

Instituto de Seguros de Portugal - Norma n.º 14/2005-R - princípios aplicáveis ao desenvolvimento dos sistemas de gestão de riscos e de controlo interno das empresas de seguros

As melhores práticas internacionais na regulamentação e supervisão da actividade seguradora identificam claramente o estabelecimento de adequados mecanismos de governação como um dos factores chave no desenvolvimento de um sistema de solvência apropriado. De entre estes mecanismos destacam-se, pela sua importância na gestão sã e prudente do negócio segurador, os sistemas de gestão de riscos e de controlo interno.

Considerando que:

- a) O órgão de administração e os directores de topo, como responsáveis principais pela gestão sã e prudente da empresa de seguros, devem desenvolver, implementar e manter estratégias que definam as políticas, os procedimentos e os controlos que compõem os sistemas de gestão de riscos e de controlo interno;
- b) Estes sistemas devem ser suportados por uma estrutura organizacional apropriada e devem ser adequados à dimensão, natureza e complexidade das operações da empresa de seguros, incluindo todos os riscos que a possam materialmente afectar;
- c) Um adequado sistema de gestão de riscos requer uma compreensão apropriada da natureza e da significância dos riscos, financeiros e não financeiros, a que se encontra exposta a empresa de seguros, factor essencial no estabelecimento dos respectivos níveis de tolerância e no desenho de estratégias destinadas à sua mitigação e controlo;
- d) Os sistemas de controlo interno devem contribuir para reforçar a confiança nos procedimentos operacionais da empresa, de modo a possibilitar a detecção atempada de falhas e ou fragilidades nos processos e estruturas operativos;

O Instituto de Seguros de Portugal, ao abrigo do artigo 122.º-A do Decreto-Lei n.º 94-B/98, de 17 de Abril, na redacção introduzida pelo Decreto-Lei n.º 251/2003, de 14 de Outubro, e nos termos do n.º 3 do artigo 4.º do seu Estatuto, aprovado pelo Decreto-Lei n.º 289/2001, de 13 de Novembro, emite a seguinte norma regulamentar:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objectivo

A presente norma tem por objectivo o estabelecimento dos princípios gerais que devem presidir ao desenvolvimento dos sistemas de gestão de riscos e de controlo interno a implementar pelas empresas de seguros.

CAPÍTULO II

Estrutura organizacional

Artigo 2.º

Definição e objectivos

- 1 - A empresa de seguros deve apresentar uma estrutura organizacional bem definida, que sirva de suporte à implementação de sistemas de gestão de riscos e de controlo interno eficientes, no sentido de assegurar que a gestão e o controlo das operações sejam efectuados de uma forma sã e prudente.
- 2 - A estrutura organizacional da empresa de seguros deve ser adequada à dimensão, natureza e complexidade da actividade desenvolvida.
- 3 - A estrutura organizacional deve promover uma definição clara e objectiva da cadeia de responsabilidades e de autoridade e contemplar uma adequada segregação de deveres, tanto ao nível individual como entre funções, de modo a assegurar, designadamente, uma separação precisa entre funções conflituantes.
- 4 - No caso de empresas de seguros com reduzida amplitude de negócio e reduzida dimensão dos riscos associados à sua actividade e em que, devido à limitação de recursos disponíveis, seja inexequível a total segregação de deveres, devem ser implementados procedimentos adicionais de controlo que garantam uma segurança equivalente.
- 5 - A estrutura organizacional deve ser documentada, analisada e revista periodicamente, no sentido de aferir da sua adequação e, sempre que necessário, ser alterada.
- 6 - Para efeitos da presente norma, no âmbito da estrutura organizacional da empresa de seguros entende-se por órgão de administração o órgão social ao qual, na estrutura orgânica da empresa, compete assegurar a respectiva gestão e representação e por directores de topo os dirigentes que, não fazendo parte do órgão de administração, constituem a primeira linha hierárquica responsável pela gestão daquela.

Artigo 3.º

Cultura organizacional

- 1 - A cultura organizacional da empresa de seguros deve garantir que toda a estrutura organizacional reconhece a importância da gestão de riscos e do controlo interno, de modo a assegurar uma gestão sã e prudente da actividade da empresa.

