar a adoção tempestiva de medidas que visem à regularização da situação.

Sendo assim, convém que a Política de Gestão de Riscos defina a periodicidade mínima de acompanhamento das exposições da supervisionada nos diversos níveis da organização, além de requisitos para a comunicação das mesmas ao Conselho de Administração (se houver) e demais partes interessadas. Especial consideração deve ser dada aos casos em que limites de exposição sejam excedidos.

Não se espera que a supervisionada monitore, especialmente no nível da Diretoria, uma quantidade muito elevada de indicadores de exposição (por exemplo, 50 indicadores), pois isso pode inclusive dificultar sua utilização prática. Como alternativa, ela pode tentar estabelecer indicadores que reflitam um conjunto de riscos.

4. SUPERVISÃO DA GESTÃO DE RISCOS

4.1. O MODELO DAS 3 LINHAS DE DEFESA

A gestão de riscos, como todo processo, deve ser desempenhada por pessoal capacitado, com funções bem definidas (art. 108-D, inc. I da Circular Susep nº 517/2015). Sendo assim, faz-se necessário entender como os papéis e responsabilidades devem ser distribuídos dentro de uma organização para que sua gestão de riscos seja mais eficaz.

Para isto, apresentamos a seguir uma figura que ilustra o Modelo das 3 Linhas de Defesa, um paradigma muito difundido atualmente no meio corporativo. Ressaltamos que, embora a regulamentação da Estrutura de Gestão de Riscos não tenha adotado explicitamente a nomenclatura do modelo, o mesmo foi utilizado como referência durante sua elaboração e discussão. Em virtude disso, espera-se que o seu conhecimento seja útil para o entendimento e implementação da norma.

Resumidamente, as 3 linhas que dão nome ao modelo são:

- 1ª Linha de Defesa – Unidades Operacionais: Na prática, o tratamento dos riscos é realizado em diversas unidades que lidam diretamente com o negócio da organização, sendo comum que cada unidade assuma a responsabilidade pelos riscos que decorrem diretamente de sua atividade. Em uma seguradora, por exemplo, o departamento atuarial, pela natureza de sua função, normalmente estará mais envolvido com a gestão de riscos de subscrição, enquanto os riscos de mercado serão gerenciados predominantemente nos setores de investimentos ou tesouraria. Quando uma área é responsável por um determinado risco ela é dita proprietária daquele risco e deve adotar procedimentos e controles adequados para que sua gestão esteja de acordo com as diretrizes definidas pela organização. Em geral, espera-se ainda que as atribuições dos cargos na 1ª Linha de Defesa sejam explícitas quanto às suas responsabilidades relativas à gestão de riscos.
- 2ª Linha de Defesa – Funções de Controle: Enquanto as Unidades Operacionais recebem atribuições da Diretoria para implementar e executar a estratégia da organização (e, naturalmente, cuidar dos respectivos riscos), as chamadas Funções de Controle recebem a responsabilidade de, dentro de um determinado escopo de atuação, fornecer orientação especializada e supervisionar se os processos e controles definidos pela 1ª Linha de Defesa estão de acordo com as diretrizes organizacionais. No contexto do mercado segurador, é comum a menção a 3 Funções de Controle, relativas aos seguintes temas: Gestão de Riscos, Conformidade (ou *compliance*) e Atuarial (IAIS ICP 8 – Novembro/2015).
- 3ª Linha de Defesa – Auditoria Interna[11]: A função de Auditoria Interna difere das Funções de Controle particularmente em dois aspectos: em primeiro lugar, ela não possui papel de

[11] Os requisitos básicos para a Auditoria Interna foram definidos pela Circular Susep nº 249/2004.

orientar sobre temas específicos e, em segundo, pressupõe-se que ela esteja ligada diretamente ao Conselho de Administração da organização, e não à sua Diretoria como a 1ª e a 2ª linhas. Em função disso, o que se espera da Auditoria Interna é uma atuação mais ampla e independente na verificação da aderência às diretrizes da companhia.

Aliás, com relação à independência, vale destacar que este é um aspecto fundamental para que a 2ª e a 3ª Linhas de Defesa possam desempenhar adequadamente seu trabalho. Em geral, quanto menor o envolvimento de uma função com a definição de procedimentos e controles, maior será sua isenção para avaliar sua adequação, o que caracteriza a independência.

Antes de seguirmos adiante, vale destacar que a figura acima limitou-se a apresentar as Linhas de Defesa e seu relacionamento com a Diretoria e o Conselho de Administração da organização. Naturalmente existem outras partes interessadas (ex.: a própria Susep, Consultorias, Auditoria Externa, etc.) que também podem desempenhar papéis que contribuam para que a gestão de riscos seja mais eficaz, porém este texto tratará mais detalhadamente da 2º e 3º Linhas de Defesa, bem como da Diretoria e do Conselho de Administração. Isto se deve à ênfase que foi dada a eles pela regulamentação da Estrutura de Gestão de Riscos, em especial no que tange à supervisão de todo o processo de gestão de riscos.

4.2. GESTOR DE RISCOS

No contexto da Circular Susep nº 517/2015, entende-se que o Gestor de Riscos corresponde à função de controle de gestão de riscos, pertencente à 2º Linha de Defesa. Desta forma, não é de se esperar (apesar do nome) que ele vá efetivamente gerenciar os riscos da organização, sendo que o seu papel deve consistir basicamente em:

- Orientar as Unidades Operacionais (1ª Linha de Defesa) e a Diretoria da companhia em relação à gestão de riscos; e
- Supervisionar os controles de riscos implementados pelas Unidades Operacionais, de forma a se certificar que eles sejam adequados e aderentes às diretrizes da organização.

O art. 108-E da norma, em seus incisos I a VIII, detalha uma série de atividades específicas que devem ser desempenhadas pelo Gestor de Riscos, sendo que todas elas podem ser sintetizadas pelos dois itens anteriores.

É interessante notar que os termos usados pela norma (monitorar, participar, avaliar, reportar, propor, etc.) ressaltam tanto o caráter consultivo como o de supervisão inerentes à função, mas não lhe atribuem responsabilidade direta pelo controle de riscos. Tal papel fica também evidente no § 4º do art. 108-E, referente ao relatório anual do Gestor de Riscos, que é muito focado na identificação de deficiências da EGR e no acompanhamento de ações corretivas.

A seguir, passamos a tratar de alguns aspectos específicos da atuação desse profissional.

4.2.1. FORMALIZAÇÃO

A regulamentação da Estrutura de Gestão de Riscos, no que se refere ao Gestor de Riscos, segue o conceito de "função", a qual pode ser desempenhada por uma área da organização ou mesmo, no limite, por uma só pessoa (tendo em vista o Princípio da Proporcionalidade – ver seção 2.2), o que confere grande flexibilidade de implementação.

Uma determinada companhia pode, por exemplo, optar por criar uma "Gerência de Riscos", cujo titular será considerado o Gestor de Riscos. Desnecessário dizer que, nesta situação, cuidados adicionais com relação à formalização dessa área serão necessários, de modo que ela se torne efetivamente capaz de desempenhar seu papel na organização. Outro exemplo pode ser o de uma empresa que decida (embora isto não seja requerido) incluir a função de Gestor de Riscos como estatutária, caso em que a modificação do estatuto será um item necessário para a efetiva formalização da função.

De forma geral, o que se espera minimamente é que as atribuições do Gestor de Riscos estejam devidamente definidas e registradas (ex.: descrição de cargo) e que exista um profissional formalmente designado para exercê-las. Nos casos em que o Gestor de Riscos pertença à própria supervisionada, a nomeação ou a destituição do profissional responsável por esta função deverão ser aprovadas pelo Conselho de Administração ou, caso este não exista, pela Diretoria (art. 108-E, §3º), devendo ainda serem comunicadas à Susep (art. 108-E-A) [12] [13] [14]. Com relação à qualificação do Gestor de Riscos ("suficiente qualificação e experiência" – também no caput do art. 108-E), frisa-se que a Susep não possui a prerrogativa de aprovar ou rejeitar *a priori* o nome do profissional escolhido pela empresa (a menos que seja um cargo estatutário, sujeito a regulamentação específica). A Autarquia entende que a escolha de um profissional adequado é uma responsabilidade da empresa e que os conhecimentos e a atuação do Gestor de Riscos serão postos à prova quando da realização de fiscalizações.

Vale destacar que, quando da análise de eventuais pedidos de terceirização das funções do Gestor de Riscos ou de sua delegação para matriz estrangeira (específica para resseguradores locais), conforme previsto nos incisos I e II do art. 108-F da Circular 517/2015, a Susep também não entra no mérito de avaliar a qualificação das empresas, pessoas ou unidades que desempenharão tais atividades. Mais detalhes sobre a análise de adequação dessas soluções e orientações para a instrução dos pedidos serão vistos nas seções 6.2 e 6.3.

