BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.

AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República».**

SUMÁRIO

BANCO DE MOÇAMBIQUE

Aviso n.º 4/GBM/2013

de 18 de Setembro

As instituições de crédito, no desenvolvimento das suas actividades, assumem riscos susceptíveis de causar impactos negativos nos retornos esperados. Deste modo, a existência de uma estrutura de gestão capaz de optimizar a relação entre a maximização do retorno e a minimização dos riscos constitui um pressuposto essencial para a solidez dessas instituições.

Tendo em vista melhorar as práticas de gestão de riscos vigentes nas instituições de crédito, bem como uniformizar a respectiva terminologia, o Banco de Moçambique decidiu emitir um conjunto de directrizes, baseadas nas melhores práticas internacionalmente aceites.

A emissão destas directrizes está igualmente em consonância com a intenção do Banco de Moçambique de tornar a sua actividade de supervisão, tanto *on-site* como *off-site*, cada vez mais focalizada no risco, em resposta ao crescente número de instituições supervisionadas e à constante inovação na prestação de serviços financeiros por parte destas.

Nestes termos, o Banco de Moçambique, no uso da competência que lhe é conferida pela alínea *d*) do n.º 2 do artigo 37 da Lei n.º 1/92, de 3 de Janeiro – Lei Orgânica do Banco de Moçambique, determina:

ARTIGO 1

(Objecto)

O presente Aviso estabelece as Directrizes de Gestão de Riscos, abreviadamente designadas por DGR, em anexo ao presente Aviso e que dele são parte integrante:

a) Anexo I - Directrizes de Gestão de Riscos; e

b) Anexo II - Directrizes de Gestão de Riscos – Risco de Tecnologias de Informação.

ARTIGO 2

(Âmbito de aplicação)

O presente Aviso aplica-se a todas as instituições de crédito com sede no território moçambicano e às sucursais em Moçambique de instituições de crédito com sede no estrangeiro.

ARTIGO 3

(Prazo de remessa dos Programas de Gestão de Riscos)

1. As instituições de crédito devem remeter ao Banco de Moçambique os seus Programas de Gestão de Riscos (PGR) no prazo de trinta dias, contados da data de publicação do presente Aviso e, subsequentemente, até ao dia 31 de Março de cada ano.

2. Sempre que os PGR não estejam em conformidade com as DGR ou se mostrem desajustados à natureza e complexidade da actividade da instituição, o Banco de Moçambique fixará um prazo para o devido ajustamento.

ARTIGO 4

(Esclarecimento de dúvidas)

As dúvidas que surgirem da interpretação e aplicação do presente Aviso serão esclarecidas pelo Departamento de Supervisão Bancária do Banco de Moçambique.

ARTIGO 5

(Entrada em vigor)

O presente Aviso entra em vigor na data da sua publicação.

Banco Moçambique, em Maputo, 24 de Maio de 2013. – O Governador, *Ernesto Gouveia Gove*.

---

1. Disposições Gerais

1.1. Objectivos

1.1.1. As presentes directrizes pretendem contribuir para o estabelecimento duma linguagem uniforme entre as instituições de crédito e o supervisor em matérias de gestão de risco, o que, por seu turno, contribuirá para a harmonização das práticas de gestão de risco na indústria bancária, tendo como referência as boas práticas internacionais nesse domínio.

1.2 Categorias de Riscos

1.2.1. As presentes Directrizes de Gestão de Riscos (DGR) compreendem as nove categorias de riscos mais relevantes na actividade bancária no País, designadamente:

a) Risco de crédito;
b) Risco de liquidez;
c) Risco de taxa de juro;
d) Risco de taxa de câmbio;
e) Risco operacional;
f) Risco estratégico;
g) Risco de reputação;
h) Risco de *compliance*; e
i) Risco de Tecnologias de Informação (TI[1]).

1.3. Programas de Gestão de Risco

1.3.1. As instituições devem desenvolver um Programa de Gestão de Risco (PGR) detalhado, ajustado à dimensão e complexidade das suas actividades. Os PGR devem ser revistos, pelo menos, anualmente, e espera-se que cubram, no mínimo, os nove riscos contidos nestas directrizes.

1.4. Processo de Gestão de Riscos

1.4.1. A gestão de riscos é uma disciplina fundamental em todas as instituições e compreende as actividades que afectam o seu perfil de risco. A gestão de riscos, como comummente é entendida, não significa minimização de risco; pelo contrário, a mesma tem como objectivo, optimizar a relação risco-retorno com que as instituições se confrontam. Este objectivo pode ser alcançado institucionalizando um quadro conceptual de gestão de risco para captar e gerir, adequadamente, todos os riscos a que uma instituição se encontra exposta.

1.4.2. A gestão de riscos comporta quatro (4) processos-chave:

1.4.2.1. Identificação – para gerir adequadamente os riscos, uma instituição deve ser capaz de identificar os riscos existentes ou os que podem surgir, tanto de iniciativas de negócio já existentes como de novas iniciativas, por exemplo, riscos inerentes à actividade creditícia, que incluem os de crédito, de liquidez, de taxa de juros e operacional. A identificação de riscos deve ser um processo contínuo e deve ocorrer tanto ao nível individual como global (i.e., em cada transacção e na carteira como um todo).

1.4.2.2. Mensuração – uma vez identificados, os riscos devem ser medidos de modo a se determinar o seu impacto no resultado ou capital da instituição. Isto pode ser feito com recurso a várias técnicas, desde as mais simples aos modelos mais sofisticados. A medição tempestiva e exacta de riscos é condição essencial para que os sistemas de gestão de riscos sejam eficazes. Uma instituição que não possua um sistema de medição de riscos tem capacidade limitada para controlar ou acompanhar os níveis de risco a que está exposta. No mínimo, uma instituição deve, periodicamente, realizar testes para assegurar que os instrumentos de medição empregues são fiáveis. Um bom sistema de medição de riscos avalia tanto os riscos de transacções individuais como os da carteira global.

1.4.2.3. Controlo – depois de medir o risco, a instituição deve estabelecer e comunicar os limites de risco, através de políticas, normas e procedimentos que definam responsabilidades e linhas de autoridade. Estes limites devem servir como elementos de controlo de exposições aos vários riscos associados às actividades da instituição. As instituições podem, igualmente, empregar várias ferramentas de mitigação ao minimizar a sua exposição aos riscos. Além disso, devem possuir um processo para autorizar excepções ou alterações aos limites, quando tal se justifique.

1.4.2.4. Acompanhamento – as instituições devem estabelecer um Sistema de Informação de Gestão (SIG) eficaz para acompanhar os níveis de risco e facilitar a revisão tempestiva das posições de risco e excepções. Os relatórios de acompanhamento devem ser frequentes, tempestivos, exactos e informativos, e devem ser distribuídos às pessoas responsáveis por assegurar o empreendimento de acções, se necessário.

1.5. Quadro Conceptual de Gestão de Riscos

1.5.1. Um quadro conceptual de gestão de riscos compreende o âmbito dos riscos a serem geridos, os processos, sistemas e procedimentos para gerir tais riscos, bem assim as atribuições e responsabilidades dos indivíduos envolvidos na sua gestão. O quadro conceptual deve ser abrangente o suficiente para captar todos os riscos aos quais uma instituição se encontra exposta e ter flexibilidade para acomodar qualquer alteração nas actividades da instituição.

1.5.2. Os elementos-chaves de um quadro conceptual de gestão de riscos eficaz são:

a) Fiscalização activa pelo órgão de administração e gestão de topo;
b) Políticas, procedimentos e limites adequados;
c) Sistemas adequados de medição, acompanhamento e de informação de gestão; e
d) Controlos internos abrangentes.

1.5.3. Fiscalização pelo Órgão de Administração[2] e Gestão de Topo[3]:

1.5.3.1. Os órgãos de administração detêm, em última instância, a responsabilidade pelo nível de riscos assumidos na instituição. Consequentemente, devem aprovar as estratégias globais de negócio e as políticas, incluindo as relacionadas com a tomada e gestão de riscos e devem, igualmente, assegurar que a gestão de topo é plenamente capaz de gerir as actividades que a instituição desenvolve. Enquanto se exige que todos os órgãos de administração sejam responsáveis por compreender a natureza

[1] Matéria tratada em documento específico.

[2] É o Conselho de Administração, Conselho de Gestão, o Conselho de Direcção ou outro órgão com funções análogas, conforme o n.º 11 do artigo 2 do Aviso 8/GBM/2007.

[3] São pessoas que têm autoridade e responsabilidade pelo planeamento, direcção e controlo das actividades, directa ou indirectamente, incluindo qualquer administrador (executivo ou outro).

dos riscos a que a instituição se expõe e por assegurar que a gestão efectua as diligências necessárias para identificar, medir, controlar e acompanhar tais riscos, o nível de conhecimento técnico exigido aos membros do órgão de administração pode variar, dependendo das circunstâncias particulares da instituição.

1.5.3.2. Os membros do órgão de administração devem possuir um entendimento claro dos riscos a que a instituição está exposta e devem receber relatórios que identifiquem a dimensão e materialidade desses riscos. Adicionalmente, devem executar acções tendentes a proporcionar-lhes um entendimento adequado dos riscos através de encontros com os auditores e peritos externos à instituição. Usando este conhecimento e informação, os membros do órgão de administração devem fornecer uma orientação clara relativamente aos níveis de exposição aceitáveis para a instituição e assegurar que a gestão de topo implemente os procedimentos e controlos necessários para a observância das políticas adoptadas.

1.5.3.3. A gestão de topo é responsável pela implementação de estratégias que limitem os riscos associados a cada estratégia específica e assegurem a observância permanente das leis e regulamentos, tanto a curto como a longo prazo. De igual modo, a gestão deve estar plenamente envolvida nas actividades da instituição e possuir conhecimento suficiente de todas as linhas principais de negócios para garantir que políticas, controlos e sistemas de gestão apropriados sejam implementados e que a prestação de contas e estabelecimento de linhas de autoridade sejam delineados de forma clara. A gestão de topo é igualmente responsável pelo estabelecimento e comunicação de um forte sentido de consciência sobre a necessidade de controlos internos eficazes e elevados padrões de ética.

1.5.3.4. Para atingir estes objectivos é necessário que a gestão de topo tenha um entendimento amplo das actividades bancárias e dos mercados financeiros, assim como conhecimento detalhado das actividades que a instituição realiza, incluindo a natureza dos controlos internos necessários para limitar os riscos relacionados.

1.5.4. Políticas, Procedimentos e Limites:

1.5.4.1. Os membros do órgão de administração e a gestão de topo de uma instituição devem conceber políticas e procedimentos de gestão de riscos ajustados aos riscos que emergem das actividades que desenvolvem. Uma vez que tais riscos tenham sido adequadamente identificados, as políticas e procedimentos devem fornecer directrizes detalhadas para implementação, no dia-a-dia, das estratégias globais de negócio, e devem incluir limites concebidos para resguardar a instituição de riscos excessivos, bem assim dos não tomados com base nos melhores critérios. A gestão deve ainda assegurar a actualização das mesmas, sempre que necessário, de modo a responder às mudanças significativas nas actividades ou condições de negócio da instituição.

1.5.4.2. Para que as políticas, procedimentos e limites de uma instituição sejam adequados, os mesmos devem, no mínimo:

(i) Assegurar uma identificação, medição, controlo e acompanhamento dos riscos decorrentes de actividades da instituição;

(ii) Ser consistentes com a complexidade e a dimensão do negócio, os objectivos, as metas e a robustez financeira da instituição;

(iii) Delinear linhas de autoridade e de responsabilização (prestação de contas) claras ao nível das actividades da instituição; e

(iv) Propiciar a revisão das actividades que sejam novas na instituição, de modo a assegurar que as infra-estruturas necessárias para identificar, controlar e acompanhar os riscos associados a uma determinada actividade sejam criadas antes que a mesma inicie.

1.5.5. Mensuração, Acompanhamento e Sistemas de Informação de Gestão de Riscos:

1.5.5.1. O acompanhamento eficaz de riscos requer que as instituições identifiquem e meçam todas exposições ao risco que sejam materiais. Consequentemente, as actividades de acompanhamento de riscos devem ser assistidas por sistemas de informação que forneçam à gestão de topo e aos membros do órgão de administração relatórios tempestivos sobre a situação financeira, desempenho operacional e exposição ao risco, bem como reportes regulares e suficientemente detalhados para os gestores de linha envolvidos na gestão diária das actividades das instituições.

1.5.5.2. As instituições devem possuir sistemas de acompanhamento e gestão de risco que proporcionem aos administradores e à gestão de topo um entendimento claro das exposições ao risco.

1.5.5.3. Para assegurar a medição e acompanhamento eficaz dos riscos e dos sistemas de informação de gestão, deve ser observado o seguinte:

(*i*) As práticas e relatórios de acompanhamento de riscos da instituição devem reflectir todos os seus riscos materiais;

(*ii*) Os pressupostos-chave, fontes de dados e procedimentos empregues na medição e acompanhamento de riscos devem ser apropriados, adequadamente documentados e a sua fiabilidade verificada numa base contínua;

(*iii*) Os relatórios e outras formas de comunicação devem ser consistentes com as actividades da instituição e estruturados para acompanhar exposições e observância dos limites, metas ou objectivos estabelecidos, bem como, na medida do necessário, comparar o desempenho actual com o esperado; e

(*iv*) Os relatórios para a gestão ou administração da instituição devem ser exactos e tempestivos e possuir informação suficiente para que os decisores possam identificar qualquer tendência adversa e avaliar adequadamente o nível de risco assumido pela instituição.

1.5.6. Controlos Internos:

1.5.6.1. A estrutura de controlos internos é crucial para o funcionamento seguro e robusto de uma instituição, em geral, e para o sistema de gestão de riscos, em particular. Uma das responsabilidades mais importantes da gestão é criar e manter um sistema de controlo eficaz, incluindo o enforcement das linhas de autoridade formais e a segregação apropriada de funções tais como o trading, a custódia e o *back-office*.

1.5.6.2. Com efeito, a segregação apropriada de funções é um elemento essencial de um sistema sólido de gestão e controlo interno de riscos. A falha na implementação e manutenção de um sistema adequado de segregação de funções pode conduzir a perdas substanciais ou de outro modo comprometer a integridade financeira da instituição.

1.5.6.3. Quando estruturado de forma apropriada, o sistema de controlo interno promove operações eficazes, relatórios financeiros e prudenciais confiáveis, resguarda os activos e auxilia a observância das leis, regulamentos e políticas institucionais relevantes. Para assegurar a adequação dos procedimentos de auditoria e de controlos internos, deve ser observado o seguinte:

a) O sistema de controlo interno deve ser apropriado ao tipo e nível dos riscos suscitados pela natureza e escopo das actividades da instituição;

b) Os controlos internos devem ser testados por um auditor independente que reporte directamente ao órgão de administração da instituição ou ao Comité de Auditoria;

c) Os resultados de auditorias ou revisões, quer sejam realizadas por um auditor interno ou por outro pessoal, devem ser adequadamente documentados, devendo acontecer o mesmo com a reacção da gestão face a esses resultados.

d) A estrutura organizacional da instituição deve estabelecer linhas de autoridade e de responsabilidade claras, para acompanhar a aderência às políticas, procedimentos e limites;

e) As linhas de reporte devem assegurar a independência das áreas de controlo em relação às linhas de negócio (tais como trading, custódia, *back-office*), garantindo assim uma adequada segregação de funções ao nível da instituição;

f) As estruturas institucionais devem reflectir as práticas operacionais efectivas;

g) Os reportes financeiros, operacionais e prudenciais devem ser exactos, confiáveis e tempestivos. Nos casos aplicáveis, as excepções devem ser anotadas e prontamente investigadas;

h) Devem existir procedimentos adequados para assegurar a observância das normas e regulamentos;

i) A auditoria interna ou outras funções de revisão interna devem assegurar a independência e objectividade;

j) Os controlos internos e sistemas de informação devem ser testados e revistos adequadamente; a abrangência, procedimentos, constatações e respostas aos resultados das auditorias e testes de revisão devem ser documentados adequadamente; as fraquezas materiais identificadas devem ter atenção apropriada e atempada ao mais alto nível. Do mesmo modo, as acções da gestão para lidar com as fraquezas materiais devem ser objectivamente revistas; e

k) O Comité de Auditoria ou o órgão de administração da instituição deve rever a eficácia das auditorias internas (e de outras actividades de revisão dos controlos internos) numa base regular.

1.5.7. Função de Gestão de Riscos:

1.5.7.1. As instituições devem estabelecer uma área funcional responsável pela fiscalização da gestão dos riscos intrínsecos nas suas operações. Tal unidade pode ter a natureza de comité, departamento ou gestor de risco, dependendo da dimensão e complexidade da instituição. O pessoal afecto à função de gestão integral de riscos deve ser independente daquele que toma ou aceita riscos em nome da instituição.

1.5.7.2. A função de gestão de riscos é responsável por assegurar a existência de processos eficazes para:

a) Identificar os riscos presentes e futuros;

b) Desenvolver sistemas de medição e avaliação de riscos;

c) Estabelecer políticas, procedimentos, práticas e outros mecanismos para a gestão de riscos;

d) Desenvolver limites de tolerância ao risco para aprovação pelo órgão de administração;

e) Acompanhar as posições tomadas, tendo como base os limites de tolerância aprovados; e

f) Reportar os resultados da monitorização de riscos ao órgão de administração e gestão de topo.

1.5.7.3. Contudo, a gestão de riscos não é restrita aos indivíduos afectos à função de gestão integral de riscos. As áreas de negócio são igualmente responsáveis pelos riscos que assumem e qualquer ausência de responsabilidade pode causar problemas. O pessoal dessas áreas, mais do que qualquer outro, deve entender os riscos do negócio.

1.5.8. Revisão Independente:

1.5.8.1. As instituições devem ter revisores independentes para avaliar a eficácia e aderência às políticas e procedimentos de gestão de risco. Os revisores podem ser auditores internos, auditores externos ou quaisquer outras entidades independentes das áreas de tomada de riscos e devem reportar directamente ao órgão de administração ou comité por este designado.

1.5.8.2. Para serem eficazes, os revisores independentes devem ter autoridade suficiente, proficiência e estatuto corporativo adequado para identificar e reportar constatações sem quaisquer impedimentos.

1.5.8.3. O revisor independente deve, entre outros aspectos, avaliar se:

a) O sistema de gestão de risco é apropriado para a natureza, escopo e complexidade da instituição e de suas actividades;

b) O órgão de administração e a gestão de topo estão activamente envolvidos no processo de gestão de riscos;

c) As políticas, procedimentos e controlos de gestão de riscos são adequadamente documentados e rigorosamente observados;

d) Os pressupostos do sistema de medição de riscos são válidos e devidamente documentados;

e) A agregação e o processamento de dados são exactos, apropriados e fiáveis; e

f) A instituição possui pessoal adequado para levar a cabo um processo de gestão de riscos sólido.

1.5.9. Integração da Gestão de Riscos:

1.5.9.1. Os riscos devem ser considerados e avaliados de forma integrada, porque uma transacção tem subjacentes vários riscos e porque um tipo de risco pode desencadear outros. Uma vez que a interacção dos vários riscos pode resultar na diminuição ou aumento do perfil de risco, o processo de gestão de risco deve reconhecer e reflectir, na medida apropriada, as interacções dos riscos em todas as actividades.

1.5.9.2. Ao avaliar e gerir os riscos, a gestão deve ter uma visão global dos riscos a que a instituição se encontra exposta. Isto requer a existência ou estabelecimento de uma estrutura que permita captar as inter-relações existentes entre os diferentes tipos de riscos em toda a instituição.

1.5.10. Plano de Contingência:

1.5.10.1. As instituições devem possuir mecanismos para identificar, antecipadamente, situações de esforço (*stress*) relativamente a todos os tipos de riscos e planos de contingência[4] para lidar com essas situações de forma tempestiva e efectiva. Estes planos devem ser revistos regularmente, para assegurar que abarcam eventos razoavelmente prováveis que possam produzir impactos adversos na instituição.

1.5.10.2. Os planos devem ser testados quanto à plausibilidade das respostas, escalonamento e canais de comunicação e o seu impacto sobre outras áreas da instituição.

2. Directrizes de Gestão do Risco de Crédito

2.1. Introdução

2.1.1. O risco de crédito é a possibilidade de ocorrência de impactos negativos nos resultados ou no capital, devido à incapacidade de uma contraparte cumprir os seus compromissos

[4] As actividades de planeamento de contingência incluem, por exemplo, o planeamento da recuperação de desastres, o controlo de danos nas relações públicas, a estratégia de litigação, respostas às recomendações do regulador, a crise de liquidez, etc.

financeiros perante a instituição, incluindo possíveis restrições à transferência de pagamentos do exterior. O risco de crédito existe, principalmente, nas exposições em crédito (incluindo o titulado), linhas de crédito, garantias e derivados. Este risco emerge da relação da instituição com particulares, empresas, instituições financeiras e soberanos.

2.1.2. O risco de crédito não ocorre necessariamente de forma isolada. A mesma fonte que origina o risco de crédito pode, igualmente, expor a instituição a outro tipo de riscos. Com efeito, uma carteira de má qualidade pode despoletar problemas de liquidez.

2.1.3. As fontes mais comuns de problemas na carteira de crédito são:

a) **Concentrações de crédito —** são vistas como qualquer exposição em que as perdas potenciais são superiores ao capital, activos totais ou quaisquer outras medidas adequadas. As concentrações podem tomar a forma de (*i*) empréstimos a um único indivíduo ou a uma contraparte, a um grupo de contrapartes correlacionadas e a sectores ou indústrias tais como comércio, agricultura, etc., ou (*ii*) factores comuns ou correlacionados; e

b) **Questões relativas ao processo de crédito —** Muitos problemas com o crédito revelam deficiências básicas nos processos de concessão e acompanhamento. Embora as lacunas nos termos de adesão (contratação) e gestão de facilidades creditícias representem importantes fontes de perdas nas instituições, muitos problemas com o crédito podem ser evitados ou mitigados por um forte processo interno de gestão.

2.2. Fiscalização pelo Órgão de Administração e Gestão de Topo

2.2.1. Fiscalização pelo Órgão de Administração

2.2.1.1. O órgão de administração tem um papel crucial na fiscalização dos processos de concessão de créditos e de gestão de risco de crédito.

2.2.1.2. Compete especialmente ao órgão de administração:

a) Aprovar a estratégia e as políticas relativas ao risco de crédito e à gestão do mesmo, devendo estas estar em consonância com a estratégia global de negócio da instituição. A estratégia global e as políticas devem ser revistas, pelo menos, uma vez por ano;

b) Estabelecer níveis de tolerância da instituição em relação ao risco de crédito;

c) Assegurar que a exposição significativa da instituição ao risco de crédito seja mantida a níveis prudenciais e consistentes com o capital disponível;

d) Estabelecer níveis de competência para concessão de crédito e delegar explicitamente na gestão de topo e no comité de crédito a autoridade para aplicar sanções, sempre que apropriado;

e) Assegurar que a gestão de topo e os indivíduos responsáveis pela gestão de risco de crédito, possuem conhecimento e proficiência razoáveis para materializar as atribuições da função de gestão de risco;

f) Assegurar que a instituição implementa princípios fundamentais sólidos que facilitem a identificação, medição, acompanhamento e controlo do risco de crédito;

g) Assegurar uma adequada implementação das políticas e procedimentos aprovados;

h) Assegurar que a auditoria interna verifica as operações de crédito para avaliar se as políticas e procedimentos da instituição são adequados e respeitados;

i) Rever exposições aos colaboradores e partes correlacionadas, incluindo as políticas a eles relacionadas;

j) Ratificar as exposições que excedam o nível de autoridade delegado na gestão e estar alerta às exposições que, embora dignas de serem consideradas, não estejam no âmbito das políticas de crédito existentes na instituição;

k) Rever as tendências na qualidade da carteira de crédito da instituição e a adequação das respectivas provisões para perdas;

l) Definir o conteúdo e a frequência dos relatórios de gestão a submeter ao órgão de administração sobre a gestão do risco de crédito; e

m) Assegurar a comunicação efectiva da estratégia e das políticas de risco de crédito na instituição. Todo o pessoal relevante deve entender de forma clara a abordagem institucional de concessão e gestão de crédito e deve ser responsabilizável pelo cumprimento das políticas e procedimentos estabelecidos.

2.2.2. Fiscalização pela Gestão de Topo

2.2.2.1. A gestão das instituições é responsável pela implementação das estratégias e políticas de gestão do risco de crédito assim como por garantir que sejam aplicados procedimentos consentâneos com essas estratégias e políticas, com a finalidade de gerir e controlar o risco de crédito e a qualidade da carteira de crédito.

2.2.2.2. Compete, especialmente, à gestão de topo:

a) Desenvolver políticas e procedimentos de gestão de crédito para aprovação pelo órgão de administração, como parte do quadro global de gestão do risco de crédito;

b) Implementar políticas de gestão do risco de crédito;

c) Assegurar a elaboração e implementação de um sistema de reporte adequado quanto ao conteúdo, formato e frequência das informações relativas à carteira de crédito e ao nível de risco de crédito, a fim de permitir uma análise eficaz e uma gestão saudável e prudente, bem como o controlo das exposições ao risco de crédito, efectivas e potenciais;

d) Acompanhar e controlar a natureza e composição da carteira da instituição;

e) Acompanhar a qualidade da carteira de crédito e assegurar que a mesma é avaliada de maneira sólida e conservadora, as exposições incobráveis são saneadas/ /abatidas e as perdas prováveis são adequadamente provisionadas;

f) Estabelecer controlos internos, incluindo institucionalização de linhas de responsabilidade e autoridade claras para assegurar um processo eficaz de gestão do risco de crédito; e

g) Desenvolver linhas de comunicação a fim de assegurar a divulgação atempada das políticas, procedimentos e outras informações de gestão do risco de crédito a todos os indivíduos envolvidos no processo.

2.3. Estratégia, Políticas, Procedimentos e Limites

2.3.1. Estratégia de Crédito

2.3.1.1. O principal objectivo da estratégia de crédito de uma instituição é determinar a sua apetência ao risco. Uma vez determinado, a instituição pode desenvolver um plano para

optimizar o retorno, mantendo o risco de crédito dentro de limites predeterminados. Assim, a estratégia de risco de crédito de uma instituição deve enunciar:

a) O plano da instituição para conceder crédito com base em vários segmentos de clientes e produtos, sectores económicos, localização geográfica, moedas e maturidades;

b) O mercado-alvo no âmbito de cada segmento de empréstimos e o nível de diversificação/concentração; e

c) A estratégia de fixação de preços.

2.3.1.2. É essencial que, ao elaborarem a estratégia do risco de crédito, as instituições dêem a devida atenção ao seu mercado-alvo. Os procedimentos de concessão de crédito devem ter como objectivo a obtenção de um conhecimento profundo dos clientes, suas credenciais e negócios.

2.3.1.3. A estratégia deve fornecer uma base de continuidade na sua abordagem e ter em conta aspectos cíclicos da economia do País e as consequentes mudanças na composição e qualidade da carteira de crédito global daí resultantes. Embora a estratégia possa ser revista periodicamente e alterada quando se mostrar necessário, a mesma deve ser viável a longo prazo e em diversos ciclos económicos.

2.3.2. Políticas

2.3.2.1. As políticas de crédito estabelecem um enquadramento para a tomada de decisões de investimento e de concessão de empréstimos e reflectem a tolerância ao risco de crédito por parte da instituição.

2.3.2.2. Para serem eficazes, as políticas devem ser comunicadas de forma tempestiva, implementadas a todos os níveis da instituição por meio de procedimentos adequados e periodicamente revistas para terem em conta as mudanças das circunstâncias internas e externas. Qualquer desvio significativo ou excepção às políticas deve ser comunicado ao órgão de administração e objecto de medidas correctivas.

2.3.2.3. As políticas de crédito devem, no mínimo, incluir:

a) Áreas gerais de crédito nas quais a instituição está preparada para penetrar ou está impedida de participar, tais como o tipo de facilidades de crédito, o tipo de garantias, os tipos de mutuários, áreas geográficas ou sectores económicos em que a instituição se pode focalizar;

b) Processo detalhado e formalizado de avaliação ou revisão, gestão e documentação de créditos;

c) Autoridade de aprovação de crédito em diferentes níveis hierárquicos, incluindo excepções como concessão de crédito além dos limites prescritos;

d) Limites de concentração individual e a grupos de contrapartes correlacionadas, indústrias ou sectores económicos específicos, áreas geográficas e produtos específicos. As instituições devem assegurar que os seus limites internos de exposição ao risco respeitam quaisquer restrições ou limites prudenciais estabelecidos pelo Banco de Moçambique;

e) Autoridade para aprovar a constituição de reservas ou provisões para perdas prováveis e saneamentos;

f) Fixação de preços para os créditos;

g) Papel e responsabilidades da área/pessoal envolvido na concessão e administração de crédito;

h) Directrizes de gestão de empréstimos problemáticos; e

i) Orientação explícita para sistemas internos de notação (rating), incluindo a definição de cada categoria de risco, critérios a serem observados ao atribuir a notação, bem como as circunstâncias em que os desvios aos critérios podem ter lugar.

2.3.3. Procedimentos

2.3.3.1. Originação de Crédito:

2.3.3.1.1. O estabelecimento de critérios de concessão de crédito robustos e bem definidos é essencial para a aprovação de créditos de forma segura e saudável. Os critérios devem estabelecer quem é elegível e para que montantes, os tipos de crédito disponíveis e os termos e condições em que o mesmo deve ser concedido.

2.3.3.1.2. As instituições devem obter informações suficientes para permitir uma avaliação exaustiva do perfil de risco real do mutuário ou contraparte. No mínimo, os factores a serem considerados e documentados na aprovação de créditos são:

a) A finalidade do crédito, bem como a fonte de reembolso;

b) A idoneidade e a reputação do mutuário ou contraparte;

c) O perfil de risco actual (incluindo a natureza e os montantes globais de riscos) do mutuário ou contraparte e sua sensibilidade aos desenvolvimentos económicos e de mercado;

d) O histórico e a capacidade actual de reembolso do mutuário, com base em tendências financeiras históricas e projecções dos fluxos de caixa;

e) Uma análise da capacidade de reembolso, orientada para o futuro, com base em vários cenários;

f) A capacidade jurídica do mutuário ou contraparte de assumir a responsabilidade;

g) Para os créditos comerciais, a perícia de realização de negócios e o estado do sector económico do mutuário e sua posição dentro desse sector;

h) Os termos e condições de crédito propostos, incluindo as cláusulas que visam limitar futuras mudanças no perfil de risco do mutuário; e

i) Se for caso disso, a adequação e exigibilidade das garantias ou colaterais.

2.3.3.1.3. Esta informação pode igualmente servir de base para a classificação de crédito, no âmbito do sistema de notação interno da instituição.

2.3.3.1.4. As instituições têm de conhecer o mutuário a quem pretendem conceder o crédito. Antes de entrar em qualquer relação de crédito, a instituição deve familiarizar-se com o mutuário ou contraparte e estar confiante de que o mesmo goza de boa reputação e credibilidade. Em particular, devem ser postas em prática políticas rigorosas para evitar envolvimento com indivíduos ligados a actividades fraudulentas e outros crimes. Isto pode ser materializado através de várias formas, incluindo a solicitação de referências de partes conhecidas, acesso às centrais de registo de crédito, familiarização com pessoas responsáveis pela gestão da empresa e verificação de referências pessoais e condição financeira. No entanto, as instituições não devem conceder crédito apenas porque o mutuário ou contraparte é conhecido ou é tido como sendo altamente reputado.

2.3.3.1.5. As instituições devem dispor de procedimentos para identificar situações em que, na análise de créditos, é adequado classificar um grupo de mutuários como partes correlacionadas e, desse modo, como um único mutuário. Isto inclui agregar exposições a grupos de contas com interdependência financeira, corporativas ou não-corporativas, sob a mesma propriedade ou controlo ou com fortes ligações (como uma gestão comum, laços familiares, entre outros).

2.3.3.1.6. Nos empréstimos sindicados, os participantes devem efectuar a sua própria análise do risco de crédito e revisão dos termos do sindicato, antes da adesão. Cada instituição deve analisar o risco e retorno dos empréstimos sindicados, do mesmo modo que outros empréstimos.

2.3.3.1.7. A fixação do preço dos créditos deve ser de tal forma a cobrir todos os custos embutidos e compensar a instituição pelos riscos incorridos. Ao avaliar o crédito e os termos em que este será concedido, as instituições devem avaliar a relação risco-retorno esperado, levando em conta, tanto quanto possível, as condições financeiras e não-financeiras (por exemplo, garantia, cláusulas restritivas, etc.). Na avaliação de risco, as instituições devem também avaliar cenários adversos prováveis e seus possíveis impactos nos mutuários ou contrapartes.

2.3.3.1.8. Ao considerar eventuais créditos, as instituições devem reconhecer a necessidade da criação de provisões para perdas esperadas e manter um nível de capital suficiente para absorver os riscos e perdas inesperadas. A instituição deve sempre ter presente estas considerações nas decisões de concessão de crédito, bem como no acompanhamento da carteira total.

2.3.3.1.9. As instituições podem utilizar mitigantes de risco de crédito tais como garantias, colaterais, derivados de crédito ou outros elementos para atenuar os riscos inerentes aos créditos individualmente. No entanto, as transacções de crédito devem ser assumidas em primeiro lugar sobre a robustez da capacidade de reembolso do mutuário. Os mitigantes do risco de crédito não devem ser substituto para uma avaliação abrangente do mutuário ou contraparte, nem podem compensar a falta de informação. Deve ser reconhecido que qualquer medida de execução do contrato de crédito tipicamente elimina a margem de lucro sobre a operação. Além disso, as instituições têm de estar conscientes de que o valor da garantia pode ser prejudicado pelos mesmos factores que levaram à diminuição das possibilidades de recuperação do crédito.

2.3.3.1.10. As instituições devem ter políticas que abranjam critérios para aceitação de diversas formas de garantia e procedimentos para avaliação contínua de tais garantias e da sua exequibilidade. Adicionalmente, as instituições devem avaliar o nível de cobertura em relação à qualidade de crédito e capacidade jurídica do fiador. No processo de decisão de crédito, as instituições devem considerar somente garantias explícitas e não aquelas que possam ser consideradas implícitas, como o apoio antecipado do Governo.

2.3.3.2. Aprovação de Novos Créditos e Prorrogação de Créditos Existentes:

2.3.3.2.1. Para manter uma carteira de crédito saudável, a instituição deve ter um processo formal de avaliação e aprovação de crédito. As aprovações devem ser feitas de acordo com as políticas e procedimentos da instituição. Os documentos e os registos devem estar organizados de tal forma que facilitem a auditoria verificar em que medida os procedimentos de aprovação foram cumpridos e identificar todos os intervenientes do processo de crédito, desde o(s) indivíduo(s) e/ou comité(s) que forneceram os dados de entrada aos que fizeram parte da tomada de decisão.

2.3.3.2.2. Cada proposta de crédito deve ser objecto de análise cuidadosa por um analista de crédito com experiência compatível com a dimensão e complexidade da operação. Um processo eficaz de avaliação observa os requisitos mínimos de informação nos quais se deve basear a análise.