- 2 - O órgão de administração deve promover um alto nível de integridade, estabelecer uma cultura que enfatize, em toda a estrutura organizacional, a importância da gestão de riscos e do controlo interno e assegurar, simultaneamente, a existência dos meios necessários ao desenvolvimento, implementação e manutenção de sistemas adequados.
- 3 - Os directores de topo são responsáveis pela implementação de uma cultura de gestão de riscos e de controlo interno que abranja toda a estrutura organizacional da empresa de seguros.
- 4 - Todos os restantes colaboradores da empresa de seguros contribuem também para a gestão de riscos e para o controlo interno, devendo, para o efeito, compreender o seu papel nos sistemas implementados.
- 5 - Para efeitos da gestão sã e prudente referida no n.º 1, e no sentido de assegurar uma cultura ética, essencial no âmbito de sistemas de gestão de riscos e de controlo interno adequados, deve ser ponderada a necessidade de elaborar e implementar códigos de conduta.

Artigo 4.º

Sistemas de informação e comunicação

- 1 - A estrutura organizacional da empresa de seguros deve contemplar a existência de sistemas de informação apropriados às suas actividades, estratégias, objectivos e necessidades e de canais de comunicação adequados.
- 2 - Devem ser implementados sistemas de informação que produzam informação fiável, de qualidade, suficiente, atempada e relevante acerca da actividade desenvolvida, dos compromissos assumidos e dos riscos a que a empresa de seguros se encontra exposta.
- 3 - Os sistemas de informação devem permitir a fácil utilização, monitorização e revisão da informação, quer interna quer externamente.
- 4 - Devem ser definidos canais de comunicação, internos e externos, e linhas de reporte que garantam uma comunicação eficaz através da organização e assegurem o reporte atempado e adequado de informação para os intervenientes e funções apropriados.

Artigo 5.º

Responsabilidades do órgão de administração

- 1 - O órgão de administração é responsável por garantir que a estrutura organizacional permite à empresa de seguros o estabelecimento de mecanismos de governação adequados à dimensão, natureza e complexidade da sua actividade.
- 2 - Para efeitos do número anterior, compete ao órgão de administração:
- Definir, aprovar e rever a estrutura organizacional da empresa de seguros por forma a garantir o seu devido enquadramento no âmbito da implementação dos sistemas de gestão de riscos e de controlo interno, estabelecendo as cadeias de responsabilidades e de autoridade, os procedimentos de tomada de decisão apropriados e uma segregação adequada de deveres, tanto ao nível individual como entre funções;
 - Definir, aprovar e rever as políticas de recursos humanos e garantir a sua suficiência e adequadas qualificações;
 - Seleccionar os directores de topo e assegurar que estes possuem, individual e colectivamente, competência, conhecimento, integridade, prudência e experiência adequados para o preenchimento da respectiva posição;
 - Definir as responsabilidades e deveres dos directores de topo;
 - Definir e aprovar, sempre que conveniente, códigos de conduta;
 - Assegurar a existência de sistemas de informação e de canais de comunicação continuamente adequados à actividade e aos riscos da empresa de seguros;
 - Assegurar que a adequação da estrutura da empresa de seguros à sua actividade é sujeita a revisões periódicas.
- 3 - O exercício das competências descritas no número anterior deve ser adequadamente documentado.

Artigo 6.º

Responsabilidades dos directores de topo

- 1 - Os directores de topo são responsáveis por assegurar o cumprimento das estratégias, políticas, objectivos e orientações definidos pelo órgão de administração no que respeita à estrutura organizacional da empresa de seguros.
- 2 - Para os efeitos do número anterior, compete aos directores de topo:
- Desenvolver, implementar e manter uma estrutura organizacional nos termos das orientações definidas pelo órgão de administração;
 - Garantir que quaisquer áreas de potenciais conflitos de interesse são identificadas antecipadamente, minimizadas e sujeitas a uma monitorização cuidadosa e independente;
 - Garantir que os colaboradores têm as capacidades e a experiência requeridas para o desempenho das suas funções;
 - Desenvolver, implementar e manter sistemas de informação e estabelecer canais de comunicação e linhas de reporte que cumpram os princípios do artigo 4.º;
 - Rever os sistemas de informação e comunicação por forma a assegurar a sua permanente adequação à actividade da empresa de seguros;
 - Informar o órgão de administração sempre que sejam identificadas quaisquer falhas e ou fragilidades na estrutura organizacional da empresa de seguros.

3 - O exercício das competências descritas no número anterior deve ser adequadamente documentado.

CAPÍTULO III

Gestão de riscos

Artigo 7.º

Definição e objectivos

1 - A gestão de riscos é um processo contínuo que serve de base à implementação da estratégia da empresa de seguros e que deve assegurar uma compreensão apropriada da natureza e da significância dos riscos a que ela se encontra exposta.