4.2.2. ÂMBITO DE ATUAÇÃO

Até este momento, quando falamos do Gestor de Riscos temos utilizado os termos "organização", "empresa" e "companhia" de forma genérica, pois é mais fácil entender o papel desse profissional quando se considera uma operação isolada.

Porém, na prática, a grande maioria das empresas supervisionadas pela Susep não atua de forma estanque, mas sim integrada com outras. No geral, essas empresas fazem parte de grupos ou conglomerados que, além de empresas do mercado segurador, possuem também companhias de outros setores (ex.: bancário), não só no Brasil como no exterior.

Sendo assim, há que se considerar que esses grupos tendem a se estruturar para gerar sinergias entre as diversas empresas que os compõem, por exemplo, concentrando funções administrativas (RH,

[12] O protocolo de expedientes deverá ser direcionado à Coordenação Geral de Supervisão Consolidada (CGCON). O envio dessa documentação pode ser feito através de **Peticionamento Eletrônico**, pelo Tipo de Processo "SUPERVISÃO – AUTORIZAÇÃO – GESTOR DE RISCO".

[13] Os expedientes enviados à Susep dando conta da nomeação do Gestor de Riscos anteriormente à existência dessa exigência (instituída em 2019 com a inclusão do art. 108-E-A) geraram processos que foram arquivados. A Autarquia poderá utilizar esta informação em seu monitoramento.

[14] Outras ferramentas utilizadas para prestar informações acerca do Gestor de Riscos são o Quadro 1 (módulo "Gestor de Riscos") e o Questionário de Riscos, ambos do FIP/SUSEP.

contabilidade, informática, etc.). É bastante comum o tipo de estrutura em que uma *holding*, que controla diversas empresas do mercado segurador, presta serviços administrativos às suas controladas enquanto estas se ocupam basicamente de seus negócios específicos.

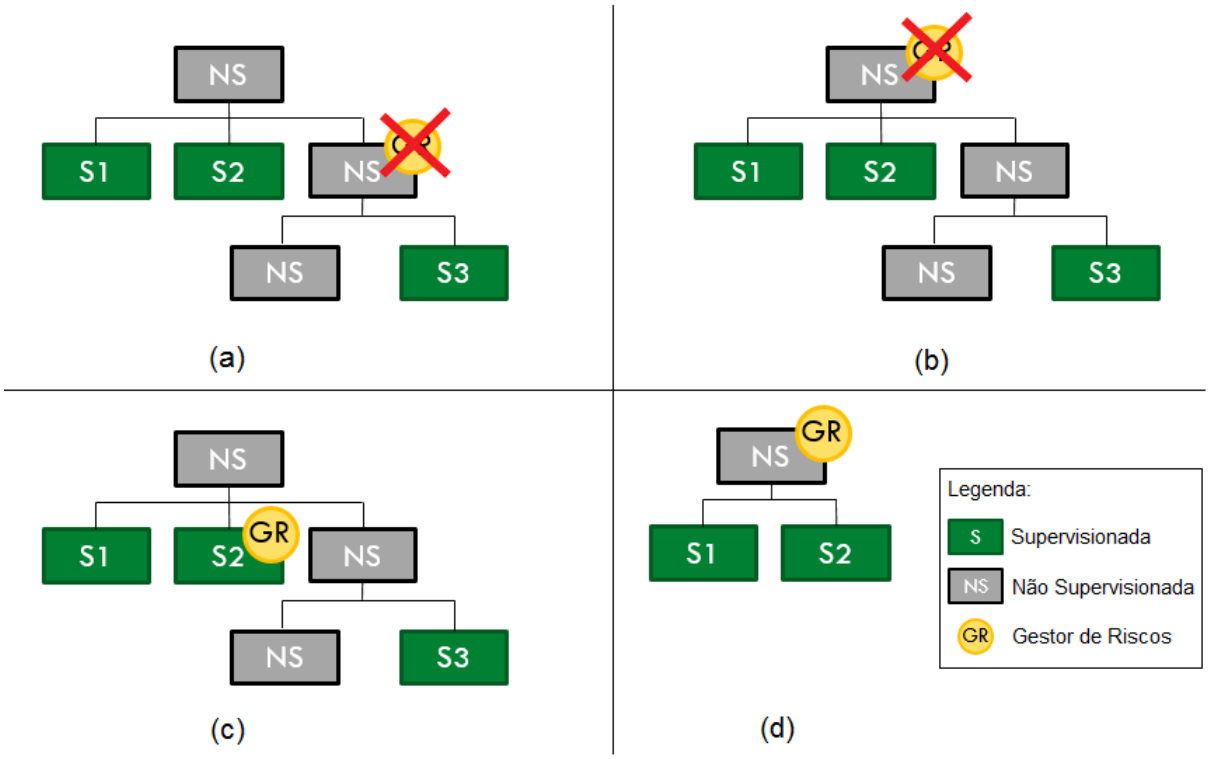
Também é muito usual a centralização de atividades de suporte técnico ou supervisão, tal como a do Gestor de Riscos. Isso se justifica pois, apesar dos riscos de cada empresa poderem ser distintos entre si, no geral a abordagem da gestão de riscos será semelhante (até mesmo a Política de Gestão de Riscos pode ser a mesma para todas as empresas do grupo, como se verá mais à frente).

Foi com base neste entendimento que a regulamentação da Estrutura de Gestão de Riscos permitiu que o Gestor de Riscos também pudesse ser constituído no âmbito de um grupo de empresas. No texto da norma:

> "§ 2.º É admitida a nomeação de um único Gestor de Riscos para duas ou mais supervisionadas que pertençam ao mesmo grupo, desde que aquele pertença a:
> I – Controladora das mesmas, que tenha por objeto exclusivo a participação em supervisionadas; ou
> II – Uma das supervisionadas atendidas por ele."
> (art. 108-E, § 2º)

Nota-se que, apesar de possibilitar esta atuação no contexto grupo, a regulamentação restringiu que o Gestor de Riscos esteja formalmente constituído em uma empresa supervisionada pela Susep (inciso II) ou, eventualmente, numa controladora que tenha por objeto exclusivo a participação em supervisionadas da Susep (inciso I). Quanto a esta controladora, pelo fato dela não se destinar a desenvolver nenhum tipo de atividade comercial (seu objeto exclusivo é a participação), muitas vezes a referenciaremos como "*holding* não operacional de seguros".

A figura a seguir apresenta algumas possibilidades para a constituição do Gestor de Riscos no âmbito de um grupo de empresas:



O quadrante (a) mostra que o Gestor de Riscos que se encontra na empresa indicada (uma não supervisionada) não pode atender às supervisionadas S1, S2 e S3 do grupo.

Já na situação do quadrante (b), o Gestor de Riscos foi deslocado para a controladora do grupo, que também não é supervisionada. Como essa controladora participa tanto em supervisionadas como em não supervisionadas (o objeto não é exclusivo), o Gestor de Riscos continua não podendo servir às supervisionadas S1, S2 e S3.

No caso mostrado no quadrante (c), como o Gestor de Riscos pertence à supervisionada S2, ele pode atender também às demais supervisionadas do grupo (S1 e S3). O mesmo aconteceria se ele estivesse nas empresas S1 ou S3.

Por fim, no quadrante (d), apresentamos o caso de uma *holding* não operacional de seguros, que participa exclusivamente em supervisionadas da Susep e não desempenha nenhum outro tipo de atividade comercial. Desta forma, seu Gestor de Riscos pode atender às supervisionadas do grupo (S1 e S2). O mesmo aconteceria se essa controladora fosse, ela mesma, uma supervisionada.

Observa-se que um Gestor de Riscos constituído, digamos, em um banco, nunca poderá atender diretamente a uma supervisionada da Susep.

Obviamente o que se espera não é que os grandes conglomerados bancários transfiram suas áreas de gestão de riscos para as seguradoras, mas sim que eles constituam Gestores de Riscos com atuação voltada especificamente para o mercado segurador. O mais provável é que esses profissionais se reportem a suas matrizes, sigam diretrizes emitidas por elas e até mesmo se utilizem de seus recursos, o que não é vedado (na verdade, é até desejável). O mesmo vale para os Gestores de Riscos das supervisionadas que pertencem a grupos estrangeiros, os quais possivelmente terão esse tipo de vínculo com suas matrizes no exterior.

A Susep acredita que a constituição desses Gestores de Riscos com foco nos segmentos de seguros, previdência complementar aberta, capitalização e resseguros contribuirão não só para uma melhor gestão de riscos no âmbito desses mercados específicos, mas também para fortalecer a gestão de riscos do grupo/conglomerado como um todo.