2.3.3.2.3. As políticas de crédito devem estabelecer requisitos para aprovação de novos créditos, renovação de créditos existentes e/ou alteração dos termos e condições dos créditos anteriormente aprovados. As informações recebidas servem de base para qualquer avaliação interna atribuída ao crédito e a sua exactidão e adequação são cruciais para a decisão de concessão do crédito.

2.3.3.2.4. O processo de aprovação de concessão de crédito de uma instituição deve imputar responsabilidade pelas decisões tomadas e designar pessoal com autoridade para aprovar créditos ou alterar as condições dos mesmos.

2.3.3.2.5. A concessão de crédito a entidades relacionadas, quer sejam empresas ou indivíduos, constitui uma área com potencial para abuso. As instituições que concedem crédito a essas entidades devem fazê-lo em condições de plena concorrência e acompanhar o montante do crédito concedido. Os controlos devem ser implementados exigindo que os termos e condições desses créditos não sejam mais favoráveis que os aplicáveis aos outros mutuários em circunstâncias semelhantes e impondo limites rigorosos a tais créditos.

2.3.3.2.6. Transacções com partes relacionadas devem ser submetidas à aprovação do órgão de administração. Qualquer membro do órgão de administração que vier a beneficiar desse tipo de transacção não deve fazer parte do processo de aprovação.

2.3.4. Fixação de limites

2.3.4.1. Um dos elementos importantes na gestão do risco de crédito é estabelecer limites de exposição a um único mutuário e grupo de mutuários, abrangendo elementos quer do activo patrimonial, quer extrapatrimonial.

2.3.4.2. Ao desenvolverem os seus próprios limites, as instituições devem ter presente os limites definidos pelo Banco de Moçambique.

2.3.4.3. A fixação dos limites deve basear-se na robustez creditícia da contraparte, na legitimidade do pedido de crédito, nas condições económicas e na tolerância ao risco da instituição. Os limites também devem ser definidos para os respectivos produtos, indústria específica ou sectores económicos e regiões geográficas, a fim de evitar o risco de concentração.

2.3.4.4. Os limites de crédito devem ser revistos regularmente, pelo menos uma vez por ano, ou com maior frequência, se a qualidade de crédito da contraparte deteriorar. Todos os pedidos de aumento de limites de crédito deverão ser fundamentados.

2.4. Mensuração, Acompanhamento e Sistemas de Informação de Gestão de Riscos

2.4.1. Mensuração e Acompanhamento

2.4.1.1. As instituições devem dispor de metodologias que lhes permitam quantificar o risco envolvido em exposições individuais a mutuários ou contrapartes. As instituições devem também ser capazes de analisar o risco de crédito ao nível do produto e da carteira total, a fim de identificar eventuais sensibilidades ou concentrações.

2.4.1.2. O processo de medição do risco de crédito deve ter em conta (*i*) a natureza específica do crédito (empréstimos, derivativos, etc.) e condições contratuais e financeiras (maturidade, taxa de juros, etc.); (*ii*) o comportamento do perfil da exposição face aos potenciais movimentos do mercado; (*iii*) a existência de colateral[5] ou garantias[6]; e (*iv*) o potencial de incumprimento baseado na notação interna de risco.

2.4.1.3. As instituições devem utilizar técnicas de medição que sejam adequadas à complexidade e níveis de riscos envolvidos em suas actividades.

2.4.1.4. A análise de dados sobre o risco de crédito deve ser realizada com frequência adequada e os resultados revistos e comparados com os limites pertinentes, devendo tal análise ser efectuada com base em dados robustos e sujeita a validação periódica.

---

[5] Colateral – garante o cumprimento de determinada obrigação através do valor ou do rendimento de certos bens do devedor (consignação de rendimentos, penhor, hipoteca, privilégios creditórios e direito de retenção).

[6] Garantia – garante o cumprimento de determinada obrigação através de outros patrimónios, que não os do devedor (fiança e aval).

2.4.1.5. A gestão das instituições deve efectuar regularmente testes de esforço (*stress test*) das principais concentrações de riscos de crédito e analisar os resultados dos mesmos, para identificar e responder a potenciais mudanças nas condições de mercado (ciclos económicos, taxas de juro, condições de liquidez) que poderão ter impacto negativo no seu desempenho.

2.4.1.6. Administração do Crédito:

2.4.1.6.1. A administração de crédito é um elemento crítico na manutenção da segurança e solidez de uma instituição. Uma vez concedido o crédito, é da responsabilidade da função de negócios, por vezes em conjugação com uma equipa de apoio de administração de crédito, garantir que o crédito é adequadamente gerido. Isto inclui manter o arquivo de crédito actualizado, obter informações financeiras actuais, enviar notificações de renovação e preparar vários documentos, tais como contratos de empréstimos.

2.4.1.6.2. Na administração de crédito, as instituições devem garantir:

a) A eficiência e eficácia da administração de operações de crédito, incluindo o controlo de documentação, requisitos contratuais, garantias, entre outros;
b) A exactidão e tempestividade da informação prestada aos sistemas de informação de gestão;
c) A adequação dos controlos sobre todos os procedimentos de *back-office*; e
d) O cumprimento/observância das políticas e procedimentos prescritos, bem como leis e regulamentos aplicáveis.

2.4.1.6.3. Para que as diferentes componentes da administração de crédito funcionem adequadamente, a gestão de topo deve compreender e demonstrar que reconhece a importância deste elemento de acompanhamento e controlo de risco de crédito.

2.4.1.6.4. Os processos de crédito devem incluir toda a informação necessária para se avaliar a actual situação financeira do mutuário ou contraparte, bem como para rastrear as decisões tomadas e o historial do crédito, nomeadamente:

a) Pedido de crédito;
b) Evidência de aprovação;
c) Informações financeiras actualizadas;
d) Registos e datas de todas as revisões de créditos;
e) Registos de todas as garantias oferecidas (devidamente avaliadas e formalizadas);
f) Contrato de crédito; e
g) Notação interna de risco.

2.4.1.6.5. As instituições devem desenvolver e implementar procedimentos e sistemas de informação abrangentes para acompanhar a condição da sua carteira de crédito, por operações individuais e por mutuários. Estes procedimentos devem definir critérios de identificação e reporte de créditos potencialmente problemáticos e de outras transacções para assegurar que os mesmos estejam sujeitos a um acompanhamento mais frequente, assim como a possíveis acções correctivas, classificação e/ou provisionamento.

2.4.1.6.6. Um sistema eficaz de acompanhamento de crédito deve incluir medidas para:

a) Assegurar que a instituição compreende a actual situação financeira do mutuário ou contraparte;
b) Assegurar que todos os créditos estão em conformidade com as cláusulas existentes;
c) Acompanhar a utilização pelo cliente das linhas de crédito aprovadas;
d) Assegurar que os fluxos de caixa projectados, relativos a grandes créditos, satisfazem requisitos do serviço da dívida;
e) Garantir, se for caso disso, que os colaterais ou garantias proporcionam uma cobertura adequada em relação à situação actual do devedor; e
f) Identificar e classificar potenciais créditos problemáticos em tempo útil.

2.4.1.6.7. As instituições devem possuir um sistema que permita o acompanhamento da qualidade da carteira de crédito numa base diária e a tomada de medidas correctivas sempre que ocorrer qualquer indício de deterioração. Tal sistema deve permitir que a instituição verifique (*i*) em que medida os empréstimos estão a ser reembolsados de acordo com os termos contratuais, (*ii*) a adequação das provisões, (*iii*) se o perfil global de risco está dentro dos limites estabelecidos pela gestão e (*iv*) o cumprimento dos limites regulamentares.

2.4.1.6.8. O estabelecimento dum sistema de monitorização efectivo auxilia a gestão sénior no acompanhamento da qualidade global da carteira total e da sua tendência. Consequentemente, a gestão pode ajustar ou reavaliar a sua estratégia e política de crédito de conformidade antes que enfrente grandes contrariedades. A política de crédito da instituição deve conter, de forma explícita, orientações relativas ao acompanhamento do risco de crédito e estabelecer, no mínimo:

a) Atribuições e responsabilidades das pessoas encarregues pelo acompanhamento do risco de crédito;
b) Necessidade de avaliação e técnicas de análise (para empréstimos individuais e carteira global);
c) Frequência de acompanhamento;
d) Reavaliação periódica das garantias e dos colaterais;
e) Frequência de visitas ao cliente; e
f) Identificação de qualquer deterioração em qualquer empréstimo.

2.4.1.7. Notação Interna de Riscos e Provisionamento:

2.4.1.7.1. Uma ferramenta importante para o acompanhamento da qualidade dos créditos individuais, assim como para a carteira global, é a utilização de um sistema de notação interna de risco.

2.4.1.7.2. Um sistema de notação interna de risco bem estruturado permite diferenciar o grau de risco de crédito nas diferentes exposições de uma instituição, bem como determinar, de forma mais exacta, as características gerais da carteira de crédito, a concentração e os créditos problemáticos, e adequar as provisões para perdas. Na determinação de provisões para perdas, as instituições devem assegurar-se de que os requisitos mínimos estabelecidos pelo Banco de Moçambique são observados.

2.4.1.7.3. Em regra, um sistema de notação interna de risco agrega os créditos em várias classes de risco, definidas tanto internamente como externamente por entidades de supervisão e outras. Sistemas mais simples podem abarcar diversas categorias, variando de satisfatório a insatisfatório; porém, sistemas mais complexos têm ainda gradações de créditos dentro de cada categoria, de modo a diferenciar realmente o risco relativo de crédito que elas representam.

2.4.1.7.4. Ao desenvolver os seus sistemas, as instituições devem decidir se atribuem uma notação de riscos ao mutuário ou contraparte, aos riscos associados a uma operação específica, ou a ambos.

2.4.1.7.5. Notações internas de risco são um importante instrumento de fiscalização e de controlo de risco de crédito. Para facilitar a identificação atempada, o sistema de notação interna de risco da instituição deve responder de modo flexível aos indicadores de deterioração real ou potencial do risco de crédito (por exemplo, posição financeira e situação do negócio do mutuário, comportamento das contas do mutuário, cumprimento dos termos contratuais, valor das garantias, etc.).

2.4.1.7.6. Créditos com notações em deterioração devem ser objecto de uma supervisão e acompanhamento redobrados (por exemplo, através de visitas mais frequentes de oficiais de crédito e inclusão numa lista que deve ser regularmente revista pela direcção).

2.4.1.7.7. As notações internas de risco podem ser utilizadas pelos gestores de linha em diversos departamentos para rastrear as características actuais da carteira de crédito e ajudar a determinar as mudanças necessárias à estratégia de crédito da instituição. Consequentemente, o órgão de administração e a gestão de topo também devem receber relatórios periódicos sobre o estado da carteira de crédito com base em tais notações.

2.4.1.7.8. As classificações atribuídas a cada um dos mutuários ou contrapartes no momento em que o crédito é concedido devem ser revistas periodicamente e reclassificadas.

2.4.1.7.9. Para assegurar que as notações internas sejam consistentes e reflictam adequadamente a qualidade de crédito numa base individualizada, a responsabilidade de fixar ou confirmar tais notações deve ser atribuída a uma função de revisão de crédito, independente da que o originou. A consistência e o rigor das notações devem ser examinados periodicamente por uma área funcional, nomeadamente um grupo independente de revisão de crédito.

2.4.1.8. Gestão de Créditos Problemáticos:

2.4.1.8.1. As instituições devem estabelecer um sistema que lhes permita identificar créditos potencialmente problemáticos, enquanto existirem opções para os remediar. Os créditos problemáticos devem ser geridos no âmbito de um processo correctivo específico.

2.4.1.8.2. A responsabilidade pela gestão dos créditos problemáticos pode ser atribuída à unidade de negócio que os originou, a uma secção especializada de recuperação, ou à combinação das duas, dependendo da dimensão e natureza do crédito, bem como das causas dos problemas. Quando os créditos problemáticos em uma instituição forem significativos, deve-se separar a função de originação do crédito da função de recuperação. Os recursos adicionais, perícia e foco mais concentrado de uma secção especializada de recuperação geralmente melhoram os resultados da cobrança.

2.4.1.8.3. O processo de gestão de créditos problemáticos deve englobar os seguintes elementos básicos:

a) **Negociação e Acompanhamento –** Ao lidar com mutuários no sentido de implementar os planos de recuperação, as instituições devem empreender esforços proactivos, mantendo contacto frequente e registos internos de acções de acompanhamento. Esforços rigorosos feitos na fase inicial, muitas vezes previnem litígios e perdas em empréstimos;

b) **Elaboração de Estratégias Correctivas –** Medidas correctivas adequadas, tais como reestruturação do empréstimo, aumento do limite de crédito ou redução das taxas de juro, permitem, por vezes, melhorar a capacidade de reembolso do mutuário. Entretanto, este efeito depende da condição do negócio do mutuário, da natureza dos problemas enfrentados e, mais importante ainda, do compromisso e do empenho do mutuário em liquidar o empréstimo. Embora as medidas correctivas produzam, por vezes, resultados positivos, as instituições devem ser bastante prudentes na sua adopção e assegurar que as mesmas não incentivem os devedores a entrarem em incumprimento intencionalmente. o órgão competente deve aprovar os planos de acção antes de sua implementação;

c) **Revisão dos Documentos de Garantia e de Títulos –** As instituições devem verificar a quantia recuperável do empréstimo actualizando os valores das garantias à disposição através de uma avaliação formal. Os documentos de garantia devem igualmente ser revistos para assegurar a autenticidade e exequibilidade dos mesmos e respectivos contratos;

d) **Relatório de Acompanhamento e Revisão –** Os créditos problemáticos devem ser objecto de revisão e acompanhamento mais frequente. A revisão deve permitir a actualização do estado e evolução dos créditos, bem como o progresso do plano de recuperação. Os progressos alcançados devem ser comunicados ao órgão de administração.

2.4.2. Sistemas de Informação de Gestão

2.4.2.1. A eficácia do processo de medição do risco de crédito de uma instituição depende em grande medida da qualidade dos sistemas de informação de gestão. As informações geradas a partir desses sistemas permitem ao órgão de administração e a todos os níveis de gestão o cumprimento das respectivas funções de fiscalização, incluindo a determinação do nível adequado de capital que a instituição deve manter. Portanto, a qualidade, o detalhe, a actualidade e tempestividade da informação são elementos cruciais. Em particular, a informação sobre a composição e qualidade das várias carteiras, incluindo em base consolidada, deve permitir à gestão avaliar, rapidamente e com exactidão, o nível de risco de crédito a que a instituição se encontra exposta e determinar se o desempenho da instituição está ou não a atingir os objectivos da sua estratégia de risco de crédito.

2.4.2.2. As instituições devem ter sistemas de informação de gestão que permitam à gestão identificar eventuais concentrações de risco na carteira de crédito e exposições próximas dos limites estabelecidos. A adequação do âmbito da informação deve ser objecto de revisão periódica pelos gestores de linha, gestão sénior e órgão de administração para assegurar que o mesmo esteja em consonância com a complexidade do negócio.

2.4.2.3. O sistema de informação deve ser capaz de agregar o crédito concedido a mutuários individuais e a grupos económicos e permitir o reporte de excepções aos limites de risco de crédito numa base tempestiva e realística.

2.5. Controlos Internos

2.5.1. Revisão do Risco

2.5.1.1. As instituições devem estabelecer um mecanismo de avaliação contínua e independente do processo de gestão do risco de crédito. O objectivo dessa revisão é avaliar o processo de administração de crédito, a precisão das notações, incluindo a adequação das provisões para perdas e a qualidade da carteira total de crédito.

2.5.1.2. Todos os créditos devem ser sujeitos à revisão de risco, pelo menos, trimestralmente. Revisões mais frequentes devem ser realizadas para novos créditos, em que as instituições podem não estar familiarizadas com o mutuário, e para os créditos com notações desfavoráveis e com maior probabilidade de incumprimento.

2.5.1.3. Os resultados dessa revisão devem ser devidamente documentados e comunicados directamente ao órgão de administração ou a um comité por este designado.

2.5.1.4. As instituições devem efectuar revisões do crédito com informações actualizadas sobre as condições financeiras e empresariais do mutuário, bem como a evolução da conta. As excepções observadas no processo de acompanhamento de crédito devem ser igualmente avaliadas, para se aferir o impacto sobre a solvabilidade do devedor.

2.5.1.5. A avaliação de crédito deve ser realizada em base consolidada ao nível do grupo, para aferir sobre as conexões entre entidades do grupo em que o mutuário se insere.

3. Directrizes de Gestão do Risco de Liquidez

3.1. Introdução

3.1.1. O risco de liquidez é a possibilidade de uma instituição enfrentar dificuldades em honrar as suas obrigações (sobretudo, as de curto prazo) à medida que vencem ou em assegurar o refinanciamento dos activos detidos no seu balanço, sem incorrer em custos ou perdas significativas (*funding liquidity risk*). Quando as condições do mercado em que a instituição opera não permitem que esta se desfaça de certos activos a preços de mercado, mas somente abaixo destes, está-se perante o que se designa por risco de liquidez de mercado (*market liquidity risk*).

3.1.2. O risco de liquidez é considerado um dos maiores riscos a que as instituições se encontram expostas e surge quando as reservas de liquidez proporcionadas pelos activos líquidos não são suficientes para cobrir as obrigações à medida que vencem. Em tais circunstâncias, as instituições recorrem ao mercado para satisfazer as suas necessidades de liquidez. Entretanto, as condições de financiamento através do mercado dependem da liquidez nele existente e da capacidade para contrair crédito. Por outro lado, uma instituição com posição curta de liquidez pode se ver forçada a realizar transacções a custos elevados, resultando em perdas e, no pior dos cenários, na insolvência da instituição, se esta for incapaz de realizar transacções mesmo a preços correntes do mercado.

3.1.3. As instituições com elevadas exposições extrapatrimoniais ou que dependem amplamente de grandes depositantes e/ou que registem um rápido crescimento dos activos, possuem risco de liquidez relativamente mais elevado. Por esta razão, nestas condições, as instituições devem focalizar as suas atenções na liquidez.

3.1.4. O risco de liquidez não deve ser visto de forma isolada, uma vez que os riscos financeiros não são mutuamente exclusivos e o mesmo é, na maioria dos casos, despoletado por outros riscos, como o risco de crédito e de mercado. Por exemplo, uma instituição que aumenta o risco de crédito, por via da concentração de activos, pode estar a aumentar, simultaneamente, o risco de liquidez. Do mesmo modo, a entrada em incumprimento de um crédito de montante elevado ou uma alteração na taxa de juro pode ter um impacto adverso na posição de liquidez da instituição. Além disso, se a gestão ajuizar de forma errónea o impacto na liquidez, decorrente da sua entrada num novo ramo de negócios ou produto, o risco estratégico da instituição pode aumentar.

3.1.5. Um problema de liquidez em estágio incipiente pode manifestar-se, num primeiro momento, no sistema de acompanhamento da instituição como uma tendência decrescente dos indicadores definidos para o efeito, com potenciais consequências de longo prazo nos resultados, capital e na continuidade da mesma.

3.1.6. A gestão deve acompanhar (ou monitorizar) cuidadosamente os indicadores de alerta prévio[7] e realizar análises substanciais sempre que se mostrar necessário. Esses indicadores nem sempre indiciam ou conduzem, necessariamente, à existência de problemas de liquidez numa instituição, mas têm o potencial de os despoletar.

3.1.7. Os indicadores de alerta prévio podem ser de natureza quantitativa ou qualitativa. São exemplo de tais indicadores:

i. Tendência decrescente ou aumento significativo do risco em qualquer área ou linha de negócio ou actividade;
ii. Concentração crescente de activos e passivos;
iii. Diminuição dos resultados ou das suas projecções;
iv. Deterioração da qualidade da carteira de crédito;
v. Crescimento acelerado de activos financiados por passivos potencialmente voláteis;
vi. Montantes elevados de exposições extrapatrimoniais;
vii. Deterioração da avaliação feita por terceiros (*rating* externo da instituição);
viii. Publicidade negativa;
ix. Aumento significativo de levantamentos nos depósitos de retalho;
x. Aumentos de mismatch nas moedas;
xi. Eliminação ou diminuição, pelos bancos correspondentes, das linhas de crédito;
xii. Incidentes frequentes de aproximação ou violação dos limites internos ou regulamentares;
xiii. Prática insustentável de preços de competição que podem pôr em causa a estabilidade da instituição; e
xiv. Dificuldades de acesso a financiamentos de longo prazo.

3.1.8. A gestão do risco de liquidez não se limita apenas à análise da posição patrimonial e extrapatrimonial da instituição (para fazer projecções dos fluxos de caixa futuros), mas também à forma como a instituição responde às suas necessidades de financiamento. A última compreende etapas como (*i*) identificar mercados em que a instituição tem acesso a financiamentos; (*ii*) compreender a natureza destes mercados; (*iii*) avaliar a frequência actual e futura do recurso a tais mercados; e (*iv*) acompanhar os sinais de quebra de confiança.

3.1.9. A formalidade e a sofisticação dos processos de gestão de riscos instituídos para gerir o risco de liquidez devem reflectir a natureza, dimensão e complexidade das actividades de uma instituição. Uma gestão sólida do risco de liquidez empregue na medição, acompanhamento e controlo é crucial para a viabilidade de qualquer instituição. As instituições devem possuir um entendimento profundo dos factores que podem originar o risco de liquidez e pôr em prática controlos de mitigação.

3.2. Fiscalização pelo Órgão de Administração e Gestão de Topo

3.2.1. Fiscalização pelo Órgão de Administração

3.2.1.1. Os pré-requisitos para uma gestão eficaz do risco de liquidez compreendem (*i*) um órgão de administração informado e habilitado; (*ii*) uma gestão capaz; (*iii*) pessoal com experiência e habilidades relevantes; e (*iv*) sistemas e procedimentos eficientes.

3.2.1.2. O órgão de administração deve compreender o perfil do risco de liquidez da instituição e as ferramentas empregues para a sua gestão.

3.2.1.3. As responsabilidades do órgão de administração incluem:

a) Aprovar a estratégia e políticas relevantes relativas à gestão de liquidez;
b) Fornecer uma orientação sobre o nível de tolerância ao risco de liquidez;
c) Estabelecer uma estrutura apropriada para gestão do risco de liquidez e definir linhas de autoridade e responsabilidade para gerir exposições ao risco de liquidez;
d) Designar gestores de topo com habilidades para gerir o risco de liquidez, delegando neles autoridade necessária para desempenharem as suas tarefas;
e) Acompanhar de forma contínua o desempenho da instituição e o perfil global do risco de liquidez através da leitura e revisão de vários relatórios;

[7] *Early Warning Indicators - EWI*

f) Assegurar que os gestores de topo tomam os passos necessários para identificar, medir, acompanhar e controlar o risco de liquidez; e

g) Rever o grau de adequação dos planos de contingência da instituição para a gestão de liquidez.

3.2.2. Fiscalização pela Gestão de Topo

3.2.2.1. A gestão de topo é responsável pela implementação de políticas e procedimentos adequados, tendo sempre presente a linha estratégica e a apetência ao risco definido pelo órgão de administração.

3.2.2.2. Para fiscalizar de forma eficaz a gestão diária e de longo prazo do risco de liquidez, a gestão de topo deve:

a) Desenvolver e implementar procedimentos e práticas que traduzam as metas, objectivos e tolerância ao risco definidos pelo órgão de administração em padrões operacionais que sejam bem assimilados pelos colaboradores da instituição e consistentes com a intenção desse órgão;

b) Aderir às linhas de comando e responsabilidades aprovadas pelo órgão de administração para a gestão do risco de liquidez;

c) Fiscalizar a implementação e manutenção de sistemas de informação de gestão e outros sistemas de identificação, medição, acompanhamento e controlo do risco de liquidez da instituição;

d) Estabelecer controlos internos eficazes do processo de gestão do risco de liquidez e assegurar que os mesmos são comunicados a todos colaboradores; e

e) Assegurar a revisão dos planos de contingência de liquidez de forma tempestiva.

3.2.3. Estrutura de Gestão de Liquidez

3.2.3.1. A responsabilidade pela gestão da liquidez global da instituição deve ser delegada num grupo específico, bem identificado dentro da instituição. Este pode ser instituído sob a forma de um Comité de Gestão de Activos e Passivos (Asset and Liability Committee – ALCO), composto por gestores de topo ou área funcional de tesouraria.

3.2.3.2. Dado que a gestão de liquidez é uma função estritamente técnica, que requer perícia e conhecimentos especializados, é importante que os técnicos responsáveis por esta tarefa tenham não somente conhecimentos relevantes, mas também um bom entendimento da natureza e nível de risco de liquidez incorrido pela instituição, bem assim dos mecanismos para a sua gestão.

3.2.3.3. Afigura-se crucial a existência de elos ou proximidade entre os indivíduos responsáveis pela gestão da liquidez e os encarregues pelo acompanhamento das condições de mercado, e ainda com outros indivíduos com acesso a informação crítica. Isto é particularmente importante na construção e análise de cenários de esforço (stress).

3.3. Estratégia, Políticas, Procedimentos e Limites

3.3.1. Estratégia de Risco de Liquidez

3.3.1.1. Cada instituição deve ter uma estratégia apropriada para a gestão diária de liquidez. A estratégia deve enunciar a abordagem geral que a instituição deve adoptar para fazer face às suas necessidades de liquidez, indicando as metas quantitativas e qualitativas. A estratégia deve, igualmente, consagrar o objectivo de salvaguardar a solidez financeira da instituição e a sua capacidade para suportar choques adversos que afectem drasticamente as condições do mercado.

3.3.1.2. A estratégia de risco de liquidez, definida pelo órgão de administração, deve enunciar políticas concretas sobre aspectos específicos da gestão do risco de liquidez, nomeadamente:

a) **Composição de Activos e Passivos –** A estratégia deve privilegiar a diversificação de activos e passivos de modo a manter a liquidez. A gestão do risco de liquidez e a dos activos e passivos deve ser integrada, de modo a evitar custos elevados associados a uma eventual necessidade de rápida reconfiguração do perfil de activos e passivos, alterando o paradigma de maximização da rendibilidade para incremento da liquidez.

b) **Diversificação e estabilidade dos Passivos –** Uma concentração do *funding*[8] existe quando uma decisão ou um único factor tem o potencial de resultar num levantamento repentino e significativo de fundos. Dado que tal situação pode resultar num risco ainda maior, o órgão de administração e a gestão de topo devem estabelecer orientações relacionadas com fontes de financiamento e assegurar que a instituição tenha fontes diversificadas para suprir as necessidades diárias de liquidez.

c) Uma instituição pode ser imune às condições de escassez de liquidez no mercado se os seus passivos forem derivados de fontes relativamente estáveis. Para analisar detalhadamente a estabilidade dos passivos e das fontes de recursos, a instituição necessita de identificar os passivos, que podem ser:

i. Mantidos na instituição, em quaisquer circunstâncias;

ii. Gradualmente retirados, caso surjam problemas; e

iii. Imediatamente retirados, ao primeiro sinal de problemas.

d) **Gestão de liquidez em diversas moedas –** A instituição deve possuir uma estratégia de gestão de liquidez nas diversas moedas.

e) **Estratégia para lidar com quebras de liquidez –** A instituição deve pôr em prática uma estratégia para lidar com potenciais quebras de liquidez quer sejam temporárias, quer sejam de longo prazo. A estratégia deve tomar em consideração que, em situações de crise, o acesso ao mercado interbancário pode ser difícil e oneroso.

3.3.1.3. A estratégia de liquidez deve ser documentada numa política de liquidez e comunicada aos gestores de topo, ao ALCO e às unidades que lidam com esta matéria na instituição. A mesma deve ser revista no mínimo anualmente, de modo a assegurar que permanece actualizada.

3.3.2. Políticas de Liquidez

3.3.2.1. O órgão de administração deve assegurar a existência de políticas adequadas que orientem o processo de gestão do risco de liquidez na instituição. Embora os detalhes específicos possam variar de instituição para instituição, em função da natureza da sua actividade, a política de liquidez deve ter os seguintes elementos:

a) Estratégia geral de liquidez (curto e longo prazo), metas e objectivos específicos em relação à gestão do risco de liquidez, processo de formulação de estratégia e nível em que é aprovado dentro da instituição;

[8] Fonte de recursos ou financiamento.

b) Atribuições e responsabilidades dos indivíduos que desempenham funções de gestão do risco de liquidez, incluindo a gestão da estrutura do balanço, formulação de preços (*pricing*), técnicas de venda de produtos e serviços, plano de contingência, informação a reportar à gestão, linhas de autoridade e responsabilidades para decisões sobre liquidez;

c) Ferramentas de gestão de risco para identificar, medir, acompanhar e controlar o risco de liquidez (incluindo os tipos de limite e rácios existentes e a racionalidade de estabelecer estes mesmos limites e rácios);

d) Plano de contingência para lidar com cenários de crises de liquidez;

e) Abordagem da gestão de liquidez nas diferentes moedas; e

f) Abordagem de gestão de liquidez diária.

3.3.2.2. Para ser eficaz, a política de liquidez deve ser comunicada aos gestores de topo, ao ALCO e às unidades da instituição que lidam com esta matéria.

3.3.2.3. A política de liquidez deve ser revista, pelo menos, uma vez ao ano e sempre que houver quaisquer alterações materiais no perfil de risco de liquidez actual e futuro da instituição. Tais alterações podem resultar de circunstâncias internas (como alterações no foco de negócio) ou circunstâncias externas (como alterações das condições económicas).

3.3.2.4. A revisão constitui uma oportunidade para a instituição ajustar a política de liquidez à luz da sua experiência de gestão nesta matéria e da evolução do seu negócio. Qualquer excepção material ou frequente à política é um indicador importante para medir a sua eficácia e impacto no perfil de risco de liquidez da instituição.

3.3.3. Procedimentos e limites

3.3.3.1. As instituições devem estabelecer procedimentos, processos e limites apropriados para implementar a sua política de liquidez. O manual de procedimentos deve descrever explicitamente os processos e procedimentos operacionais necessários para executar os controlos relevantes de risco de liquidez.

3.3.3.2. O manual deve ser revisto e actualizado periodicamente, no mínimo anualmente, para incluir novas actividades, alterações nos sistemas e na abordagem de gestão de riscos.

3.3.3.3. Além de manter a liquidez nos termos definidos pelo Banco de Moçambique, o órgão de administração e a gestão de topo devem estabelecer limites sobre a natureza e a magnitude do risco de liquidez que estão dispostos a assumir. Os limites devem ser revistos e ajustados periodicamente e sempre que os níveis de tolerância ao risco se alterem.

3.3.3.4. Ao impor limites de exposição ao risco, a gestão de topo deve tomar em consideração a natureza da actividade e a estratégia da instituição, desempenho passado, nível dos resultados, capital existente para absorver potenciais perdas e a tolerância ao risco estabelecida pelo órgão de administração. A complexidade do balanço determina quanto e que tipo de limites a instituição deve estabelecer para o dia-a-dia e longo prazo.

3.3.3.5. Embora os limites não previnam crises de liquidez, as excepções aos mesmos podem sinalizar risco excessivo, uma gestão inadequada de riscos ou necessidade de revisão das metas e limites.

3.4. Mensuração, Acompanhamento e Sistemas de Informação de Gestão de Risco

3.4.1. Para além da estrutura institucional acima descrita, uma gestão de liquidez efectiva deve incluir sistemas de informação de gestão que permitam identificar, medir, acompanhar e controlar o risco de liquidez presente e futuro, e reportar à gestão de topo e ao órgão de administração.

3.4.2. A gestão da instituição deve ser capaz de identificar e quantificar correctamente e em tempo útil as fontes principais do risco de liquidez. Para identificar de forma apropriada as fontes, a gestão deve compreender os riscos actuais e futuros a que a instituição possa estar exposta. A gestão deve estar sempre alerta ao surgimento de novas fontes de risco de liquidez ao nível das transacções e das carteiras.

3.4.3. No que concerne ao sistema de informação de gestão, as diversas áreas ou unidades funcionais relacionadas com a actividade de tesouraria e a função de gestão de riscos devem estar integradas. Adicionalmente, a gestão deve assegurar, de forma apropriada e tempestiva, o fluxo de informação entre o front-office, o back-office e o middle-office, de forma integrada. Contudo, as respectivas linhas de reporte devem estar separadas para garantir a independência dessas funções.

3.4.4. Devem ser efectuadas revisões periódicas para aferir se a instituição cumpre com as suas políticas e procedimentos de risco de liquidez. As revisões periódicas do processo de gestão de risco devem abarcar quaisquer alterações significativas na natureza dos instrumentos adquiridos, os limites e os controlos internos introduzidos desde a última revisão. As posições que excedam os limites estabelecidos devem receber pronta intervenção da gestão, que deve resolver de acordo com o processo descrito nas políticas aprovadas.

3.4.5. Mensuração e Acompanhamento do Risco de Liquidez:

3.4.5.1. A instituição deve ter um sistema de medição e acompanhamento do risco de liquidez.

3.4.5.2. A nível mais elementar, a medição de liquidez envolve a avaliação de todas as entradas e saídas de caixa da instituição, de modo a identificar o potencial de qualquer défice poder durar por um longo período. Isto inclui, igualmente, o *funding* de compromissos extrapatrimoniais.

3.4.5.3. Várias técnicas podem ser empregues para medir o risco de liquidez, desde cálculos simples e simulações estáticas (baseadas nas posições existentes) a técnicas sofisticadas de modelação. Uma vez que todas instituições são afectadas pelas alterações nas condições económicas e de mercado, o acompanhamento da tendência dessas condições é crucial na gestão do risco de liquidez.

3.4.5.4. A formulação de hipóteses sobre as necessidades futuras de *funding* constitui um aspecto importante na gestão de liquidez. Embora certas entradas de caixa possam ser previstas ou calculadas com facilidade, as instituições devem adoptar hipóteses sobre necessidades futuras de liquidez para curto e longo prazo. Um dos factores a considerar é o papel crucial que a reputação da instituição desempenha na capacidade de aceder prontamente aos recursos de financiamento e a custos razoáveis. Por esta razão, o pessoal responsável por gerir a liquidez global deve estar a par de qualquer informação pública ou de qualquer outra natureza (ex., anúncio de diminuição dos resultados ou da notação de risco atribuída à instituição por agências de *rating*) que possa ter impacto no mercado e na percepção do público sobre a condição financeira da instituição.

3.4.5.5. Um sistema eficaz de medição e acompanhamento do risco de liquidez não é útil somente em tempos de crises de liquidez, mas também maximiza os resultados através de utilização eficiente de recursos.

3.4.5.6. Apresentam-se a seguir algumas técnicas de medição e de acompanhamento de liquidez comummente empregues pelas instituições.

3.4.6. Planos Contingentes de Liquidez:

3.4.6.1. Com vista a desenvolver um quadro de gestão de liquidez detalhado, as instituições devem possuir um plano para lidar com cenários de esforço (stress). Tal plano, comummente

conhecido por Plano Contingente de Liquidez (*Contingency* Funding Plan – CFP) compreende um conjunto de políticas, procedimentos e planos de acção para responder a uma quebra grave na capacidade da instituição de financiar algumas das suas actividades em tempo útil e a custos razoáveis.