2 - O objectivo da gestão de riscos é a identificação, avaliação, mitigação, monitorização e controlo de todos os riscos materiais a que a empresa de seguros se encontra exposta, tanto ao nível interno como externo, por forma a assegurar que aqueles se mantêm a um nível que não afecte significativamente a sua situação financeira e os interesses dos credores específicos de seguros.

3 - O processo de gestão de riscos deve ter uma influência activa na definição do perfil de risco da empresa de seguros e nas tomadas de decisão do órgão de administração e dos directores de topo.

Artigo 8.º

Princípios aplicáveis aos sistemas de gestão de riscos

1 - O sistema de gestão de riscos deve ser suportado por uma estrutura organizacional bem definida e por um adequado sistema de controlo interno e ser proporcional à dimensão e complexidade da actividade da empresa de seguros, tomando, nomeadamente, em consideração a natureza e a especificidade dos riscos que a mesma assume e ou pretende assumir.

2 - Um sistema de gestão de riscos adequado deve tomar em consideração:

- a) Os riscos directamente associados à actividade seguradora;
- b) Os riscos relevantes que, embora não estejam directamente associados à actividade seguradora, sejam subjacentes a essa actividade;
- c) As oportunidades de negócio subjacentes aos diferentes riscos.

3 - O sistema de gestão de riscos deve tomar em consideração os riscos específicos de seguros, os riscos de mercado, crédito, liquidez e operacional, bem como todos os riscos que, em face da situação concreta da empresa de seguros, nomeadamente o facto de pertencer a um grupo, se possam revelar materiais.

4 - Para efeitos da presente norma entende-se por:

- a) "Risco específico de seguros" o risco inerente à comercialização de contratos de seguro, associado ao desenho de produtos e respectiva tarifação, ao processo de subscrição e de provisionamento das responsabilidades e à gestão dos sinistros e do resseguro;
- b) "Risco de mercado" o risco de movimentos adversos no valor de activos da empresa de seguros relacionados com variações dos mercados de capitais, dos mercados cambiais, das taxas de juro e do valor do imobiliário. O risco de mercado inclui ainda os riscos associados ao uso de instrumentos financeiros derivados e está fortemente relacionado com o risco de mismatching entre activos e responsabilidades;
- c) "Risco de crédito" o risco de incumprimento ou de alteração na qualidade creditícia dos emitentes de valores mobiliários aos quais a empresa de seguros está exposta, bem como dos devedores, prestatários, mediadores, tomadores de seguro e resseguradores que com ela se relacionam;
- d) "Risco de liquidez" o risco que advém da possibilidade da a empresa de seguros não deter activos com liquidez suficiente para fazer face aos requisitos de fluxos monetários necessários ao cumprimento das obrigações para com os tomadores de seguros e outros credores à medida que eles se vencem;
- e) "Risco operacional" o risco de perdas resultantes da inadequação ou falha nos procedimentos internos, pessoas, sistemas ou eventos externos.

5 - O processo de identificação, avaliação, mitigação, monitorização e controlo de riscos deve assegurar o desenvolvimento, a implementação e a manutenção de procedimentos, organizacionais e de controlo, necessários à gestão prudente dos riscos a que a empresa de seguros está exposta.

6 - O sistema de gestão de riscos deve ser devidamente planeado, revisto e documentado e deve explicitar, nomeadamente, os riscos materiais a que a empresa de seguros se encontra exposta com a descrição da sua natureza, as análises efectuadas, os modelos utilizados e os pressupostos considerados.

7 - O sistema de gestão de riscos a implementar deve, nomeadamente:

- a) Incluir a definição das regras e procedimentos para identificar e hierarquizar os riscos e os activos, passivos e operações associados a esses riscos;
- b) Incluir análises qualitativas e quantitativas de risco adequadas, identificando as medidas de risco consideradas;
- c) Incluir a definição dos níveis de tolerância a respeitar para cada risco, os quais devem ser revistos periodicamente, no mínimo anualmente;
- d) Incluir a definição e monitorização de indicadores de alerta no sentido de permitir uma detecção atempada dos riscos potencialmente adversos.

8 - As análises quantitativas previstas na alínea b) do número anterior devem incluir a realização de exercícios de stress test que permitam a determinação, quer individualmente quer de uma forma agregada, da probabilidade de a empresa de seguros cumprir os seus compromissos face ao desenvolvimento adverso, num dado horizonte temporal, dos diferentes factores de risco.