Por fim, ressalta-se que quando o Gestor de Riscos for constituído no âmbito do grupo, todas as supervisionadas por ele atendidas deverão comunicar à Susep sua eventual nomeação ou destituição, nos termos do art. 108-A-E. Entretanto, a aprovação de nomeação ou destituição pelo Conselho de Administração ou, caso este não exista, pela Diretoria (art. 108-E, §3º), deverá ser realizada somente no âmbito da supervisionada à qual o Gestor de Risco pertença.

4.2.3. CONFLITOS DE INTERESSES

Conforme antecipado, a independência é um aspecto chave para a atuação do Gestor de Riscos, que pode ser prejudicado por eventuais conflitos de interesse relativos às suas próprias atividades ou às de seus superiores hierárquicos.

Pelo menos em tese, o Gestor de Riscos será mais isento para realizar suas avaliações e apontar eventuais deficiências na Estrutura de Gestão de Riscos quanto menos ele tiver participado de:

- Decisões que levaram a empresa a assumir riscos; e
- Definições de processos, metodologias, ferramentas e técnicas adotados pelas unidades operacionais para gestão de riscos.

De fato, a norma tem dispositivos específicos para tratar esses dois casos, como por exemplo, o transcrito a seguir:

> "O Gestor de Riscos não deverá ser responsável primário por decisões que levem a supervisionada a assumir riscos." (art. 108-I, caput)

Na visão da Susep, não seria razoável que o profissional responsável por monitorar as exposições a riscos da organização, zelando por mantê-las dentro dos limites definidos pela alta administração, decida pela realização de uma operação que traz riscos para a empresa. Neste sentido, um equívoco claro seria colocar como Gestor de Riscos o gerente da área de Subscrição que, em última análise, é responsável pela assunção de riscos de seguros (Riscos de Subscrição). Da mesma forma, o Diretor Financeiro, responsável por toda a estratégia de investimentos (que implicam em Riscos de Mercado, Crédito etc.), também não poderia desempenhar o papel de Gestor de Riscos.

Nos casos citados acima, ainda que se alegue que a tomada efetiva de decisão ocorre em níveis hierárquicos mais baixos (ex.: gerências subordinadas ao Diretor Financeiro), considera-se que a responsabilidade por elas é indelegável, portanto, o superior também estaria impedido de desempenhar a função de Gestor de Riscos. Seguindo esse raciocínio, fica claro que o presidente da empresa jamais poderá responder pela função de Gestor de Riscos.

Por outro lado, admite-se que o Gestor de Riscos seja subordinado a pessoa ou área responsável por decisões que levem a supervisionada a assumir riscos (art. 108-I, §1º), desde que haja *"procedimentos*

adicionais de controle que visem a mitigar conflitos de interesse". Para continuar com o exemplo, o Gestor de Riscos pode estar subordinado ao Diretor Financeiro, mas, neste caso, a empresa poderia criar de uma comissão multidisciplinar que avaliasse casos de divergências entre o Gestor de Riscos e alguma outra área ligada à Diretoria Financeira. O livre acesso do Gestor de Riscos à Diretoria e ao Conselho de Administração (este último previsto no art. 108-H, inciso III) também funciona como um importante mecanismo para dirimir eventuais impasses, principalmente se esses impasses ocorrerem em relação ao próprio superior hierárquico.

Antes de seguirmos adiante, vale a pena mencionar que muitas vezes o caput do art. 108-I pode ser mal interpretado. Isto porque toda atividade carrega intrinsecamente algum tipo de risco, por exemplo, a possibilidade de multas e sanções pelo seu desempenho inadequado (um tipo de Risco Operacional). Esta interpretação estrita não está de acordo com o espírito da norma, que, como já foi possível perceber, visa a impedir que o Gestor de Riscos tenha poder de decidir sobre a aceitação ou não de um risco (ex.: subscrição de uma apólice) ou definir que tipo de risco correr (ex.: escolha de alternativas de investimentos, contratação de resseguro, etc.). De acordo com esta interpretação, espera-se que certas funções, como a de Contador, possam ser acumuladas. Já outras, como, por exemplo, a de Atuário ou chefe do departamento jurídico, devido ao seu espectro mais amplo de atuação, demandariam uma análise caso-a-caso por parte da empresa (ex.: o atuário pode estar responsável apenas pelo cálculo da provisão, o que a princípio não configuraria um conflito, mas, em outros casos, ele pode também ter papel determinante no desenvolvimento e precificação de produtos, atividades que carregam elevado risco de subscrição). De toda forma, o acúmulo de outras funções pelo Gestor de Riscos não é uma melhor prática, mas este pode ser um caminho para empresas que estão expostas a menos riscos e que possuem poucos funcionários (Princípio da Proporcionalidade – ver seção 2.2) e não desejem recorrer à alternativa de terceirização (art. 108-F, inciso I). De qualquer forma, mesmo nos casos de acúmulo de funções, o profissional designado como Gestor de Riscos deverá demonstrar capacidade técnica para tal cargo.

A outra situação em que podem surgir conflitos de interesse na atuação do Gestor de Riscos diz respeito à validação de processos, metodologias e ferramentas utilizados para a gestão de riscos, requerida pelo seguinte dispositivo:

> "Validação dos processos, metodologias e ferramentas mencionados no inciso anterior por pessoa, setor ou entidade competente que não tenha participado ativamente da definição ou elaboração dos mesmos e não seja diretamente envolvida em sua execução;"
> (art. 108-D, inciso III)

No caso, o "inciso anterior" é o que fala da maioria das etapas do processo de gestão de riscos (ver seção 3). Embora o dispositivo acima não estabeleça que o Gestor de Riscos seja necessariamente o responsável pela validação dos citados processos, metodologias e ferramentas, como os mesmos são voltados para a gestão de riscos ele surge como uma opção natural para a maioria das empresas.

Vale destacar que esta validação não é periódica (como, por exemplo, uma auditoria), mas sim pontual, por ocasião da adoção do processo, metodologia ou ferramenta. Se for o caso do Gestor de Riscos desempenhar o papel de validador, não é adequado que ele tenha participado da definição dos itens a serem validados. Por exemplo, em se tratando de um processo, o Gestor de Riscos pode ser consultado sobre alternativas de implementação, mas não cabe a ele escolher qual delas adotar ou

definir os detalhes de sua implementação. Até por isso, o inciso VIII do art. 108-E limita um pouco o papel de orientação do Gestor de Riscos.

Ainda com relação à validação, ressaltamos que a empresa é livre para definir o responsável por esta atividade, podendo atribuí-la, por exemplo, a uma comissão multidisciplinar, consultorias externas ou qualquer outro ente que tenha capacidade técnica para tal (exceto a Auditoria Interna, para que não comprometa sua própria atuação). Estas também podem ser opções nos casos em que a participação do Gestor de Riscos seja necessária, como, por exemplo, na elaboração do Perfil de Riscos (ver seção 3.1).

4.3. AUDITORIA INTERNA

As características da Auditoria Interna já haviam sido definidas pela Circular Susep nº 249/2004, sendo que a Circular 517/2015 apenas deixou claro que ela também é parte fundamental da Estrutura de Gestão de Riscos. Como a atuação da Auditoria Interna já é bastante consolidada, a Circular 517 dedica apenas o art. 108-O a ela.

Tal dispositivo, em seu §1º, admite a adoção do enfoque de "rotação de ênfase", o que significa que nem todas as áreas ou processos relevantes para a Estrutura de Gestão de Risco precisarão ser auditados todo ano. Na verdade, o que ele determina é que isto ocorra num ciclo de 3 anos. Vale destacar que, a interpretação deste parágrafo em conjunto com o caput do mesmo artigo leva ao entendimento de que, apesar da rotação de ênfase, a cada ano pelo menos alguns itens da norma deverão ser avaliados, não sendo admitido, por exemplo, que a Auditoria Interna passe 2 anos sem auditar nada relativo à Gestão de Riscos para se concentrar nisso apenas no terceiro ano. Entretanto, o mais recomendável, pelo menos na visão da Susep, seria uma distribuição equilibrada de todos os itens auditados ao longo dos 3 anos.

Nenhuma dessas avaliações da Auditoria Interna precisa ser enviada à Susep, a menos que explicitamente requerido pela Autarquia (como é o caso da reavaliação periódica da autorização para uso de Fatores Reduzidos de Risco – Circular Susep nº 517/15, art. 91-C, inciso II). O que se espera é que elas, além de contribuírem para a melhoria contínua do processo de gestão de riscos, também possam ser usadas pela fiscalização da Susep quando da realização de inspeções *in loco*.

Vale destacar que a Auditoria Interna é considerada a 3ª Linha de Defesa (vide seção 4.1) e, por isso, a natureza de suas revisões tende a diferir das validações que podem ser realizadas pelo Gestor de Riscos (vide seção 4.2.3), principalmente por se aterem basicamente ao cumprimento do que foi definido pela empresa, e não propriamente à adequação técnica de cada processo auditado. Além disso, a atuação do próprio Gestor de Riscos está sujeita a revisão pela Auditoria interna, não sendo, portanto, adequado o acúmulo das duas funções (art. 108-I, §2º).