3.4.6.2. Um CFP é uma projecção de fluxos de caixa e de fontes de financiamento de uma instituição em cenários adversos (de esforço). Para ser eficaz, o CFP deve representar a melhor estimativa da gestão sobre as alterações no balanço que podem resultar de eventos de liquidez ou crédito. O CFP pode ser uma plataforma útil para a gestão de risco de liquidez quer a curto, quer a longo prazo. Além disso, permite assegurar à instituição financeira a gestão prudente e eficiente das flutuações rotineiras e extraordinárias de liquidez.

3.4.6.3. Para integração da gestão diária do risco de liquidez, os cenários de liquidez asseguram que a instituição esteja melhor preparada para responder a um problema inesperado. Neste sentido, o CFP é uma extensão do processo contínuo de gestão de liquidez e formaliza os objectivos desta gestão, assegurando:

a) A manutenção de um nível razoável de activos líquidos;

b) A medição e a projecção das necessidades de *funding* ao longo de vários cenários; e

c) A gestão de acesso a fontes de financiamento.

3.4.6.4. Nem sempre as crises de liquidez se manifestam de forma gradual. Em casos de distúrbios repentinos na liquidez, é importante a instituição mostrar-se organizada, serena, e eficiente na satisfação das suas obrigações perante os seus stakeholders. Uma vez que estas situações requerem uma acção espontânea, as instituições que possuem planos para lidar com as mesmas podem enfrentar o problema de liquidez de forma mais eficiente e eficaz. O CFP permite assegurar que a gestão e o pessoal-chave estejam de prontidão para responder a tais situações.

3.4.6.5. A liquidez da instituição é altamente sensível a tendências negativas no crédito, capital ou reputação. Uma deterioração nas condições financeiras da instituição (consubstanciada nos indicadores de qualidade de activos, rendibilidade, ou capital), na composição da gestão e outras inquietações podem resultar na diminuição do acesso ao *funding*.

3.4.6.6. A sofisticação do CFP depende da dimensão, natureza, complexidade do negócio, exposição ao risco e estrutura da instituição, mas, no mínimo, o mesmo deve:

a) Antecipar todas necessidades de funding e de liquidez através de:

i. Análise e realização de projecções quantitativas de todos os fluxos de recursos de activos patrimoniais e extrapatrimoniais significativos, bem como todos os efeitos relacionados;

ii. Mapeamento das potenciais origens e aplicações de fundos; e

iii. Estabelecimento de indicadores de alerta à gestão para níveis de riscos potenciais predeterminados.

b) Projectar a posição de funding da instituição em situações de alterações de liquidez, tanto temporárias como de longo prazo.

c) Identificar, quantificar e classificar, explicitamente, todas as fontes de financiamento por preferência, tais como:

i. Redução de activos;

ii. Modificação ou incremento da estrutura de passivos; e

iii. Utilização de alternativas para controlar flutuações no balanço.

d) Conter políticas e procedimentos claros que permitam à gestão do banco tomar decisões tempestivas e com informações suficientes, executar medidas de contingência de forma rápida e proficiente, incluindo:

i. Especificação clara das funções e responsabilidades, incluindo autoridade para accionar o plano. O estabelecimento de uma "equipa de crise" formal pode facilitar a coordenação interna e a tomada de decisão durante a crise de liquidez;

ii. Nomes e contactos dos membros da equipa responsável pela implementação do CFP e a localização dos mesmos; e

iii. Designação de alternativas para as funções principais.

e) Indicar o sistema de informação de gestão entre o ALCO, os traders, o Banco de Moçambique e o público em geral.

3.4.6.7. Para facilitar a gestão de quebras graves de liquidez em tempo útil, o plano deve estabelecer claramente o processo de tomada de decisão a respeito de que acções tomar, em que momento, quem as pode tomar, quais os assuntos que precisam ser escalados ao mais alto nível da gestão da instituição, quem deve ser notificado, que relatórios precisam de ser produzidos e para quem, e quais são os passos que podem ser tomados para melhorar a liquidez ou para compensar fluxos de caixa. O plano deve incluir como e em que situações devem ser contactadas as partes externas como o Banco de Moçambique.

3.4.6.8. O CFP deve incluir uma estratégia tanto do lado dos activos como dos passivos. A estratégia do lado do activo deve incluir (*i*) situações em que podem ser liquidados os excedentes dos activos do mercado monetário, (*ii*) situações em que os activos líquidos ou de longo prazo podem ser vendidos, etc. A estratégia do lado do passivo especifica políticas tais como a política de preços para financiamento, a instituição ou o dealer que pode prestar assistência em tempos de crises de liquidez, política para resgate antecipado a pedido de clientes, uso das facilidades do Banco de Moçambique, etc..

3.4.6.9. A gestão de topo deve rever, actualizar e testar o CFP pelo menos uma vez por ano, para a aprovação pelo órgão de administração, ou com maior frequência quando as circunstâncias do negócio ou mercado se alterem. O teste deve assegurar que as funções e as responsabilidades são adequadas e entendidas, confirmar se os contactos estão actualizados, provar a transferibilidade de fundos e colaterais (especialmente entre países e entidades) e verificar se existe documentação legal e operacional necessária para executar o plano em tempo reduzido.

3.4.6.10. O CFP deve ser consistente com o plano de continuidade de negócios da instituição e ser operacional sempre que os arranjos de continuidade de negócio forem accionados. Assim sendo, a instituição deve assegurar que haja coordenação eficaz entre as equipas que gerem questões relacionadas com liquidez e continuidade de negócio.

3.4.7. Escalonamento Cumulativo de Maturidades Residuais:

3.4.7.1. O escalonamento de maturidades residuais é uma ferramenta importante para comparar as entradas e saídas de caixa quer numa base diária, quer por uma série de períodos específicos. O horizonte temporal no escalonamento de maturidades é de extrema importância e, de alguma forma, depende da natureza e das fontes de recursos da instituição. As instituições que depositam confiança nas fontes de recursos de curto prazo tendem a concentrar-se, fundamentalmente, na gestão de liquidez de muito

curto prazo. Contrariamente, outras instituições podem gerir activamente as suas necessidades de recursos por um período relativamente longo.

3.4.7.2. A curto prazo, o fluxo de fundos pode ser estimado com maior precisão e tais estimativas são de maior importância, uma vez que indicam acções a serem tomadas pontualmente. Adicionalmente, análises para períodos relativamente longos permitem à instituição maximizar a oportunidade de gerir antecipadamente o gap antes que o mesmo se cristalize. Assim, as instituições devem usar bandas temporais curtas para medir exposições de curto prazo e mais longas para exposições de médio e longo prazos. Sugere-se que as instituições calculem gaps (*i*) diários (para uma ou duas semanas seguintes); (*ii*) mensais (para o semestre ou ano seguinte); e (*iii*) trimestrais, subsequentemente.

3.4.7.3. Ao se estimar os fluxos de caixa, os aspectos que se seguem devem ser tomados em consideração:

a) Necessidades de recursos decorrentes de compromissos extrapatrimoniais;

b) Comportamento dos clientes, ao invés de se cingirem à maturidade contratual. Neste aspecto, a experiência passada desempenha um papel fundamental na definição de pressupostos;

c) Fluxos de caixa sazonais e cíclicos; e

d) Aumentos ou diminuições de liquidez susceptíveis de ocorrer durante várias fases do ciclo económico.

3.4.7.4. As instituições devem possuir liquidez suficiente para responderem a flutuações nos créditos e depósitos, e como medida de precaução devem manter uma margem razoável de excesso de liquidez. Para se certificar de que tal excesso é mantido, a gestão deve estimar as necessidades de liquidez em diferentes cenários.

3.4.8. Rácios e Limites de Liquidez:

3.4.8.1. As instituições podem usar uma variedade de rácios para quantificar as suas posições de liquidez. Esses rácios podem igualmente ser usados como limites para a gestão de liquidez. Entretanto, os mesmos não têm qualquer significado a menos que sejam usados regularmente e interpretados tendo em conta factores qualitativos. Os rácios devem ser sempre usados em conexão com informações mais qualitativas acerca da capacidade de endividamento, tais como a possibilidade de aumento inesperado de levantamentos, diminuição das linhas de crédito, do tamanho das transacções ou de fundos de longo prazo disponíveis para a instituição.

3.4.8.2. Uma vez que as decisões de gestão de activos e passivos da instituição são baseadas em rácios financeiros, os gestores devem compreender a forma como os rácios são computados, o conjunto de informação alternativa que pode ser usada como numerador ou denominador e o âmbito das conclusões que podem ser extraídas desses rácios. Uma vez que os componentes dos rácios (tal como calculados pelas instituições) são algumas vezes inconsistentes, a comparação entre instituições com base em rácios ou mesmo comparações de períodos diferentes numa instituição pode ser enganadora.

3.4.8.3. Os rácios e os limites que podem ser usados pelas instituições são:

a) **Rácios e Limites de Concentração de Passivos –** Ajudam a prevenir que a instituição confie excessivamente num número reduzido de financiadores e fontes de recursos. Os limites são geralmente expressos em percentagem dos depósitos ou passivos;

b) **Mismatches Cumulativos de Fluxos de Caixa Contratuais –** É um limite de mismatches cumulativos de fluxos de caixa contratuais em percentagem do passivo total, em vários horizontes temporais;

c) **Outros Rácios Baseados na Informação do Balanço –** São exemplos de rácios habitualmente usados pelas instituições para acompanhar os níveis de liquidez corrente e potencial os seguintes: crédito total/ /depósitos totais, activos líquidos/passivo exigível, empréstimos contraídos/activo total.

3.4.8.4. Além dos requisitos prudenciais exigidos pelo Banco de Moçambique o órgão de administração e a gestão de topo devem estabelecer limites sobre a natureza e o montante do risco de liquidez que estão dispostos a assumir. Os limites devem ser revistos periodicamente e ajustados sempre que as condições e os níveis de tolerância ao risco se alterem.

3.4.8.5. Ao limitar a exposição ao risco, a gestão de topo deve ter em consideração a estratégia e as actividades da instituição, o desempenho em anos anteriores, o capital existente para absorver as perdas inesperadas e o nível de tolerância definido pelo órgão de administração. A complexidade do balanço determina o número e tipo de limites que a instituição deve estabelecer para o dia-a-dia e a longo prazo. Embora os limites não impeçam que crises de liquidez ocorram, excepções aos limites podem ser sinalizadores de riscos excessivos ou de gestão inadequada do risco de liquidez.

3.4.9. Gestão da Liquidez em Moeda Estrangeira:

3.4.9.1. Cada instituição deve possuir um sistema para medir, acompanhar e controlar as suas posições de liquidez nas principais moedas em que se encontra activa.

3.4.9.2. A instituição deve avaliar as suas necessidades de liquidez agregada em moeda estrangeira e de desfasamento (*mismatch*) aceitável em combinação com os seus compromissos em moeda nacional, e realizar análises separadas da sua estratégia para cada moeda.

3.4.9.3. A dimensão dos *mismatches* em moeda estrangeira deve tomar em consideração:

a) A capacidade da instituição de obter fundos no mercado cambial;

b) A possibilidade de estender as facilidades existentes de obtenção de recursos em moeda estrangeira no mercado doméstico;

c) A habilidade de transferir o excesso de liquidez em uma moeda para outra e entre jurisdições e entidades; e

d) A convertibilidade da moeda em que a instituição se encontra activa.

3.4.9.4. A instituição deve ter o cuidado e a capacidade de gerir exposições ao risco de liquidez decorrentes do uso de depósitos em moeda estrangeira e linhas de crédito de curto prazo para financiar activos em moeda nacional, bem como do financiamento de activos em moeda estrangeira por recursos em moeda nacional. A instituição deve ter em consideração os riscos de uma alteração repentina das taxas de câmbio ou da liquidez no mercado, ou ambos, que podem agravar o *mismatch* existente e alterar a eficácia dos instrumentos e estratégias de cobertura do risco cambial.

3.4.9.5. Adicionalmente, a instituição deve avaliar a possibilidade de perda de acesso aos mercados cambiais, bem como de convertibilidade das moedas em que conduz a sua actividade.

3.4.10. Acesso ao Mercado:

3.4.10.1. Um componente essencial para assegurar a diversificação de funding é manter acesso ao mercado. O acesso ao mercado é crucial para a gestão eficaz do risco de liquidez, dado que afecta tanto a habilidade da instituição de obter novos recursos como a de liquidar os activos. A gestão de topo deve assegurar que o acesso ao mercado é activamente gerido, acompanhado e testado por pessoal apropriado.

3.4.10.2. Gerir o acesso ao mercado pode incluir o desenvolvimento de mercados para venda de activos ou o fortalecimento de acordos pelos quais a instituição pode contrair empréstimos com ou sem garantia. A instituição deve manter uma presença activa nos mercados relevantes para a sua estratégia de funding. Isto requer compromisso e investimento contínuo em infra-estruturas, processos e recolha de informação.

3.4.10.3. Normalmente, mercados fiáveis de funding podem ser seriamente afectados quando colocados sob esforço. A instituição deve identificar e criar fortes relações com os investidores existentes e potenciais, mesmo em mercados cujo acesso é facilitado por correctores ou outros intermediários.

3.4.10.4. Embora seja importante desenvolver e manter fortes relações com provedores de fundos, a instituição deve ser prudente, dado que essas relações podem ser afectadas em situações de esforço. As instituições que em condições normais infalivelmente fornecem recursos podem não o fazer em períodos de severo esforço por causa da incerteza das suas próprias necessidades de liquidez. Na formulação de cenários de esforço e de planos de contingência, a instituição deve considerar esses efeitos de segunda ordem e tomar em consideração que fontes de recursos podem se esgotar e o mercado encerrar.

3.4.10.5. A instituição deve identificar fontes alternativas de recursos que fortaleçam a sua capacidade de resistir à variedade de choques severos, mas plausíveis, específicos à instituição e à liquidez do mercado como um todo.

3.4.11. Revisão dos Pressupostos Usados na Gestão de Liquidez:

3.4.11.1. Uma vez que a posição futura de liquidez da instituição é afectada por factores que nem sempre podem ser previstos com exactidão, os pressupostos de gestão de liquidez devem ser revistos com frequência para se determinar a sua validade contínua, especialmente tendo em conta a rapidez das mudanças nos mercados.

3.4.12. Testes de Esforço:

3.4.12.1. As Instituições, com envolvimento activo da gestão do topo, devem realizar regularmente testes de esforço, considerando vários cenários rigorosos e desafiadores, mesmo nos momentos em que a liquidez é abundante sobre as suas posições, para garantir que mantêm liquidez suficiente para resistir a situações de esforço (*stress*).

3.4.12.2. A extensão e a frequência dos testes devem ser proporcionais à dimensão da instituição e sua exposição ao risco de liquidez, bem como à importância relativa da mesma no sistema financeiro. As instituições devem criar condições para aumentar a frequência dos testes em circunstâncias especiais (por exemplo, a pedido do Banco de Moçambique).

3.4.12.3. Os órgãos de administração e a gestão de topo devem analisar os resultados dos testes de esforço e formular estratégias adequadas para resolver as necessidades de liquidez reveladas pela análise do cenário. Por exemplo, pode haver necessidade de redução do risco de liquidez, obtendo mais financiamento de longo prazo ou reestruturando a composição dos activos.

3.4.12.4. Ao realizarem testes de esforço de liquidez, é importante que as instituições o façam com cenários adversos plausíveis, e analisem as necessidades de liquidez que deles resultarem. As instituições são incentivadas a abranger diferentes tipos e níveis de adversidade, devendo, entretanto, privilegiar os seguintes cenários:

a) Cenários de crise típicos de cada instituição; e
b) Cenários de crise típicos do mercado.

3.4.12.5. Os cenários típicos de cada instituição abrangem situações em que há percepção ou existência de problemas a nível institucional, como, por exemplo, problemas operacionais, preocupações com a solvência e mudanças adversas na notação de crédito.

3.4.12.6. Em geral um cenário de crise típico de mercado é o que afecta a liquidez do maior número de instituições em um ou mais mercados.

3.4.12.7. As instituições devem detalhar os pressupostos subjacentes ao comportamento dos fluxos de caixa de seus activos, passivos e elementos extrapatrimoniais em cenários plausíveis de crise. O timing e a dimensão dos fluxos de caixa são factores importantes a considerar. Os pressupostos podem diferir de forma acentuada de cenário para cenário, dado que o timing e o tamanho dos fluxos de caixa podem se comportar de maneira diferente em diferentes situações. As instituições devem tomar em consideração o período de liquidação ou o tempo necessário para liquidar activos.

3.4.12.8. O principal pressuposto subjacente a cenários de crise típicos de cada instituição é o facto de muitos dos passivos da instituição não poderem ser renegociados ou substituídos, resultando em reembolso na maturidade exigida, de tal modo que a instituição teria de contrair, em certa medida, a sua carteira de activos.

3.4.12.9. Os requisitos mínimos para a utilização de diferentes cenários na realização de testes de esforço de liquidez são os seguintes:

a) Os pressupostos devem ser consistentes e razoáveis para cada cenário;
b) Os pressupostos devem ser verificados e sustentados por evidência específica, experiência passada ou desempenho, ao invés de serem meramente arbitrários;
c) As instituições devem documentar os pressupostos comportamentais na sua declaração de política de gestão de liquidez. O tipo de análise realizada no âmbito de cada pressuposto também deve ser documentado para facilitar a revisão periódica; e
d) A gestão de topo deve assegurar que os pressupostos fundamentais sejam avaliados, pelo menos anualmente, para testar a sua razoabilidade.

3.4.12.10. Num cenário de crise generalizada no mercado, assume-se que uma instituição pode ter menos controlo sobre o nível e tempestividade dos fluxos de caixa futuros. As características deste cenário podem incluir uma forte diminuição de liquidez, incumprimento da contraparte, a necessidade de efectuar descontos substanciais para liquidar activos e grandes diferenças no acesso ao financiamento entre as instituições, devido a incertezas no mercado.

3.4.12.11. Ao realizar análises de cenários, as instituições podem incluir o apoio que podem receber a nível intragrupo ou da sede. Esse apoio será de extrema importância em situações de crises que apenas afectem as operações domésticas (por limitações de natureza territorial e jurisdicional), mas poderá revelar-se ineficaz se as crises afectarem o grupo como um todo. Além disso, as instituições devem documentar:

a) Os pressupostos de fluxos de caixa em cenários de crises específicos da instituição e do mercado; e
b) As estimativas do número mínimo de dias necessários para mobilizar apoios financeiros de emergência a partir de outras fontes.

3.4.12.12. Os cenários devem ser sujeitos a revisão regular para assegurar que a natureza e a severidade dos cenários testados permaneçam apropriados e relevantes para a instituição. As revisões devem ter em consideração as mudanças nas condições de mercado, na natureza, dimensão e complexidade do modelo de negócio e das actividades da instituição e experiências actuais em cenários de esforço.

3.4.13. Sistemas de Informação de Gestão:

3.4.13.1. Um Sistema de Informação de Gestão (SIG) eficaz é essencial para a tomada de decisões de gestão de liquidez numa base sustentável. As informações devem estar disponíveis para o dia-a-dia de gestão e de controlo de risco de liquidez, bem como durante períodos de esforço.

3.4.13.2. Os dados devem ser consolidados, abrangentes, sucintos, objectivos e estar disponíveis de forma atempada. Em condições normais, os relatórios periódicos gerados permitem que a instituição acompanhe a liquidez durante crises; tais relatórios devem ser preparados com maior frequência em situação de crise. Ao desenvolver sistemas de informação de gestão de liquidez, os gestores devem ter sempre presente o acompanhamento da crise.

3.4.13.3. Há sempre um trade-off entre exactidão e tempestividade. Problemas de liquidez podem surgir muito rapidamente e a gestão eficaz de liquidez pode exigir relatórios internos diariamente. Uma vez que a liquidez é afectada em grande medida pelos fluxos agregados de caixa, mostra-se irrelevante analisar informações detalhadas sobre cada operação, pelo facto de não se poder melhorar a análise.

3.4.13.4. O sistema de informação de gestão deve ser utilizado para verificar o cumprimento das políticas, procedimentos e limites estabelecidos pela instituição, bem como os requisitos prudenciais sobre liquidez estabelecidos pelo Banco de Moçambique. O relato de medidas de risco deve ser feito em tempo oportuno e as posições de liquidez corrente devem ser comparadas com quaisquer limites fixados. O sistema de informação deve igualmente permitir à gestão uma avaliação da tendência do nível global de exposição ao risco de liquidez na instituição.

3.4.13.5. A gestão deve desenvolver sistemas que permitam captar informações significativas. O conteúdo e o formato dos relatórios dependem das práticas de gestão de liquidez, riscos e outras características da instituição. Os relatórios de rotina podem incluir uma relação das principais fontes de recursos, fluxo de caixa, etc.

3.4.13.6. A gestão do dia-a-dia pode exigir informações mais detalhadas, dependendo da complexidade da instituição e dos riscos incorridos. A gestão de linha deve regularmente ponderar a melhor forma de resumir questões detalhadas e complexas para gestores do topo ou órgão de administração. Além disso, outro tipo de informações importantes para a gestão das actividades do dia-a-dia e para a compreensão do perfil do risco de liquidez inerente à instituição incluem:

a) Qualidade de activos e sua evolução;
b) Projecção dos resultados;
c) Reputação geral da instituição no mercado e as condições do próprio mercado;
d) Composição global da estrutura do balanço; e
e) Tipo de depósitos (novos produtos) a serem captados, bem como a sua fonte, maturidade e preço.

3.5. Controlos Internos

3.5.1. As instituições devem dispor de controlos internos para garantir a integridade do seu processo de gestão de risco de liquidez. Esses controlos devem ser parte integrante do sistema global de controlo interno da instituição, o qual deve promover a eficiência e a eficácia das operações, relatórios financeiros e regulamentares fiáveis e de conformidade com as leis, regulamentos e políticas institucionais.

3.5.2. O sistema de controlo interno para o risco de liquidez deve incluir:

a) Forte ambiente de controlo;
b) Processo adequado de identificação e avaliação de risco de liquidez;
c) O estabelecimento de actividades de controlo, tais como políticas e procedimentos;
d) Sistemas de informação adequados; e
e) Revisão contínua da aderência às políticas e procedimentos.

3.5.3. No que diz respeito às políticas e procedimentos de controlo, deve ser dada atenção a processos apropriados de aprovação, limites, revisão e outros mecanismos destinados a fornecer uma garantia razoável de que os objectivos da gestão de risco de liquidez da instituição serão alcançados.

3.5.4. Os atributos de um bom processo de gestão de riscos, incluindo a função de medição, acompanhamento e controlo de riscos, são aspectos fundamentais de um sistema eficaz de controlo interno. As instituições devem assegurar que todos os aspectos do sistema de controlo interno são eficazes, incluindo os aspectos que não fazem directamente parte do processo de gestão de risco.

3.5.5. Outros elementos importantes no sistema de controlo interno de uma instituição, no processo de gestão de risco de liquidez, são a avaliação periódica e a revisão. Isto inclui assegurar que os colaboradores estão a cumprir com as políticas e procedimentos estabelecidos, bem como assegurar que os procedimentos que foram estabelecidos realmente cumprem os objectivos pretendidos. Essas revisões e avaliações devem abordar, igualmente, qualquer alteração significativa que possa ter impacto na eficácia dos controlos.

3.5.6. O órgão de administração deve assegurar que todas as revisões e avaliações são efectuadas regularmente por pessoas independentes da função a ser revista. Quando as revisões ou melhorias para os controlos internos são justificadas, deve haver um mecanismo para assegurar que estas são implementadas de forma atempada.

4. Directrizes de Gestão do Risco de Taxa de Juro

4.1. Introdução

4.1.1. O risco de taxa de juro é a possibilidade de ocorrência de impactos negativos nos resultados ou no capital, devido a movimentos adversos nas taxas de juro, por via de desfasamentos de maturidades ou de prazos de refixação das taxas de juro, da ausência de correlação perfeita entre as taxas das operações activas e passivas nos diferentes instrumentos, ou da existência de opções embutidas em instrumentos financeiros do balanço ou elementos extrapatrimoniais.

4.1.2. A exposição a este risco faz parte do curso normal da actividade de intermediação financeira e pode ser uma importante fonte de rendibilidade e de criação de valor para os accionistas. No entanto, o risco excessivo de taxa de juro pode representar uma ameaça significativa para a base de proveitos e capital de uma instituição.

4.1.3. As variações nas taxas de juro afectam os resultados de uma instituição por via da alteração da margem financeira e do nível de outros proveitos e custos operacionais sensíveis a variações da taxa de juro. Afectam, igualmente, o valor subjacente dos activos, passivos e instrumentos extrapatrimoniais de uma instituição, visto que o valor actual de fluxos de caixa futuros (e em alguns casos, os próprios fluxos de caixa) varia sempre que houver variações nas taxas de juro. Deste modo, a institucionalização de um processo eficaz de gestão de riscos que mantenha o risco de taxa de juro a níveis prudentes é importante para garantir a segurança e a solidez das instituições.

4.2. Fontes e Efeitos de Risco de Taxa de Juro

4.2.1. Fontes de Risco de Taxa de Juros

4.2.1.1. As principais formas de risco de taxa de juro a que as instituições estão normalmente expostas compreendem o risco

de refixação de taxa de juro (*repricing risk*), risco da "curva de rendimentos" (*yield curve risk*[9]), risco de indexante e risco de opção (basis risk e optionality risk), cada uma das quais é abordada em detalhe a seguir:

a) **Risco de Refixação da Taxa (*Repricing Risk*) –** A principal e a mais discutida forma de risco de taxa de juro, emerge de desfasamentos entre as maturidades (para taxas fixas) ou refixação (para taxas variáveis) dos activos, passivos e posições extrapatrimoniais da instituição. Embora tais desfasamentos de refixação das taxas (repricing mismatches) sejam fundamentais para a intermediação financeira, eles podem expor os resultados e o valor económico subjacente de uma instituição a flutuações inesperadas à medida que as taxas de juro variam. Por exemplo, uma instituição que financiou um crédito de longo prazo à taxa fixa (por meio de um depósito de curto prazo) pode registar uma diminuição tanto dos rendimentos futuros (decorrente das posições assumidas), como do respectivo valor, caso as taxas de juro aumentem. Esta diminuição ocorre porque os fluxos de caixa do crédito são fixos, durante a sua vigência, enquanto o juro pago sobre o financiamento é variável e aumenta após o vencimento do depósito de curto prazo.

b) ***Yield Curve Risk* –** Os desfasamentos de refixação da taxa podem, igualmente, expor a instituição a alterações no formato e inclinação da "yield curve". Este risco surge quando alterações inesperadas na "yield curve" produzem um impacto adverso nos resultados da instituição ou no seu valor económico subjacente.

c) **Risco de Indexante (*Basis Risk*) –** Este risco decorre da inexistência de correlação perfeita entre as taxas recebidas e pagas nos diferentes instrumentos, motivada por diferenças nos indexantes de taxa de juro. Quando as taxas de juro variam, estas diferenças podem dar origem a variações inesperadas nos fluxos de caixa e nas margens (*spreads*) de proveitos entre activos, passivos e instrumentos extrapatrimoniais com maturidade ou frequência de refixação das taxas de juro similares. Por exemplo, uma estratégia de financiar um crédito com maturidade de um ano (cuja taxa de juro é ajustada ou refixada mensalmente, em função da MAIBOR ou qualquer outra taxa de referência) por um depósito de igual maturidade (cuja taxa é refixada mensalmente na base da taxa mensal de um Bilhete de Tesouro) expõe a instituição ao risco de o spread entre as duas taxas de indexação se alterar inesperadamente.

d) **Risco de Opção (*Optionality Risk*) –** Este risco resulta da existência de opções embutidas em instrumentos financeiros do balanço ou elementos extrapatrimoniais, tais como opções de resgate ou de amortização antecipados em depósitos ou empréstimos.

4.2.1.2. Do ponto de vista formal, uma opção dá ao seu detentor o direito, mas não a obrigação, de comprar, vender ou de algum modo alterar o fluxo de caixa de um contrato ou instrumento financeiro. Uma opção pode ser um instrumento do tipo "stand alone" ou embutido em outros instrumentos padronizados. Embora as instituições usem opções tanto para negociação como para outras finalidades, os instrumentos com opções embutidas são geralmente mais importantes nas actividades cuja intenção da gestão não seja a negociação. Incluem-se nesta categoria os vários tipos de obrigações e títulos com opções de compra ou venda, empréstimos que conferem ao mutuário o direito de antecipar o pagamento da dívida, e vários outros tipos de instrumentos de depósito sem maturidade especificada que conferem ao depositante o direito de efectuar levantamentos de fundos a qualquer momento e sem encargos.

4.2.1.3. Se não for gerida de forma adequada, a vantagem assimétrica que os instrumentos com opções apresentam pode representar um risco significativo, principalmente para quem os vende, uma vez que as opções detidas, tanto as explícitas como as embutidas, são geralmente exercidas em benefício do titular (em desvantagem do vendedor).

4.2.2. Efeitos do Risco de Taxa de Juro

4.2.2.1. Variações nas taxas de juro podem ter impactos negativos tanto nos resultados como no valor económico de uma instituição. Isto deu origem a duas ópticas ou perspectivas distintas, mas complementares, de avaliação da exposição da instituição ao risco de taxa de juro.

4.2.2.2. **Óptica dos Resultados –** Do ponto de vista dos resultados, o foco da análise centra-se no impacto das variações das taxas de juro nos proveitos. Esta é a abordagem tradicional de avaliação do risco de taxa de juro realizada por muitas instituições. Variações nos proveitos representam um ponto focal importante para a análise do risco de taxa de juro, pois a diminuição de proveitos ou as perdas absolutas podem pôr em causa a estabilidade financeira de uma instituição através do impacto no capital ou na redução dos níveis de confiança no mercado.

4.2.2.3. Em face disso, a componente dos proveitos objecto de maior atenção é a margem financeira, i.e., a diferença entre os juros e proveitos equiparados e juros e custos equiparados. Este enfoque reflecte tanto a importância da margem financeira no produto bancário como a sua ligação directa (e facilmente compreensível) às variações nas taxas de juro. No entanto, uma vez que as instituições se envolvem largamente em actividades que geram comissões e outras margens complementares, tem-se tornado mais comum adoptar um enfoque mais amplo centrado no resultado líquido global. Mesmo as fontes tradicionais da margem complementar, como por exemplo as comissões decorrentes do processamento de operações, estão a tornar-se mais sensíveis a variações das taxas de juro. Este aumento na sensibilidade deve levar a gestão de uma instituição a considerar uma abordagem mais abrangente dos potenciais efeitos das variações das taxas de juro de mercado nos proveitos da instituição e incorporar esses efeitos nas suas estimativas de proveitos em diferentes cenários de taxas de juro.

4.2.2.4. **Óptica do Valor Económico –** Variações nas taxas de juro de mercado podem, igualmente, afectar o valor económico dos activos, passivos e elementos extrapatrimoniais de uma instituição. Assim, a sensibilidade do valor económico da instituição às flutuações das taxas de juro deve merecer a devida consideração por parte do órgão de administração e pela gestão das instituições.

4.2.2.5. O valor económico de um instrumento representa a avaliação do valor presente dos seus fluxos de caixas líquidos expectáveis, descontados para reflectir taxas de mercado. Analogamente, o valor económico de uma instituição pode ser entendido como o valor presente dos fluxos de caixa líquidos expectáveis, definido como fluxos de caixa expectáveis dos activos deduzido dos fluxos de caixa expectáveis dos passivos e adicionado dos fluxos de caixa líquidos expectáveis em operações extrapatrimoniais. Neste sentido, o efeito, do ponto de vista do valor económico, reflecte outra abordagem da sensibilidade do património líquido da instituição às flutuações das taxas de juro.

[9] Risco da curva de rendimentos ou da taxa de Juro.

4.2.2.6. Perdas Embutidas - Os efeitos nos resultados e no valor económico discutidos anteriormente centram-se na forma como as variações nas taxas de juro futuras podem afectar o desempenho financeiro da instituição. Ao avaliar o nível de exposição ao risco de taxa de juro, uma instituição deve considerar o impacto que as taxas de juros passadas podem ter no desempenho futuro. Em particular, os instrumentos que não estejam contabilizados ao justo valor podem conter ganhos e perdas embutidas devido a movimentos passados das taxas de juro. Estes ganhos e perdas podem, ao longo do tempo, reflectir-se nos resultados da instituição.

4.3. Fiscalização pelo Órgão de Administração e Gestão de Topo

4.3.1. A fiscalização eficaz pelo órgão de administração e gestão de topo de uma instituição é crucial para uma gestão sólida do risco de taxa de juro. É importante que estes órgãos estejam conscientes das suas responsabilidades em relação à gestão do risco de taxa de juro e desempenhem adequadamente as suas funções de fiscalizar e gerir esta categoria de risco.

4.3.2. Fiscalização pelo Órgão de Administração:

4.3.2.1. Compete, em especial, ao órgão de administração:

a) Aprovar as estratégias de negócio e políticas que governam ou influenciam o risco de taxa de juro da instituição;

b) Rever os objectivos gerais da instituição em relação ao risco de taxa de juro;

c) Fornecer orientações claras sobre o nível aceitável de risco de taxa de juro para a instituição;

d) Aprovar políticas que estabeleçam linhas de autoridade e responsabilidade para gestão das exposições ao risco de taxa de juro;

e) Assegurar que a gestão de topo possua conhecimentos adequados, seja competente e capaz de dirigir as actividades relacionadas com a taxa de juro e de tomar as medidas necessárias para identificar, medir, acompanhar e controlar esta categoria de risco;

f) Assegurar que a administração ou um comité específico passe periodicamente em revista informação suficientemente pormenorizada e actual que permita compreender e avaliar o desempenho da gestão de topo no acompanhamento e controlo deste risco, tendo em conta as políticas aprovadas pelo órgão de administração. Tal revisão deve ser efectuada regularmente, e com maior frequência ainda, em instituições com posições significativas em instrumentos complexos; e

g) Assegurar que a administração ou um comité específico reavalia periodicamente as políticas de gestão de risco de taxa de juro, bem como a estratégia global que afecta as exposições da instituição a esta categoria de risco.

4.3.3. Fiscalização pela Gestão de Topo:

4.3.3.1. A gestão de topo tem a responsabilidade de:

a) Desenvolver e estabelecer políticas e procedimentos para gerir o risco de taxa de juro no dia-a-dia, bem como a longo prazo;

b) Manter linhas claras de autoridade e responsabilidade para gerir e controlar o risco de taxa de juro;

c) Implementar estratégias de forma a limitar os riscos associados a cada uma das estratégias específicas e assegurar o cumprimento ou observância das leis e regulamentos;

d) Manter padrões para avaliar posições e medir o desempenho;

e) Manter limites apropriados para a tomada de riscos;

f) Manter sistemas e padrões adequados para a medição do risco;

g) Manter um sistema detalhado de reporte e um processo de revisão da gestão do risco de taxa de juro;

h) Manter um sistema de controlo interno e padrões éticos eficazes;

i) Assegurar que os relatórios de risco de taxa de juro para gestores de topo fornecem informação agregada, bem como detalhes suficientes para permitir que esta avalie a sensibilidade da instituição às variações nas condições do mercado e outros factores importantes de risco;

j) Rever periodicamente as políticas e procedimentos de gestão de risco de taxa de juro da instituição para assegurar que os mesmos se mantêm adequados e robustos;

k) Assegurar que as análises e actividades de gestão de riscos relacionadas com o risco de taxa de juro são realizadas por pessoal competente, com conhecimentos técnicos e experiência consistentes com a natureza e âmbito das actividades da instituição; e

l) Assegurar que haja pessoal suficiente para gerir as actividades relacionadas com o risco e acomodar temporariamente a ausência de pessoal-chave.