9 - Os exercícios de stress test referidos no número anterior podem englobar diferentes níveis de sofisticação, incorporando desde a realização de análises de sensibilidade simplificadas à realização de testes de cenários adversos que envolvam a evolução conjunta de diferentes factores de risco.

10 - No âmbito do sistema de gestão de riscos, as empresas de seguros devem ainda definir, implementar e manter planos de continuidade de negócio e ou de recuperação em caso de catástrofe.

Artigo 9.º

Responsabilidades do órgão de administração

1 - O órgão de administração deve ter um conhecimento adequado dos tipos de riscos a que a empresa de seguros se encontra exposta e das técnicas utilizadas para avaliar e gerir esses riscos eficientemente, sendo responsável pelo estabelecimento e manutenção de um sistema de gestão de riscos apropriado e eficaz.

2 - No âmbito de um adequado sistema de gestão de riscos, o órgão de administração é responsável pela definição, aprovação e revisão periódica das principais orientações estratégicas e políticas de negócio globais da empresa de seguros, devendo proceder-se regularmente à monitorização e avaliação do seu desempenho.

3 - Para efeitos dos números anteriores, compete ao órgão de administração:

- a) Definir orientações no que se refere à política de tolerância ao risco da empresa e aprovar os níveis de tolerância a respeitar;
- b) Definir orientações no que se refere às políticas de exposição, gestão, monitorização e reporte sobre os principais riscos a que a empresa de seguros está sujeita e aprovar as políticas a implementar;
- c) Requerer e assegurar a existência de um processo para a determinação do nível de capital adequado aos riscos e da sua afectação às áreas de negócio/risco da empresa;
- d) Requerer e assegurar que os directores de topo implementem as políticas aprovadas e as instruções dadas e monitorizem as mesmas, no sentido de garantir o seu cumprimento e a sua eficácia;
- e) Requerer e assegurar que os directores de topo efectuem um reporte preciso e tempestivo sobre os principais riscos a que a empresa de seguros se encontra exposta e que identifique os procedimentos de controlo implementados para gerir esses riscos;
- f) Rever as orientações e políticas de tolerância, exposição, gestão, monitorização e reporte sobre os principais riscos no sentido de corrigir e ou melhorar o sistema de gestão de riscos implementado;
- g) Assegurar que as actividades de gestão de riscos têm uma independência, estatuto e visibilidade suficientes e que são sujeitas a revisões periódicas.

4 - O exercício das competências descritas no número anterior deve ser adequadamente documentado.

Artigo 10.º

Responsabilidades dos directores de topo

1 - Os directores de topo devem garantir que é efectuada a identificação, a avaliação e a mitigação dos riscos a que a empresa de seguros se encontra exposta e assegurar a existência dos mecanismos necessários para a sua monitorização e controlo.

2 - Para efeitos do número anterior, compete aos directores de topo:

- a) Definir os níveis de tolerância ao risco em linha com as orientações definidas pelo órgão de administração;
- b) Definir políticas concretas de aceitação e gestão dos riscos a que a empresa está exposta, através da implementação de procedimentos eficazes e adequados em linha com as orientações definidas e aprovadas pelo órgão de administração;
- c) Definir, implementar e rever processos para a determinação do nível de capital adequado aos riscos e da sua afectação às áreas de negócio/risco da empresa;
- d) Definir, implementar e rever os mecanismos de monitorização para verificar, de forma regular, o cumprimento dos níveis de tolerância ao risco e das políticas e procedimentos de gestão de riscos e avaliar a sua eficácia e contínua adequação à actividade da empresa de seguros, no sentido de possibilitar a correcção de quaisquer falhas e ou fragilidades detectadas;
- e) Definir, implementar e rever procedimentos de reporte, periódico e extraordinário, no sentido de ser disponibilizada, aos intervenientes e funções apropriados, informação sobre a eficácia e adequação do sistema de gestão de riscos;
- f) Manter o órgão de administração informado, através de reportes periódicos, sobre a eficácia e adequação do sistema de gestão de riscos, incluindo, nomeadamente, informação relacionada com os riscos a que a empresa de seguros está exposta, assim como os procedimentos de controlo implementados para a sua gestão e, se necessário, efectuando propostas no que se refere a quaisquer falhas e ou fragilidades detectadas;
- g) Implementar as orientações e recomendações efectuadas pelo órgão de administração no sentido de introduzir correcções e ou melhorias no sistema de gestão de riscos e monitorizar o seu efectivo cumprimento.