4.4. DIRETORIA E CONSELHO DE ADMINISTRAÇÃO

A responsabilidade da Diretoria e do Conselho de Administração está definida no seguinte dispositivo da circular Susep nº 517/2015:

> "É responsabilidade da Diretoria e do Conselho de Administração, quando houver, zelar pela adequação da Estrutura de Gestão de Riscos da supervisionada." (art. 108-C, caput)

Ou seja, em última instância, a responsabilidade pela adequação da Estrutura de Gestão de Riscos recai sobre esses órgãos. Conceitualmente a Diretoria, que é constituída para implementar a estratégia da companhia, deve fazer o máximo para evitar que os riscos atrapalhem a consecução dos objetivos organizacionais. O mesmo vale para o Conselho de Administração, que tem como um de seus principais papéis a supervisão da gestão da empresa de forma a garantir que o interesse de logo prazo de seus acionistas – a continuidade – seja atingido.

Naturalmente que a Diretoria, enquanto órgão executivo, possui atribuições mais específicas e diretas, como, por exemplo o monitoramento das exposições a riscos e a avaliação periódica da eficácia da Estrutura de Gestão de Riscos (art. 108-C, §1º). Entretanto, como a norma requer o reporte ao Conselho de Administração, indiretamente este também estará a par desses aspectos, inclusive das propostas de ação da Diretoria, devendo fornecer direcionamento e orientação sempre que necessário. Até por isso, convém que esse reporte seja tempestivo.

Sobre a avaliação da EGR pela Diretoria, a norma determina a que seja feita no mínimo anualmente, ou em face de mudança significativa no Perfil de Riscos. Já para o monitoramento de exposições não há uma periodicidade definida, porém, a Susep acredita que o ideal seria realizar tal monitoramento no mínimo trimestralmente. Em ambos os casos, é importante que a Política de Gestão de Riscos estabeleça a periodicidade de realização dessas atividades, bem como o critério para disparar avaliações extraordinárias.

A Susep espera que a avaliação da EGR pela Diretoria faça uso, no mínimo, de informações e relatórios gerados pelo Gestor de Riscos (inclusive seu relatório anual, estabelecido pelo art. 108-E, § 4º) e pela Auditoria Interna no exercício de suas atribuições. Além disso, a norma prevê a possibilidade de constituição de comitês ou comissões, utilização de prestadores de serviço externos (ex.: consultorias) entre outros (art. 108-C, §2º) com o objetivo de auxiliá-la nessa tarefa, o que é opcional. O mesmo vale para o Conselho de Administração, sendo que os entes que prestam auxílio a ele e à Diretoria podem ser distintos.

É importante destacar que não foi definida uma forma de documentação específica para a avaliação da Diretoria bem como para o reporte ao Conselho de Administração, entretanto, ambos devem ser documentados de forma a possibilitar a verificação pela Susep (ex.: atas de reunião, relatórios, etc.).

Ressalta-se ainda que a norma veda a delegação de quaisquer responsabilidades ou atribuições que ela confere à Diretoria e ao Conselho de Administração, relativas à Estrutura de Gestão de Riscos (art. 108-S).

5. POLÍTICAS E DIRETRIZES

Na seção 2 dividimos a Estrutura de Gestão de Riscos em 3 partes básicas: o processo de gestão de riscos, a supervisão desse processo e o ambiente interno da organização. As duas primeiras foram

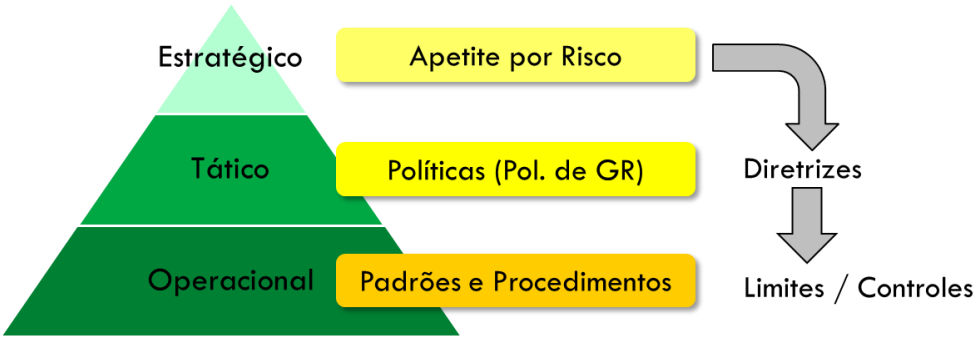
tratadas respectivamente nas seções 3 e 4, portanto, seria esperado que a presente seção abordasse o ambiente interno como um todo.

O ambiente interno compreende muito mais do que as políticas e diretrizes, englobando, por exemplo, a cultura da organização, toda a sua filosofia de gestão de riscos, seus valores éticos, sua estrutura organizacional, seus recursos humanos e tecnológicos, enfim, tudo aquilo que, de um modo ou de outro, interfere na maneira como o risco é percebido e gerenciado pela companhia. No entanto, a Circular 517/2015 não abordou todos estes aspectos diretamente, tendo dado maior ênfase às políticas e diretrizes organizacionais. É por este motivo que esta seção se dedica especificamente a este tema.

Vale observar que tais políticas e diretrizes são um aspecto fundamental do ambiente, além de constituírem um importante mecanismo de disseminação cultural pelo simples motivo de deixarem claro para toda a organização a forma como a alta administração espera que ela funcione, especificando, por exemplo, os riscos que ela deve assumir e a forma de trata-los.

5.1. APETITE POR RISCO

O Apetite por Risco é a diretriz mais fundamental em termos de gestão de riscos para uma organização, pois, pelo menos em tese, todas as políticas e procedimentos que definem como os riscos devem ser gerenciados deveriam derivar dele, conforme ilustrado abaixo.



Conceitualmente, pode-se dizer que o Apetite por Risco se situa no nível estratégico, estando intimamente ligado ao plano de negócios da companhia. A Circular Susep nº 517/2015 chama a atenção para isso, estabelecendo inclusive a necessidade de reavaliação do Apetite por Risco a cada revisão do plano de negócios (art. 108-J, parágrafo único).

Como exemplo, consideremos o caso de uma empresa que decide começar a operar numa nova linha de negócios, adotando uma estratégia de vendas mais agressiva para conquistar *market share*. Naturalmente a alta administração precisará estar disposta a assumir mais riscos e o Apetite por Risco deverá refletir isso[15].

Outro aspecto que ressalta esse caráter estratégico é o fato de que o Apetite por Risco deve ser definido pelo Conselho de Administração (art. 108-J, caput), sendo que, se este órgão não existir, é

[15] Conceitualmente, o ideal é que a empresa também avalie se seu capital é suficiente para suportar eventuais perdas decorrentes dessa estratégia, alinhando assim sua gestão de riscos com a gestão de capital, o que pode ser conseguido através do ORSA (Own Risk and Solvency Assessment). Neste sentido, salientamos que, embora o ORSA ainda não seja exigido pela regulamentação, a Susep já vem trabalhando em um Guia de Orientação sobre o assunto, que deverá ser disponibilizado em breve como uma ferramenta de auxílio para o mercado.

admitido que a Diretoria o faça. Neste caso, no entanto, o ideal é que a Diretoria envolva os acionistas da empresa (ou sua controladora) para que estes participem desta definição.

Outro ponto importante que vale a pena destacar se refere ao que o Apetite por Risco deve conter. De acordo com os incisos I e II do art. 108-J, ele deverá trazer necessariamente duas definições:

- Qualitativa: o Apetite por Risco deve indicar explicitamente os riscos que a empresa deve assumir em virtude de seu direcionamento estratégico. Em nosso exemplo anterior, supondo que a nova linha de negócio seja a de seguro de automóveis, o Conselho de Administração poderia indicar que a margem de lucro do prêmio seja reduzida de forma a angariar mais clientes (o que aumenta o risco de subscrição). Por outro lado, também seria interessante estabelecer alguns riscos que deveriam ser evitados, como a concentração excessiva em clientes do sexo masculino e com idade inferior a 25 anos (o que poderia elevar muito a sinistralidade, comprometendo o resultado final). O importante é que este tipo de direcionamento reflita riscos que o Conselho de Administração anteviu quando discutiu e elaborou o plano de negócios, de forma a fornecer à Diretoria uma visão mais clara do que fazer (e do que não fazer) para aumentar a probabilidade de atingir os objetivos desejados.
- Quantitativa: a norma requer que o Apetite por Risco defina *"pelo menos em nível global, a perda financeira ou de valor que considera aceitável frente aos riscos assumidos e a capacidade financeira da supervisionada"* (art. 108-J, inc. II), ou seja, de alguma maneira o Conselho de Administração deverá estabelecer o quanto está disposto a perder em virtude da estratégia adotada, o que, em última análise, reflete sua tolerância a riscos. Como este montante também deve guardar relação com a capacidade financeira da companhia, uma possibilidade seria, por exemplo, limitar a perda máxima aceitável (considerando a nova operação em automóveis) a, digamos, 10% do Patrimônio Líquido da empresa ao ano. Isto não quer dizer que a empresa espera operar no vermelho, mas sim que ela tolera que, eventualmente, ocorram perdas neste montante. Assim como as indicações qualitativas, espera-se que este tipo de parâmetro forneça subsídios que ajudem a Diretoria a implementar a estratégia definida. Vale destacar que a norma não veda a adoção de limites por linha de negócio em complemento ao limite global.