4.4. Políticas, Procedimentos e Limites

4.4.1 Políticas e Procedimentos

4.4.1.1. As instituições devem possuir políticas e procedimentos claramente definidos e consistentes com a sua natureza, complexidade e actividades para limitar e controlar o risco de taxa de juro.

4.4.1.2. As políticas e procedimentos devem fixar:

a) Linhas de responsabilidade e de prestação de contas sobre decisões de gestão de risco de taxa de juro;

b) Estratégias de cobertura de risco; e

c) Parâmetros quantitativos que definem o nível apropriado e aceitável de risco para a instituição. Nos casos em que se mostrar apropriado, tais limites devem ser especificados para certos tipos de instrumentos, carteiras e actividades.

4.4.1.3. As políticas devem ainda identificar:

a) Os tipos de instrumentos e actividades que a instituição pode empregar ou desenvolver, sendo uma forma de comunicar o nível de tolerância de risco da instituição;

b) Os instrumentos permitidos, identificando-os quer pelos nomes, quer pelas características, devendo descrever os propósitos ou objectivos para os quais podem ser usados (por exemplo, assumir e ou cobrir posições); e

c) O conjunto de procedimentos institucionais para aquisição de instrumentos específicos, gestão de carteiras, bem como para o controlo da exposição agregada ao risco de taxa de juro.

4.4.1.4. Todas as políticas de risco de taxa de juro devem ser revistas no mínimo anualmente e actualizadas sempre que for necessário.

4.4.1.5. A gestão da instituição deve definir procedimentos e aprovações específicos para a aplicação de excepções às políticas, limites e autorizações.

4.4.1.6. Os produtos e serviços que sejam novos para a instituição devem ser submetidos a um escrutínio cuidadoso antes da sua introdução, de modo a assegurar que a instituição compreenda as características de risco de taxa de juro e as incorpore no processo de gestão de riscos.

4.4.1.7. Ao analisar se um produto ou actividade introduz novos elementos de exposição ao risco, a instituição deve estar atenta ao facto de que alterações na maturidade dos instrumentos, refixação das taxas de juro ou das condições de reembolso podem afectar materialmente as características do risco de taxa de juro do produto.

4.4.1.8. Antes de introduzir um produto novo, um instrumento de cobertura, uma estratégia de tomada de posições, a gestão da instituição deve assegurar que estejam em prática políticas e procedimentos adequados. O órgão de administração ou o comité por este designado deve aprovar os principais instrumentos de cobertura ou iniciativas de gestão de risco antes da sua implementação.

4.4.1.9. As propostas para a introdução de novos produtos ou estratégias de negócio devem consagrar os seguintes aspectos:

a) Descrição do produto ou da estratégia relevante;

b) Identificação dos recursos necessários para estabelecer uma gestão sólida e eficaz do risco de taxa de juro associado ao produto ou actividade;

c) Análise da razoabilidade das actividades propostas em relação à situação financeira global da instituição e dos níveis de capital; e

d) Políticas e procedimentos a serem usados para medir, acompanhar e controlar os riscos associados ao produto ou actividade proposta.

4.4.2. Limites

4.4.2.1. As instituições devem pôr em prática directrizes que as orientem na tomada de riscos, com vista a manter a exposição ao risco de taxa de juro dentro dos parâmetros pré-determinados, tendo presente possíveis alterações.

4.4.2.2. As directrizes atrás referidas devem fixar limites de risco de taxa de juro aplicáveis às diferentes carteiras (individualmente), actividades ou linhas de negócios, e ajustadas à dimensão, complexidade e níveis de adequação do capital da instituição, bem como à sua capacidade de medição e gestão de riscos.

4.4.2.3. Um sistema de limites apropriado deve permitir à gestão da instituição o controlo das exposições ao risco de taxa de juro e o acompanhamento das exposições existentes face aos níveis de tolerância pré-estabelecidos. Os limites devem assegurar que as posições que excedam os níveis pré-determinados recebem uma atenção imediata por parte da gestão.

4.4.2.4. Os limites de risco de taxa de juro devem ser aprovados pelo órgão de Administração e reavaliados periodicamente.

4.4.2.5. As excepções aos limites devem ser prontamente comunicadas à gestão de topo. Devem existir políticas claras sobre como a gestão de topo deve ser informada e as acções que devem ser tomadas em tais casos.

4.4.2.6. As directrizes devem especificar se os limites são absolutos ou se, em certas circunstâncias, claramente definidas, as ultrapassagens podem ser toleradas durante um curto período de tempo. Neste contexto, o carácter conservador dos limites seleccionados pode ser um factor importante.

4.5. Mensuração, Acompanhamento e Sistema de Informação de Gestão de Risco

4.5.1. As instituições devem possuir sistemas de medição do risco de taxa de juro consistentes com a sua complexidade e leque de actividades, para avaliar o efeito das alterações das taxas de juro nos resultados e no valor económico. Esses sistemas devem fornecer medidas concretas dos níveis reais de exposição ao risco de taxa de juro de uma instituição e ser capazes de identificar qualquer exposição excessiva que possa surgir.

4.5.2. Os sistemas de medição devem:

a) Avaliar todos os riscos de taxa de juro materiais associados aos activos, passivos e elementos extrapatrimoniais de uma instituição;

b) Usar técnicas de medição de riscos e conceitos financeiros geralmente aceites; e

c) Possuir pressupostos e parâmetros bem documentados.

4.5.3. Como princípio geral, é desejável que qualquer sistema de medição incorpore exposições de risco de taxa de juro decorrentes de todas as actividades da instituição, incluindo as fontes do trading como as que não sejam do trading. Isto não exclui a utilização de diferentes sistemas de medição e abordagens de gestão de riscos para as diversas actividades; no entanto, a gestão deve ter uma visão integrada do risco de taxa de juro em todos os produtos e segmentos de actividade.

4.5.4. O sistema de medição de risco de taxa de juro de uma instituição deve consagrar todas as fontes materiais desta categoria de risco, incluindo exposições ao risco de refixação, da *yield curve*, de opção e de indexante. Em muitos casos, as características de taxas de juros das posições significativas de uma instituição dominam o seu perfil global de risco. Apesar de todas as posições da instituição terem de receber tratamento adequado, os sistemas de medição devem avaliar tais concentrações com especial rigor. Os sistemas de medição de risco de taxa de juro devem também proporcionar tratamento rigoroso daqueles instrumentos que podem afectar significativamente a posição global de uma instituição, ainda que não representem uma concentração principal. Os instrumentos significativos com opções embutidas ou explícitas devem receber especial atenção.

4.5.5. Existe um conjunto variado de técnicas disponíveis para medir exposições ao risco de taxa de juro, tanto dos resultados como do valor económico de uma instituição. A complexidade das mesmas varia de simples cálculos para simulações estáticas usando posições existentes, a técnicas de modelação dinâmicas altamente sofisticadas que reflectem potenciais negócios futuros.

4.5.6. As técnicas mais simples para medir a exposição ao risco de taxa de juro de uma instituição começam com a construção de um quadro (de maturidades ou de refixação de taxas) que faz a distribuição das posições activas, passivas e extrapatrimoniais sensíveis a variações da taxa de juro por «bandas temporais» (*time band*) de acordo com as suas maturidades (taxas fixas) ou período residual até a próxima refixação (taxas variáveis).

4.5.7. Estes quadros podem ser utilizados para gerar indicadores simples da sensibilidade dos proveitos e do valor económico ao risco de taxa de juro. Quando esta abordagem é empregue para determinar o nível actual do risco de taxa de juro dos proveitos designa-se por *Gap Analysis*. O tamanho do «gap» para uma determinada banda temporal – i.e., activos menos passivos mais exposições extrapatrimoniais que refixam ou maturam dentro da mesma banda temporal – dá uma indicação da exposição ao risco de refixação de taxa de juro de uma instituição.

4.5.8. O quadro de maturidade ou refixação de taxa pode, igualmente, ser usado para avaliar o efeito das variações das taxas de juro no valor económico de uma instituição através da aplicação de ponderadores de sensibilidade a cada banda temporal. Em geral, tais ponderadores são baseados em estimativas da *Duration* dos activos e passivos que se enquadram em cada banda temporal, onde a duration é uma medida da variação percentual do valor económico da posição que ocorre dada uma ligeira variação no nível das taxas de juro. Os ponderadores baseados na duration podem ser usados em combinação com os quadros de maturidades/refixação, com vista a fornecer uma aproximação elementar da variação do valor económico de uma instituição que pode ocorrer dado um conjunto específico de alterações nas taxas de juro de mercado.

4.5.9. Os sistemas mais sofisticados de medição de risco de taxa de juro incluem técnicas de simulação. As técnicas de simulação tipicamente envolvem avaliações detalhadas dos potenciais efeitos das alterações nas taxas de juro, nos resultados e no valor económico através da simulação do possível comportamento futuro das taxas de juro e seu impacto nos fluxos de caixa. Em simulações estáticas, somente os fluxos de caixas que resultam das posições correntes dos activos e elementos extrapatrimoniais são avaliados.

4.5.10. Numa abordagem de simulação dinâmica, a simulação é assente em pressupostos detalhados acerca do comportamento futuro das taxas de juro e das alterações esperadas no curso das actividades da instituição ao longo do período em causa. Estas técnicas mais sofisticadas permitem uma interacção dinâmica do fluxo de pagamentos e das taxas de juro e uma melhor captação do efeito das opções embutidas ou explícitas.

4.5.11. Independentemente do sistema de medição, a utilidade de cada técnica depende da validade dos pressupostos assumidos e da exactidão das metodologias básicas empregues para modelar as exposições ao risco de taxa de juro.

4.5.12. Ao desenhar sistemas de medição do risco de taxa de juro, as instituições devem assegurar que o grau de detalhe acerca da natureza das posições sensíveis a variações da taxa de juro é comensurado à complexidade e risco intrínseco nessas posições. Por exemplo, usando a técnica *gap analysis*, a exactidão da medição do risco da taxa de juro depende, em parte, do número de bandas temporais nas quais as posições são agregadas. Certamente que a agregação das posições/fluxos de caixa em bandas temporais largas implica, de alguma forma, perda de precisão. Na prática, a instituição deve avaliar a relevância da perda potencial de precisão ao determinar a medida de agregação e simplificação a ser incorporada na abordagem de medição.

4.5.13. Estimativas de exposição ao risco de taxa de juro quer sejam ligadas aos resultados, quer ao valor económico, utilizam, de alguma forma, previsões do provável comportamento futuro das taxas de juro. Para fins de gestão de riscos, as instituições devem incorporar variações suficientemente grandes nas taxas de juro de modo a consagrar os riscos atinentes às suas posições.

4.5.14. As instituições podem consagrar o uso de múltiplos cenários, incluindo efeitos potenciais em alterações nas relações entre as taxas de juro (i.e., risco da *yield curve* e o risco de indexante) bem com alterações no nível geral das taxas de juro.

4.5.15. Para determinar prováveis variações na taxa de juro, as instituições podem empregar técnicas de simulação. Análises estatísticas podem, igualmente, desempenhar um papel importante na avaliação dos pressupostos em relação ao risco de indexante ou da «curva de rendimentos».

4.5.16. Ao avaliar os resultados dos sistemas de medição de risco, é necessário que:

a) Os pressupostos subjacentes ao sistema sejam claramente compreendidos pelos gestores de risco e gestão de topo;

b) As técnicas sofisticadas de simulação sejam usadas cuidadosamente para que não se tornem "caixas negras", produzindo números que aparentam ser exactos quando na verdade não o são, nos casos em que os seus parâmetros e pressupostos específicos são revelados;

c) Os pressupostos principais sejam reconhecidos pela gestão de topo e gestores de riscos e revistos, pelo menos, numa base anual;

d) Os pressupostos principais sejam bem documentados e o seu alcance compreendido; e

e) Os pressupostos empregues na avaliação da sensibilidade dos instrumentos complexos (com maturidade incerta) à taxa de juro sejam sujeitos a uma documentação e revisão rigorosa.

4.6. Testes de Esforço

4.6.1. O sistema de medição de risco deve permitir uma avaliação real do efeito, na instituição, de alterações adversas nas condições de mercado. O teste de esforço deve ser concebido de modo a fornecer informação sobre o tipo de condições susceptíveis de tornar vulneráveis as posições ou estratégias da instituição, podendo, deste modo, adaptar-se às características de risco da instituição.

4.6.2. Os cenários possíveis de esforço podem incluir:

a) Mudanças bruscas no nível geral das taxas de juro;

b) Alterações na relação entre as principais taxas de juro de mercado (risco de indexante);

c) Alterações na inclinação e formato da curva de rendimentos (*yield curve risk*);

d) Alteração na liquidez dos principais mercados financeiros ou na volatilidade das taxas de juro de mercado; e

e) Condições em que os principais parâmetros e pressupostos do negócio perdem consistência.

4.6.3. As instituições devem realizar testes de esforço aos pressupostos e parâmetros empregues para os instrumentos ilíquidos e os de maturidade contratual não especificada para obter um entendimento do seu perfil de risco. Na realização de testes de esforço deve-se prestar atenção especial aos instrumentos ou mercados onde existam concentrações, na medida em que tais posições podem ser mais difíceis de liquidar ou compensar em situações de esforço. As instituições devem considerar cenários extremos em complemento aos eventos mais prováveis.

4.6.4. A gestão e o órgão de administração da instituição devem rever periodicamente o modelo e os resultados dos testes de esforço, e assegurar que são postos em prática planos de contingência apropriados.

4.7. Sistema de Informação de Gestão

4.7.1. As instituições devem ter um sistema de informação de gestão preciso, informativo e tempestivo, para gerir exposições ao risco de taxa de juro e informar a gestão, bem como para auxiliar na observância das políticas aprovadas pelo órgão de administração.

4.7.2. O relato das medidas de risco deve ser regular, devendo comparar, de forma clara, as exposições actuais com os limites fixados nas políticas. Outrossim, previsões anteriores ou estimativas de risco devem ser comparados com os resultados observados (reais) para identificar quaisquer inconsistências na modelação.

4.7.3. Os relatórios que apresentam detalhes sobre exposições ao risco de taxa de juro da instituição devem ser revistos pelo órgão de administração de forma regular. Embora os tipos de relatório preparados para o órgão de administração e para outros níveis de gestão possam variar em função do perfil de risco de taxa de juro da instituição, os mesmos devem, no mínimo, conter:

a) Resumos da exposição agregada da instituição ao risco de taxa de juro;

b) Grau de cumprimento das políticas e limites da instituição;

c) Principais pressupostos (por exemplo, comportamento dos depósitos sem maturidade e informações sobre pagamentos antecipados);

d) Resultados dos testes de esforço incluindo os que avaliam a perda de consistência dos parâmetros e pressupostos principais; e

e) Resumo das constatações das revisões das políticas de taxas de juro, procedimentos e a adequação dos sistemas de medição de risco, incluindo quaisquer constatações dos auditores internos e externos ou de outro revisor independente.

4.8. Controlos Internos

4.8.1. As instituições devem possuir sistemas de controlo interno adequados para assegurar a integridade do processo de gestão de risco de taxa de juro. Estes controlos devem ser parte integrante do sistema global de controlo interno da instituição. Os mesmos devem promover:

a) Operações eficazes e eficientes;
b) Relato financeiro e regulamentar fiável; e
c) Cumprimento das leis, regulamentos e políticas institucionais relevantes.

4.8.2. Um sistema eficaz de controlo interno para risco de taxa de juro deve assegurar a existência de:

a) Um forte ambiente de controlo;
b) Um processo adequado para a identificação e avaliação do risco;
c) Ferramentas de controlo adequadas tais como políticas, procedimentos e metodologias; e
d) Um sistema eficaz de informação de gestão.

4.8.3. As instituições devem ter as suas funções ou áreas funcionais de medição, acompanhamento e controlo de risco revistas regularmente por contrapartes independentes tais como auditor interno ou externo. É essencial que qualquer revisor independente assegure que o sistema de medição de risco da instituição é suficiente para captar todos elementos materiais de risco de taxa de juro, quer resultem dos elementos patrimoniais, quer das actividades extrapatrimoniais.

4.8.4. Ao efectuar a avaliação, o revisor deve considerar os seguintes aspectos:

a) A quantidade do risco de taxa de juro, por exemplo:
i. O grau da sensibilidade ao preço de diversos produtos;
ii. A vulnerabilidade dos resultados e do capital às variações diversas nas taxas de juro, incluindo alterações na curva de rendimentos; e
iii. A exposição dos resultados e do valor económico a várias outras formas de risco de taxa de juro, incluindo o risco de indexante e o de opção.

b) A qualidade de gestão da taxa de juro, por exemplo:
i. Existência (ou não) de um sistema interno adequado de medição em função da natureza, âmbito e complexidade das actividades da instituição;
ii. Existência (ou não) de uma unidade de controlo responsável pelo desenvolvimento e administração das funções de medição, acompanhamento e controlo de riscos;
iii. Grau de envolvimento do órgão de administração e gestão de topo no controlo de riscos;
iv. Existência de políticas, controlos e procedimentos relativos ao risco de taxa de juro devidamente documentados e respeitados; e
v. Existência de pessoal adequado para conduzir o processo de gestão de risco.

4.8.5. Nos casos em que a revisão independente é efectuada por um auditor interno, as instituições devem ter a função de medição, acompanhamento e controlo periodicamente revista por um auditor externo.

4.8.6. Linhas de Responsabilidade e Autoridade:

4.8.6.1. As instituições devem assegurar que haja segregação de funções nos elementos-chave do processo de gestão de risco, com vista a reduzir potenciais conflitos de interesse.

4.8.6.2. A gestão deve assegurar ainda que haja salvaguardas suficientes para minimizar o potencial de que indivíduos que iniciam as operações de tomada de risco influenciem, de forma inapropriada, as principais funções de controlo do processo de gestão de riscos, tais como o (*i*) desenvolvimento e execução de políticas e procedimentos, (*ii*) o reporte de riscos à gestão de topo e (*iii*) a realização de operações do *back-office*.

4.8.6.3. A natureza e âmbito de tais mecanismos de segurança devem estar de acordo com a dimensão e estrutura da instituição. Estes devem ser comensurados com o volume e complexidade de risco de taxa de juro incorrido pela instituição e a complexidade das suas transacções e compromissos.

5. Directrizes de Gestão do Risco de Taxa de Câmbio

5.1 Introdução

5.1.1. O risco da taxa de câmbio consiste na possibilidade de ocorrência de impactos negativos nos resultados ou no capital, devido a movimentos adversos nas taxas de câmbio, provocados por alterações no preço de instrumentos que correspondam a posições abertas em moeda estrangeira ou pela alteração da posição competitiva da instituição devido a variações significativas das taxas de câmbio. Isto envolve o risco de liquidação que surge quando uma instituição incorre em perdas financeiras devido às posições cambiais assumidas tanto na carteira de negociação como na carteira bancária.

5.2. Fiscalização pelo Órgão de Administração e Gestão do Topo

5.2.1. O órgão de administração e a gestão do topo detêm, em última instância, a responsabilidade de compreender a natureza e o nível de risco cambial assumidos pela instituição e a subsequente gestão do mesmo.

5.2.2. A fiscalização pelo órgão de administração pode ser delegada a um subcomité apropriado, como o Comité de Gestão de Activos e Passivos (ALCO – *Asset and Liability Committee*) ou o Comité de Gestão de Risco.

5.2.3. As responsabilidades do órgão de administração e da gestão de topo são:

a) Definir a estratégia de gestão do risco cambial e os níveis de tolerância;
b) Assegurar que são implementados sistemas de gestão de riscos e controlos internos eficazes;
c) Acompanhar as exposições significativas ao risco cambial;
d) Assegurar que as operações cambiais na instituição cumprem com as normas de controlo cambial vigentes;
e) Assegurar que as operações cambiais são suportadas por sistemas de informação de gestão adequados complementares à estratégia de gestão de risco; e
f) Rever regularmente as políticas, procedimentos e limites por moeda em consonância com as mudanças no ambiente económico.

5.3. Políticas e Procedimentos

5.3.1. As instituições devem possuir políticas e procedimentos escritos para identificar, medir e controlar o risco de taxa de câmbio, que sejam consistentes com as estratégias, condições financeiras e níveis de tolerância ao risco da instituição.

5.3.2. As políticas e procedimentos devem ser complementados com ética e observância dos padrões estabelecidos pelos empregados envolvidos na negociação de moeda estrangeira. Devem, igualmente, identificar os riscos de taxa de câmbio inerentes aos serviços e actividades para assegurar que as características de risco sejam percebidas de modo a serem incorporadas nos processos de gestão de risco.

5.3.3. As políticas e procedimentos devem:

a) Definir linhas de responsabilidade e identificar indivíduos ou comités responsáveis por desenvolver estratégias de gestão de risco cambial, tomar decisões de gestão de risco cambial e fazer a fiscalização;

b) Identificar os diferentes tipos de instrumentos financeiros permitidos e estratégias de cobertura de risco;

c) Descrever um conjunto de estratégias de controlo da exposição agregada ao risco de taxa de câmbio da instituição;

d) Definir os limites quantitativos do nível aceitável de risco cambial para a instituição, incluindo limites por moeda, por contraparte, por dealer, limites de concentração e limites de perdas acumuladas (*stop loss*); e

e) Definir procedimentos e condições para lidar com as excepções às políticas, limites e autorizações.

5.4. Identificação, Mensuração, Acompanhamento e Controlo de Riscos

5.4.1. Identificação de Risco

5.4.1.1. As exposições ao risco de taxa de câmbio enquadram-se nas seguintes categorias (estruturais e de negociação):

a) Risco de Conversão – advém de alterações no valor contabilístico pela conversão para a moeda de escrituração das posições abertas em moeda estrangeira, causadas por alterações das taxas de câmbio;

b) Risco de Transacção – surge quando há alterações nas taxas de câmbios entre o momento em que se incorre na obrigação e o momento em que esta é liquidada, afectando consequentemente os fluxos de caixa efectivos; e

c) Risco Económico – Reflecte as alterações do valor actual dos fluxos de caixa esperados de uma instituição em resultado de alterações inesperadas nas taxas de câmbio ou alteração da posição competitiva da instituição devido a variações significativas das taxas de câmbio.

5.4.2. Mensuração do Risco

5.4.2.1. As instituições de crédito devem dispor de sistemas de medição que tomem em conta todas as fontes do risco de taxa de câmbio.

5.4.2.2. Os sistemas de medição devem:

a) Avaliar o efeito de alterações das taxas de câmbio na rentabilidade e no valor económico das instituições;

b) Avaliar todos os riscos cambiais por maturidade, numa base bruta e líquida, decorrentes de toda a gama de posições dos activos, passivos e elementos extrapatrimoniais da instituição;

c) Empregar modelos financeiros reconhecidos ou métodos para medir o risco de opções cambiais;

d) Ser capaz de calcular a sensibilidade dos factores de risco abrangentes com a finalidade de captar a natureza não linear do risco de preço das posições cambiais.

e) Possuir dados correctos e actuais;

f) Incorporar as reavaliações periódicas do justo valor das posições de negociação; e

g) Possibilitar às instituições o acompanhamento, em tempo real, do risco de taxa de câmbio de compensações, de modo a assegurar que os limites de compensação não são excedidos.

5.4.3. Limites de Risco

5.4.3.1. Em complemento à observância dos limites às Posições Cambiais instituídos pelo Banco de Moçambique, as instituições devem dispor de um quadro conceptual abrangente de limites para controlar as posições de risco cambial nos diferentes níveis de reporte.

5.4.3.2. No mínimo, as instituições devem ter os seguintes limites de operações cambiais:

a) Limites de posição cambial aberta, por moeda, para as quais as instituições têm uma exposição material, ao longo do dia ou de um dia para o outro (*overnight*).

b) Limites globais de posições cambiais abertas para posições assumidas durante o dia e de um dia para o outro;

c) Limites de posições cambiais abertas por cada centro a partir do qual a instituição realiza operações;

d) Limites para perdas acumuladas e/ou limites para desencadear a intervenção da gestão; e

e) Limites para o risco de compensação de todas as contrapartes.

5.4.3.3. Os limites devem ser revistos anualmente ou com maior frequência de acordo com as variações do ambiente de negócios.

5.4.4. Testes de Esforço

5.4.4.1. As instituições de crédito devem realizar testes de esforço das suas posições cambiais, para avaliar o impacto de alterações das taxas de câmbio na rendibilidade e valor económico dos seus capitais próprios. No estabelecimento de cenários de esforço, devem considerar-se os efeitos de alterações significativas de movimentos das taxas de câmbio (incluindo reduções acentuadas na liquidez) de uma determinada moeda.

5.4.4.2. Os resultados dos testes de esforço devem ser incorporados na revisão das estratégias de negócio, políticas e limites do risco de taxa de câmbio. Os pressupostos usados no modelo de teste de esforço devem ser claramente documentados e revistos continuamente, de forma a reflectirem as alterações no ambiente de negócio.

5.4.5. Acompanhamento e Controlo do Risco

5.4.5.1. As instituições devem instituir processos de acompanhamento do risco de taxa de câmbio, avaliar o desempenho das estratégias de risco, políticas e procedimentos no alcance dos seus objectivos globais. A função ou departamento de acompanhamento deve ser independente das unidades ou áreas que assumem riscos e deve reportar directamente à gestão de topo ou órgão de administração.

5.4.5.2. O *middle-office* deve desempenhar a função de revisão do risco relativamente às actividades do dia-a-dia. Compete ainda a esta unidade:

a) Preparar relatórios para a gestão de topo bem como para o ALCO; e

b) Reconciliar regularmente posições assumidas pelos traders para assegurar que estas estão dentro dos limites atribuídos.

5.4.5.3. Por ser uma função altamente especializada, o *middle-office* deve possuir pessoal com experiência e conhecimentos relevantes.

5.4.5.4. As instituições devem ter sistemas de informação de gestão que forneçam informação correcta e actual. Reavaliações periódicas e frequentes às taxas correntes de mercado devem permitir o acompanhamento dos ganhos ou perdas na carteira de posições cambiais da instituição.

5.4.6. Relatório de Risco

5.4.6.1. Os tipos de relatórios variam dependendo do perfil global de risco cambial da instituição de crédito. No mínimo, os relatórios devem conter:

a) Exposições ao risco de taxa de câmbio individual e agregada;
b) Informação sobre o grau de aderência aos limites e políticas; e
c) Constatações da actividade de revisão das políticas e procedimentos do risco cambial, incluindo as constatações dos auditores internos/externos.

5.5. Controlo Interno e Auditorias Independentes

5.5.1. As instituições devem realizar revisões periódicas das suas unidades ou funções de controlo interno e processos de gestão de risco cambial. Tais revisões devem ser conduzidas por partes independentes da função ou unidade a ser revista.

5.5.2. As revisões devem, entre outros, assegurar:

a) Exactidão e integralidade do registo de todas as operações;
b) Segregação efectiva de deveres entre as unidades de *trading*, compensação/liquidação e contabilidade; e
c) Eficácia e exactidão dos relatórios de ultrapassagem de limites e outras excepções.

5.5.3. Deve-se prestar maior atenção às irregularidades nos lucros e perdas, tendências ou padrões anormais no *trading* e desenquadramentos (excessos) frequentes dos limites. Os auditores internos devem assegurar que tais incidentes sejam devidamente acompanhados. Quaisquer questões relativas ao controlo da área do trading devem ser adequada e atempadamente encaminhadas à gestão de topo.

5.5.4. As instituições devem responder prontamente às constatações sobre eventuais violações dos procedimentos estabelecidos e assegurar que existam procedimentos adequados para lidar com as deficiências ou irregularidades detectadas pelas funções de controlo de riscos, auditores internos ou externos e autoridades de supervisão.

5.5.5. A Auditoria interna e outras funções de controlo de risco devem ser apetrechadas por pessoal especializado, com experiência e autoridade para rever as operações comerciais.

6. Directrizes de Gestão do Risco Operacional

6.1. Introdução

6.1.1. O risco operacional é a probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de falhas na análise, processamento ou liquidação das operações, de fraudes internas e externas, de a actividade ser afectada devido à utilização de recursos em regime de *outsourcing*, da existência de recursos humanos insuficientes ou inadequados ou da inoperacionalidade das infra-estruturas.

6.1.2. A globalização, a par do crescimento da inovação de produtos e serviços financeiros, está a tornar as actividades das instituições bancárias, assim como os seus perfis de risco (isto é, o nível de risco subjacente às actividades da instituição e/ou categorias de risco) mais complexos. Como consequência desses desenvolvimentos, o risco operacional torna-se mais evidente.

6.1.3. O risco operacional é um termo que tem uma variedade de sentidos no sector bancário e em toda indústria de serviços financeiros, daí que as instituições bancárias possam optar por adoptar as suas próprias definições. Seja qual for a definição exacta, uma clara compreensão pelas instituições de crédito do que se entende por risco operacional é fundamental para a gestão eficaz e controlo desta categoria de risco. É também importante que a definição considere a gama completa de elementos materiais do risco operacional que uma instituição enfrenta e inclua as mais importantes causas de perdas operacionais graves.

6.1.4. O risco operacional pode advir de diversas fontes, como por exemplo:

a) Pessoas: Actos que podem resultar em perdas substanciais incluem fraudes (como a prestação de relatórios falseados), furtos de empregados, insider dealings, roubos, falsificação, emissão de cheques sem cobertura e pirataria informática. Alguns dos factores contribuintes são:
i. Falta de habilidades e conhecimentos adequados;
ii. Formação e desenvolvimento insuficientes;
iii. Esquemas de compensação e incentivos inapropriadamente alinhados;
iv. Falta de entendimento dos padrões ou expectativas de desempenho; e
v. Controlo inadequado de recursos humanos (incluindo a supervisão e segregação de funções incompatíveis).

b) Processos Internos e Sistemas: Interrupções no negócio e falhas nos sistemas de hardware e software, problemas de telecomunicações, interrupções de serviços de utilidade pública, erros de entrada de dados, falhas na gestão de colaterais, atribuição de acesso não autorizado às contas de clientes, fraco desempenho e litígios com fornecedores e prestadores de serviços são exemplos de risco operacional resultante de processos internos e sistemas. Alguns dos factores contribuintes são:
i. Destruição de activos físicos;
ii. Tecnologia inadequada ou obsoleta;
iii. Falta de documentação apropriada;
iv. Falta ou inadequação de políticas, procedimentos e controlos;
v. Sistema de informação de gestão pobre; e
vi. Falta ou inadequação de planos de contingência.

c) Eventos Externos: Terrorismo, vandalismo, terramotos, fogo e inundações.

6.1.5. O risco operacional difere de outros riscos na medida em que normalmente não é directamente tomado em troca de uma recompensa esperada, mas ocorre no curso normal da actividade bancária, e isso afecta o processo de gestão de risco. Ao mesmo tempo, a incapacidade de gerir adequadamente o risco operacional pode resultar numa inexactidão do perfil de risco da instituição e expô-la a perdas significativas.

6.2. Fiscalização pelo Órgão de Administração e Gestão de Topo

6.2.1. A incapacidade de compreender e gerir o risco operacional, presente em todas as transacções e actividades, pode aumentar a probabilidade de ignorar e perder o controlo de alguns riscos. O órgão de administração e a gestão de topo são responsáveis pela criação de uma cultura organizacional que atribui elevada prioridade à gestão eficaz do risco operacional e aderência a um adequado controlo operacional.

6.2.2. A gestão do risco operacional é mais eficaz quando a cultura da instituição destaca padrões elevados no comportamento ético em todos os níveis da entidade. O órgão de administração e a gestão de topo devem promover uma cultura organizacional que estabeleça, através de acções e palavras, as expectativas de integridade de todos os trabalhadores na condução de negócios.

6.2.3. Fiscalização pelo Órgão de Administração:

6.2.3.1. O órgão de administração tem, em última instância, responsabilidade pelo nível de risco operacional tomado pela instituição.

6.2.3.2. Compete ao órgão de administração:

a) Aprovar o quadro institucional para gerir o risco operacional como um risco distinto para a segurança e solidez da instituição.

b) Estabelecer uma estrutura de gestão capaz de implementar o quadro conceptual de gestão do risco operacional da instituição. Uma vez que o estabelecimento de forte controlo interno é um aspecto importante da gestão do risco operacional, é de particular importância que o órgão de administração estabeleça linhas claras de responsabilidades de gestão, prestação de contas e reporte.

c) Fornecer à gestão de topo directrizes claras quanto aos princípios subjacentes ao quadro conceptual e aprovar as respectivas políticas desenvolvidas pela gestão de topo.

d) Rever regularmente o quadro conceptual para:

i. Garantir que a instituição esteja a gerir os riscos operacionais associados a novos produtos, serviços ou sistemas; e

ii. Avaliar as melhores práticas de gestão de riscos operacionais na indústria adequadas às actividades, sistemas e processos da instituição.

6.2.3.3. O quadro conceptual de risco operacional deve:

a) Basear-se numa definição adequada, que claramente articule o que constitui o risco operacional na instituição;

b) Abranger a apetência e a tolerância da instituição face ao risco operacional, tal como especificado através de políticas de gestão deste risco;

c) Priorizar as actividades de gestão de risco operacional, incluindo a dimensão e a forma como o risco operacional é transferido fora da instituição;

d) Incluir políticas da instituição que definam uma abordagem para identificação, avaliação, acompanhamento e controlo/mitigação do risco; e

e) Articular os processos-chave que a instituição precisa ter para gerir o risco operacional.

6.2.3.4. Os graus de formalidade e sofisticação do quadro conceptual de gestão do risco operacional da instituição devem ser compatíveis com o perfil de risco global.

6.2.3.5. Para evitar conflitos de interesse, deve haver separação de responsabilidades e linhas de reporte entre as funções de controlo de risco operacional, linhas de negócio e funções de apoio.

6.2.4. Fiscalização pela Gestão de Topo:

6.2.4.1. Compete à gestão de topo:

a) Traduzir o quadro conceptual de gestão do risco operacional instituído pelo órgão de administração em políticas, processos e procedimentos específicos que podem ser implementados nas diferentes unidades de negócio;

b) Atribuir claramente autoridade, responsabilidade e linhas de reporte para encorajar e manter a responsabilização;

c) Garantir que os recursos necessários estejam disponíveis para gerir eficazmente o risco operacional;

d) Avaliar a adequação do processo de fiscalização, à luz dos riscos intrínsecos às políticas da unidade de negócio;

e) Assegurar que as actividades da instituição sejam realizadas por pessoal qualificado, com a necessária experiência, capacidade técnica e acesso aos recursos, e que o pessoal responsável em acompanhar e impor o cumprimento das políticas de risco da instituição tenha autoridade e seja independente das unidades que supervisiona;

f) Assegurar que a política de gestão do risco operacional da instituição seja transmitida a todos os colaboradores em todos os níveis e unidades expostas ao risco operacional; e

g) Assegurar que as políticas de remuneração da instituição sejam coerentes com a apetência pelo risco. Políticas de remuneração que premeiam funcionários que não observam as políticas enfraquecem o processo de gestão de riscos.