3 - O exercício das competências descritas no número anterior deve ser adequadamente documentado.

Artigo 11.º

Função de gestão de riscos

1 - A empresa de seguros deve estabelecer na sua estrutura organizacional uma função de gestão de riscos adequada à dimensão, natureza e complexidade das respectivas operações.

2 - A função de gestão de riscos deve ser exercida por pessoal competente e qualificado, com uma clara compreensão do seu papel e responsabilidades.

3 - A função de gestão de riscos deve desempenhar as suas competências objectivamente e de forma independente relativamente às actividades operacionais da empresa de seguros, podendo, no entanto, no caso de empresas com reduzida amplitude de negócio e reduzida dimensão dos riscos associados à sua actividade, ser utilizada uma tipologia estrutural que não verifique completamente o requisito de independência, desde que sejam implementados procedimentos adicionais de controlo que garantam uma segurança equivalente.

4 - O pessoal que executa a função de gestão de riscos deve ter acesso pleno a todas as actividades da empresa de seguros, pelo que lhe deve ser disponibilizada toda a informação necessária ao desempenho das suas competências.

5 - A função de gestão de riscos deve concretizar as políticas definidas pelos directores de topo e aprovadas pelo órgão de administração, através do planeamento, análise, monitorização e reporte do impacte dos riscos a que a empresa de seguros está exposta, e deve propor planos de mitigação e ou transferência de riscos para fazer face às diferentes situações.

6 - A função de gestão de riscos deve ser adequadamente documentada e reportada aos intervenientes e áreas funcionais apropriados e, no mínimo, aos directores de topo e ao órgão de administração.

7 - A função de gestão de riscos deve assegurar um acompanhamento contínuo do sistema de gestão de riscos no sentido de garantir a introdução e implementação de alterações que venham a ser sugeridas e ou recomendadas.

CAPÍTULO IV

Controlo interno

Artigo 12.º

Definição e objectivos

O controlo interno compreende um conjunto coerente, abrangente e contínuo de procedimentos concretizados pelo órgão de administração, pelos directores de topo e por todos os restantes colaboradores da empresa de seguros com o objectivo de assegurar:

- a) A eficiência e a eficácia das operações;
- b) A existência e prestação de informação, financeira e não financeira, fiável e completa;
- c) A eficiência do sistema de gestão de riscos, incluindo, nomeadamente, o risco específico de seguros, bem como os riscos de mercado, de crédito, de liquidez e operacional;
- d) Uma correcta e adequada avaliação dos activos e responsabilidades;
- e) Um desempenho prudente da actividade;
- f) O cumprimento da legislação e demais regulamentação, assim como das políticas e procedimentos internos;
- g) A verificação de outros mecanismos de governação definidos pelo órgão de administração.

Artigo 13.º

Princípios aplicáveis ao sistema de controlo interno

1 - O sistema de controlo interno da empresa de seguros deve ter por base um eficiente sistema de gestão de riscos, actividades de controlo e procedimentos de monitorização apropriados e claramente definidos, suportados por uma estrutura organizacional adequada.

2 - O sistema de controlo interno deve ser adequado à dimensão, natureza e complexidade da actividade, ao grau de centralização e delegação de autoridade estabelecidos e à capacidade e eficácia das tecnologias de informação, tendo por base os níveis de tolerância de risco definidos, nos termos do capítulo III, para cada área da empresa de seguros.

3 - O sistema de controlo interno deve ser devidamente planeado e revisto continuamente e o seu desenvolvimento, implementação e manutenção devem ser adequadamente documentados.

4 - No âmbito do sistema de controlo interno, devem ser definidas, implementadas e monitorizadas actividades específicas de controlo a todos os níveis e, nomeadamente, para as principais unidades funcionais da empresa de seguros.

Artigo 14.º

Responsabilidades do órgão de administração

1 - O órgão de administração é responsável por definir uma estratégia de controlo interno e pelo estabelecimento e manutenção de um sistema de controlo interno adequado e eficaz.

2 - No âmbito do sistema de controlo interno, o órgão de administração é responsável por proporcionar orientação e controlo prudencial adequados que permitam garantir uma gestão e um controlo da empresa de seguros apropriados e eficazes e que assegurem a conformidade da sua actividade com a legislação e demais regulamentação em vigor.