Qualquer inadequação das exposições da companhia em relação ao seu Apetite por Risco deve ser vista como uma deficiência, gerando planos de ação que visem ao seu saneamento.

Por fim, salientamos que o Apetite por Risco deverá estar expresso num documento aprovado formalmente pelo Conselho de Administração da companhia (ou a Diretoria, se for o caso). Qualquer revisão deste Apetite por Riscos (ex.: por ocasião da elaboração de um novo plano de negócios) deverá seguir estes mesmos critérios de documentação e aprovação.

5.2. POLÍTICAS

5.2.1. O CONCEITO DE POLÍTICA

Conforme apresentado na figura da seção anterior, é através das políticas que os executivos da empresa começam a traduzir o Apetite por Risco em ações efetivas que devem ser adotadas pelas unidades operacionais (1ª Linha de Defesa).

No entanto, é importante observar que diferentes organizações utilizam terminologias distintas para se referirem aos documentos que estabelecem suas diretrizes internas nos diversos níveis gerenciais (estratégico, tático e operacional). Por este motivo, um mesmo documento (exatamente com o mesmo conteúdo) pode ser chamado de "política" por uma empresa e de "padrão" por outra. A Circular Susep nº 517/2015 não requer que as companhias ajustem obrigatoriamente seus jargões, mas, para fins de aplicação da norma, convém identificar algumas características básicas para que, independentemente do nome que recebe, um documento de diretrizes possa ser considerado uma "política", de acordo com o espírito da regulamentação.

Para isto, consideremos primeiramente o seguinte dispositivo:

> "A Política de Gestão de Riscos deverá definir estratégias e diretrizes para gestão dos riscos mais relevantes, ou considerados prioritários, associados aos principais processos de trabalho da supervisionada, dentre os quais deverão estar incluídos, no mínimo:" (art. 108-L, §1º)

Nota-se que, no conceito adotado pela norma, uma "política" deve, pelo menos, definir estratégias e diretrizes para a gestão dos riscos mais relevantes ou considerados prioritários pela organização. Quanto a este critério de relevância, é importante que a supervisionada o associe à sua classificação interna de Níveis de Risco (ver seção 3.2).

Por exemplo, numa empresa que adote os Níveis de Risco "Alto", "Médio" e "Baixo", poderão ser considerados "políticas" os documentos que definam, pelo menos, as diretrizes gerais para a gestão dos riscos classificados como "Alto"[16]. Estes documentos não precisam entrar em detalhes de procedimentos específicos, mas sim servir de base para que os mesmos sejam definidos em linha com as expectativas da alta administração.

Outro aspecto importante de uma política pode ser percebido no dispositivo abaixo:

> "A Diretoria da supervisionada e seu Conselho de Administração, quando houver, deverão aprovar a Política de Gestão de Riscos, bem como quaisquer outras políticas elaboradas com base na faculdade prevista no § 3º" (art. 108-L, §4º)

Deste comando, depreende-se a necessidade de que as políticas que tratam de gestão de riscos sejam formalmente aprovadas pela Diretoria da supervisionada e pelo seu Conselho de Administração

[16] Observação: A norma definiu ainda alguns processos de trabalho cujos riscos deverão ser obrigatoriamente abordados por políticas (art. 108-L, §1º, incisos I a V). Nestes casos, se algum dos referidos processos não possuir riscos classificados como "Alto", o ideal é que o documento faça referência aos seus riscos com Nível de Risco mais elevado, que pode ser, por exemplo, "Médio". A exceção são os riscos relacionados ao processo intitulado "Concessão de resgates e portabilidades", que poderão não estar contidos em políticas se forem considerados pouco relevantes (ex.: operação modesta em produtos que preveem estes institutos, o que leva a um baixo Nível de Risco – art. 108-L, §2º).

(sempre que este existir). Isto é bastante importante, pois, conforme destacado anteriormente, esses documentos tratam dos principais riscos da empresa, os quais espera-se que sejam monitorados regularmente pela alta administração (ver seção 3.4).

Em suma, um documento interno que forneça diretrizes para a gestão de riscos poderá ser considerado uma "política", independentemente de sua nomenclatura oficial, se: (i) tratar dos riscos considerados mais relevantes pela organização; e (ii) for aprovado pela Diretoria e pelo Conselho de Administração (se houver). Logo, o conceito de política adotado pela norma refere-se a um documento de alto nível, que reflete as orientações da alta administração da empresa em relação aos principais riscos de sua operação.

Por fim, atualmente existem casos de empresas que utilizam um único documento para tratar tanto das diretrizes de alto nível como de orientações muito específicas para determinados processos (ex.: Subscrição), abordando desde o nível estratégico até o operacional. Nestes casos, há duas estratégias possíveis para cumprir o requisito de aprovação da alta administração, a saber:

- Submeter o documento completo à aprovação: É uma solução aceitável para a Susep, mas a Diretoria e principalmente o Conselho de Administração podem se sentir desconfortáveis em ter que avaliar detalhes específicos de procedimentos que não são de seu conhecimento. Além disso, tal aprovação demandará mais esforço dos referidos órgãos, não só no momento inicial como nas revisões subsequentes; ou
- Segregar diretrizes: Consiste em transferir para um documento separado as diretrizes de mais alto nível e submeter apenas este documento à aprovação da Diretoria e do Conselho de Administração. É considerada a alternativa mais desejável, pois confere maior flexibilidade na definição de processos nos níveis gerenciais mais baixos.

5.2.2. Política de Gestão de Riscos (e outras políticas relacionadas)

O art. 108-L da Circular Susep nº 517/2015 exige que as supervisionadas possuam uma Política de Gestão de Riscos:

> "A supervisionada deverá possuir uma Política de Gestão de Riscos que descreva formalmente sua Estrutura de Gestão de Riscos e explique, de forma geral, como a mesma se integra às suas operações e ao seu Sistema de Controles Internos." (art. 108-L, caput)

Como se pode observar, um dos principais objetivos dessa política é estabelecer as bases gerais para o próprio funcionamento da Estrutura de Gestão de Riscos.

A Política de Gestão de Riscos deve, portanto, definir parâmetros para o processo de gestão de riscos e para sua supervisão. Neste contexto, alguns exemplos de itens relevantes a serem incluídos, já mencionados ao longo deste documento, são:

- Definições de categorias de riscos adicionais, se houver (vide seção 3.1);
- Critérios para mensuração de riscos e para determinação dos Níveis de Risco (vide seção 3.2);

- Periodicidade mínima para o acompanhamento das exposições a riscos pela Diretoria (vide seções 3.4 e 4.4), incluindo seu reporte ao Conselho de Administração; e
- Periodicidade de reavaliação da Estrutura de Gestão de Riscos pela Diretoria, incluindo critérios para disparar uma reavaliação extraordinária (vide seção 3.1 e 4.4).

Note que todos os itens acima se referem a aspectos não rigidamente definidos pela norma, mas que precisam ser estabelecidos pela companhia para que sua Estrutura de Gestão de Riscos funcione adequadamente. Obviamente a empresa sentirá necessidade de incluir diversos outros itens que ajudem a cumprir este objetivo, sendo que a lista acima deve ser considerada não exaustiva.

Outro aspecto geral que merece ser incluído na Política de Gestão de Riscos refere-se às funções (ex.: Gestor de Riscos[17] ou área de Gestão de Riscos) e órgãos auxiliares (ex.: Comitês ou comissões) que supervisionam o processo de gestão de riscos. A política pode, além de instituí-los, definir suas atribuições, estabelecer como será sua relação com outras unidades da companhia e, no caso de comitês/comissões, até mesmo definir sua composição.

Já com relação ao tratamento dos riscos da empresa, o § 1º do art. 108-L (vide seção 5.2.1) elencou diversos processos de trabalho considerados relevantes (incisos I a V) para cada tipo de supervisionada, exigindo que a Política de Gestão de Riscos defina as estratégias e diretrizes para a gestão dos principais riscos associados a eles.