6.2.4.2. Deve ser dada especial atenção à qualidade dos controlos dos documentos e à forma como as transacções são executadas. Em particular, as políticas, processos e procedimentos relacionados com altas tecnologias de processamento de elevados volumes de transacções devem ser bem documentados e divulgados a quem de direito.

6.3. Políticas, Procedimentos e Limites

6.3.1. A instituição deve estabelecer uma política de gestão do risco operacional que inclua, no mínimo:

a) A estratégia traçada pelo órgão de administração;

b) Os sistemas e procedimentos para instituir um quadro conceptual eficaz de gestão de risco operacional; e

c) A estrutura da função de gestão do risco operacional e as atribuições e responsabilidades das pessoas envolvidas.

6.3.2. A política deve estabelecer um processo que garanta que quaisquer operações novas ou modificadas, tais como novos produtos ou conversão de sistemas, sejam avaliadas em relação ao risco operacional intrínseco antes de serem implementadas.

6.3.3. A política deve ser documentada e aprovada pelo órgão de administração e ser revista e actualizada anualmente, de forma a garantir que continue a reflectir o ambiente no qual a instituição opera.

6.3.4. Cabe à gestão de topo assegurar que a política seja comunicada e compreendida em toda a instituição.

6.3.5. A política deve prever ainda a gestão dos riscos associados à terceirização (subcontratação) de actividades. A terceirização de actividades pode reduzir o perfil de risco da instituição através da transferência de actividades para outras instituições mais especializadas para gerir os riscos associados a tais actividades. No entanto, a utilização de terceiros pela instituição não isenta a responsabilidade do órgão de administração e da gestão de topo de assegurar que as actividades terceirizadas sejam executadas com segurança, em conformidade com as normas aplicáveis. Os acordos de terceirização devem estatuir uma clara repartição de responsabilidades entre os prestadores de serviços e a instituição. Além disso, as instituições devem gerir os riscos residuais associados aos acordos de terceirização, incluindo rescisão de serviços.

6.3.6. Plano de Continuidade de Negócio e de Recuperação de Desastres:

6.3.6.1. Por razões que podem estar fora do seu controlo, um evento grave pode resultar na incapacidade de a instituição cumprir algumas ou todas as suas obrigações, especialmente quando as suas infra-estruturas física, de telecomunicações, ou

de tecnologia de informação tiverem sido danificadas ou tornadas inacessíveis. Isto pode, por sua vez, resultar em significativas perdas financeiras para a instituição, bem como em perturbações no sistema financeiro, através de canais como o sistema de pagamentos.

6.3.6.2. As instituições devem estabelecer planos de recuperação de desastres e de continuidade das operações que levem em conta diferentes tipos de cenários possíveis aos quais a instituição possa ser vulnerável, tendo em conta a dimensão e complexidade das suas operações.

6.3.6.3. As instituições devem identificar processos críticos de negócio, incluindo aqueles em que haja dependência de fornecedores externos, para os quais uma rápida retomada é essencial. Para estes processos, as instituições devem identificar mecanismos alternativos para retomar os serviços em caso de falhas. Deve ser dada especial atenção à capacidade de restaurar registos electrónicos ou físicos que sejam necessários para o reatamento do negócio. Sempre que tais registos tenham cópia de segurança em uma instalação remota, ou quando as operações da instituição tiverem de ser transferidas para um novo local, todo o cuidado deve ser tomado para que estes locais estejam à distância suficiente para minimizar o impacto do risco de indisponibilidade dos registos primários e de backup, bem como do par de instalações.

6.3.6.4. Os planos de continuidade de negócio e de recuperação de desastres devem ser revistos, no mínimo anualmente, para se manter a consistência com as operações correntes e estratégias de negócio da instituição. Além disso, estes planos devem ser testados periodicamente para garantir que possam ser executados na eventualidade de uma severa interrupção da actividade.

6.3.6.5. As instituições devem seguir as directrizes específicas de gestão de continuidade de negócio emitidas, em documento separado, pelo Banco de Moçambique.

6.4. Identificação do Risco, Avaliação, Acompanhamento, Controlo e Gestão de Sistemas de Informação

6.4.1 Identificação e Avaliação de Risco

6.4.1.1. As Instituições devem identificar e avaliar o risco operacional intrínseco a todos os produtos, serviços, processos e sistemas significativos. Além disso, antes de introduzirem novos produtos, serviços, processos e sistemas, o risco operacional intrínseco deve ser sujeito a procedimentos adequados de avaliação.

6.4.1.2. A identificação do risco é fundamental para o desenvolvimento posterior de um sistema viável de acompanhamento e controlo do risco operacional. A identificação eficaz do risco considera tanto factores internos (por exemplo, a estrutura da instituição, a natureza das suas actividades, a qualidade dos recursos humanos, mudanças organizacionais e rotatividade de empregados) como factores externos (por exemplo, mudanças na indústria e avanços tecnológicos) que podem afectar adversamente a realização dos objectivos da instituição.

6.4.1.3. Uma vez identificados os riscos potencialmente mais adversos, as instituições devem avaliar o seu grau de vulnerabilidade perante os mesmos. Uma avaliação eficaz dos riscos permite que a instituição compreenda melhor o seu perfil de risco e, com maior eficácia, direccione os recursos para a sua gestão.

6.4.1.4. As instituições podem utilizar as seguintes ferramentas para identificação e avaliação de risco operacional:

a) Auto-avaliação ou Avaliação de Risco: uma instituição avalia os processos que sustentam as suas operações contra uma biblioteca de ameaças e vulnerabilidades potenciais e considera os seus impactos. Este processo é conduzido internamente e muitas vezes incorpora listas de verificação e/ou palestras (*workshops*) para identificar os pontos fortes e fracos do ambiente do risco operacional. Um processo similar, denominado Auto-avaliação de Controlos de Risco (RCSA), avalia o risco intrínseco (o risco antes da consideração dos controlos), a eficácia do ambiente de controlo e o risco residual (a exposição ao risco após consideração dos controlos). Os Scorecards[10] sobre as RCSA, por exemplo, fornecem um meio de traduzir avaliações qualitativas em métricas quantitativas que atribuem pontuação relativa dos diferentes tipos de exposição ao risco operacional. A classificação pode se referir aos riscos intrínsecos, bem como aos controlos para os mitigar. Adicionalmente, os scorecards podem ser usados para alocar capital económico para áreas de negócio em função do desempenho na gestão e controlo de vários aspectos do risco operacional.

b) Mapeamento de Risco: neste processo, diversas unidades de negócios, fluxos de processos organizacionais ou funções são mapeados pelo tipo de risco. Este exercício pode revelar áreas de fraqueza e ajudar a priorizar acções subsequentes de gestão.

c) Indicadores de Risco e de Desempenho: os indicadores de risco e de desempenho são métricas e/ou estatísticas, muitas vezes financeiras, que podem fornecer informação sobre a posição de risco de uma instituição. Os indicadores de risco, geralmente designados de Indicadores Chave de Risco (KRI), são usados para acompanhar os principais factores de exposição associados aos principais riscos. Os indicadores de desempenho, geralmente designados de Indicadores Chave de Desempenho (KPI), fornecem informações sobre o estado dos processos operacionais, que por seu turno podem fornecer informações sobre vulnerabilidades operacionais, falhas e perdas potenciais. Estes indicadores tendem a ser revistos numa base periódica (por exemplo, mensal ou trimestral) para alertar as instituições das mudanças que podem ser indicadores de risco. Tais indicadores podem incluir o número de transacções mal sucedidas, taxas de rotatividade do pessoal e da frequência e/ou gravidade dos erros e omissões. Podem ser indexados limites a estes indicadores, de tal modo que, quando ultrapassados, possam alertar a gestão sobre as áreas de potenciais problemas.

d) Análises de Cenário: a análise de cenários é um processo de obtenção de opinião dos gestores séniores do negócio e de risco para identificar potenciais eventos de risco operacional e avaliar o seu impacto. Este processo representa uma ferramenta eficaz de identificação das principais fontes de risco operacional e de controlos ou soluções de mitigação para a sua gestão. Dada a subjectividade do processo de análise de cenário, é essencial o estabelecimento dum quadro robusto de governação para assegurar sua integridade e consistência.

e) Mensuração: A utilização de dados sobre o historial de perdas duma instituição pode prover informações relevantes para a avaliação da sua exposição ao risco operacional, que, por sua vez, permitem o desenvolvimento de políticas para mitigar tal risco.

[10] *Scorecards* – metodologia de medição e gestão de desempenho.

Uma forma eficaz de fazer bom uso dessas informações é através do estabelecimento de um quadro para a captação e registo sistemático da frequência, severidade e demais informação relevante concernente a eventos de perdas individuais. Complementarmente, as instituições podem combinar dados de perdas internas com dados de perdas externas (de outras instituições), análises de cenários e factores de avaliação de risco.

f) Análise Comparativa: a análise comparativa consiste na comparação de resultados de várias ferramentas de avaliação para fornecer uma visão mais abrangente do perfil de risco operacional da instituição. Por exemplo, a comparação da frequência e severidade de dados internos com RCSA pode ajudar a instituição a determinar se os processos de auto-avaliação funcionam de forma eficaz. Os dados de cenários podem ser comparados a dados internos e externos para um melhor entendimento da severidade da exposição a eventos potenciais de risco.

6.4.2. Acompanhamento do Risco e Sistema de Informação de Gestão

6.4.2.1. As instituições devem implementar um processo para acompanhar regularmente perfis de risco operacional e exposição a perdas significativas. Deve haver apresentação regular de informações pertinentes à gestão de topo e ao órgão de administração, que asseguram a gestão pró-activa do risco operacional.

6.4.2.2. Um processo de acompanhamento eficaz é essencial para a gestão adequada do risco operacional. O acompanhamento regular das actividades pode oferecer a vantagem de rápida detecção e correcção de deficiências nas políticas, processos e procedimentos de gestão do risco operacional. A rápida detecção e tratamento destas anomalias pode reduzir substancialmente a frequência e/ou gravidade dos eventos de natureza operacional.

6.4.2.3. Adicionalmente, para o acompanhamento de eventos de natureza operacional, as instituições devem identificar indicadores adequados que proporcionem pré-aviso do aumento do risco de perdas futuras. Esses indicadores (frequentemente referidos como principais indicadores de risco ou indicadores de pré-aviso) devem estar focalizados no futuro e podem reflectir potenciais fontes de risco operacional, tais como rápido crescimento, introdução de novos produtos, rotação de empregados, quebra nas transacções, interrupção do sistema e assim por diante. Quando os limites estiverem directamente ligados a esses indicadores, um processo de acompanhamento eficaz pode ajudar a identificar riscos materiais relevantes de forma transparente e permitir que a instituição actue sobre esses riscos de forma adequada.

6.4.2.4. A frequência de acompanhamento deve reflectir os riscos envolvidos, bem como a natureza das mudanças no ambiente operacional. O acompanhamento deve ser parte integrante das actividades da instituição. Os resultados destas actividades de acompanhamento deverão ser incluídos na gestão corrente e nos relatórios da administração, bem como análises de conformidade realizados pela auditoria interna e pela função de gestão do risco.

6.4.2.5. A gestão de topo deve receber relatórios periódicos das respectivas áreas, tais como unidades de negócios, grupo de funções, unidade de gestão de risco operacional e da auditoria interna.

6.4.2.6. Os relatórios de risco operacional devem conter informação financeira, operacional e de compliance, bem como informações externas disponíveis no mercado, sobre eventos e condições relevantes para a tomada de decisão. Os relatórios devem ainda reflectir plenamente todas as áreas problemáticas identificadas e devem motivar a acção correctiva e tempestiva relativamente a questões pendentes.

6.4.2.7. Para garantir a utilidade e fiabilidade desses relatórios, a gestão deve verificar regularmente a actualidade, precisão e relevância dos sistemas de comunicação e de controlos internos em geral. A gestão pode usar também relatórios elaborados por fontes externas (auditores, supervisores) para avaliar a utilidade e fiabilidade dos relatórios internos. Os relatórios devem ser analisados com vista a melhorar o desempenho de gestão dos riscos correntes, bem como o desenvolvimento de novas políticas de gestão de riscos, procedimentos e práticas.

6.4.2.8. O órgão de administração deve receber informação de alto nível, que lhe permita compreender o perfil de risco operacional e focalizar atenção na materialidade e implicações na estratégia do negócio.

6.4.3. Mitigação/Controlo de Risco

6.4.3.1. As instituições devem ter políticas, processos e procedimentos para controlar e/ou mitigar os riscos operacionais. As mesmas devem igualmente rever periodicamente os limites de risco, estratégias de controlo e ajustar os seus perfis de risco operacional em conformidade com as estratégias adequadas, à luz do seu perfil global de risco e apetência.

6.4.3.2. As actividades de controlo são concebidas para atender os riscos operacionais que tenham sido identificados. Para todos os riscos operacionais significativos que tenham sido identificados, a instituição deve decidir se usa os procedimentos adequados para os controlar e/ou mitigar. Para os riscos que não podem ser controlados, a instituição deve decidir se os assume, se reduz o volume de negócio envolvido ou se se retira completamente dessa actividade.

6.4.3.3. Dependendo da dimensão e natureza da actividade, as instituições devem estar cientes do potencial impacto nas suas operações e nos seus clientes de eventuais deficiências dos serviços prestados por terceiros, ou prestadores de serviços intragrupo, incluindo tanto falhas operacionais como potenciais falhas do negócio ou de incumprimento da contraparte externa. O órgão de administração e a gestão de topo devem assegurar que as expectativas e as obrigações de cada parte sejam claramente definidas, entendidas e cumpridas.

6.4.3.4. A dimensão da responsabilidade e capacidade financeira da parte externa para compensar a instituição por erros, negligências e outras falhas operacionais devem ser explicitamente considerados como parte da avaliação dos riscos. Inicialmente, as instituições devem realizar testes (due dilligence) e acompanhar as actividades prestadas por terceiros, especialmente aqueles sem experiência do ambiente regulado da indústria bancária, bem assim rever este processo (incluindo as reavaliações de due dilligence), numa base regular. Para as actividades críticas, a instituição pode necessitar de planos de contingência, incluindo a disponibilidade de parceiros externos, os custos e recursos necessários para mudar de parceiros externos, no muito curto prazo.

6.4.3.5. Alguns riscos operacionais significativos têm pouca probabilidade de ocorrer, mas potencialmente têm impacto financeiro muito elevado. Além disso, nem todos os eventos de natureza operacional podem ser controlados (por exemplo, desastres naturais). Ferramentas ou programas de mitigação de riscos podem ser usados para reduzir a exposição, a frequência e/ou a gravidade de tais ocorrências. Por exemplo, apólices de seguro podem ser utilizadas para “externalizar” o risco de perdas em eventos de "baixa frequência e alta gravidade" que podem ocorrer em resultado de acontecimentos como reclamações de terceiros resultantes de erros e omissões, perdas físicas de valores mobiliários, fraude de empregados ou terceiros, e desastres naturais.

6.4.3.6. Contudo, as ferramentas de mitigação de riscos devem ser vistas como complementares, não substitutos de um minucioso controlo interno do risco operacional. Havendo mecanismos para rapidamente reconhecer e corrigir erros do risco operacional pode-se reduzir, em grande medida, a exposição. Especial atenção deve ser dada à dimensão em que os instrumentos de mitigação de riscos, tais como seguros, realmente reduzem o risco ou o transferem para outro sector ou área de negócio, ou até mesmo criam um novo risco (por exemplo, legal ou de contraparte).

6.4.3.7. Investimentos em tecnologias de processamento adequadas e na segurança de tecnologia da informação também são importantes para a mitigação de risco. No entanto, as instituições devem estar cientes de que o incremento da automatização pode transformar eventos de natureza operacional de frequência elevada e pouca gravidade, em baixa frequência e elevada gravidade. Este último pode ser associado a perdas ou interrupção prolongada de serviços causadas por factores internos ou fora do controlo imediato da instituição (por exemplo, factores externos). Tais problemas podem causar graves dificuldades e comprometer a capacidade da instituição de assegurar a condução de principais actividades do seu negócio. As instituições devem, portanto, estabelecer planos de recuperação de desastres e de continuidade do negócio que focalizam este risco.

6.5. Controlo Interno

6.5.1. As instituições devem ter um ambiente de controlo interno robusto que utilize políticas, procedimentos e sistemas de controlo adequados de mitigação de risco e/ou estratégias de transferência. Os sistemas de controlo interno devem ser projectados para fornecer uma razoável garantia de execução de operações de forma eficiente e eficaz, constituir uma salvaguarda do património, produzir relatórios financeiros fiáveis e cumprir a regulamentação aplicável.

6.5.2. Um sistema de controlo interno consiste em cinco componentes, que são parte integrante do processo de gestão de risco: (*i*) ambiente de controlo, (*ii*) avaliação do risco; (*iii*) actividades de controlo; (*iv*) informação e comunicação; e (*v*) actividades de monitoramento.

6.5.3. Os processos e procedimentos de controlo interno devem incluir um sistema para assegurar o cumprimento das políticas. Os principais elementos deste sistema incluem:

a) Revisão ao mais alto nível do progresso da instituição face aos objectivos estabelecidos;

b) Verificação da conformidade com controlos de gestão;

c) Políticas, processos e procedimentos relativos à análise, tratamento e resolução de questões de falta de conformidade;

d) Um mecanismo de aprovações e autorizações documentado para assegurar a responsabilização a um nível apropriado de gestão; e

e) Relatório de verificação de excepções aprovadas relativamente aos limites estabelecidos, substituições de gestão e outros desvios de política.

6.5.4. Embora o quadro conceptual formal de políticas e procedimentos devidamente documentado seja crucial, é importante reforçá-lo por meio de uma forte cultura de controlo, que promova boas práticas de gestão de riscos. Tanto o órgão de administração como a gestão de topo são responsáveis por estabelecer uma forte cultura de controlo interno em que as actividades de controlo são parte integrante das actividades regulares da instituição. Controlos que são parte integrante das actividades regulares possibilitam respostas rápidas às mudanças de condições e evitam custos desnecessários.

6.5.5. O risco operacional pode ser mais acentuado quando as instituições se envolvem em novos serviços ou desenvolvem novos produtos (em especial se esses serviços ou produtos não são compatíveis com a principal estratégia de negócio), entram em mercados desconhecidos ou participam em negócios que estão geograficamente distantes da sede. Incumbe, portanto, às instituições assegurar que seja dada atenção especial às actividades de controlo interno, incluindo revisão de políticas e procedimentos para incorporar tais condições.

6.5.6. As instituições devem dispor de uma auditoria interna qualificada para verificar se as políticas e procedimentos operacionais têm sido implementados de forma eficaz. O órgão de administração (directamente ou através do comité de auditoria) deve garantir que o âmbito e a frequência dos programas de auditoria sejam adequados às exposições ao risco. A auditoria deve periodicamente certificar se o quadro conceptual de gestão do risco operacional da instituição é aplicado com efectividade em toda instituição.

6.5.7. Na medida em que a função de auditoria estiver envolvida na supervisão do quadro conceptual de gestão do risco operacional, a administração deve assegurar que a sua independência seja mantida. Esta independência pode ser comprometida se a função de auditoria estiver directamente envolvida no processo de gestão do risco operacional. A função de auditoria pode prestar um valioso contributo para os responsáveis pela gestão do risco operacional, mas não deve ela própria ter responsabilidades directas na gestão do risco operacional. Na prática, reconhece-se que a auditoria em algumas instituições (em especial as mais pequenas) pode ter responsabilidade inicial pelo desenvolvimento de um programa de gestão de risco operacional. Se este for o caso, as instituições devem verificar se a responsabilidade do dia-a-dia da gestão de risco operacional é transferida de forma atempada.

6.5.8. Um sistema de controlo interno eficaz requer também que haja segregação adequada de funções e que ao pessoal não sejam atribuídas responsabilidades que possam criar conflito de interesse. A atribuição de funções conflituosas a indivíduos ou equipas pode permitir-lhes ocultar perdas, erros ou executar acções inapropriadas. Assim, as áreas de potenciais conflitos de interesse devem ser identificadas, minimizadas e sujeitas a um controlo independente e cuidadosa revisão.

6.5.9. Para além da segregação de funções, as instituições devem garantir que outras práticas internas adequadas ao controlo do risco operacional sejam estabelecidas. São exemplo dessas práticas:

a) Definição clara das competências para o processo de aprovações;

b) Acompanhamento estrito da aderência aos limites de risco estabelecidos;

c) Manutenção de protecções nos acessos e utilização de activos e registos da instituição;

d) Garantia de que o pessoal tenha competência e formação adequada;

e) Identificação de linhas de negócio ou produtos cujo retorno aparenta estar fora das expectativas razoáveis (por exemplo, nos casos em que uma actividade supostamente de baixo risco e com baixa margem gera rendimentos elevados que podem colocar em questão o estrito seguimento dos controlos internos nessas transacções);

f) Verificação e reconciliação regular de contas e transacções; e

g) Estabelecimento de políticas de férias que prevêem que os gestores e funcionários que ocupam funções relevantes se ausentem (em licença disciplinar) por um período não inferior a duas semanas consecutivas.

7. Directrizes de Gestão do Risco Estratégico

7.1. Introdução

7.1.1. O risco estratégico é a possibilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de decisões estratégicas inadequadas, da deficiente implementação das decisões ou da incapacidade de resposta a alterações do meio envolvente (interno e externo) da instituição. Este risco é uma função da compatibilidade dos objectivos estratégicos duma instituição, das estratégias de negócio desenvolvidas, dos recursos empregues para alcançar tais objectivos estratégicos e da qualidade de implementação dos mesmos.

7.1.2. O risco estratégico pode surgir de duas fontes principais: factores de risco internos e externos.

7.1.3. Os factores externos de risco são difíceis e por vezes impossíveis de controlar por parte da instituição e afectam ou impedem a concretização dos objectivos determinados no plano estratégico. Tais factores incluem:

a) Concorrência: o plano estratégico e o plano de negócios devem estar em linha com a concorrência actual e futura. Factores de competitividade devem ser tomados em consideração nas práticas de pricing da instituição e no desenvolvimento de novos produtos;

b) Alterações no nicho de mercado: as alterações demográficas e de perfis de consumo podem afectar a base de clientes, os proveitos e as fontes de financiamento de capital duma instituição;

c) Alterações tecnológicas: uma instituição pode enfrentar riscos decorrentes de alterações tecnológicas, porque os seus concorrentes podem desenvolver sistemas e serviços mais eficientes a custos baixos. A instituição deve assegurar-se de que o seu nível tecnológico é suficiente para reter a sua base de clientes;

d) Factores económicos: as condições económicas globais, regionais ou nacionais afectam o nível de lucros duma instituição. Assim, avaliações e acompanhamento contínuos de tendências e previsões são necessários; e

e) Regulamentação: alterações nas leis e regulamentos do supervisor, das autoridades fiscais, das autoridades locais e de outras agências autorizadas podem afectar a implementação do plano estratégico e de negócios estabelecidos para alcançar os objectivos institucionais e podem requerer ajustamentos aos planos de modo a assegurar a conformidade.

7.1.4. Os factores internos de risco são controlados pela instituição, no entanto podem afectar a implementação do plano estratégico. Tais factores incluem:

a) Estrutura organizacional: para uma boa implementação dos planos estratégico e de negócios e alcance dos objectivos globais de maneira mais eficiente, é importante que a instituição estabeleça uma estrutura organizacional compreensível, consistente com os planos e que previna conflitos de interesse entre os administradores, gestores, accionistas e colaboradores;

b) Processos e procedimentos de trabalho: estes factores permitem uma implementação tempestiva e precisa dos planos de negócios. O órgão de administração e a gestão de topo devem estabelecer responsabilidades e directrizes claras, políticas e procedimentos de modo a prevenir deficiências nos controlos internos;

c) Pessoal: o sucesso da realização dos planos estratégicos e de negócios depende do conhecimento, experiência e visão do órgão de administração, gestão de topo e colaboradores. Os colaboradores devem possuir perícia e treinamento necessários para a condução das suas tarefas de maneira eficiente e eficaz. A ausência dos necessários níveis de competência do pessoal pode incrementar exposições ao risco, prejudicar o desempenho financeiro e danificar a reputação da instituição;

d) Informação: a existência de informação adequada, precisa e tempestiva fornece um entendimento claro da instituição e do seu nicho de mercado, afectando de forma positiva a formulação dos planos estratégico e de negócios, assim como as decisões da gestão; e

e) Tecnologia: os sistemas tecnológicos devem servir e suportar transacções complexas e as necessidades de todos os clientes, assim como manter a competitividade e suporte de novas linhas de negócio.

7.1.5. Os factores de mitigação de risco ajudam na implementação de planos estratégicos. Tais factores incluem a existência dum órgão de administração qualificado, preparação adequada dos planos estratégico e de negócios, a qualidade de pessoal e sua formação contínua, um sistema eficaz de gestão de risco, acesso adequado a informação e introdução tempestiva e eficiente de novos produtos e serviços.

7.1.6. O risco estratégico, se não for adequadamente gerido, pode se manifestar gradualmente em diferentes unidades duma instituição. Este risco possui a tendência para se imiscuir na 'cultura institucional', pode não ser facilmente reconhecido e pode ainda afectar a posição da instituição no mercado.

7.2. Fiscalização pelo Órgão de Administração e Gestão de Topo

7.2.1. Fiscalização pelo Órgão de Administração

7.2.1.1. O órgão de administração é responsável por fornecer a direcção estratégica da instituição, que deve constar do plano estratégico. A visão e missão da instituição devem reflectir a direcção que a mesma pretende seguir a médio e longo prazos.

7.2.1.2. Um plano estratégico é um documento que reflecte a missão e os objectivos estratégicos duma instituição, geralmente por um período de pelo menos três anos. Um bom plano estratégico deve ser claro, consistente com os objectivos, flexível e ajustável às alterações na envolvente. Um plano estratégico deve conter, no mínimo, o seguinte:

a) Análise do ambiente externo no qual a instituição opera, incluindo a análise PESTEL;

b) Revisão crítica do desempenho institucional, incluindo a análise SWOT;

c) Metas e objectivos estratégicos institucionais;

d) Descrição do sistema institucional de gestão de risco;

e) Missão, metas e planos operacionais para cada uma das unidades operacionais; e

f) Projecção quantitativa de demonstrações financeiras para o período planejado.

7.2.1.3. Na base do plano estratégico aprovado, o órgão de administração deve, entre outros:

a) Estabelecer a estrutura de governação da instituição, que deve indicar de forma clara as linhas de responsabilidade e de prestação de contas;

b) Estabelecer os canais de comunicação apropriados à efectiva implementação dos planos;

c) Aprovar as políticas de gestão do risco estratégico;

d) Assegurar que a gestão de topo é suficientemente qualificada e experiente; e

e) Garantir que o plano estratégico é implementado de forma eficaz e que é revisto, pelo menos, anualmente.

7.2.1.4. O órgão de administração deve receber relatórios relevantes, precisos e tempestivos, que possam ser utilizados de forma apropriada no processo de tomada de decisões. O mesmo deve estar adequadamente informado sobre as dinâmicas económicas, do mercado e sobre as condições de competitividade da instituição.

7.2.2. Fiscalização pela Gestão de Topo

7.2.2.1. A gestão da instituição é responsável pela implementação dos planos estratégicos e de negócios aprovados. A criação de condições adequadas à implementação, incluindo o desenho e a adopção de política e procedimentos de gestão do risco estratégico, assim como de deveres e responsabilidades das diferentes unidades, é o passo mais importante visando a eficaz implementação dos planos estratégico e de negócios. É também de importância crucial, na efectiva implementação do plano estratégico, a arquitectura da infra-estrutura interna, incluindo uma estrutura organizacional eficaz, pessoal qualificado, processo de orçamentação robusto, disponibilidade de recursos, sistema de informação de gestão eficaz e tempestivo, e sistemas de acompanhamento e controlo que realizem os objectivos de negócio de modo eficiente e eficaz.

7.2.2.2. A gestão deve traduzir os objectivos estratégicos em objectivos operacionais atingíveis, estabelecendo prioridades em função da sua importância estratégica. Os objectivos estratégicos devem ser desdobrados em pedaços menores e atribuídos às diferentes unidades de negócio dentro da estrutura da instituição.

7.2.2.3. Os planos e objectivos devem ser compatíveis com a natureza, dimensão e complexidade da instituição e das actividades que desempenha, bem como o nicho de mercado da sua actuação.

7.3 Políticas, Procedimentos e Limites

7.3.1. A gestão do risco estratégico deve ser baseada em política, procedimentos e limites compatíveis com a política global de gestão de riscos na instituição.

7.3.2. A política de gestão do risco estratégico deve fornecer directrizes gerais de gestão do risco estratégico. Portanto, são expectáveis os seguintes elementos mínimos:

a) Definição do risco estratégico;
b) Fontes de risco estratégico (factores internos e externos de risco);
c) Factores mitigadores de risco estratégico;
d) Modo de gestão do risco estratégico; e
e) Tolerância aceitável de exposição ao risco estratégico.

7.4. Mensuração, Acompanhamento e Sistemas de Informação de Gestão de Riscos

7.4.1. Identificação, Mensuração e Acompanhamento do Risco Estratégico

7.4.1.1. Um processo eficaz de medição e acompanhamento é essencial para uma adequada gestão do risco estratégico. A identificação e medição deste risco podem ser feitas por via do planeamento estratégico. O plano estratégico, os planos operacionais e orçamento devem ser consistentes com o âmbito de negócio, complexidade, ambiente externo e factores internos da instituição, incluindo o seu tamanho e recursos.

7.4.1.2. A gestão de topo deve participar no processo de planeamento de forma plena e, cuidadosamente, decidir na base da informação disponível quanto à viabilidade e adequação dos planos de negócio e estratégico. A gestão deve assegurar uma boa comunicação e cooperação entre todos os colaboradores e departamentos envolvidos no processo de planeamento estratégico.

7.4.1.3. As metas dos planos operacionais devem ser consistentes com o plano estratégico e objectivos globais da instituição, assim como com a alocação orçamental. A instituição deve estabelecer metas (por exemplo, em relação à qualidade da carteira de crédito) consistentes com a sua capacidade, quota de mercado e ambiente competitivo.

7.4.1.4. As instituições devem avaliar periodicamente o seu desempenho actual em relação ao plano estratégico de modo a acompanhar e ajustar os seus planos de forma apropriada e consistente com as alterações. A avaliação deve ser mensurável e com a frequência adequada.

7.4.1.5. Para avaliar a adequação do acompanhamento e reportes do risco estratégico, bem como do sistema de informação da instituição, cada unidade de negócio deve considerar os factores seguintes:

a) Conteúdos dos relatórios submetidos para o suporte à tomada de decisões de alto nível;
b) Frequência dos reportes;
c) O estilo de apresentação da informação deve facilitar a compreensão; e
d) Os relatórios devem enfatizar os riscos materiais e as estratégias estabelecidas para os contrariar.

7.4.2. Sistema de Informação de Gestão

7.4.2.1. Para um acompanhamento eficaz do risco estratégico, deve ser estabelecido um Sistema de Informação de Gestão (SIG) robusto. Tal SIG deve auxiliar a instituição na implementação dos planos estratégicos através de:

a) Disponibilização, colecção e processamento de dados;
b) Redução de custos operacionais;
c) Melhoramento da comunicação entre os colaboradores; e
d) Identificação e medição tempestivas do risco estratégico e geração de dados e relatórios para uso pelo órgão de administração e gestão.

7.4.2.2. A eficácia do acompanhamento do risco depende da capacidade de identificação e medição de todos os factores de risco e deve ser suportada por um SIG apropriado, preciso e tempestivo, permitindo a realização de análises e tomada de decisões. Consequentemente, a gestão deve desenvolver e actualizar o seu sistema de informação para identificar e medir riscos de forma precisa e tempestiva.

7.4.2.3. O SIG deve ser consistente com a complexidade e diversidades de operações de negócio da instituição. Por exemplo, as instituições que tenham muitas transacções complexas devem possuir um sistema de reporte e um sistema de acompanhamento de risco que possa medir o nível global de risco. Deve possuir a capacidade de colectar, armazenar e recuperar tanto dados internos como externos, incluindo dados financeiros, sobre as condições económicas, sobre a concorrência, requisitos tecnológicos e regulamentares.

7.4.2.4. O SIG deve assegurar um acompanhamento tempestivo e continuado e o controlo do risco estratégico, bem assim o reporte ao órgão de administração e gestão de topo em relação à implementação do processo de gestão do risco estratégico. Adicionalmente, o SIG deve fornecer dados e informação apropriados sobre as actividades de negócio da instituição.

7.4.2.5. Um SIG eficaz deve suportar adequadamente os objectivos, as metas e o fornecimento de serviços da instituição. Ademais, deve ser capaz de reportar tempestivamente e em formato desejado, e especificar apropriadamente os níveis de acesso à informação.

7.5. Controlo do Risco Estratégico

7.5.1. O órgão de administração e a gestão de topo devem acompanhar as alterações de mercado e os avanços na tecnologia para conceber novos serviços e produtos que mantenham a competitividade da instituição e permitam uma resposta atempada às necessidades dos clientes.

7.5.2. No entanto, o fornecimento de novos serviços e produtos pode incrementar o risco para a instituição, caso não sejam tomadas medidas apropriadas. Deste modo, o órgão de administração e a gestão de topo devem formular um plano estratégico para todos os produtos novos.

7.5.3. De modo a cumprir de forma plena o plano estratégico, as instituições devem:

a) Rever o desempenho da gestão de topo em relação às metas estabelecidas pelo menos uma vez por ano. A revisão deve determinar se o desempenho é satisfatório e se a gestão é capaz de alcançar as metas;

b) Estabelecer uma política ou plano de sucessão para a gestão. Tal política ou plano deve ser revista/o pelo menos anualmente, ser consistente com a estrutura organizacional e com os termos de referência dos postos, e cobrir formação necessária e qualificações mínimas para cada posto e carreira profissional;

c) Acompanhar e controlar o desempenho dos acordos de *outsourcing*;

d) Estabelecer directrizes e métodos de compensação para a gestão e diversos colaboradores. A compensação deve ser apropriada à robustez financeira da instituição; e

e) Estabelecer um plano de formação e um orçamento adequado para a sua execução. Adicionalmente, devem estabelecer planos de retenção dos colaboradores que possuam conhecimento e entendimento apropriados sobre o negócio e operações da instituição.

8. Directrizes de gestão de risco de compliance

8.1. Introdução

8.1.1. O Risco de Compliance é a possibilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de violações ou a não conformidade com leis, regulamentos, contratos, códigos de conduta, práticas instituídas ou princípios éticos, bem como interpretação incorrecta das leis em vigor ou regulamentos. As instituições são expostas ao risco de compliance devido às relações com um grande número de *stakeholders* (accionistas, reguladores, clientes, etc.) e autoridades fiscais e locais.

8.1.2. O risco de compliance pode traduzir-se em sanções de carácter legal ou regulamentar, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais. Pode ainda traduzir-se na redução da reputação decorrente de uma percepção negativa da imagem da instituição por parte dos *stakeholders*.