3 - Para efeitos dos números anteriores, compete ao órgão de administração:

- a) Definir e aprovar orientações de controlo interno que sirvam de base para o sistema de controlo interno;
- b) Definir, aprovar e rever programas, procedimentos e controlos internos específicos para combater o branqueamento de capitais;
- c) Requerer e assegurar que os directores de topo implementem as orientações e políticas aprovadas e as instruções dadas;
- d) Requerer e assegurar a existência e a eficácia de mecanismos de monitorização do sistema de controlo interno;
- e) Requerer e assegurar dos directores de topo um reporte preciso e tempestivo sobre a eficiência e eficácia do sistema de controlo interno, incluindo a identificação dos principais procedimentos de controlo implementados;
- f) Rever as orientações e políticas de controlo interno no sentido de corrigir e ou melhorar o sistema de controlo interno implementado;
- g) Assegurar que as actividades de controlo interno têm um estatuto e visibilidade adequados e são sujeitas a revisões periódicas.

4 - O exercício das competências descritas no número anterior deve ser adequadamente documentado.

Artigo 15.º

Responsabilidades dos directores de topo

- 1 - Os directores de topo são responsáveis por, no cumprimento das estratégias e orientações estabelecidas pelo órgão de administração, desenvolver, implementar, manter e monitorizar o sistema de controlo interno e assegurar a sua eficácia e adequação.
- 2 - Os directores de topo são igualmente responsáveis pela eficácia dos controlos organizacionais e procedimentais da empresa de seguros.
- 3 - Para efeitos dos números anteriores, compete aos directores de topo:
 - a) Definir políticas concretas de controlo interno e assegurar a implementação de procedimentos eficazes e adequados, aplicáveis em toda a estrutura organizacional, em linha com as orientações definidas pelo órgão de administração e enquadrados nas actividades diárias da empresa de seguros;
 - b) Assegurar a implementação dos programas, procedimentos e controlos definidos pelo órgão de administração no âmbito do combate ao branqueamento de capitais e garantir que esses procedimentos são executados eficientemente;
 - c) Definir, implementar e rever mecanismos de monitorização para verificar, de forma regular, o cumprimento das políticas e procedimentos de controlo, avaliar a adequação e eficácia do sistema de controlo interno implementado e possibilitar a correcção de quaisquer falhas e ou fragilidades detectadas;
 - d) Definir, aprovar e rever requisitos de periodicidade e conteúdo do reporte interno relativo à eficácia e adequação do sistema de controlo interno implementado, por forma a possibilitar a avaliação do cumprimento dos objectivos definidos e a facilitar a melhoria do próprio sistema;
 - e) Implementar procedimentos de reporte, periódico e extraordinário, a todos os níveis da empresa de seguros, no sentido de ser disponibilizada informação sobre a eficácia e a adequação do sistema de controlo interno, no sentido de possibilitar a correcção de quaisquer falhas e ou fragilidades detectadas;
 - f) Manter o órgão de administração informado, através de reportes periódicos, sobre a eficácia e adequação do sistema de controlo interno, incluindo, nomeadamente, os principais procedimentos de controlo implementados e efectuando propostas no que se refere a quaisquer falhas e ou fragilidades detectadas;
 - g) Implementar as orientações e instruções dadas pelo órgão de administração no sentido de introduzir correcções e ou melhorias no sistema de controlo interno e monitorizar o seu efectivo cumprimento.
- 4 - O exercício das competências descritas no número anterior deve ser adequadamente documentado.

Artigo 16.º

Monitorização e revisão do sistema de controlo interno

- 1 - A empresa de seguros deve desenvolver, implementar e manter mecanismos apropriados para a monitorização do sistema de controlo interno, de forma a assegurar o cumprimento das políticas definidas e dos procedimentos estabelecidos e garantir a sua eficácia e adequação face à actividade da empresa.
- 2 - Os mecanismos referidos no número anterior devem permitir a obtenção de uma perspectiva abrangente da situação da empresa de seguros e proporcionar ao órgão de administração e aos directores de topo informação relevante para a tomada de decisões.
- 3 - O processo de monitorização do sistema de controlo interno deve ser efectuado numa base contínua, no decurso das operações normais, e deve ser complementado com avaliações periódicas e ou extraordinárias, eficazes e completas.
- 4 - A frequência das avaliações referidas no número anterior deve depender da avaliação dos riscos e da eficácia dos procedimentos continuados de monitorização.
- 5 - As avaliações referidas no n.º 3 devem ser executadas pela função de auditoria interna ou, no caso de a sua existência não ser exequível ou apropriada face à estrutura organizacional da empresa de seguros, o órgão de administração deve aplicar procedimentos de monitorização adicionais e ou subcontratar esta função a um revisor oficial de contas independente do que procede à certificação legal de contas e à auditoria para efeitos de supervisão

prudencial, com o objectivo de garantir a adequação do sistema de controlo interno.