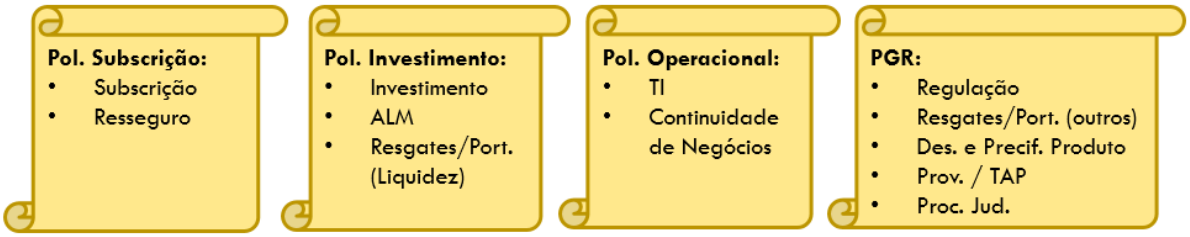
Vale destacar que, embora o referido §1º mencione especificamente a "Política de Gestão de Riscos", o §3º do mesmo artigo abre a possibilidade de que as estratégias e diretrizes referentes aos riscos de um processo específico (ex.: Investimentos) constem de outras políticas (ex.: "Política de Investimentos"). No texto da norma:

> "A critério da supervisionada, as estratégias e diretrizes de gestão de riscos poderão estar contidas em outras políticas que tratem especificamente de determinadas atividades, processos ou riscos, as quais deverão ser referenciadas na Política de Gestão de Riscos."
> (art. 108-L, §3º)

Isto é importante pois fornece à empresa uma maior flexibilidade para documentar suas diretrizes de gestão de riscos da maneira que considere mais conveniente. Nota-se que outra possibilidade, também prevista no texto acima é a utilização de políticas por tipo de risco, como, por exemplo, uma "Política de Risco de Mercado", que também pode abordar aspectos relativos ao processo de Investimento utilizado como exemplo.

A figura a seguir ilustra uma implementação possível para uma sociedade seguradora, que estaria de acordo com a regulamentação:

[17] Este tipo de informação sobre o Gestor de Riscos na Política de Gestão de Riscos poderá ser considerado como um item relevante na formalização da função (vide seção 4.2.1).



Note que a empresa do exemplo possui uma "Política de Subscrição", que trata dos processos de Subscrição (inc. I-a) e Resseguro (inc. I-d); uma "Política de Investimentos", que trata dos processos de Investimento (inc. V-a), ALM (inc. V-b) e Resgates/Portabilidades (inc. I-c); uma "Política Operacional", que trata da gestão de TI (inc. V-f) e da continuidade de negócios (inc. V-g) e, enfim, a "Política de Gestão de Riscos" propriamente dita, que trata dos demais processos requeridos pela norma. É interessante destacar ainda que os aspectos relativos à necessidade de liquidez para o processo de Resgates/Portabilidades encontram-se na "Política de Investimentos", enquanto outros riscos relevantes do mesmo processo são tratados na "Política de Gestão de Riscos".

Apenas para complementar o exemplo, a "Política de Subscrição" poderia definir limites máximos para a subscrição de riscos para cada linha de negócio, acima dos quais seria necessária a contratação de resseguro[18]. Poderia ainda definir critérios para uso de resseguro proporcional e não proporcional, além de diretrizes para a seleção dos Resseguradores contrapartes com base em critérios técnicos.

Quanto a essas outras políticas, que cumprem parte do papel da política de Gestão de Ricos, cabe destacar que a regulamentação exige que sejam referenciadas por esta (art. 108-L, §3º), ou seja, a PGR deve listar explicitamente que políticas são essas e os tipos de riscos a que se referem. Além disso, tais políticas também precisam ser aprovadas pela Diretoria da empresa e pelo seu Conselho de Administração, sempre que este existir (art. 108-L, §4º).

Como observação final, em 2019, foi incluído, entre os processos de trabalho cujos principais riscos deveriam ter estratégias e diretrizes definidas pela Política de Gestão de Riscos, a "prevenção, detecção e resposta a fraudes" (art. 108-L, §1°, inc. V, alínea "h"). Ao mesmo tempo, foi revogada a Circular Susep nº 344/2007 que tratava do assunto e previa que fosse estabelecida uma "política de prevenção, detecção e correção de fraudes". Com esta alteração, as diretrizes de tal política passam então a fazer parte da Política de Gestão de Riscos. Nos termos do §3º do art. 108-L, a supervisionada pode optar por manter uma "política de prevenção, detecção e correção de fraudes" apartada da Política de Gestão de Riscos, desde que, em linha com o explicado no parágrafo anterior, seja referenciada na PGR e aprovada pela Diretoria da empresa e pelo seu Conselho de Administração, sempre que este existir.

5.2.3. Âmbito de Definição das Políticas

Na seção 4.2.2 tivemos a oportunidade de discutir o quanto a gestão de riscos das supervisionadas que pertencem a grupos ou conglomerados pode se utilizar de funções instituídas no âmbito dos mesmos (e vice-versa).

Tal raciocínio pode ser estendido também para a Política de Gestão de Riscos e outras que, eventualmente, definam estratégias e diretrizes para o tratamento de riscos. Isto porque, como em

[18] Deverá ser observada a regulamentação do limite de retenção (Res. 321/2015, Título II, Capítulo I).

tese a estratégia e o Apetite por Riscos de uma empresa emanam de suas controladoras, espera-se que as políticas destas últimas forneçam diretrizes gerais consistentes para a gestão dos riscos das primeiras.

Entretanto, há que se considerar que as políticas definidas no âmbito de grupo podem não ser tão específicas a ponto de abrangerem tudo o que a Circular Susep nº 517/2015 exige. É por este motivo que a norma requer que a Diretoria e o Conselho de Administração (se houver) da supervisionada atestem explicitamente que a política do grupo é adequada diante dos riscos das operações da empresa. No texto regulamentar:

> "As supervisionadas que pertençam a grupos poderão seguir as políticas definidas no âmbito dos mesmos, desde que sua Diretoria e seu Conselho de Administração, quando houver, avaliem que elas contemplam as especificidades de suas operações" (art. 108-L, §5º)

Esta previsão evita que, para cumprir a norma, as diversas empresas de um grupo tivessem que transcrever e aprovar uma mesma política, o que traria uma complexidade administrativa desnecessária.

Apenas para um melhor entendimento, no exemplo da seção anterior a "Política Operacional" poderia ser do conglomerado, definida por um banco controlador, enquanto as demais seriam específicas da seguradora do grupo.

Para dar outro exemplo, um grupo composto somente por supervisionadas da Susep poderia ter uma única política de Gestão de Riscos (devidamente validada pelas Diretorias de cada supervisionada), que apenas definisse critérios gerais para o processo de gestão de riscos e para sua supervisão (inclusive os órgãos envolvidos no âmbito do grupo). Adicionalmente, cada supervisionada do grupo teria outras políticas para definir as estratégias e diretrizes para o tratamento de seus riscos específicos.

Enfim, diante de tantas possibilidades cabe à empresa escolher a que melhor lhe atende.

6. CASOS ESPECIAIS

6.1. POSSIBILIDADE DE DISPENSAS (DPVAT E RUN-OFF)

6.1.1. ASPECTOS GERAIS

A Circular Susep nº 517/2015 estabelece que:

> "As supervisionadas que, a qualquer tempo, se enquadrem nas situações listadas abaixo, poderão requerer à Susep dispensa total ou parcial do cumprimento do disposto neste Capítulo mediante apresentação de relatório que indique os itens considerados não aplicáveis tendo em vista os riscos de suas operações, o qual deverá ser assinado pela Diretoria e pelo Conselho de Administração, quando houver:
>
> I – Seguradoras que operem exclusivamente no ramo DPVAT, desde que não sejam responsáveis pela administração dos consórcios; ou
>
> II – Supervisionadas que, exceto por uma possível participação no DPVAT, possuam somente ramos/planos em run-off."
> (art. 108-A, § 3º)

Sendo assim, a norma permite que as empresas enquadradas nas situações acima (que estejam em *run-off* ou atuem no DPVAT – exclusivamente ou com outros ramos em *run-off*) solicitem dispensa de implementação de quaisquer dispositivos do Capítulo II do Título II, desde que devidamente justificado através de um relatório assinado pela Diretoria e Conselho de Administração (quando houver)[19]. Caberá à Susep, com base nas justificativas apresentadas, deferir ou não os pedidos, portanto, convém que a empresa seja bastante específica com relação aos itens da norma que não deseja implementar e que apresente justificativas consistentes para cada um deles com base nas orientações deste documento. O deferimento do pedido poderá ser parcial, através da aprovação de alguns itens e negativa de outros.