8.1.3. As leis e regulamentos a serem cumpridos pelas instituições possuem várias fontes, incluindo legislação primária, regras e normas estabelecidas pelos legisladores e os supervisores do mercado, convenções, códigos de boas práticas promovidos pelas associações industriais e códigos de conduta aplicáveis ao pessoal ou colaboradores das instituições. Por conseguinte, o risco de compliance ultrapassa o que é juridicamente vinculativo e abarca os mais amplos padrões de integridade e conduta ética.

8.1.4. O risco de compliance é difícil de medir, mas pode ser definido, entendido e controlado dentro da capacidade e prontidão da instituição para enfrentar casos de incumprimento. Este risco pode ocorrer de forma deliberada ou não.

8.1.5. As instituições, com vista a mitigação do risco de compliance, devem tomar acções apropriadas que incluem: (*i*) reduções das exposições de fontes de risco de compliance; (*ii*) um processo adequado de gestão de risco; e (*iii*) designação de uma efectiva função de compliance.

8.1.6. As instituições devem identificar as fontes de risco de compliance, sendo as mais comuns as seguintes:

a) Violações ou não conformidade com as leis e regulamentos prescritos;

b) Falta de cumprimento de obrigações contratuais e inadequada documentação legal;

c) Identificação inadequada dos direitos e responsabilidades entre as instituições e clientes;

d) Reclamações de clientes e outras contrapartes;

e) Dano contra interesses de terceiros;

f) Envolvimento em lavagem de dinheiro, violação das regras de tributação, falsificação e danos causados pelos colaboradores não autorizados no sistema (*computer hacking*), seus intermediários e clientes; e

g) Conhecimento limitado e resposta tardia da administração na implementação da gestão de risco legal e reputacional.

8.2. Fiscalização pelo Órgão de Administração e Gestão de Topo

8.2.1. Fiscalização pelo Órgão de Administração

8.2.1.1. O órgão de administração deve compreender a natureza e o nível do risco de compliance a que a instituição está exposta e como o seu perfil de risco se encaixa dentro da estratégia global do negócio. São responsabilidades do órgão de administração:

a) Aprovar a política de compliance, incluindo um documento formal que estabelece de forma permanente e eficaz a função de compliance;

b) Estabelecer uma estrutura de gestão capacitada para a implementação dos processos de gestão de risco de compliance;

c) Garantir que a gestão tome medidas necessárias para identificar, medir, acompanhar e controlar o risco de compliance, e assegurar que a função de compliance seja revista pela auditoria interna;

d) Rever periodicamente as políticas de gestão do risco de compliance para garantir uma devida orientação para a sua gestão efectiva; e

e) Fiscalizar a implementação da política de compliance, incluindo assegurar que questões de compliance são resolvidas de forma eficaz e célere.

8.2.2. Fiscalização pela Gestão de Topo

8.2.2.1. A gestão de topo é responsável pela gestão eficaz do risco de compliance da instituição, por estabelecer políticas escritas que incluam os princípios básicos a serem seguidos pela instituição, bem como explicar os principais processos através dos quais o risco de compliance deve ser identificado e gerido a todos os níveis da organização.

8.2.2.2. A gestão de topo, assistida pela função de compliance, deve:

a) Implementar o sistema de gestão de risco de compliance aprovado pelo órgão de administração;

b) Estabelecer uma estrutura organizacional efectiva de gestão de risco de compliance e manter contactos regulares com os colaboradores directamente afectos ao sector (técnicos e advogados);

c) Identificar e avaliar os principais problemas associados ao risco de compliance enfrentados pela instituição

e os planos para gerir eventuais falhas, bem como a necessidade de quaisquer outras políticas ou procedimentos para lidar com os novos riscos de compliance;

d) Assegurar que o quadro conceptual de gestão do risco de compliance da instituição apresente linhas claras de autoridade, reporte e comunicação;

e) Reportar periodicamente ao órgão de administração ou um comité designado sobre a gestão do risco de compliance;

f) Informar prontamente o órgão de administração ou o comité designado sobre quaisquer falhas relevantes no compliance (por exemplo, falhas que possam redundar em risco significativo de sanções legais e regulamentares, prejuízos financeiros elevados ou perda de reputação);

g) Assegurar que haja recursos humanos com conhecimentos profundos e habilidades para gerir o risco legal e de compliance, e garantir que estejam a trabalhar para proteger a reputação da instituição;

h) Assegurar uma formação permanente, para todas as linhas de negócio, que cubra o cumprimento dos requisitos de compliance, em particular quando a instituição entrar em novos mercados ou oferecer novos produtos;

i) Fornecer garantia razoável, através da função de auditoria, de que todas as actividades e todos os aspectos do risco legal e de compliance estão cobertos pelo processo de gestão de risco;

j) Efectuar, pelo menos uma vez por ano, uma avaliação sobre o risco de compliance; e

k) Rever periodicamente a estrutura conceptual de gestão do risco de compliance, para assegurar que continua adequada e saudável.

8.2.2.3. O âmbito da função de compliance e a necessidade do pessoal (numero e competências) depende da dimensão e da complexidade dos negócios da instituição. Esta função pode ser exercida por diferentes colaboradores em diversos departamentos, devendo os mesmos reportar a um gestor que não tenha responsabilidades directas na tomada de risco.

8.2.2.4. Independentemente da forma como a função de compliance é organizada dentro da instituição, esta deve ser independente, com recursos suficientes e actividades claramente definidas. O gestor responsável não deve estar numa posição de conflito de interesses, ou seja, de executor e fiscalizador.

8.2.2.5. A função de compliance deve estar separada da auditoria interna para garantir que as suas actividades estejam sujeitas a uma revisão independente. No entanto, a função de auditoria deve manter o gestor de compliance informado em relação às suas constatações.

8.2.2.6. O risco de compliance deve ser incluído na metodologia de avaliação de risco da função de auditoria interna, e deve ser estabelecido um programa de auditoria que cubra a sua adequação e eficácia, incluindo uma testagem de controlos compatível com os níveis percebidos de risco.

8.3. Políticas, Procedimentos e Limites

8.3.1. As políticas e procedimentos de gestão do risco de compliance devem ser claramente definidas e coerentes com a natureza e a complexidade das actividades da instituição.

8.3.2. As políticas de compliance devem ser formuladas por escrito e fazer parte da política global de gestão de risco da instituição. As mesmas devem:

a) Determinar com precisão todos os processos e procedimentos importantes para minimizar a exposição ao risco de compliance da instituição;

b) Definir o risco de compliance e objectivos da sua gestão;

c) Estabelecer procedimentos para identificar, avaliar, monitorar, controlar e gerir o risco de compliance;

d) Delimitar as responsabilidades e estabelecer que o órgão de administração e a gestão de topo devem estar plenamente cientes da dimensão dos eventos associados ao compliance;

e) Definir claramente os limites de tolerância de exposição ao risco de compliance;

f) Estabelecer a relação com outras funções de gestão de risco dentro da instituição e com a função de auditoria interna;

g) Definir a forma como as responsabilidades de compliance devem ser repartidas entre os departamentos, nos casos em que a função de compliance é executada por colaboradores de diferentes departamentos; e

h) Estabelecer o direito de acesso às informações necessárias ao desempenho de suas responsabilidades, e do correspondente dever, do pessoal da instituição, de cooperar para fornecer esta informação.

8.4. Mensuração, Acompanhamento e Sistemas de Informação de Gestão

8.4.1. Identificação, Mensuração e Acompanhamento do Risco de Compliance

8.4.1.1. Um processo de medição e acompanhamento eficaz é essencial para a gestão adequada do risco de compliance. A fim de compreender o seu perfil de risco de compliance, a instituição deve identificar as fontes de risco a que está exposta e avaliar a sua vulnerabilidade a esses riscos. Assim, a instituição deve identificar e avaliar o risco de compliance inerente a todos produtos (novos e já existentes), regras e procedimentos, processos internos e actividades.

8.4.1.2. As instituições devem definir métodos adequados para avaliação de cada fonte de risco identificada. Existem vários instrumentos usados para identificar e avaliar o risco de compliance, tais como:

a) Auto-avaliação ou Avaliação de Risco: uma instituição avalia os processos que sustentam as suas operações contra uma biblioteca de ameaças e vulnerabilidades potenciais, e considera os seus impactos. Este processo é conduzido internamente e muitas vezes incorpora listas de verificação para identificar os pontos fortes e fracos do ambiente do risco de compliance;

b) Mapeamento de Risco e Fluxo de Processos: Estas duas ferramentas são amplamente usadas pela auditoria interna e podem ser muito úteis para rever o risco de compliance. Estas ferramentas consistem em resumos gráficos e diagramas que ajudam a instituição a identificar, discutir, compreender e abordar os riscos, por representarem fontes, tipos de riscos e as áreas de negócio envolvidas. A revisão dos mapas de risco e do fluxo de processos pela função de compliance permite que o risco de compliance seja identificado e procedimentos apropriados de mitigação sejam implementados. Os mapas de riscos também contribuem para o desenvolvimento de procedimentos e medidas de mitigação para os riscos identificados; e

c) Indicadores de Risco: são estatísticas ou matrizes que podem fornecer a posição do risco da instituição. Tais indicadores podem incluir o volume e/ou frequência das violações da lei, a frequência das reclamações, número de processos judiciais e frequência

de fraudes (reais ou suspeitas) ou actividades de branqueamento de capitais. Podem fornecer ainda bons incentivos, indexando o risco ao capital necessário para melhoria desejável no cumprimento da função.

8.4.1.3. A instituição deve considerar métodos de medição de risco de compliance usando os indicadores de desempenho, tais como: (*i*) aumento do número de reclamações de clientes; (*ii*) medidas correctivas tomadas contra a instituição; e (*iii*) processos litigiosos por incumprimento de leis e regulamentos.

8.4.1.4. O risco de compliance pode ser medido através de revisões regulares da legislação em diferentes instituições, produtos, serviços e documentação relevante, a fim de assegurar que todos os contratos estão em conformidade com as leis e regulamentos. Esta revisão pode ocorrer em cada operação individualmente ou pode cobrir a adequação legal da documentação e procedimentos padronizados.

8.4.1.5. As instituições são responsáveis por acompanhar o seu perfil de risco de compliance numa base contínua de avaliação de cumprimento dos indicadores definidos, com vista a proporcionar uma gestão antecipada dos riscos. O acompanhamento deve ser parte integrante das actividades da instituição, sendo que os seus resultados devem ser incluídos em relatórios periódicos de gestão.

8.4.1.6. As instituições devem ter processos e procedimentos para o controlo do risco de compliance. Deve haver uma revisão constante do progresso da instituição em relação ao cumprimento dos objectivos legais e verificação do cumprimento de políticas e procedimentos, deveres e responsabilidades definidos.

8.4.2. Sistemas de Informação de Gestão

8.4.2.1. Para um monitoramento eficaz do risco de compliance, as instituições devem ter um SIG robusto, que permita identificar e medir o seu risco de compliance em tempo útil e gerar dados e reportes para gestão.

8.4.2.2. A eficácia de controlo de risco depende da habilidade de identificar e medir todos os factores de risco e deve ser apoiado por um SIG apropriado e preciso que permita a análise e tomada de decisões de forma tempestiva. O SIG deve ser consistente com a complexidade de negócios e operações da instituição.

8.4.2.3. A instituição deve estabelecer uma base de dados dos seus documentos legais que inclua: (*i*) tipos de documentos – contratos, memorandos de entendimento, etc.; (ii) período de validação de documentos; e (*iii*) unidades ou departamentos responsáveis pela documentação.

8.4.3. Controlos Internos

8.4.3.1. As instituições devem possuir sistemas de controlo interno apropriados que integrem a gestão do risco de compliance no processo global de gestão de riscos. A auditoria da gestão do risco de compliance deve ser incorporada no plano anual da função de auditoria interna.

8.4.3.2. A função de auditoria interna, dentro do seu âmbito de actividades, deve cobrir os seguintes aspectos da gestão do risco de compliance:

a) Verificar se as políticas e procedimentos de gestão do risco de compliance foram implementados de forma efectiva na instituição;

b) Avaliar a eficácia dos controlos para a mitigação de fraudes e atentados à reputação;

c) Determinar se a gestão de topo toma as medidas correctivas apropriadas quando são identificadas falhas de compliance;

d) Garantir que o âmbito e frequência do plano de auditoria são apropriados às exposições ao risco;

e) Determinar o nível de conformidade da gestão em relação às normas estabelecidas pelo Banco de Moçambique;

f) Monitorizar os perfis de risco de compliance de forma regular; e

g) Analisar a tempestividade e precisão dos reportes de compliance à gestão de topo e ao órgão de administração.

8.5. Ferramentas de Gestão do Processo de Compliance

8.5.1. Programa de Compliance

8.5.1.1. Para controlar o processo de compliance, as instituições devem preparar um programa ou uma agenda. O programa deve apresentar todos os aspectos e as actividades específicas da função de compliance para um período determinado. Além disso, deve descrever como, quando e por quem o programa será executado.

8.5.2. Sensibilização, Formação e Comunicação

8.5.2.1. A sensibilização, formação e comunicação regular são três elementos essenciais de um sistema eficaz de compliance. A boa sensibilização garante que as pessoas compreendem os temas relevantes. A formação garante que as pessoas que têm de realizar tarefas de compliance compreendem como o seu trabalho se insere num contexto mais alargado e saibam como executar as funções necessárias.

8.5.2.2. A formação em compliance é necessária para aqueles cujo trabalho contém tarefas ou responsabilidades específicas de compliance. O pessoal de compliance deve receber treinamento específico sobre o tipo de técnicas de acompanhamento utilizadas pela auditoria interna. Além disso, podem necessitar de formação em matérias como programação de actividades de compliance, comunicação eficaz, noções de direito e competências de gestão. A resolução de conflitos pode ser também, muitas vezes, uma área de formação útil.

8.5.3. Acompanhamento Eficaz

8.5.3.1. O acompanhamento eficaz tem por objectivo verificar se as pessoas cumprem com os seus termos de referência e assegurar que o sistema funciona adequadamente. Uma parte importante do acompanhamento é identificar as principais áreas potenciais de risco e prestar especial atenção às mesmas, regularmente. Além destes objectivos, o acompanhamento tem como finalidade:

a) Assegurar que os procedimentos críticos estão a ser observados correctamente;

b) Ajudar a resolver dificuldades ainda no estágio inicial; e

c) Servir como um dispositivo de alerta.

8.5.4. Sistema Eficaz de Reclamações

8.5.4.1. Um sistema de reclamações que mantém registos eficazes é parte valiosa do sistema de compliance. Trata-se de um dispositivo de alerta de valor inestimável.

8.5.5. Certificações

8.5.5.1. As certificações consistem num mecanismo que sujeita determinados processos e actividades do negócio à aprovação prévia pela função de compliance, a fim de minimizar riscos nesta área. As certificações possuem as seguintes vantagens:

a) Chamar a atenção para uma possível ocorrência de problemas em áreas que de outra forma não poderiam acontecer num ambiente operacional de actividade intensa;

b) Providenciar cobertura e protecção máxima em áreas em que não é prático efectuar verificações independentes regularmente;

c) Direccionar a mentalidade do pessoal para a observância dos padrões organizacionais e/ou requisitos regulamentares; e

d) Se o sistema de compliance alguma vez tiver que ser reconhecido em tribunal, demonstrar que sempre houve intenção de assegurar que todas as áreas fossem abrangidas, tanto quanto possível, ainda que a cobertura total não seja praticável.

9. Directrizes de Gestão de Risco de Reputação

9.1. Introdução

9.1.1. O risco de reputação consiste na probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de uma percepção negativa da imagem da instituição, fundamentada ou não, por parte de clientes, fornecedores, analistas financeiros, colaboradores, investidores, órgãos de imprensa ou pela opinião pública em geral. Este risco pode afectar a capacidade da instituição de estabelecer novas relações com os seus clientes, contrapartes, colaboradores, investidores, assim como manter os relacionamentos existentes, podendo conduzir não só a perdas financeiras directas e imediatas, mas também a processos litigiosos, erosão da base de clientes, dificuldades na obtenção de recursos ou saída de colaboradores-chave.

9.1.2. O risco de reputação pode emergir em todas as áreas de negócio e tem os seguintes componentes principais:

a) Risco de reputação corporativa: que diz respeito ao desempenho, estratégia e fornecimento de serviços de uma instituição. Este aspecto está intrinsecamente ligado à capacidade de a gestão criar valor para os accionistas e de gerir a valorização do seu capital;

b) Risco de reputação operacional ou de negócio: onde uma actividade, acção ou atitude tomada por uma instituição, suas filiais ou seus colaboradores prejudica a sua imagem com um ou mais dos seus *stakeholders*, resultando em perda de negócios e/ou diminuição significativa do valor da instituição.

9.1.3. O risco de reputação pode emergir a partir de uma variedade de causas, nomeadamente:

a) Fraude e inobservância ou incumprimento dos dispositivos estatutários ou regulamentares;

b) Quebra de sigilo ou falhas na conservação de informações confidenciais dos clientes da instituição através de relacionamentos de terceirização (*outsourcing*);

c) Um volume elevado de reclamações dos clientes ou sanções regulamentares; e

d) Ocorrências em outras categorias de riscos que podem ameaçar a imagem de uma organização e a consideração dos stakeholders.

9.1.4. Categorias de Risco de Reputação:

9.1.4.1. As instituições devem prestar especial atenção a três categorias gerais de eventos ou circunstâncias que dão origem ao risco de reputação. Contudo, as metodologias de gestão empregues devem ser suficientemente abrangentes para cobrir todos os riscos em cada categoria.

a) Risco Intrínseco ou Inerente – Este é o risco que surge a partir de produtos e serviços ou do modo de seu fornecimento, que produz impacto negativo na satisfação do cliente e do mercado. Assim, o risco inerente deriva principalmente de desafios em matéria de risco operacional, controlo de qualidade e satisfação do cliente.

b) Risco do Ambiente de Negócio – Inclui os riscos decorrentes da forma como os negócios são conduzidos (por exemplo, numa área geográfica, industrial, política, social), o que, embora não esteja relacionado com a qualidade dos produtos ou serviços, pode ter um impacto negativo no mercado e na aceitação da marca pelos clientes.

c) Risco de "Governance" e Controlo – Estes riscos decorrem de perdas em resultado da má execução ou falha de procedimentos internos, do pessoal e de sistemas. Estes podem igualmente incluir as perdas causadas por falhas de uma organização na observância das leis aplicáveis, regulamentos, padrões e práticas industriais, que criam um impacto negativo no mercado e na percepção da integridade institucional pelos clientes.

9.2. Fiscalização pelo Órgão de Administração e Gestão de Topo

9.2.1. A responsabilidade pela gestão do risco de reputação cabe, em última instância, ao órgão de administração. Este deve tratar o risco reputacional de forma explícita, distinta e controlável de modo a garantir a segurança e robustez da instituição.

9.2.2. Compete, em especial, ao órgão de administração:

a) Aprovar uma estratégia de risco reputacional e estabelecer uma estrutura de gestão capaz de a implementar; e

b) Efectuar revisões regulares da estratégia para garantir que a instituição gere o risco reputacional de forma efectiva e incorporar as inovações da indústria nos processos e sistemas de gestão do risco reputacional.

9.2.3. A gestão de topo deve possuir um entendimento profundo de todos os aspectos do risco operacional e demonstrar cometimento claro para o seu cumprimento. O cometimento deve ser comunicado em toda a instituição.

9.2.4. A responsabilidade pela reputação corporativa deve estar a cargo da gestão de topo e requer uma equipa multifuncional para criar e implementar a estratégia de protecção.

9.2.5. A gestão de topo deve assegurar que seja instituído um procedimento de gestão de crises para gerir potenciais eventos susceptíveis de afectar a reputação da instituição. Outrossim, deve assegurar que não haja divulgação de informações ao público ou à imprensa sem a devida autorização da gestão.

9.2.6. A gestão de topo deve implementar um processo sólido e abrangente de gestão de riscos para identificar, acompanhar, controlar e reportar todos os riscos que podem causar danos à reputação da instituição.

9.2.7. A auditoria e comité de gestão de risco de uma instituição devem ser responsáveis por analisar a adequação e eficácia dos sistemas de controlo interno, incluindo os relacionados com o risco de reputação e os meios através dos quais as exposições relacionadas com o risco de reputação são geridas.

9.3. Políticas, Procedimentos e Limites

9.3.1. A instituição deve possuir políticas, processos e procedimentos para mitigar o risco reputacional material. As políticas de privacidade institucional devem considerar aspectos legais e litigiosos.

9.3.2. A gestão de topo deve traduzir a estratégia de risco reputacional estabelecida pelo órgão de administração em políticas, processos e procedimentos que possam ser implementados e verificados.

9.3.3. Não obstante a responsabilidade pela adequação e eficácia das políticas, processos, procedimentos e controlos recair sobre cada nível de gestão, a gestão de topo deve atribuir claramente autoridade, responsabilidade e linhas de reporte para encorajar a prestação de contas. Esta responsabilidade inclui assegurar que estejam disponíveis os recursos necessários para uma eficaz gestão do risco reputacional.

9.3.4. A gestão de topo deve estabelecer indicadores não financeiros para o risco de reputação, a fim de gerir a transmissão de informações no mercado.

9.4. Identificação e Mensuração do Risco

9.4.1. O órgão de administração deve adoptar um modelo de risco desenvolvido especificamente para identificar a estrutura do ambiente de controlo, bem como o tipo específico de controlos de risco e métricas que possam ser implementadas em toda a instituição. O órgão de administração deve conceber, especificamente, controlos e métricas para lidar com a categoria de risco de reputação numa perspectiva qualitativa.

9.4.2. A identificação do risco é crucial para posterior desenvolvimento de métricas, acompanhamento e controlo viáveis do risco reputacional. A instituição deve possuir um entendimento claro das principais ameaças à sua reputação, que podem se manifestar através de cobertura sustentada dos mídia, queda repentina do preço das acções e perda de confiança de clientes. Estas podem ser causadas por factores como activismo, discriminação nos postos de trabalho, negócios não éticos, falhas de *marketing*, ou outros risco mais tradicionais como falhas nos produtos/serviços.

9.4.3. Uma vez identificados, os riscos devem ser priorizados de modo a ajudar os gestores na alocação de esforços e recursos. Este processo de priorização deve ser ligado às estratégias institucionais de gestão de riscos.

9.5. Acompanhamento e Sistema de Informação de Gestão do Risco

9.5.1. Cada instituição deve realizar uma revisão do diagnóstico de risco para identificar áreas potenciais de risco de reputação. O órgão de administração deve exigir que a gestão utilize metodologias comprovadas de análise, bem como revisões independentes e objectivas, concebidas para detectar e analisar factores de risco, tanto quantitativos como qualitativos, e pontos de controlo críticos dentro da instituição.

9.5.2. O exame da probabilidade e impacto do risco reputacional somente mostra uma face da moeda. A outra face requer uma avaliação da capacidade da instituição de evitar o risco ou de assumi-lo caso ocorra.

9.5.3. Uma vez mapeados os riscos importantes, a instituição deve estabelecer procedimentos para acompanhar sinais de alerta prévio em relação à sua ocorrência ou agravamento. Um posto importante de escuta na instituição é o departamento de serviço ao cliente, que pode estabelecer sinais de alerta prévio de certa tendência antes que o problema chegue ao domínio público. A frequência de acompanhamento deve reflectir os riscos envolvidos e a frequência e natureza das alterações no ambiente operacional. Os resultados desse acompanhamento devem ser incluídos nos reportes à gestão de topo e ao órgão de administração.

9.5.4. Deve existir um sistema para assegurar que as deficiências identificadas são tempestivamente geridas e que são implementadas acções correctivas eficazes. Os programas de formação devem ser efectivos e disponibilizados recursos necessários para assegurar a conformidade.

9.5.5. Este processo deve ajudar a instituição a desvendar os principais factores de risco com elevada probabilidade de dar origem ao risco de reputação. Cada instituição deve garantir que a metodologia de análise utilizada é altamente sensível às suas necessidades e exigências específicas, bem como os aspectos de risco colocados pela indústria. O processo de revisão deve ser totalmente objectivo.

10. Mapeamento do Risco Intrínseco às Áreas Funcionais

10.1. As actividades que as instituições desenvolvem encerram uma vastidão de riscos intrínsecos, tais como os riscos de crédito, de liquidez, de mercado (taxa de juro e taxa de câmbio), operacional, estratégico de compliance e de reputação. O nível e tipo de riscos inerentes a uma certa actividade dependem da sua natureza e âmbito. Se, por um lado, um risco pode ser transversal a diversas áreas funcionais, por outro uma actividade pode envolver muitos riscos intrínsecos. Ademais, é comum que um determinado risco active outros. Consequentemente, as instituições devem preparar uma matriz funcional de risco para assegurar que todos os riscos intrínsecos relevantes para as suas actividades sejam captados.

10.2. As actividades mais comuns desenvolvidas pelas instituições incluem concessão de empréstimos, tesouraria, investimentos, mercado cambial, mobilização de depósitos, etc. Para o propósito de preparação da matriz funcional de risco, estas actividades devem ser derivadas dos itens do balanço e extrapatrimoniais da instituição, bem assim das maiores fontes de proveitos, da estrutura organizacional, plano de negócios para actividades e produtos novos e de expansão, e/ou outras actividades da instituição. A seguir um exemplo de matriz funcional de riscos:

		Riscos Intrínsecos					
		Crédito	Liquidez	Mercado	Operacional	Estratégico	Compliance
1.	Empréstimos	x	x	x	x	x	x
2.	Depósitos		x	x	x	x	x
3.	Tesouraria e actividades de investimento:						
	- Investimentos	x	x	x	x	x	x
	- Aplicações no mercado interbancário	x	x	x	x	x	x
	- Gestão de liquidez		x		x	x	x
	- Participações financeiras		x	x		x	x
	- Mercado cambial	x	x	x	x	x	x
4.	Sistema de informação de gestão	x	x	x	x	x	x
5.	Operações bancárias		x	x	x	x	x

Índice

I Introdução

1.1. Gestão de Riscos Associados às Tecnologias de Informação

1.1.1. O contínuo desenvolvimento tecnológico tem impacto significativo na forma de interacção das instituições de crédito com os seus clientes, fornecedores e entidades relacionadas, bem assim na forma como operam.

1.1.2. A *Internet*, em particular, oferece grandes oportunidades para as instituições de crédito alcançarem novos mercados e expandirem o leque de produtos e serviços que disponibilizam aos seus clientes. No entanto, a sua grande acessibilidade e dinamismo tanto trazem benefícios como riscos.

1.1.3. Como as instituições de crédito dependem cada vez mais das tecnologias de informação (TI) e da *Internet* para a operacionalização do seu negócio e interacção com os mercados, o reconhecimento da magnitude e intensidade dos riscos tecnológicos inerentes, tanto a nível individual das instituições de crédito como de todo o sistema financeiro, deve ser incrementado. Para tal, é crítico que as instituições de crédito tenham processos de gestão de risco que permitam:

a) Identificar, avaliar e classificar os riscos relevantes para as suas operações e sistemas;
b) Desenvolver planos documentados contendo políticas, práticas e procedimentos que controlem esses riscos e assegurem a continuidade do negócio;
c) Implementar e testar os planos regularmente;
d) Monitorizar os riscos e a efectividade dos planos numa base contínua;
e) Actualizar periodicamente os planos para considerar as alterações no ambiente tecnológico e do negócio, assim como nos requisitos legais, incluindo as ameaças externas e internas e vulnerabilidades de segurança.

1.1.4. O objectivo deste conjunto de directrizes é assistir as instituições de crédito:

a) No estabelecimento dum quadro sólido e robusto de gestão do risco tecnológico e da continuidade do negócio;
b) No reforço do sistema de segurança, fiabilidade, disponibilidade e capacidade de recuperação e retomada de funções críticas do negócio;
c) Na implementação de mecanismos robustos de criptografia e autenticação para a protecção dos dados e transacções dos clientes.

1.2. Aplicabilidade das Directrizes de Gestão de Riscos de Tecnologias de Informação

1.2.1. As directrizes são declarações de boas-práticas da indústria que as instituições são encorajadas a adoptar. Elas não afectam e nem devem ser consideradas como declarações do padrão de cuidados devidos pelas instituições de crédito aos seus clientes. Onde apropriado, as instituições de crédito podem adaptar as directrizes, tomando em consideração as suas diversas actividades, os mercados nos quais realizam transacções e o seu perfil de risco. É expectável que as instituições de crédito leiam as directrizes em conjunto com os requisitos regulamentares relevantes e os padrões da indústria.

1.2.2. A administração e a gestão de topo da instituição de crédito são os responsáveis pela gestão de risco, incluindo os riscos tecnológicos, que se tornam cada vez mais complexos, dinâmicos e ubíquos. O processo de gestão de risco requer da administração e gestão de topo a revisão e avaliação do custo-benefício quanto ao investimento em medidas de controlo e segurança em relação a sistemas computarizados, redes, centros de dados, operações e instalações alternativas de recuperação.

1.2.3. Os objectivos destas directrizes são a promoção da adopção de processos sólidos na gestão de riscos tecnológicos e de continuidade do negócio e da implementação de práticas de segurança, pelo que o Banco de Moçambique irá incorporá-las no seu processo de supervisão com o propósito de averiguar se os controlos relativos a riscos tecnológicos e as medidas de segurança adoptadas pelas instituições de crédito são adequados.

1.3. Glossário

Terminologia	Definições (no contexto do presente documento)
BCM	*Business Continuity Management* (Gestão da Continuidade do Negócio). Refere-se a um quadro abrangente que inclui políticas, normas e procedimentos que propiciam a continuidade de funções da instituição diante de rupturas operacionais. Deve ser compatível com a natureza das instituições, dimensão e complexidade das actividades empresariais.
BCP	*Business Continuity Plan* (Plano de Continuidade do Negócio). É um plano de acção que define os procedimentos e estabelece os processos e sistemas necessários para restaurar a instituição ao estado de funcionamento de forma organizada e expedita, em caso de interrupção.
BIA	*Business Impact Analysis* (Análise de Impacto no Negócio). É o processo de avaliação (quantitativa e qualitativa) do impacto no negócio ou perda para a instituição face a uma interrupção. A BIA é útil para identificar as prioridades de recuperação, os requisitos de recursos de recuperação, as estratégias de recuperação e o pessoal crítico.

[1] Risco tecnológico relaciona-se com qualquer resultado adverso (dano, perda, interrupção, violação, irregularidade ou falha) decorrente do uso ou dependência de hardware, software, dispositivos electrónicos, redes e sistemas de telecomunicações. Estes riscos podem também estar associados a falhas de sistemas, erros de processamento, defeitos de software, erros de operação, falhas de hardware, deficiência de capacidade, vulnerabilidade de rede, fraquezas de controlo, brechas de segurança, sabotagem interna, espionagem, ataques maliciosos, incidentes de hacking, conduta fraudulenta e capacidades de recuperação deficientes.

Terminologia	Definições (no contexto do presente documento)
Recuperação do Negócio	É o curso de acção para a reconstrução de funções de suporte para a condição em que possam processar dados ou informação. Esta condição deve situar-se a um nível suficiente para cumprir as obrigações do negócio.
Retomada do Negócio	É a colocação de funções, após a sua recuperação, na condição de aptidão para assumir tarefas e actividades visando cumprir novas obrigações do negócio.
Estratégias de Recuperação	É o curso de acção definido, aprovado e testado para resposta a rupturas operacionais.
RTO	*Recovery Time Objective*. É o tempo necessário para recuperar uma função específica do negócio. É composto por dois elementos: (1) o tempo que decorre desde o momento da interrupção e a declaração da activação do BCP; (2) e o tempo que decorre desde a activação do BCP e o momento em que a função específica do negócio é recuperada. Indica o tempo máximo aceitável para a recuperação de uma função específica do negócio, após o qual a não recuperação resultaria num impacto significativo no negócio e perdas graves para a instituição.
Risco Residual	É o risco que permanece após a aplicação de medidas mitigadoras.
Risco Sistémico	É o risco de a falha de uma instituição em cumprir suas obrigações comprometer o cumprimento de obrigações das demais instituições do sistema financeiro, potenciando problemas de crédito e/ /ou liquidez e ameaçando a estabilidade do mercado financeiro.

II **Directrizes de Gestão de Riscos Tecnológicos e de *Internet Banking***

2.1. Quadro de Gestão de Riscos

2.1.1. Um quadro de gestão de riscos sólido e robusto requer que a administração e a direcção sejam responsáveis pela gestão e controlo dos riscos tecnológicos. Esta responsabilidade obriga as instituições de crédito a efectuarem análises de risco através da identificação de activos de sistemas de informação, determinação de ameaças de segurança e vulnerabilidades, estimativa de probabilidade de exploração ou ataques, avaliação de perdas potenciais associadas a estes eventos de risco e adopção de medidas de segurança e controlo apropriados para a protecção de activos. A análise de risco consiste no processo de exame das infra-estruturas tecnológicas e sistemas para identificar possíveis exposições, e na consequente ponderação dos prós e contras das diferentes acções de mitigação de risco. Este passo requer uma avaliação dos danos que podem ocorrer nos activos e das respectivas fontes ou causas. São necessários controlos efectivos de segurança dos sistemas de informação para garantir a confidencialidade, integridade e disponibilidade de recursos de tecnologias de informação e dos respectivos dados associados. Estes activos devem ser adequadamente protegidos de acessos não autorizados, mau uso deliberado ou modificação, inserção, eliminação, substituição, supressão ou revelação fraudulenta. Os riscos que se mostrem materiais para a instituição devem ser exaustivamente avaliados e deve-se-lhes atribuir um carácter prioritário, com vista a permitir o desenvolvimento de uma estratégia para o seu tratamento e mitigação.

2.1.2. Devido à natureza aberta e complexa da *Internet*, os riscos associados à utilização desta infra-estrutura para a banca electrónica são acentuados. As instituições de crédito devem tomar este factor em consideração nos seus processos de gestão de risco. Um entendimento claro da interacção entre aplicações baseadas na *Internet* e os sistemas de suporte do *back-end* é necessário para garantir que a gestão e os controlos operativos e técnicos são efectivos e adequados.

2.1.3. Aspectos do risco relacionados com a *internet banking* e com o lançamento de novos produtos ou serviços devem ser avaliados e resolvidos durante as fases de conceptualização e de desenvolvimento. Devem ser estabelecidos procedimentos de controlo de risco e medidas de segurança antes ou durante a fase de implementação.

2.1.4. Dentro da estrutura organizacional, a administração e a direcção de topo devem fiscalizar todas as funções de gestão de risco. Numa base centralizada, delegada ou distribuída, esta fiscalização deverá envolver as áreas do negócio, operacionais e de suporte relevantes que tenham responsabilidades de gestão do risco tecnológico a nível de linha ou funcional. A monitorização e reporte da efectividade e conformidade da gestão do risco deverá em última instância escalar para o presidente da comissão executiva e para a administração.