6 - Os mecanismos de monitorização devem identificar falhas e ou fragilidades do sistema de controlo interno, quer na sua concepção quer na sua implementação e ou utilização.

7 - As falhas e ou fragilidades detectadas devem ser devidamente registadas, documentadas e reportadas aos níveis de gestão apropriados por forma a serem prontamente ultrapassadas.

8 - O órgão de administração e os directores de topo devem, periodicamente, receber reportes relativos à monitorização do sistema de controlo interno da empresa de seguros, incluindo a identificação das falhas e ou fragilidades detectadas, quer quando avaliadas isoladamente quer de forma agregada.

9 - No âmbito do processo de monitorização do sistema de controlo interno, e na sequência das falhas e ou fragilidades detectadas ou comunicadas à empresa de seguros por entidades terceiras, devem ser efectuadas, pelos níveis de gestão apropriados e, quando adequado, pelo órgão de administração e pelos directores de topo, as alterações consideradas necessárias.

10 - O processo de monitorização deve prever o acompanhamento das alterações introduzidas no sistema de controlo interno.

Artigo 17.º

Função de auditoria interna

1 - Para efeitos das avaliações referidas no n.º 3 do artigo anterior, e dependendo da dimensão e complexidade da actividade da empresa de seguros, pode justificar-se a existência de uma função de auditoria interna na sua estrutura organizacional.

2 - A função de auditoria interna deve ser exercida por pessoal competente, qualificado e experiente, com uma clara compreensão do seu papel e responsabilidades.

3 - A função de auditoria interna deve ter autoridade suficiente para desempenhar as suas competências objectivamente e de forma independente, não devendo, neste sentido, ter ligação directa às funções operacionais da empresa de seguros que serão objecto de avaliação.

4 - Para garantir uma adequada autoridade nos termos do número anterior, a função de auditoria interna deve ter acesso directo ao órgão de administração.

5 - Para efeitos de um adequado desempenho da função de auditoria interna, a realização de avaliações deve respeitar os seguintes princípios:

a) Devem ser realizadas no âmbito de um programa completo de auditoria desenhado para assegurar um exame abrangente da eficácia dos sistemas de gestão de riscos e de controlo interno, assim como das actividades de monitorização;

b) Para cada avaliação deve ser delineado um plano que regule os objectivos de auditoria para o período em revisão, identifique as actividades de risco a serem objecto de avaliação e os procedimentos de controlo interno que devem ser revistos e identifique os recursos necessários para a sua execução;

c) Devem ser claramente definidos os critérios para avaliar a adequação de políticas, procedimentos e controlos específicos implementados pela empresa de seguros;

d) O pessoal que executa a auditoria interna deve ter acesso pleno a todas as actividades da empresa de seguros, incluindo sucursais, pelo que lhe deve ser disponibilizada toda a informação necessária à realização de uma adequada avaliação;

e) A realização de uma acção de auditoria deve compreender a elaboração ou actualização do dossier permanente da actividade de risco alvo de avaliação;

f) As conclusões, falhas e ou fragilidades identificadas pela auditoria interna, assim como as consequentes recomendações, devem ser oportunamente registadas, documentadas e reportadas aos níveis de gestão adequados e, quando justificável, directamente ao órgão de administração, de modo a garantir que a avaliação não é enviesada e que as questões identificadas são prontamente tomadas em consideração;

g) Deve ser previsto um acompanhamento contínuo por parte da função de auditoria interna das situações identificadas, no sentido de garantir que as medidas necessárias são tomadas e que as mesmas são geridas adequadamente.

6 - Anualmente deve ser elaborado um relatório de auditoria no qual são apresentados os resultados das acções de auditoria realizadas e o estado de implementação e cumprimento das recomendações eventualmente efectuadas.

CAPÍTULO V

Formalização dos sistemas, relatório e certificação

Artigo 18.º

Formalização dos sistemas

1 - A empresa de seguros deve formalizar em documento(s) específico(s) as principais políticas, estratégias e processos de gestão de riscos e de controlo interno.