É importante frisar que a situação prevista no artigo transcrito acima pode ocorrer a qualquer tempo, como, por exemplo, no caso de uma empresa que transfere todas as suas operações e mantém unicamente sua participação no DPVAT, ou decide fazer o *run-off* de todos os seus planos de seguros e/ou previdência. Nestas situações, caso a empresa já possua uma Estrutura de Gestão de Riscos implantada, esta só poderá deixar de atender a qualquer item da norma após o consentimento expresso da Susep.

No entanto, para que as empresas possam embasar melhor seus eventuais pedidos de dispensa, faz-se necessário entender a razão de ser desta previsão normativa.

Um equívoco comum é associá-la ao porte dessas empresas (que tende a ser menor), ou aos recursos (normalmente mais limitados) de que elas dispõem para implantar uma Estrutura de Gestão de Riscos. Entretanto, a Susep entende que esta não é uma questão que deva ser tratada via dispensa, mas sim tomando por base o princípio da proporcionalidade (vide seção 2.2), que dá margem à adoção de mecanismos mais simplificados no caso de operações de baixa complexidade, de pequeno porte e/ou com menos riscos (ex.: políticas mais simples, controles mais rudimentares, etc.). Ou seja, o custo ou complexidade de implementação da Estrutura de Gestão de Riscos, por si só, não são considerados argumentos para a solicitação de dispensa.

[19] O protocolo de expedientes deverá ser direcionado à Coordenação Geral de Supervisão Consolidada (CGCON). O envio do pedido de aprovação prévia pode ser feito através de **Peticionamento Eletrônico**, pelo Tipo de Processo "SUPERVISÃO – AUTORIZAÇÃO – GESTÃO DE RISCO – DISPENSA".

Outro pensamento errôneo é o de que as operações em questão não possuem risco, o que costuma acontecer mais em relação ao DPVAT. Apesar da "operação do DPVAT" estar excluída da apuração da maioria dos capitais de risco (a exceção é o Risco Operacional), a Susep entende que existem outros fatores de risco dentro das empresas que atuam exclusivamente nesse ramo, que podem afetar sua continuidade. Um exemplo são os riscos referentes aos ativos próprios mantidos por elas, tanto é que, na apuração dos capitais de Risco de Crédito e Risco de Mercado, os fundos exclusivos dos consórcios DPVAT (relacionados diretamente à "operação") não são levados em conta, mas outros fundos, ativos e investimentos que a empresa detenha sim. Outros riscos, como o de fraudes, por exemplo, podem ser bastante significativos e, por isso, precisarão ser tratados. Neste contexto, a Estrutura de Gestão de Riscos é essencial para resguardar a continuidade dessas empresas e, em última instância, dos próprios consórcios.

Então o que justifica a possibilidade de dispensas para as empresas do DPVAT ou em run-off?

É inegável que, quando o tema Gestão de Riscos foi discutido na Subcomissão de Riscos da Susep, os debates sempre focaram em supervisionadas que se encontram em plena operação, as quais desempenham uma ampla gama de atividades. Sendo assim, a Circular 517/2015 prevê elementos que podem não se aplicar aos casos de run-off e DPVAT, dado que as empresas com este tipo de operação, em geral, possuem um conjunto de funções/atividades mais reduzido. Por exemplo, a atividade de subscrição (que a norma exige que seja tratada explicitamente na Política de Gestão de Riscos) pode ser bastante limitada, senão inexistente.

Porém, nem todos os casos "não aplicáveis" são tão claros assim, por isso a Susep optou por solicitar uma análise das empresas exclusivas do DPVAT e/ou em run-off e, com base nos argumentos apresentados, definir caso a caso os comandos que não precisariam ser seguidos por elas. Frise-se que é essencial que eles estejam associados a funções/atividades que não fazem parte da operação da empresa ou sejam bastante limitadas na mesma.

Outro aspecto interessante de se destacar refere-se à precariedade das autorizações que eventualmente sejam concedidas pela Susep. Tendo em vista que as mesmas se baseiam em características da operação, quaisquer mudanças nessas características devem invalidá-la.

Como exemplo, uma empresa que tenha obtido autorizações para certas dispensas enquanto atuava exclusivamente no DPVAT, terá as referidas autorizações revogadas tacitamente se, num determinado momento, começar a atuar em outros ramos. Por este motivo, qualquer autorização que venha a ser concedida deverá ser bastante clara em relação à característica operacional específica que a motivou. A manutenção dessas características deverá ser objeto de verificação numa eventual fiscalização.

Com relação ao exemplo citado acima, vale ressaltar que a empresa não fica impedida de começar a atuar em outros ramos, porém, antes de iniciar essas novas operações, ela terá que ajustar sua Estrutura de Gestão de Riscos (implementando itens que haviam sido dispensados anteriormente) de forma a torna-la compatível com a nova realidade.

6.1.2. Considerações Específicas Sobre a Operação do DPVAT

As empresas que participam dos consórcios do DPVAT normalmente têm pouca ou nenhuma influência sobre a operação em si, que é gerida de forma centralizada pela Seguradora Líder. Para se ter uma ideia, esta é a responsável por receber os prêmios, aplicar os recursos e pagar os sinistros, entre outras

atividades. Também é a Seguradora Líder que informa a cada consorciada os valores correspondentes de ativos (quotas de fundos) e provisões, de acordo com sua participação no consórcio, para fins de registro contábil.

A parte da operação que pode sofrer interferência mais direta das consorciadas é a regulação dos sinistros. Não são todas as consorciadas que realizam esta atividade, mas algumas o fazem. Nos pedidos de dispensa encaminhados, as empresas devem considerar esta característica, pois, dado que a regulação tem um importante papel no combate a fraudes, as empresas que desempenham esta atividade provavelmente precisarão ter uma Estrutura de Gestão de Riscos mais robusta que as demais.

6.1.3. CONSIDERAÇÕES ESPECÍFICAS SOBRE RAMOS EM RUN-OFF

Inicialmente é importante observar que, embora o termo "*run-off*" seja corrente no mercado de seguros, não há uma definição amplamente aceita para ele.

Em geral, a Susep tem entendido que o *run-off*, no sentido mais estrito, ocorre quando, por razões estratégicas, a empresa decide parar de comercializar seus produtos. Em outras palavras, ela não aceitará mais novos segurados/participantes e não renovará apólices/planos nos casos em que tenha tal opção. Esta situação sinaliza que a empresa não possui mais qualquer apetite por risco relativo às atividades supervisionadas pela Susep.

Note que não se trata de uma circunstância de mercado, que eventualmente faça com que os produtos oferecidos não sejam mais procurados pelos consumidores, mas sim de uma decisão consciente, devidamente formalizada pela empresa.

No entanto, destacamos que as obrigações assumidas junto aos segurados aceitos anteriormente continuam existindo, até que decorra a vigência das respectivas coberturas ou ocorra uma transferência da carteira. A exigência de uma Estrutura de Gestão de Riscos visa exatamente a garantir o adequado cumprimento dessas obrigações.

Existem também casos em que a empresa pode decidir não receber mais novos clientes, mas, mesmo assim, renovar voluntariamente apólices/planos já contratados antes. Para uma parte do mercado, esta situação também é chamada de *run-off*. Por conta disso, pedidos de empresas com essa característica poderão ser analisados pela Susep, entretanto, há que se ter especial atenção nesses casos, pois, de alguma forma, elas continuam com a possibilidade de escolher os riscos de seguros que assumem. Ao contrário do conceito mais estrito de *run-off*, cuidados especiais na subscrição (no caso, renovações) podem ser necessários.

6.2. TERCEIRIZAÇÃO DAS FUNÇÕES DO GESTOR DE RISCOS

A Circular Susep nº 517/2015 prevê a possibilidade de terceirização da função do Gestor de Riscos, ainda que sob certas condições e mediante aprovação prévia da Susep[20]. No texto da norma:

[20] O protocolo de expedientes deverá ser direcionado à Coordenação Geral de Supervisão Consolidada (CGCON). O envio do pedido de aprovação prévia pode ser feito através de **Peticionamento Eletrônico**, pelo Tipo de Processo "SUPERVISÃO – AUTORIZAÇÃO – GESTÃO DE RISCO – TERCEIRIZAÇÃO DE GESTOR DE RISCO".

> "Como alternativa à nomeação do Gestor de Riscos prevista no artigo 108-E, a Susep poderá autorizar, mediante solicitação prévia da supervisionada, que as funções do Gestor de Riscos sejam desempenhadas por:
>
> I – Empresa terceirizada, no caso de supervisionadas que consigam comprovar que a contratação de um Gestor de Riscos próprio representa impacto relevante em seu quadro funcional e nas despesas com pessoal, seus procedimentos operacionais e sistemas de informática apresentam baixa complexidade e os produtos comercializados possuem pouca diversidade em termos de coberturas oferecidas. (...)"
> (art. 108-F, caput e inc. I)

Cabe destacar que esta terceirização é considerada uma alternativa interessante para que empresas de porte reduzido possam, dentro de um custo razoável, contar com uma função de gestão de riscos (2º Linha de Defesa – vide seções 4.1 e 4.2) efetiva, que atenda aos propósitos da regulamentação.