2.1.5. Políticas, procedimentos e práticas para definir os riscos, estipular as responsabilidades, especificar os requisitos de segurança, implementar medidas para proteger os sistemas de informação, administrar os controlos internos e impor a conformidade devem ser definidos como especificações essenciais do quadro de gestão do risco. A gestão deve conduzir avaliações periódicas de risco para identificar as ameaças internas e externas que possam fragilizar a integridade dos sistemas, interferir com o serviço ou resultar na interrupção das operações. A avaliação das ameaças e vulnerabilidades poderá assistir a gestão na tomada de decisões em relação à natureza e extensão dos controlos de segurança necessários. Devem ser conduzidas, internamente e externamente, acções de sensibilização sobre a segurança para promover e amadurecer um ambiente de segurança consciente.

2.1.6. Como parte do quadro de controlo de risco, a recuperação de desastres e o planeamento de continuidade do negócio são cruciais no desenvolvimento dos planos de contingência para o restabelecimento das operações críticas do negócio após um desastre nas instalações de processamento primário. Nenhum sistema é infalível ou imune a infortúnios. Por conseguinte, é crítico que existam meios efectivos para a recuperação tempestiva. Uma instituição de crédito deve identificar de forma abrangente que tipos de desastres são elegíveis para o plano de recuperação. Os desastres podem variar de uma perda total de serviço devido a eventos naturais a uma falha catastrófica do sistema causada por falhas de sistemas, mau funcionamento de *hardware* ou erros de operação. Uma tarefa substancial no planeamento de recuperação de desastres é compilar um conjunto de procedimentos confiáveis de contingência que cubram vários cenários de interrupção de operações ou falha de sistemas.

2.1.7. Os requisitos de recuperação e prontidão do local de processamento alternativo devem ser periodicamente testados e validados, bem assim avaliados no que diz respeito à adequação, efectividade e capacidade do pessoal para executar os procedimentos de contingência e repor a capacidade de operação.

2.1.8. O ritmo acentuado das inovações tecnológicas mudou o escopo, complexidade e magnitude dos riscos que as instituições de crédito enfrentam na disponibilização de *internet banking*.

É exigido às instituições de crédito que tenham operações e processos resilientes, que lhes permitam gerir os riscos inerentes, responder aos mesmos e ajustar-se a novos riscos.

2.1.9. Processo de gestão de riscos:

2.1.9.1. O primeiro passo em qualquer processo de gestão de risco é averiguar o valor dos activos de sistemas de informação da instituição que devem ser protegidos. Esta avaliação quantitativa pode permitir à instituição classificar e dar primazia aos activos de informação por valor, de modo que a gestão possa tomar decisões do negócio suportadas sobre as medidas de controlo que deverão ser implementadas para proteger os activos. Ao mesmo tempo, é essencial para a instituição que haja cometimento claro em relação à política de protecção dos activos e seus objectivos de segurança. Tipos diferentes de sistemas terão diferentes valores para a instituição, dependendo do seu impacto em caso de perda de confidencialidade, integridade e disponibilidade decorrente de ataques, exploração de vulnerabilidade ou incidentes adversos.

2.1.9.2. Uma estratégia de segurança de TI abrangente é uma componente vital de um processo efectivo de gestão de risco, que não deve ser considerado como uma função meramente técnica a ser relegada aos especialistas de TI. É uma função essencial de gestão, que deve ter o suporte da gestão de topo. Esta função envolve identificar, medir e avaliar riscos, assim como formular um plano para mitigar riscos a um nível aceitável.

2.1.10. Identificação de riscos:

2.1.10.1. Com sistemas de *internet banking*, as diferentes manifestações de riscos, a sua magnitude e consequências assumem novas dimensões. A identificação de riscos implica a determinação de todos os tipos de ameaças, vulnerabilidades e exposições presentes na configuração do sistema de *internet banking*, constituído de componentes tais como redes internas e externas, *hardware*, *software*, aplicações, interfaces de sistemas, operações e elementos humanos.

2.1.10.2. Durante o processo de identificação de riscos, é preciso tomar em consideração tanto as aplicações de *internet* e as suas interfaces, como também os sistemas de suporte de *back-end*. Os riscos e ameaças cobrindo ambos os lados e as suas respectivas interdependências devem ser considerados. Este aspecto é importante, na medida em que estabelece os fundamentos para o entendimento do risco e da postura de segurança das aplicações de internet de uma forma mais abrangente.

2.1.10.3. Ameaças de segurança como as manifestadas em ataques de negação de serviços, sabotagem interna e infestação por *malware* podem causar interrupções severas das operações de uma instituição de crédito, com consequentes perdas para todas as partes afectadas. A monitorização contínua destes riscos em mutação e em crescimento é um passo crucial no exercício da contenção de risco.

2.1.11. Avaliação de riscos:

2.1.11.1. A seguir à tarefa de identificação de riscos, têm de ser analisados e quantificados o efeito potencial e consequências dos mesmos no negócio e nas operações. Na eventualidade de certos riscos não serem quantificáveis, a gestão tem na mesma de os definir e tomar medidas para entender o seu potencial impacto e consequências em caso de ocorrência de incidentes. Com esta informação, a gestão estará apta para estabelecer prioridade para os riscos, efectuar análises de custo-benefício e tomar decisões de mitigação.

2.1.11.2. A amplitude de impacto de risco é uma função da probabilidade da conjugação ou paridade de várias ameaças e vulnerabilidades capazes de causar males para a instituição em caso de ocorrência de eventos adversos. Uma ameaça pode ser definida como sendo qualquer condição, circunstância, incidente ou pessoa com potencial para causar um dano tirando partido de uma vulnerabilidade num sistema. A fonte de ameaça pode ser natural, humana ou ambiental. Humanos com motivação e capacidade para efectuar ataques são fontes sérias de ameaças através de actos deliberados ou omissões, que podem infligir danos imensos à instituição e aos seus sistemas de informação. Um entendimento da motivação, recursos e capacidade que possam ser requeridos para com sucesso efectuar ataques deve ser desenvolvido quando fontes de ameaças e vulnerabilidades relacionadas tiverem sido identificadas. Uma ameaça em particular não representa um perigo quando não está associada uma vulnerabilidade passível de ser explorada no sistema. A matriz de ameaças e vulnerabilidades pode diferir entre instituições.

2.1.12. Tratamento de riscos:

2.1.12.1. Para cada tipo de riscos materiais identificados e analisados, a gestão deve desenvolver e implementar estratégias de mitigação e controlo consistentes com o valor do activo de informação e com o nível de tolerância ao risco da instituição de crédito. A mitigação de risco implica uma abordagem metódica no estabelecimento de prioridades, avaliação e implementação de controlos de redução de risco e medidas de segurança apropriadas, que emanam do processo de avaliação de risco. Uma combinação de controlos técnicos e procedimentos operacionais pode, provavelmente, prover um modo mais vigoroso de redução de riscos de segurança. Na medida em que pode não ser prático tratar simultaneamente de todos os riscos identificados, deverá ser atribuída uma prioridade aos emparelhamentos de ameaças e vulnerabilidades com uma classificação de risco elevada, que podem causar dano ou impacto significante. A gestão deve também avaliar a quantidade de danos e perdas que pode suportar na eventualidade de materialização de um evento de risco relacionado. Os custos dos controlos de riscos devem ser balanceados em função dos benefícios derivados.

2.1.12.2. É imperativo que as instituições de crédito estejam aptas para gerir e controlar riscos de modo a poderem absorver quaisquer perdas relacionadas que possam ocorrer sem perigar a sua capacidade e estabilidade financeira. Na decisão pela adopção de controlos alternativos e medidas de segurança, a gestão deve estar ciente dos custos e efectividade em relação aos riscos a serem tratados ou mitigados. Onde o risco à segurança e robustez do sistema não pode ser adequadamente controlado, a instituição de crédito deverá abster-se de implementar e utilizar tal sistema precário.

2.1.12.3. Na visão das constantes mudanças ocorrendo no ambiente de Internet e canais de distribuição online, a gestão deve instituir um regime de monitorização e conformidade numa base contínua, para averiguar o desempenho e efectividade do processo de gestão de risco. Quando os parâmetros de risco mudam, o processo de gestão de risco deve ser actualizado e melhorado de conformidade. Devem ser conduzidas reavaliações de equações de risco anteriores, testes renovados e auditoria da adequação e efectividade do processo de gestão do risco e dos controlos e medidas de segurança subordinados.

2.1.12.4. O impacto de *internet banking* na gestão de risco é complexo e dinâmico. A gestão deve, numa base constante, reavaliar e actualizar suas abordagens de controlo e mitigação de risco para tomar em consideração circunstâncias variáveis e mudanças ao seu perfil de risco no ambiente da Internet.

2.2. Tipo de Serviços Financeiros Baseados na *Internet*

2.2.1. Devido à natureza aberta e dinâmica da Internet, os riscos associados à disponibilização de serviços online por essa via são maiores e de longe mais extensivos do que em redes fechadas e canais de distribuição proprietários.

2.2.2. Devem ser formulados controlos e medidas de segurança específicos alinhados com o processo de gestão de risco. É importante que as instituições de crédito estabeleçam controlos apropriados e *benchmarks* de segurança para as suas operações de *Internet*.

2.2.3. O nível de riscos de *Internet* está directamente ligado ao tipo de serviços disponibilizados pelas instituições de crédito. Tipicamente, os serviços financeiros baseados na *Internet* podem ser classificados em serviços de informação, de troca interactiva de informação e transaccionais.

2.2.4. Serviço de informação:

2.2.4.1. Esta é a forma elementar de serviço *online* de *Internet*. É uma comunicação unidireccional, através da qual se pode disponibilizar informação, publicidade ou material promocional aos clientes. Muitas instituições de crédito pequenas escolhem apenas disponibilizar informação na *Internet*, configurando servidores standalone ou comprando espaços de publicidade em outros *websites* hospedados por terceiros.

2.2.4.2. Embora os riscos associados a tais serviços *online* sejam baixos, estes *websites* são alvos frequentes de *hacking*, que vandalizam e mutilam a informação original. Uma instituição de crédito pode sofrer um dano de reputação como resultado de um ataque e vulgarização do seu *website*.

2.2.4.3. Quando uma instituição de crédito compra um espaço publicitário de um terceiro, deve efectuar uma monitorização regular não só da publicidade da instituição de crédito, mas também, dos conteúdos associados do provedor de serviços. Danos na reputação podem ser causados por associação a publicidade injuriosa sendo hospedada no mesmo serviço.

2.2.5. Serviços de troca interactiva de informação:

2.2.5.1. Esta forma de serviço de *Internet* oferece um pouco mais de interacção entre a instituição de crédito e o cliente, quando comparada com a anterior. Os clientes são capazes de se comunicar com a instituição de crédito, consultar as suas contas e preencher formulários de adesão a serviços adicionais ou comprar os produtos oferecidos. Os riscos relacionados a estes *websites* dependem da existência ou não de ligações directas à rede interna da instituição de crédito. Estes riscos variam de baixo a moderado, dependendo da conectividade entre a *Internet* e a rede interna e as aplicações a que os clientes podem aceder.

2.2.6. Serviços transaccionais:

2.2.6.1. Esta categoria de serviços de *internet banking* permite aos clientes executar transacções *online*, como a transferência de fundos, pagamento de contas e outras transacções financeiras.

2.2.6.2. Esta é a categoria de risco mais elevado que requer controlos mais fortes, dado que transacções online são normalmente irrevogáveis, uma vez executadas. Os sistemas de Internet da instituição de crédito podem estar expostos a ataques internos ou externos se os controlos forem inadequados. Um elemento acrescido de risco consiste no facto de que ataques contra sistemas de *Internet* não requerem presença física no local a ser atacado. Em alguns momentos, não é claro ou detectável quando e como os ataques são lançados a partir de múltiplos locais.

2.3. Objectivos e Segurança eControlo

2.3.1. A Internet é uma rede global intrinsecamente insegura. Ameaças à segurança decorrentes de ataques de negação de serviços, *spamming*, *spoofing*, *sniffing*, *hacking*, *keylogging*, *phishing*, *middleman interception*, vírus mutantes, *worms* e outras formas de *malware* representam níveis elevados de risco tecnológico que as instituições de crédito enfrentam com frequência cada vez maior. É imperativo que as instituições de crédito implementem medidas de segurança fortes que possam tratar e controlar estes tipos de riscos e ameaças de segurança. As instituições de crédito devem garantir que os acessos online e as transacções efectuadas através da Internet estão adequadamente protegidos e autenticados. Isto requer o estabelecimento de uma estratégia de segurança para permitir o alcance dos seguintes objectivos:

a) Confidencialidade de dados;
b) Integridade de sistemas;
c) Disponibilidade de sistemas;
d) Autenticidade do cliente e transacção;
e) Protecção do cliente.

2.3.2. Confidencialidade de dados:

2.3.2.1. A confidencialidade de dados diz respeito à protecção de informação sensível de olhos curiosos e permissão de acesso autorizado. Os sistemas *online* da instituição de crédito devem utilizar um nível de encriptação apropriado ao tipo e extensão de risco presente nas suas redes, sistemas e operações.

2.3.2.2. Não obstante a ausência de prescrição de robustez específica ou de certo tipo de encriptação, é expectável que as instituições de crédito avaliem de forma apropriada os requisitos de segurança associados aos seus sistemas de *Internet* e adoptem uma solução de encriptação adequada ao grau de confidencialidade e integridade requerido. Adicionalmente, as instituições de crédito devem apenas seleccionar algoritmos que sejam padrões internacionalmente aceites e que tenham sido sujeitos a um escrutínio rigoroso por uma comunidade internacional de criptógrafos ou aprovados por organismos profissionais oficiais, vendedores de segurança reputados ou agências governamentais.

2.3.2.3. O aspecto mais importante da encriptação de dados é a protecção e confidencialidade das chaves criptográficas usadas, quer sejam chaves-mestre, chaves principais de encriptação ou chaves de encriptação de dados. Nenhum indivíduo deve saber inteiramente quais são as chaves ou ter acesso a todos os componentes que fazem as chaves. Todas as chaves devem ser criadas, armazenadas, distribuídas ou alteradas sob as mais rigorosas condições. A sensibilidade de dados e criticidade operacional devem determinar a frequência de alteração das chaves.

2.3.2.4. A aplicação principal da criptografia consiste na protecção da integridade e privacidade de dados por um tempo determinado, em vez de por um período indefinido. Nenhum processo de encriptação é mais seguro que os sistemas hospedeiros que o executam. Módulos de segurança de *hardware* e dispositivos similares resistentes a violações disponibilizam a forma mais segura de execução de funções de encriptação e desencriptação. Outros métodos também podem ser considerados aceitáveis se os mesmos oferecerem protecção suficiente de chaves de encriptação e de dados confidenciais numa operação de encriptação de ponta a ponta.

2.3.2.5. A encriptação de segurança em relação ao PIN do cliente e outros dados sensíveis devem ser mantidos de ponta a ponta ao nível da camada de aplicação. Isto significa que o processo de encriptação é mantido intacto desde o ponto de entrada de dados até o sistema destinatário final onde a desencriptação e/ou autenticação ocorre.

2.3.3. Integridade de sistemas:

2.3.3.1. A integridade de sistemas diz respeito à exactidão, fiabilidade e totalidade da informação processada, armazenada ou transmitida entre a instituição de crédito e os seus clientes. Um nível elevado de integridade de sistema e de dados deve ser alcançado de forma consistente com o tipo e a complexidade dos serviços prestados *online*.

2.3.3.2. Com a conexão de *Internet*, qualquer pessoa pode potencialmente aceder, a partir de qualquer lugar e a qualquer momento, às redes internas das instituições de crédito. Além disso, erros de transacções e falhas operativas resultantes do processamento ou transmissão podem permanecer latentes e indetectáveis por períodos indeterminados, na medida em que sistemas de *internet* geralmente empregam mais processos automatizados que outros sistemas menos complexos.

2.3.3.3. As instituições de crédito devem instalar sistemas de monitorização ou vigilância capazes de alertá-las sobre quaisquer actividades errantes dos sistemas ou sobre transacções online não usuais que ocorram.

2.3.3.4. Determinantes de controlo que são pertinentes para a integridade dos sistemas incluem:

a) Segurança de acesso lógico[2];

b) Segurança de acesso físico[3];

c) Controlos de processamento e transmissão[4].

2.3.4. Disponibilidade de sistemas:

2.3.4.1. Um nível elevado de disponibilidade de sistemas é requerido para manter a confiança pública num ambiente de rede em *online*. Todos os componentes de segurança e controlos anteriores são de pequeno valor se um serviço online não estiver disponível quando necessário. Em termos gerais, os utilizadores de serviços de *internet banking* esperam estar aptos para aceder aos sistemas *online* 24 horas por dia em todos os dias do ano, equivalente a quase zero de indisponibilidade de sistemas.

2.3.4.2. Factores importantes associados à manutenção de elevada disponibilidade de sistemas são: capacidade adequada, desempenho fiável, tempo de resposta rápido, escalabilidade e rápida capacidade de recuperação. As instituições de crédito, os seus provedores de serviço e vendedores que disponibilizam serviços de internet banking devem garantir que têm recursos amplos e capacidade em termos de *hardware*, *software* e outras capacidades operativas para disponibilizar serviços consistentemente fiáveis.

2.3.4.3. No contexto dos serviços bancários online, os sistemas de suporte de interface são tão importantes quanto o sistema hospedeiro. Na disponibilização de aplicações que correm na Internet, as instituições de crédito estarão também a utilizar mainframes existentes ou sistemas hospedeiros de *back-end*. O mesmo perfil de disponibilidade para ambos os sistemas de *front-end e back-end* pode ser necessário para disponibilizar o nível de fiabilidade e consistência de serviço esperado pelos clientes.

2.3.4.4. O processamento via *Internet* normalmente implica um número de sistemas complexos interdependentes e componentes de rede. Um sistema pode tornar-se inoperacional quando um componente crítico de *hardware* ou módulo de *software* funcionar mal ou estiver danificado. Portanto, as instituições de crédito devem manter os componentes de *hardware*, software e rede necessários para uma recuperação tempestiva.

2.3.4.5. É expectável que a gestão estabeleça procedimentos e ferramentas de monitorização para acompanhar o desempenho dos sistemas, processos do servidor, volumes do tráfego, duração das transacções e capacidade de utilização numa base contínua para garantir um nível elevado de disponibilidade dos seus serviços de *internet banking*.

2.3.5. Autenticidade do cliente e da transacção:

2.3.5.1. Na internet banking, as tecnologias de criptografia desempenham um papel importante na garantia da confidencialidade, autenticidade e integridade. Os clientes são requeridos a fornecer sua combinação de User ID e PIN ou uma senha de utilização única (OTP[5]), código de acesso dinâmico ou assinatura digital, de modo que a identidade e autenticidade possam ser verificadas antes que o acesso às suas contas seja garantido. Em termos básicos, este processo de autenticação serve para validar a identidade do cliente, verificando "o que o cliente sabe" (normalmente uma senha ou número pessoal de identificação) e "o que o cliente tem" (como um dispositivo de hardware que gera OTP em intervalos de tempo predeterminados ou um token de USB que contém um certificado digital e a sua chave privada associada).

2.3.5.2. Uma autenticação de dois factores para o login nos sistemas e autorização de transacções pode ser baseada em dois de quaisquer factores a seguir:

a) O que sabe (por exemplo, PIN);

b) O que tem (por exemplo, OTP token);

c) Quem é (por exemplo, biometria).

2.3.5.3. Dada a proliferação e a diversidade de ataques cibernéticos, as instituições de crédito devem implementar autenticações de dois factores no momento de login para todos os tipos de sistemas de internet banking e para a autorização de transacções. Os principais objectivos da autenticação de dois factores são proteger a confidencialidade dos dados das contas dos clientes e dos detalhes das transacções, assim como melhorar a confiança na internet banking, combatendo o phishing, keylogging, spyware, malware, ataques middleman e outras formas de defraudação através da Internet, tendo como alvo as instituições de créditoe seus clientes.

2.3.5.4. As instituições de crédito devem também exigir o uso repetitivo do segundo factor de autenticação (por exemplo, OTP) para transacções de elevado valor ou para alterações de dados sensíveis dos clientes (por exemplo, o endereço do local de trabalho e de residência dum cliente, detalhes de contacto de correio electrónico e telefónico) durante uma sessão de login. Uma sessão autenticada, conjuntamente com o seu protocolo de encriptação, deve manter-se intacta ao longo da interacção com o cliente. Em caso de interferências, a sessão deve ser terminada e as transacções afectas anuladas. O cliente deve ser prontamente notificado do incidente ocorrido enquanto a sessão estiver a ser terminada ou subsequentemente por correio electrónico, telefone ou por outros meios.

2.3.5.5. Requisitos de autenticação são normalmente alcançados pelo uso de criptografia ou protocolos relacionados e funções fortes, tais como Triple DES, AES, RC4, IDEA, RSA, ECC, OATH e RFC 2104 HMAC. Funções criptográficas, algoritmos e protocolos devem ser utilizados para autenticar logins e proteger as sessões de comunicação entre o cliente e a instituição de crédito. A robustez das cifras depende largamente do seu desenho, construção e tamanho das suas chaves.

2.3.5.6. Os constantes avanços no hardware de computador, teoria numérica computacional, criptanálise e técnicas de força

[2] A segurança lógica está associada a como os dados são acedidos e guardados num sistema ou meio de armazenamento. Controlos de acesso lógico são medidas preventivas e detectivas que restringem o acesso do utilizador a dados/informação permitidos.

[3] A segurança de acesso físico está associada ao local e como os recursos dos sistemas, activos de dados e meios de armazenamento estão localizados e protegidos. Controlos de acesso físico incluem medidas preventivas que concedem acesso físico selectivo a indivíduos específicos.

[4] Os controlos de processamento e transmissão estão associados a dados de entrada, processamento, comunicação, transmissão, saída, armazenamento e obtenção de dados. Os controlos podem ser preventivos, detectivos ou correctivos no tratamento de erros, irregularidades ou desvios.

[5] OTP: *One-time password*

bruta distribuída podem induzir a utilização de chaves de maior comprimento no futuro. Alguns algoritmos contemporâneos de cifras podem necessitar de melhoramento ou substituição quando perderem a sua potência ante o aumento progressivo de velocidade e potência dos computadores.

2.3.5.7. Além da aplicação óbvia da encriptação na autenticação e privacidade de transacções online, uma criptografia forte disponibiliza as bases para o alcance de controlo de acesso, autorização de transacções, integridade de dados e responsabilidade. Para incrementar a segurança no processamento *online*, um canal secundário de confirmação[6] e procedimentos devem ser aplicados em relação às transacções acima de valores predefinidos, criação de novas ligações de contas, registo de detalhes de pagamento a entidades, alteração de detalhes das contas ou revisão de limites de transferência. Na organização destas funcionalidades de segurança, a instituição de crédito deve tomar em consideração a sua eficácia e as diferentes preferências dos clientes no que concerne à protecção *online*.

2.3.5.8. Baseado em protocolos mútuos de autenticação, os clientes poderão ser autenticados no website da instituição de crédito através de mecanismos de segurança tais como mensagens/imagens de certificação pessoal, resposta a códigos de segurança de mecanismos de challenge, verificação do certificado do servidor secure sockets *layer* (SSL). De realçar que o SSL é apenas utilizado para encriptar dados em trânsito na camada de transporte de rede, não fornecendo segurança de encriptação de ponta-a-ponta ao nível da camada de aplicação.

2.3.6. Protecção do cliente:

2.3.6.1. A *internet banking* tornou-se num meio fundamental e até num canal electrónico primário de distribuição para um grande número de bancos. Os clientes regularmente acedem aos websites dos seus bancos para consultarem suas respectivas contas e para efectuarem um variado leque de transacções bancárias para fins pessoais ou profissionais. Todavia, a popularidade e a acessibilidade à escala global da *internet banking* atrai um número crescente de ameaças de *hacking*.

2.3.6.2. A protecção do cliente é de grande importância na *internet banking*. A instituição de crédito deve garantir que o cliente é adequadamente identificado e autenticado, antes de lhe ser concedido acesso a informação sensível de clientes ou a funções bancárias. Informação sensível de clientes inclui detalhes particulares ou de conta, que podem ser utilizados para identificar um cliente.

2.3.6.3. Nos anos passados, as ameaças de segurança de Internet eram normalmente de natureza passiva, envolvendo principalmente a bisbilhotagem e a adivinhação de *passwords*. Actualmente, ataques directos a sistemas bancários e PIN de clientes acentuaram-se. Através de ataques direccionados como *phishing*, *websites* falsos, *spamming*, vírus, *worms*, cavalos de tróia, *trapdoors*, *keylogging*, *spyware* e *middleman infiltration*, os PIN de clientes estão sob constante ameaça a partir de vários tipos de vulnerabilidade de sistemas, falhas de segurança e *scams*.

2.3.6.4. A essência da tecnologia de autenticação de dois factores é a disponibilidade de um leque de ferramentas de segurança, dispositivos, técnicas e procedimentos para conter as ameaças e ataques cibernéticos descritos acima. Como parte integral de uma arquitectura de autenticação de dois factores, as instituições de créditos devem implementar medidas apropriadas para minimizar a exposição a ataques middleman, os quais são comummente conhecidos como os ataques *man-in-the-middle* (MITMA)[7], *man-in-the browser* ou *man-in-the application* (anexo A para detalhes).

2.3.6.5. A distribuição de *software* via *internet* está a tornar-se cada vez mais popular. Todavia, no contexto da internet banking, baixar e executar código de *software*, *plug-ins*, applets, programas ActiveX e outros ficheiros executáveis de fontes anónimas ou não verificáveis é, possivelmente, uma das acções mais arriscadas que um cliente pode tomar no seu computador pessoal. As ameaças associadas ao *downloading* são significantes se o cliente não puder legitimar a fonte. Muitos incidentes ocorrem onde utilizadores de internet são enganados por hackers a baixarem cavalos de tróia, backdoors, vírus e outro software malicioso, que causa danos e consequências nocivas.

2.3.6.6. As instituições de crédito não devem distribuir *software* para os clientes via *Internet* ou através de um sistema baseado na *web*, a não ser que possam disponibilizar medidas adequadas de segurança e protecção. Isto implica que os clientes devem estar aptos para verificar a proveniência e integridade do s*oftware* baixado e autenticar a assinatura digital da instituição de crédito incorporada no *software* fornecido, através dum certificado digital fornecido pela instituição de crédito. Por outro lado, a instituição de crédito deve estar apta para verificar a autenticidade e a integridade do *software* em utilização pelos clientes.

2.4. Princípios e Práticas de Segurança

2.4.1. Os princípios e práticas de segurança podem limitar o risco de ameaças externas e internas contra a segurança e integridade de sistemas baseados na Internet. Quando adequadamente implementados e observados, estes também salvaguardam a autenticidade e confidencialidade dos dados e dos processos operacionais.

2.4.2. As práticas de segurança normalmente envolvem combinações de ferramentas de *hardware* e de *software*, procedimentos administrativos e funções de gestão de pessoal que contribuem para construir sistemas e operações seguras. Estes princípios de segurança, práticas e procedimentos são colectivamente conhecidos como as funções da política e processo de segurança de uma instituição.

2.4.3. Gestão de recursos humanos:

2.4.3.1. Em última análise, para a segurança na *internet*, confia-se num pequeno grupo de pessoas especializadas, que devem ser sujeitas a controlos apropriados. As suas actividades e acesso a recursos de sistemas por quaisquer razões devem estar sujeitas a um exame minucioso. É importante que critérios rígidos e meticulosos sejam aplicados na indicação do pessoal para as operações de *internet* e funções de segurança. O pessoal envolvido no desenvolvimento, manutenção e operação de *websites* e sistemas deve ser adequadamente formado em princípios e práticas de segurança.

[6] O segundo canal é qualquer mecanismo de comunicação separado do sistema de *internet banking* e seu canal de disponibilização. Pode ser telefone, SMS, correio electrónico ou um processo manual envolvendo formulários e assinaturas à mão.

[7] Num ataque *man-in-the-middle*, o intruso está apto para ler, inserir e modificar mensagens entre duas partes em comunicação sem os intervenientes aperceberem-se que a ligação entre eles foi comprometida. Pontos possíveis de ataques MITMA podem ser computadores de clientes, redes internas, provedores de serviços de informação, servidores *web* ou em qualquer sítio na internet ao longo do caminho entre o utilizador e o servidor da instituição de crédito.

2.4.3.2. Três dos princípios mais básicos de segurança interna[8] para a protecção de sistemas são:

a) Princípio nunca sozinho:

Certas funções e procedimentos de sistemas são de tal forma sensíveis que devem ser tratados conjuntamente por mais de uma pessoa ou executados por uma pessoa e imediatamente verificados por outra. Estas funções incluem a inicialização de sistemas, configurações de segurança da rede, instalação de sistemas de controlos de acesso, alteração de parâmetros de sistemas operativos, implementação de *firewalls* e de sistemas de prevenção de intrusão, modificação de planos de contingência, invocação de procedimentos de emergência, obtenção de acesso a recursos de *backup* e criação de senhas-mestre e chaves criptográficas.

b) Princípio de segregação de funções:

A segregação de funções é um elemento essencial de controlo interno. As responsabilidades e tarefas que devem ser separadas e executadas por diferentes grupos de pessoas são a função de operação de sistemas, desenho e desenvolvimento de sistemas, programação de manutenção de sistemas, operação de computadores, administração de base de dados, administração do controlo de acesso, segurança de dados, custódia de bibliotecas de dados de *backup*. É também desejável a instituição de rotação de tarefas e de formação cruzada para as funções de administração de segurança. Os processos de transacções devem ser desenhados de modo que ninguém possa individualmente iniciar, aprovar, executar e introduzir transacções num sistema duma maneira que possa permitir a perpetração de acções fraudulentas e a ocultação de detalhes de processamento.

c) Princípio de controlo de acesso:

Os direitos de acesso e privilégios de sistema devem ser baseados nas responsabilidades de cada posição e na necessidade de execução de tarefas alocadas. Ninguém deve, pela categoria ou posição que ocupa, ter qualquer direito intrínseco para aceder a dados confidenciais, aplicações, recursos de sistemas ou instalações. Apenas aos colaboradores com autorização adequada se deve consentir o acesso a informação confidencial e o uso dos recursos de sistemas, somente para os propósitos legitimados.

2.4.3.3. A sabotagem interna, a espionagem ou os ataques furtivos por empregados confiados, fornecedores e vendedores estão potencialmente entre os riscos mais sérios que uma instituição de crédito enfrenta. Colaboradores actuais e desvinculados, fornecedores, vendedores e aqueles que possuem um conhecimento profundo do funcionamento interno dos sistemas da instituição de crédito, operações e controlos internos têm uma vantagem significativa sobre os atacantes externos. Um ataque com sucesso pode potencialmente perigar a confiança do cliente nos sistemas de controlo interno e processos da instituição de crédito.

2.4.3.4. Ninguém deve ter acesso simultâneo aos sistemas de produção e de *backup*, particularmente aos ficheiros de dados e aos centros de computação. Qualquer pessoa que necessite de aceder aos ficheiros de *backup* ou aos recursos de recuperação de sistema deve ser devidamente autorizada para um propósito específico e por um período determinado. Acessos que não sejam para um propósito específico e por um período determinado não devem ser concedidos.

2.4.3.5. Os vendedores e provedores de serviços, incluindo consultores, a quem tenha sido concedido acesso aos recursos de rede e computacionais críticos da instituição representam riscos similares. Este pessoal externo também deve estar sujeito a supervisão estrita, monitorização e restrição de acessos de forma similar ao pessoal interno.

2.4.3.6. Algumas das tácticas comuns utilizadas por insiders incluem a implantação de bombas lógicas, instalação de scripts furtivos, criação de *backdoors* nos sistemas para obter acesso não autorizado, *sniffing* e *cracking* de *passwords*. Os administradores de sistemas[9], oficiais de segurança de TI, programadores e pessoal que executa tarefas críticas possuem, invariavelmente, a capacidade de infligir danos severos nos sistemas de internet banking que mantêm ou operam em virtude das suas funções e acesso privilegiado.

2.4.3.7. Pessoas com elevado acesso aos sistemas devem ser supervisionadas de forma estrita e todas as suas actividades de sistemas devem ser registadas, pois conhecem os sistemas por dentro e possuem recursos para contornar controlos de sistemas e procedimentos de segurança. A seguir são elencados alguns controlos e práticas de segurança recomendados:

a) Implementar a autenticação de dois factores para utilizadores privilegiados;

b) Instituir controlos fortes sobre o acesso remoto por utilizadores privilegiados;

c) Restringir o número de utilizadores privilegiados;

d) Conceder acessos privilegiados com base na necessidade;

e) Manter registos de auditoria de actividades de sistema efectuadas por utilizadores privilegiados;

f) Garantir que os utilizadores privilegiados não tenham acesso aos registos de sistema nos quais as suas actividades são captadas;

g) Conduzir auditorias regulares ou revisões pela gestão das trilhas de auditoria;

h) Proibir a partilhas de ID privilegiados e dos respectivos códigos de acesso;

i) Não permitir que os fornecedores e vendedores tenham acesso privilegiado aos sistemas sem estrita supervisão e monitorização; e

j) Proteger dados de backup de acesso não autorizado.

2.4.4. Práticas de segurança:

2.4.4.1. As instituições de crédito devem conformar-se com as seguintes práticas de segurança:

a) Implementar sistemas operativos robustos:

Os sistemas de *software* e *firewalls* devem ser configurados para os parâmetros de segurança mais elevados, consistentes com o nível de

[8] Estes princípios de controlo interno podem ser adaptados dependendo da separação de responsabilidades, divisão de tarefas, variáveis ambientais, configurações de sistemas e controlos compensativos. Onde seja relevante, a segurança física é imputada aos princípios e práticas de controlo aplicáveis.