2 - O(s) documento(s) referido(s) no número anterior deve(m) identificar de forma clara e detalhada os sistemas implementados para a identificação, avaliação, mitigação, monitorização e controlo dos riscos referidos no n.º 3 do

artigo 8.º, bem como as actividades específicas de controlo implementadas no âmbito do sistema de controlo interno.
3 - A empresa de seguros deve manter o(s) documento(s) referido(s) no n.º 1 devidamente actualizado(s).

Artigo 19.º

Relatório

- 1 - O órgão de administração deve requerer e assegurar que seja elaborado um relatório anual sobre a estrutura organizacional e os sistemas de gestão de riscos e de controlo interno da empresa de seguros.
- 2 - Tomando em consideração os requisitos previstos na presente norma, o relatório a que se refere o número anterior deve contemplar, no mínimo, um resumo explicativo das principais alterações ocorridas durante o exercício ao nível dos seguintes aspectos:
 - a) Estrutura organizacional;
 - b) Sistemas de informação e canais de comunicação;
 - c) Principais procedimentos de gestão de riscos;
 - d) Principais procedimentos de controlo interno e respectivos mecanismos de monitorização;
 - e) Procedimentos específicos para o combate ao branqueamento de capitais.
- 3 - O relatório a que se refere o n.º 1 deve ainda contemplar uma descrição detalhada do acompanhamento efectuado pela função de gestão de riscos e pela função de auditoria interna no decurso do exercício a que se reporta o relatório, identificando as principais falhas e ou fragilidades detectadas e as medidas tomadas no sentido de melhorar os sistemas de gestão de riscos e de controlo interno implementados.
- 4 - O relatório a que se refere o n.º 1 deve ser remetido pelo órgão de administração ao Instituto de Seguros de Portugal conjuntamente com os elementos de reporte relativos ao final de cada exercício.

Artigo 20.º

Certificação

- 1 - A implementação e efectiva aplicação das estratégias, políticas e processos identificados no(s) documento(s) que formaliza(m) os princípios de gestão de riscos e os princípios de controlo interno elaborado(s) pela empresa de seguros devem ser objecto de apreciação por um revisor oficial de contas no âmbito dos trabalhos efectuados para a elaboração do relatório de auditoria para efeitos de supervisão prudencial das empresas de seguros.
- 2 - Nesse relatório, o revisor oficial de contas deve incluir um parecer sobre a adequação dos sistemas de gestão de riscos e de controlo interno aos objectivos da presente norma, referindo eventuais falhas e ou fragilidades detectadas e medidas tomadas no sentido de melhorar os sistemas implementados.

CAPÍTULO VI

Disposições transitórias e finais

Artigo 21.º

Requisitos e orientações

Sem prejuízo das competências específicas da empresa de seguros, o Instituto de Seguros de Portugal pode estabelecer requisitos mínimos e ou orientações de índole técnica para efeitos da implementação dos sistemas de gestão de riscos e de controlo interno, nomeadamente no que se refere às áreas e ou aos riscos que se considerem mais relevantes.

Artigo 22.º

Disposições transitórias

- 1 - As exigências previstas na alínea c) do n.º 3 do artigo 9.º e na alínea c) do n.º 2 do artigo 10.º são de aplicação facultativa.
- 2 - As empresas de seguros devem remeter ao Instituto de Seguros de Portugal, conjuntamente com os elementos de reporte relativos ao final do exercício de 2005, um plano de implementação detalhado que identifique de forma precisa e calendarizada as actividades a desenvolver durante os anos de 2006 e 2007 para efeitos da implementação dos requisitos da presente norma.
- 3 - As empresas de seguros devem remeter ao Instituto de Seguros de Portugal, conjuntamente com os elementos de reporte relativos ao final do exercício de 2006, um relatório de progresso relativo ao cumprimento do plano referido no número anterior.
- 4 - As empresas de seguros devem remeter ao Instituto de Seguros de Portugal, conjuntamente com os elementos de reporte relativos ao final do exercício de 2007, o(s) documento(s) que formaliza(m) os princípios de gestão de riscos e os princípios de controlo interno referido(s) no n.º 1 do artigo 18.º

Artigo 23.º

Produção de efeitos

Sem prejuízo do disposto no artigo anterior, as empresas de seguros devem dar cumprimento ao estabelecido na presente norma até 31 de Dezembro de 2007.

29 de Novembro de 2005. - O Conselho Directivo: Rui Leão Martinho, presidente - Rodrigo Lucena, vogal.