Entretanto, para empresas que pertençam a grupos, a alternativa do Gestor de Riscos no âmbito do grupo também deve ser considerada (vide seção 4.2.2). Na realidade, a Susep a encara até como preferível, pois, quando se fala de terceirização, deve-se levar em conta as eventuais limitações que um ente externo pode ter para desempenhar este papel.

A propósito, foi exatamente em virtude dessas limitações que o dispositivo transcrito acima estabeleceu que, para solicitar a terceirização da função do Gestor de Riscos, a empresa deve possuir baixa complexidade operacional (em termos de procedimentos, produtos e sistemas). Naturalmente, isto deve ser evidenciado quando da submissão de um pedido à Susep.

Algumas informações que podem ser incluídas nos pedidos de forma a melhor instruí-los são:

- Quanto ao Impacto no quadro funcional/despesas com pessoal – Demonstrativo que compare o custo estimado de um Gestor de Riscos (incluindo os recursos materiais e humanos de que ele deveria dispor, se relevantes) com as atuais despesas da empresa com pessoal.
- Quanto aos procedimentos operacionais e sistemas de informática – Manuais de procedimentos operacionais relativos à atividade finalística da empresa e uma descrição resumida dos principais sistemas de informática utilizados pela mesma.
- Quanto à diversidade de produtos/coberturas – Breve descrição dos produtos e coberturas oferecidos, indicando se há ramos em *run-off* ou outras peculiaridades que possam representar simplificações em sua gestão.

Vale ressaltar que a lista acima é meramente exemplificativa, ficando a empresa livre para apresentar qualquer documentação adicional que julgue pertinente. Da mesma forma, a Susep reserva-se o direito de exigir quaisquer comprovações adicionais que considere necessárias em cada caso concreto.

Outro ponto importante diz respeito à escolha da empresa terceirizada que desempenhará o papel do Gestor de Riscos. Assim como para a escolha do Gestor de Riscos próprio (vide seção 4.2.1), a Susep não possui a prerrogativa de aprovar ou rejeitar *a priori* a empresa escolhida. A Autarquia entende que

esta escolha é uma responsabilidade da contratante e que a adequação da terceirizada para a tarefa será avaliada quando da realização de fiscalizações.

Por fim, assim como nos casos de dispensas (seção 6.1), este tipo de autorização também possui caráter essencialmente precário, pois mudanças supervenientes na operação da supervisionada podem alterar substancialmente as características que a embasaram. Por exemplo, se a empresa começar a operar em novos ramos, a autorização para terceirização poderá ser considerada revogada tacitamente em função do aumento de complexidade. Desta forma, para as empresas que possuam este tipo de autorização, recomenda-se sua revalidação junto à Susep sempre que houver perspectiva de alteração relevante na operação.

6.3. DELEGAÇÃO DAS FUNÇÕES DO GESTOR DE RISCOS PARA MATRIZ ESTRANGEIRA (RESSEGURADORES)

Para os resseguradores locais pertencentes a grupos estrangeiros, existe ainda a possibilidade de delegar as funções do Gestor de Riscos para uma área especializada em gestão de riscos da matriz sediada no exterior. Assim como para a terceirização (vide seção 6.2), existem condições específicas para isso e há necessidade de aprovação prévia pela Susep[21]. No texto regulamentar:

> "Como alternativa à nomeação do Gestor de Riscos prevista no artigo 108-E, a Susep poderá autorizar, mediante solicitação prévia da supervisionada, que as funções do Gestor de Riscos sejam desempenhadas por:
> (...)
> II – Área especializada em gestão de riscos localizada em matriz estrangeira, no caso de Resseguradores locais que consigam comprovar que a contratação de um Gestor de Riscos no país representa impacto relevante em seu quadro funcional e nas despesas com pessoal, que é baixa a sua flexibilidade para implantar procedimentos operacionais e sistemas de informática diferentes dos adotados mundialmente pela matriz, que sua aceitação de riscos está submetida a rigoroso controle pela matriz e que sua gestão é separada da de outras supervisionadas pertencentes ao mesmo grupo."
> (art. 108-F, caput e inc. II)

Nota-se claramente que, assim como no caso de terceirização, existe uma questão de custo x benefício, ou seja, uma preocupação no sentido de que o ressegurador possa contar com uma solução aceitável a um custo razoável. No entanto, ainda comparado ao caso de terceirização, a segunda preocupação não é propriamente com a complexidade operacional, mas sim com o nível de autonomia que a operação local (Brasil) tem em relação às diretrizes que vêm de fora. Isto porque, como a natureza da operação de resseguro tende a ser global, em alguns casos os principais controles de um ressegurador local que são definidos e implementados no país são aqueles relativos à contabilidade, pagamento de

[21] O protocolo de expedientes deverá ser direcionado à Coordenação Geral de Supervisão Consolidada (CGCON). O envio do pedido de aprovação prévia pode ser feito através de **Peticionamento Eletrônico**, pelo Tipo de Processo "SUPERVISÃO – AUTORIZAÇÃO – GESTÃO DE RISCO – DELEGAÇÃO DE GESTOR DE RISCO".

tributos e envio de informações à Susep[22], o que faz com que um gestor de riscos local não seja de muita valia.

De acordo com o texto da norma, a referida falta de autonomia pode ser demonstrada a partir da flexibilidade para implantação de sistemas e procedimentos localmente, bem como pelo rigor dos limites impostos pela matriz para a aceitação de riscos no Brasil.

Sendo assim, algumas informações que podem ser incluídas nos pedidos de forma a melhor instruí-los são:

- Quanto ao Impacto no quadro funcional/despesas com pessoal – Demonstrativo que compare o custo estimado de um Gestor de Riscos (incluindo os recursos materiais e humanos de que ele deveria dispor, se relevantes) com as atuais despesas da empresa com pessoal.
- Quanto aos procedimentos operacionais e sistemas de informática – Manuais de procedimentos operacionais relativos à atividade finalística da empresa e uma descrição resumida dos principais sistemas de informática utilizados pela mesma. Em relação aos sistemas, identificar quais são fornecidos pela matriz e quais são implementados localmente.
- Quanto à aceitação de riscos – Políticas e outros documentos emitidos pela matriz que evidenciem suas diretrizes com relação à aceitação de riscos.

Vale ressaltar que a lista acima é meramente exemplificativa, ficando a empresa livre para apresentar qualquer documentação adicional que julgue pertinente. Da mesma forma, a Susep reserva-se o direito de exigir quaisquer comprovações adicionais que considere necessárias em cada caso concreto, bem como solicitar a tradução de documentos cuja língua original não seja de domínio de seus analistas.

Outro requisito previsto na norma diz respeito à não integração da gestão do ressegurador local em relação a outras supervisionadas consideradas do mesmo grupo. Isto porque, caso contrário, a solução do Gestor de Riscos no âmbito do grupo seria preferível.

Este último aspecto pode ser mais subjetivo que os anteriores, mas espera-se que possa ser demonstrado, por exemplo, pela composição da Diretoria (integrantes distintos), pela existência de um Conselho de Administração separado (se for o caso) e pelo limitado compartilhamento de recursos/funções com as demais empresas do grupo constituídas no Brasil.

Outro ponto análogo refere-se à necessidade de revalidação da autorização junto à Susep sempre que houver perspectiva de alterações relevantes na operação, pois, uma vez que tais alterações podem modificar substancialmente as características que a embasaram, a autorização poderá ser considerada tacitamente revogada em virtude das mesmas (precariedade).

[22] Isto não significa que tais aspectos não impliquem em riscos para a supervisionada, mas sim que o controle desses riscos, mais voltados para questões legais e regulatórias, pode ser suprido em grande parte pelo Sistema de Controles Internos (Circular Susep nº 249/2004).

ANEXO I – CONTROLE DE VERSÕES DESTE DOCUMENTO

VERSÃO	DESCRIÇÃO
V1.0	1ª versão do documento, concluída em março de 2017.
V2.0	Atualização em abril de 2020, contemplando: - Adaptação do manual à reestruturação da Susep, com atualização na seção 1 das informações relativas às unidades responsáveis e suas competências, inclusive quanto à recepção de dívidas e contatos externos; - Atualização geral do manual para adequação às alterações realizadas entre março de 2017 e abril de 2020 na base legal deste manual (Capítulo II do Título II da Circular Susep n° 512, de 2015).