[9] Para os propósitos deste documento, administradores de sistemas são aquelas pessoas a quem se tenha concedido acesso privilegiado para manter ou operar sistemas, equipamentos computacionais, dispositivos de rede, ferramentas de segurança, base de dados e aplicações.

protecção requerido, mantendo-se a par das actualizações, patches e melhorias recomendadas por vendedores de sistemas. As *passwords* por defeito devem ser alteradas imediatamente após a instalação de novos sistemas.

b) Instalar *firewalls* entre as redes interna e externa e entre sites geograficamente separados.

c) Instalar dispositivos de detecção-prevenção de intrusão (incluindo aparelhos de segurança contra ataques do tipo DoS).

d) Desenvolver redundâncias embutidas para pontos únicos de falhas, os quais podem danificar a rede.

e) Efectuar revisões de segurança de sistemas usando uma combinação de revisão de código fonte, stress *loading* e teste de excepção para identificar técnicas de codificação não segura e vulnerabilidades de sistemas.

f) Contratar especialistas de segurança independentes[10] para avaliar a robustez e fraquezas das aplicações baseadas na *Internet*, sistemas e redes antes da implementação inicial e pelo menos anualmente, após a implementação, de preferência sem notificação prévia ao pessoal interno que opera ou responde pelos sistemas ou actividades.

g) Conduzir testes de penetração, pelo menos numa base anual.

h) Estabelecer supervisão da rede e procedimentos de monitorização com recurso a scanners de rede, detectores de intrusões e alertas de segurança.

i) Implementar programas antivírus.

j) Conduzir revisões regulares de configurações dos sistemas e da rede e verificações de integridade dos dados.

k) Manter registos de acessos e trilhas de auditoria.

l) Analisar os registos de auditoria em relação a tráfego suspeito e tentativas de intrusões.

m) Implementar uma gestão de incidentes e planos de resposta.

n) Testar os planos predeterminados de resposta de incidentes de segurança.

o) Instalar monitores da rede, que possam assistir na determinação da natureza de um ataque e ajudar na sua contenção.

p) Desenvolver e manter uma estratégia de recuperação e plano de continuidade do negócio baseado na totalidade de necessidades das tecnologias de informação, operacionais e de negócio.

q) Manter uma capacidade de recuperação rápida.

r) Conduzir programas educacionais de consciencialização de segurança.

s) Solicitar auditorias frequentes de TIC a serem conduzidas por profissionais de segurança ou por auditores internos que tenham competências para o efeito.

t) Considerar a contratação de seguros para riscos seguráveis, incluindo os custos de recuperação e restituição.

u) Criar ambientes separados física ou logicamente para o desenvolvimento, teste e produção de sistemas. Conectar apenas o ambiente de produção à *Internet*.

v) Implementar uma arquitectura aplicacional multicamadas, que diferencie o controlo de sessão, a lógica de apresentação, a validação de entradas do lado do servidor, a lógica do negócio e o acesso à base de dados.

w) Implementar a autenticação de dois factores no login para todos os tipos de sistemas de *internet banking* e OTP específico ou assinaturas digitais para cada transacção acima de um valor predeterminado pelo cliente ou pela instituição de crédito.

x) Implementar criptografia forte e encriptação na camada de aplicação de ponta a ponta para proteger os PIN dos clientes, senhas de utilizadores e outros dados sensíveis na rede e nos dispositivos de armazenamento de dados.

y) Encriptar contas de clientes e dados de transacções quando transmitidos, transportados, entregues ou distribuídos por correio a entidades externas ou em locais diversos, tomando em consideração todos os momentos intermediários e pontos de trânsito.

z) Implantar forte autenticação de utilizador em redes locais *wireless* e proteger dados sensíveis com encriptação e controlos de integridade fortes.

2.5. Desenvolvimento e Teste de Sistemas

2.5.1. Muitos sistemas falham devido a problemas de desenho e inadequação dos testes conduzidos. As deficiências de sistemas devem ser detectadas quanto antes, durante o desenho ou teste. Para projectos de grande dimensão, deve ser estabelecido um comité de direcção, constituído pela gestão das várias áreas, elementos da equipa de desenvolvimento e utilizadores-chave. A este comité caberá a responsabilidade de fiscalização e monitorização do progresso dos projectos, incluindo os entregáveis e os *milestones* a serem alcançados de acordo com o plano de projecto.

2.5.2. Ciclo de vida de desenvolvimento de sistemas:

2.5.2.1. No quadro de gestão do ciclo de vida de desenvolvimento de sistemas, as tarefas e processos para o desenvolvimento ou aquisição de novos sistemas devem incluir a atribuição e delineamento de responsabilidades pelos entregáveis e *milestones* de projectos. Os requisitos funcionais, as especificações do desenho e técnicas e as expectativas de desempenho dos sistemas devem ser adequadamente documentados e aprovados por um órgão competente de gestão.

2.5.2.2. Adicionalmente às funcionalidades do negócio, requisitos de segurança relacionados com o controlo de acesso ao sistema, autenticação, autorização de transacções, integridade de dados, *log* de actividade do sistema, trilho de auditoria, registo de eventos de segurança e tratamento de excepções devem ser claramente especificados. É expectável a verificação de conformidade do sistema com os padrões de segurança da instituição de crédito e com os requisitos regulamentares.

2.5.2.3. Uma metodologia aprovada pela gestão deve estabelecer como é que testes[11] de sistema devem ser conduzidos. O escopo dos testes deve cobrir a lógica do negócio, controlos de segurança e desempenho do sistema sobre vários cenários de esforço e condições de recuperação. Um teste completo de regressão deve ser executado antes da implementação de rectificações ou de melhorias de vulto. Os resultados dos testes devem ser revistos e aceites pelos utilizadores cujos sistemas e operações são afectados pelas novas alterações (ver o apêndice B para detalhes relativos a testes de segurança de sistemas)

[10] Ao longo deste documento, a independência tem um significado funcional, porquanto uma revisão ou avaliação pode ser efectuada por especialistas proficientes e competentes ou auditores que não sejam operacionalmente responsáveis pela função, tarefa ou actividade a ser revista, auditada ou avaliada.

[11] Os testes incluem, de um modo geral, o teste unitário, o teste de integração, o teste de sistema e o teste de aceitação do utilizador.

2.5.2.4. Testes de penetração devem ser conduzidos antes da entrada em produção de um novo sistema que oferece acessibilidade através da *Internet* e interfaces de rede abertas. A sua complementaridade com o *scanning* de vulnerabilidades de componentes da rede externa e interna que suportam o novo sistema constitui um resultado lógico esperado. O *scanning* de vulnerabilidades deve ser conduzido pelo menos trimestralmente, com testes de penetração pelo menos anualmente.

2.5.2.5. Para controlar a migração de novos sistemas ou alterações ao ambiente produtivo, é importante que estejam estabelecidos ambientes físicos ou lógicos separados para o teste unitário, de integração, de sistema e de aceitação do utilizador. O acesso de fornecedores e desenvolvedores ao ambiente de Testes de Aceitação do Utilizador (TAU) deve ser monitorizado de forma estrita.

2.5.3. Revisão do código fonte:

2.5.3.1. Existem maneiras diferentes de codificação de programas, que podem esconder vulnerabilidades e brechas (*loopholes*) de segurança deliberadas ou não. Os testes de sistema e de aceitação de utilizadores não são efectivos na detecção de código maligno, cavalos de tróia, *backdoors*, bombas lógicas e outros tipos de *malware*. Nenhum conjunto de testes à caixa-negra é capaz de identificar ou detectar estas vulnerabilidades de segurança.

2.5.3.2. A revisão do código fonte é um exame metódico do código fonte de uma aplicação com o objectivo de encontrar defeitos de segurança que são devidos a erros de codificação, práticas inseguras de codificação ou tentativas maliciosas. É desenhada para detectar vulnerabilidades de segurança, gaps e erros (relacionados com a estrutura de controlo, a segurança, a validação de entrada, o tratamento de excepções, a actualização de ficheiro, a verificação de parâmetros de funções, a confiabilidade, a integridade, a resiliência e a execução) na fase de desenvolvimento e corrigi-los antes da implementação do sistema. Simultaneamente, a qualidade do código e práticas de programação também podem ser melhorados. A conveniência do processamento directo a partir de sistemas altamente integrados com *front-end na Internet* acoplado a *hosts* de *back-end* pode criar oportunidades para que dados corrompidos ou códigos maliciosos se propaguem entre sistemas contíguos, passando de um segmento de rede para outro. Estes tipos de infecções e propagação podem ter repercussões sistémicas.

2.5.3.3. É requerido um alto grau de integridade de sistemas e dados para todas as aplicações com acesso à *Internet*. Das instituições de créditos esperam-se as devidas diligências para garantir que estas aplicações tenham controlos de segurança apropriados, tomando em consideração o tipo e a complexidade dos serviços *online* que prestam.

2.5.3.4. Com base na análise de risco da instituição de crédito, módulos aplicacionais específicos e suas protecções de segurança devem ser rigorosamente testados com uma combinação de revisão do código fonte, teste de excepções e revisões de conformidade para identificar práticas errantes de codificação e vulnerabilidades de sistemas, que podem conduzir a incidentes de segurança e violações. Embora possam divergir para várias aplicações, as metodologias de teste de segurança devem cobrir o seguinte:

a) Identificar fugas de informação:

Informação sensível como chaves criptográficas, detalhes de contas e senhas, configurações de sistema e instruções de conexão à base de dados não devem ser revelados. Fontes potenciais de fuga de informação como mensagens de erro e banners verbosos, operações hard-coded de dados, ficheiros e directórios devem ser escrutinadas para detectar revelação inapropriada de informação.

b) Avaliar a resiliência contra manipulações de entradas (*input*):

O teste deve rever todas as rotinas de validação de entradas e avaliar a sua efectividade contra vulnerabilidades conhecidas.

c) Identificar práticas inseguras de programação:

O teste deve identificar práticas inseguras de programação tais como a utilização de chamadas vulneráveis de funções, a gestão inadequada de memória, a passagem não verificada de argumentos, o *logging* e comentários inadequados, o uso de caminhos relativos (relative *paths*), o *logging* de senhas e credenciais de autenticação, e a atribuição inapropriada de privilégios de acesso.

d) Detectar desvios em relação às especificações de desenho:

O descuido de implementação é uma das mais comuns fontes de vulnerabilidades duma aplicação bem desenhada. Módulos críticos contendo funções de gestão de autenticação e sessões devem ser controlados em relação a discrepâncias entre o desenho do código e sua implementação.

e) Avaliar o tratamento de excepções:

Quando ocorrem excepções ou condições anormais, controlos adequados devem ser estabelecidos para assegurar que os erros resultantes não possam permitir que os utilizadores escapem das verificações de segurança ou que obtenham *core dumps*. Detalhes suficientes de processamento devem ser registados na fonte da excepção para auxiliar no diagnóstico do problema. No entanto, detalhes de sistema ou aplicação, tais como apontadores de pilha, não devem ser revelados.

f) Avaliar a implementação criptográfica:

Somente módulos criptográficos baseados em padrões autorizados e protocolos bem conceituados devem ser instalados. Funções envolvendo algoritmos criptográficos e configurações de chaves criptográficas devem ser controladas em relação a deficiências e brechas de segurança. Esta revisão deve, igualmente, avaliar a escolha da cifra, tamanho das chaves, protocolos de controlo de troca de chaves, funções de *hashing* e geradores de números aleatórios.

2.6. Recuperação e Continuidade do Negócio

2.6.1. Dado o facto de nenhum sistema computarizado ser indestrutível ou possuir segurança inexpugnável, a necessidade de preparação de contingência e capacidade de recuperação é crítica. As prioridades de recuperação e continuidade do negócio devem ser definidas e os procedimentos de contingência devem ser testados e praticados, de tal sorte que sejam minimizadas as interrupções resultantes de incidentes sérios. O plano de recuperação e os procedimentos de resposta a incidentes devem ser avaliados periodicamente e actualizados sempre que se observem alterações nas operações do negócio, sistemas e redes.

2.6.2. Durante uma interrupção de sistema, as instituições de créditos devem evitar adoptar medidas de recuperação improvisadas e não testadas em detrimento de acções de recuperação pré-determinadas que tenham sido ensaiadas e endossadas pela gestão. Medidas *ad-hoc* de recuperação encerram elevado risco operacional, dado que a sua efectividade não foi verificada através de testes e validações rigorosos.

2.6.3. Deve ser estabelecido um centro de recuperação geograficamente separado do centro primário de processamento para garantir a restauração de sistemas críticos e a continuidade das operações do negócio na eventualidade de ocorrência de interrupção no centro primário. Deve ser estabelecida e mantida uma capacidade rápida de recuperação, através de um *hotsite*[12]. A rapidez requerida de recuperação dependerá da criticidade de retoma das operações do negócio, do tipo de serviços *online* e da existência de caminhos alternativos e meios de processamento para manter níveis adequados de continuidade de serviços.

2.6.4. É vital que as instituições de crédito incluam nos seus procedimentos de resposta a incidentes um plano de acção pré--determinado para endereçar questões de relações públicas. É de grande importância para a reputação e solidez da instituição de crédito que este consiga manter a confiança dos clientes durante o período de crise ou de situação de emergência.

2.6.5. Os preparativos de resposta a incidentes, de recuperação de desastres e de continuidade do negócio devem ser revistos regularmente, actualizados e testados para assegurar a sua efectividade e a capacidade do pessoal responsável para empreender procedimentos de emergência e de recuperação quando necessário. A prontidão de recuperação deve antecipar integralmente um *shutdown* total ou incapacitação do centro primário de processamento.

2.6.6. Bancos que tenham sua rede e sistemas ligados a provedores de serviços e vendedores devem conduzir testes de recuperação bilaterais ou multilaterais e garantir que as interdependências são igualmente atendidas.

2.6.7. É de suma importância a posse de planos de acção pré-determinados para contrariar e conter ataques de negação de serviços. A capacidade de restaurar as operações normais rápida e efectivamente após um ataque de negação de serviços deve ser parte integral do processo de reatamento e recuperação do sistema.

2.7. Gestão de Outsourcing

2.7.1. Em internet banking, tornou-se frequente que as instituições de créditos façam o outsourcing de parte ou de todo o processamento computacional, de sistemas e das operações administrativas a provedores de serviços, empresas de telecomunicações, empresas especializadas e outros operadores (genérica e colectivamente tratados por provedores de serviços).

2.7.2. Independentemente das razões para o outsourcing, que podem incluir rápido desenvolvimento de tecnologias e acesso a competências não disponíveis internamente, cabe às instituições de crédito garantir que os seus provedores de serviços são capazes de disponibilizar o nível de desempenho e confiabilidade de serviço, capacidade e segurança necessários no seu negócio de Internet banking. A responsabilidade e prestação de contas da instituição de crédito não se reduzem pelo outsourcing de suas operações a terceiros.

[12] A réplica do centro de processamento primário deve possuir capacidades operacionais e recursos que permitam alcançar um objectivo de tempo de recuperação de 4 horas ou menos.

2.7.3. Gestão de riscos de *outsourcing*:

2.7.3.1. O conselho de administração e a gestão sénior devem compreender completamente os riscos associados ao *outsourcing* das suas operações de *internet banking*. Antes que um provedor de serviços seja escolhido, devem ser realizadas as diligências devidas para determinar a sua viabilidade, capacidade, confiabilidade, histórico e posição financeira. Os termos e condições contratuais que governam os papéis, relacionamentos, obrigações e responsabilidades das partes devem ser cuidadosa e apropriadamente definidos em acordos escritos. A substância coberta nos acordos deve, no geral, cobrir objectivos de desempenho, níveis de serviço, disponibilidade, confiabilidade, escalabilidade, conformidade, auditoria, segurança, planeamento de contingência, capacidade de recuperação de desastres e instalação de processamento de *backup*.

2.7.3.2. A menos que haja acordos mútuos aceitáveis, o provedor de serviços deve ser requerido a prover acesso a todas as entidades indicadas pela instituição de crédito aos seus sistemas, operações, documentação e instalações para que possam conduzir revisões ou avaliações de conformidade regulamentar ou de auditoria. Não obstante a excepção acima mencionada, os acordos devem prever a condução de inspecções ao papel, responsabilidades, obrigações, funções, sistemas e instalações pelo Banco de Moçambique.

2.7.3.3. As instituições de créditos e provedores de serviços devem observar os requisitos de dever de segredo previstos na Lei das Instituições de Crédito e Sociedades Financeiras. Os contratos com provedores de serviços devem levar em consideração a necessidade de protecção de confidencialidade da informação dos clientes, bem como a necessidade de conformidade com leis e regulamentos aplicáveis.

2.7.4. Monitorização de arranjos de outsourcing:

2.7.4.1. A instituição de crédito deve solicitar que o provedor de serviços implemente políticas de segurança, procedimentos e controlos que satisfaçam os requisitos contratuais. Adicionalmente, deve rever e monitorizar as práticas de segurança e processos do provedor de serviços numa base regular, incluindo o comissionamento ou obtenção de reportes periódicos de peritos em relação à adequação da segurança e conformidade em relação às operações do provedor de serviços. Deve ser estabelecido um processo de revisão contínua da prestação de serviços, em termos de confiabilidade, desempenho e capacidade de processamento com a finalidade de aferir a conformidade com os níveis de serviço acordados e a viabilidade de suas operações.

2.7.4.2. À medida que as relações de *outsourcing* e as dependências aumentam de complexidade e importância, uma abordagem rigorosa de gestão de riscos deve ser adoptada para garantir que não sejam dissipadas as responsabilidades da gestão pela protecção das operações e serviços nucleares da instituição de crédito.

2.7.5. Planeamento de contingência e de continuidade do negócio:

2.7.5.1. A gestão deve requerer que o provedor de serviços desenvolva e estabeleça um quadro de contingência e procedimentos de recuperação de desastre que defina o seu papel e responsabilidades na documentação, manutenção e teste dos planos de contingência e dos procedimentos de recuperação. Dado que o erro humano tem maior contribuição no número de falhas e tempo de inactividade dos sistemas, todas as partes e pessoal envolvidos devem receber treinamento regular na activação do plano de contingência e execução dos procedimentos de recuperação. Este plano deve ser revisto, actualizado e testado regularmente de acordo com as condições da evolução tecnológica e com os requisitos operacionais.

2.7.5.2. A instituição de crédito deve, igualmente, estabelecer um plano de contingência baseado nos piores cenários credíveis de interrupção de serviços, para se preparar para a possibilidade de que o seu actual provedor de serviços não seja capaz de continuar as operações ou a prestar os serviços necessários. O plano deve incorporar a identificação de alternativas viáveis para prosseguir o seu *internet banking* a partir de outro local.

2.8. Ataques Distribuídos de Negação de Serviços (Ddos)

2.8.1. Pese embora os ataques distribuídos de negação de serviços (DDoS) tenham sempre imposto uma grande ameaça para os sistemas de *internet banking*, a proliferação de *botnets*[13] e o advento de novos vectores de ataque juntamente com a rápida adopção global da banda larga nos últimos anos têm aumentado a potência de tais ataques.

2.8.2. O tamanho normal de largura de banda e a capacidade do sistema de qualquer organização, por maior que seja, provavelmente não possam resistir a uma ofensiva DDoS sustentada por um *botnet* considerável ou por um grupo de *botnets*. A imensa quantidade de recursos computacionais acumulada por *botnets* para desencadear um ataque rapidamente esgotaria a largura de banda da rede e os recursos computacionais de um sistema-alvo, causando, inevitavelmente, uma interrupção maciça do serviço ou completa cessação.

2.8.3. Não obstante a maioria das instituições de crédito ter instituído protecções efectivas dos seus sistemas contra infecções por cavalos de tróia e *worms*, o que as torna menos susceptíveis de integrarem *botnets*, mais deve ser feito para reforçar a robustez dos seus sistemas contra ataques DDoS. A este respeito, espera-se que as instituições de crédito possuam uma estratégia para endereçar as ameaças de *botnets*.

2.8.4. Detecção e resposta a ataques:

2.8.4.1. Bancos com serviços de *internet banking* devem poder responder a condições incomuns[14] de tráfego de rede, desempenho volátil do sistema ou aumento súbito na utilização de recursos do sistema, pois podem ser sintomáticos de uma investida de DDoS. Consequentemente, o sucesso de quaisquer acções preventivas e reactivas depende do desenvolvimento de ferramentas apropriadas para, de forma efectiva, detectar, monitorizar e analisar anomalias em redes e sistemas.

2.8.4.2. Como parte da estratégia de defesa, as instituições de crédito devem instalar e configurar *firewalls*, sistemas de detecção/prevenção de intrusão, roteadores e outro equipamento especializado de rede para alertar o pessoal de segurança e desviar e/ou filtrar o tráfego de rede em tempo real logo que um ataque for suspeito ou confirmado. Devido ao volume significativo de tráfego que necessita de ser processado, deve ser considerada a utilização de aparelhos construídos à medida e projectados para prover altos níveis de desempenho. O objectivo aqui é remover pacotes maliciosos, de modo que tráfego legítimo para o sistema de *internet banking* possa fluir.

2.8.4.3. Nós de estrangulamento potenciais e pontos únicos de falha vulneráveis a ataques do tipo DDoS podem ser identificados através da revisão do código fonte, análise do desenho da rede e teste de configuração. A eliminação dessas fraquezas pode incrementar a resiliência do sistema.

2.8.5. Selecção de provedores de serviços de Internet:

2.8.5.1. Sem a cooperação de provedores de serviços de *Internet* (ISP), muitas organizações encaram como assustadora a tarefa de prevenção contra ataques do tipo DDoS. Uma contra-medida efectiva pode ser depender de ISP para amortecerem um ataque do tipo DDoS em redes *upstream*.

2.8.5.2. Dado o facto de que as instituições de crédito e seus ISP devem adoptar uma abordagem colaborativa, é importante que incorporem considerações sobre ataques do tipo DDoS no seu processo de selecção de ISP. Para tal devem averiguar:

a) Se o ISP oferece protecção contra ataques do tipo DDoS ou serviços de limpeza para auxiliar na detecção e desvio de tráfego malicioso;
b) A capacidade do ISP de expandir a largura de banda da rede quando necessário;
c) A adequação do plano de resposta a incidentes do ISP; e
d) A capacidade e prontidão do ISP para rapidamente responder a um ataque.

2.8.6. Planeamento de resposta a incidentes:

2.8.6.1. Deve ser idealizado e rotineiramente validado um quadro de resposta a incidentes para facilitar uma rápida resposta a investidas DDoS ou a um iminente ataque. Este quadro deve incluir um plano que detalhe os passos imediatos a seguir para contrariar um ataque, invocar procedimentos de escalonamento, activar arranjos de continuidade do negócio, accionar alertas de clientes e reportar ao Banco de Moçambique, bem como a outras autoridades.

2.8.6.2. As instituições de crédito devem estar familiarizadas com os planos de reposta a incidentes do ISP e assimilá-los no seu quadro de resposta a incidentes. Para favorecer uma melhor coordenação, as instituições de crédito devem estabelecer um protocolo de comunicação com os seus ISP e conduzir exercícios periódicos conjuntos de resposta a incidentes.

2.9. Divulgação da Instituição de Crédito

2.9.1. As instituições de crédito devem prover informação clara aos seus clientes sobre os riscos e benefícios de utilização de *internet banking* antes da subscrição a estes serviços. Os clientes devem estar informados de forma clara e precisa sobre os direitos, obrigações e responsabilidades (do cliente e da instituição de crédito) em todas as matérias relacionadas com as transacções *online* e, particularmente, quaisquer problemas que possam surgir de erros de processamento e brechas de segurança. Informações escritas de forma não sintética e/ou usando terminologia técnica podem causar dificuldades de legibilidade e compreensão aos clientes.

2.9.2. Os termos e condições aplicáveis a produtos e serviços de banca online devem estar disponíveis aos clientes através da aplicação de *internet banking*. No logon inicial ou na subscrição a um serviço ou produto particular deve ser exigido um reconhecimento positivo dos termos e condições pelos clientes.

2.9.3. As instituições de crédito devem tornar pública a sua política de segurança e de privacidade do cliente. A forma de tratamento de disputas com os clientes, o reporte e os procedimentos para a sua resolução, incluindo o tempo esperado de resposta da instituição de crédito, devem estar claramente definidos. Toda esta informação deve estar disponível no *website* da instituição de crédito. A divulgação de informação pode ser útil para que os clientes tomem decisões informadas.

2.9.4. Nos *websites*, as instituições de crédito devem orientar seus clientes em relação às medidas de segurança e precauções razoáveis a tomar no acesso a contas online. Os procedimentos de precaução devem incluir os passos a seguir para a prevenção de transacções não autorizadas e de uso fraudulento de suas contas,

---

[13] *Botnets* são colecções de computadores (*ou bots*) infectados com software malicioso, operando sob um comando e infra-estrutura de controlo comum – o *botnet master* ou *botnet originator*. Um *botnet master* é capaz de recorrer às máquinas comprometidas para lançar um ataque DDoS.

[14] Uma *baseline* para processos normais do sistema, indicadores e padrões de tráfego deve ser usada como guia para a identificação de comportamentos incomuns do sistema.

assim como garantir que ninguém possa observar ou roubar suas credenciais de acesso ou outras informações de segurança que permitam a personificação ou a obtenção de acesso não autorizado às suas contas *online*.

2.9.5. Na eventualidade de ocorrência de brechas de segurança e de acesso e realização de transacções fraudulentas a partir de contas *online* de clientes, as instituições de crédito devem explicar em seus websites que processos serão evocados para resolver o problema ou disputa, assim como as condições e circunstâncias nas quais as perdas ou estragos resultantes serão imputados à instituição de crédito ou aos clientes.

2.10. Educação de Clientes

2.10.1. A importância da educação de clientes em relação à segurança e confiabilidade de sua interacção com a instituição de crédito não deve ser subestimada. A confiança dos clientes em relação à segurança e solidez dos produtos e serviços *online* da instituição de crédito depende, em larga escala, do seu entendimento e conformidade com os requisitos de segurança associados à operação de suas contas bancárias.

2.10.2. A educação de clientes pode ser *online* com base na *Web* ou pode ser definida uma abordagem de aprendizagem orientada. Sempre que a instituição de crédito introduzir novas características ou funções operacionais, particularmente as relacionadas com segurança, integridade e autenticação, deve garantir que os clientes tenham instrução e informação suficientes para que possam utilizá-las apropriadamente. A educação contínua e a provisão de informação tempestiva aos clientes pode ajudá-los a compreender os requisitos de segurança e a tomar medidas apropriadas no reporte de problemas de segurança.

2.10.3. Para incrementar a consciência de segurança, as instituições de crédito devem exortar os clientes sobre a necessidade de protecção de seus PIN, *tokens* de segurança, detalhes pessoais e outros dados confidenciais. As instruções de segurança de PIN e OTP devem ser exibidas de forma proeminente na página de *login* ou na página de entrada do USER ID, PIN e OTP. As seguintes recomendações podem ser instrutivas no auxílio dos clientes na construção de PIN robustos e na adopção de melhores procedimentos de segurança:

a) O PIN deve ser constituído de, no mínimo, 6 dígitos ou 6 caracteres alfanuméricos, sem que um mesmo dígito esteja repetido;
b) O PIN não deve ser baseado no USER ID, número de telefone pessoal, data de nascimento ou outra informação pessoal;
c) Os PIN devem ser mantidos confidenciais e jamais divulgados;
d) Os PIN devem ser memorizados e não escritos;
e) Os PIN devem ser alterados regularmente;
f) Não deve ser usado o mesmo PIN para *websites*, aplicações ou serviços diferentes, particularmente quando estejam relacionados a diferentes entidades;
g) O cliente não deve seleccionar a opção do navegador de guardar ou reter o username e *password*;
h) O cliente deve verificar a autenticidade do *website* da instituição de crédito através da comparação do URL com o nome da instituição de crédito constante do certificado digital ou através da observação dos indicadores fornecidos por um certificado alargado de validação;
i) O cliente deve verificar se o endereço do *website* da instituição de crédito muda de http:// para https:// e se aparece um ícone de segurança que se assemelha a um cadeado ou chave, quando espera pela autenticação e encriptação;
j) O cliente não deve permitir que alguém guarde ou mexa no seu *token* de segurança OTP;
k) O cliente não deve revelar o OTP gerado pelo seu token de segurança;
l) O cliente não deve divulgar o número de série de seu token de segurança;
m) O cliente deve verificar seu extracto de conta bancária regularmente e reportar qualquer discrepância.

2.10.4. Os clientes devem ser recomendados a adoptar as seguintes precauções e práticas de segurança:

a) Instalar *software* antivírus, *anti-spyware* e *firewall* nos seus computadores pessoais, particularmente quando estejam ligados através de conexões de banda larga, DSL[15] ou modems de cabo;
b) Actualizar regularmente produtos antivírus e *firewall* com patches de segurança ou novas versões;
c) Remover o "*file and printer sharing*" de seus computadores, especialmente quando tenham acesso à Internet através de modems de cabo, conexões de banda larga ou instalações similares;
d) Realizar *backups* regulares de dados críticos;
e) Considerar a utilização de tecnologia de encriptação para proteger dados altamente sensíveis;
f) Encerrar sessões (*log off*) *online* e desligar o computador quando o mesmo não estiver em uso;
g) Não instalar *software* ou executar programas de origem desconhecida;
h) Eliminar e-mails indesejados ou em cadeia;
i) Não abrir anexos de *e-mails* enviados por estranhos;
j) Não divulgar informações pessoais, financeiras ou de cartões de crédito em *websites* pouco conhecidos ou suspeitos;
k) Não utilizar um computador ou equipamento não confiável;
l) Não utilizar computadores públicos ou de *Internet* cafés para aceder à banca *online* ou executar transacções financeiras.

2.10.5. A informação sobre precauções de segurança e boas práticas acima apresentada não pretende ser exaustiva e nem estática. A mesma deve ser apresentada aos clientes de forma amigável e actualizada com regularidade.

2.10.6. As instituições de crédito são directamente responsáveis pela segurança e solidez dos serviços e sistemas que fornecem aos seus clientes. A este respeito, elas são obrigadas a operar e manter sistemas adequados e efectivos de autenticação e outros relacionados com segurança para proteger e verificar os seus clientes antes de permitir o acesso a contas bancárias e a execução de transacções, de acordo com procedimentos apropriados de autorização e validação. Reciprocamente, é importante que os clientes tomem medidas apropriadas de segurança para proteger seus dispositivos e sistemas computacionais e garantam que o seu hardware ou a integridade do sistema não esteja comprometido ao se envolverem na banca *online*. Os clientes devem ouvir os conselhos dos seus bancos sobre como proteger os seus dispositivos ou computadores que utilizam para o acesso aos serviços bancários.

III Princípios de Gestão da Continuidade do Negócio

3.1. Princípio 1: O Conselho de Administração e a Gestão Sénior Devem Ser Responsáveis pela Gestão da Continuidade de Negócio da Instituição

3.1.1. A responsabilidade por assegurar o estado de preparação de continuidade do negócio da instituição, em última análise, recai sobre o conselho de administração e a gestão sénior.

[15] DSL: Digital subscriber line.

3.1.2. A gestão sénior é responsável pela direcção da gestão da continuidade do negócio com políticas e estratégias necessárias para a prossecução de funções críticas do negócio. Deve demonstrar ter consciência suficiente dos riscos, medidas de mitigação e estado de prontidão por meio de fornecimento de atestado (de preparação relativa à continuidade do negócio) ao conselho de administração.

3.1.3. O atestado é um documento interno dirigido ao conselho de administração para sua ratificação. Cabe à gestão sénior determinar a forma com que o mesmo melhor fornece o nível de conforto e a necessidade de garantia adicional. O atestado deve indicar claramente o seguinte:

a) O nível de prontidão da instituição; e

b) O grau de alinhamento com as directrizes, que seja compatível com a natureza e dimensão da instituição e a complexidade das actividades efectuadas.

3.1.3.1. O Banco de Moçambique incentiva também a divulgação e inclusão do risco residual no atestado.

3.1.4. O atestado deverá ser actualizado pelo menos uma vez por ano ou mais frequentemente, caso haja alterações substanciais dentro da instituição.

3.1.5. As instituições são responsáveis por decidir sobre os conteúdos do atestado a divulgar aos seus clientes e contrapartes, caso entendam por necessário.

3.2. Princípio 2: As Instituições Devem Incorporar a Gestão da Continuidade de Negócio nas suas Operações

3.2.1. A gestão da continuidade do negócio é um quadro focalizado no risco que aborda a componente operacional, através do desenvolvimento de políticas claras, estratégias e responsabilidades para a recuperação das funções críticas do negócio. É um processo proactivo. As instituições devem, portanto, esforçar-se para construir uma cultura organizacional que incorpore a gestão da continuidade do negócio como parte de suas operações usuais do negócio e de gestão quotidiana de risco.

3.2.2. Dependendo da dimensão e complexidade de suas actividades, as instituições podem adoptar boas práticas de gestão da continuidade do negócio que incluem as seguintes componentes:

a) Política, estratégia e orçamento claros para a gestão da continuidade do negócio;

b) Funções e responsabilidades bem definidas para o programa de gestão da continuidade do negócio;

c) BCP compreendendo tarefas e actividades detalhadas;

d) Planos de sucessão para o pessoal crítico e gestão sénior;

e) BIA ou processo similar;

f) Programa para o desenvolvimento, implementação, teste e manutenção do BCP;

g) Programas para o treinamento e consciencialização;

h) Respostas de emergência;

i) Programas de coordenação de comunicações externas e gestão de crises;

j) Coordenação com entidades externas (incluindo autoridades, partes interdependentes, etc.).

3.2.3. O BCP é uma importante evidência tangível da iniciativa institucional de gestão da continuidade do negócio. Deve ser exequível, regularmente revisto, actualizado conforme as mudanças no negócio e significativamente testado para garantir a sua relevância, eficácia e viabilidade operacional.

3.3. Princípio 3: As Instituições Devem Testar o Seu Plano de Continuidade de Negócio Regularmente, Plenamente e Significativamente

3.3.1. O teste é um elemento vital para a implementação de uma gestão da continuidade do negócio eficaz. As mudanças na tecnologia, processos do negócio, funções e responsabilidades de pessoal podem afectar a adequação do BCP e, em última análise, a preparação relativa à continuidade do negócio das instituições. Portanto, é importante testar regularmente a sua funcionalidade e eficácia. Por outro lado, os testes propiciam a familiarização do pessoal com a localização de centros de recuperação, bem como com os procedimentos de recuperação. As instituições devem obter a garantia através de testes das respectivas capacidades de, uma vez activados os seus BCP, continuarem a operar de forma confiável, responsável e eficiente conforme planeado.

3.3.2. A indicação de que os testes devem ser regulares significa que as instituições são incentivadas a efectuar diferentes tipos de testes, levando em consideração a criticidade e complexidade das funções do negócio e recursos necessários. Os testes podem ser realizados em módulos e em intervalos diferentes, mas regulares. A gestão sénior e o pessoal devem participar nestes exercícios e estar familiarizados com as suas funções e responsabilidades para eventuais activações.

3.3.3. A indicação de que os testes devem ser **plenos e significativos** pretende comunicar que todos os componentes de um processo do negócio devem ser testados de forma significativa. Isto deve incluir testes de conectividade, funcionalidade e de capacidade da infra-estrutura instalada nos locais de recuperação. As instituições devem certificar-se de que os seus programas de teste abrangem adequadamente tanto os aspectos qualitativos (ex., tempo de resposta) como quantitativos (ex., capacidade de carga). Devem, de forma crítica e regular, testar todos os pressupostos estratégicos e de planeamento para verificar a sua aplicabilidade, especialmente quando o escopo ou direcção do negócio se altera. Para observância da plenitude, os testes devem incluir também a consciencialização e preparação do pessoal e a coordenação com entidades externas, bem como o teste completo de todas as interdependências, incluindo os prestadores de serviços sediados fora do país.

3.3.4. Testes abrangendo toda a instituição são também incentivados, pois oferecem uma perspectiva diferente dos testes modulares. As instituições devem progressivamente incorporar mais desafios nos seus exercícios (testes) e introduzir cenários diferentes cada vez que realizarem o mesmo tipo de exercício. Isso transmitirá maior confiança em relação à sua preparação para a continuidade do negócio. Os exercícios podem incluir:

a) *Desktop walkthrough* para testar integralmente o sistema;

b) Activação do call tree de pessoal (com e sem mobilização);

c) Activação de *backup* sites[16] (incluindo a invocação de provedores de serviços externos);

d) Arranjos alternativos de serviços partilhados;

e) Restauração de tapes de *backup*; e

f) Recuperação de registos vitais.

3.3.5. Em última análise, as instituições têm que se certificar de que tais testes/exercícios contribuem significativamente para a melhoria da sua preparação relativa à continuidade do negócio.

3.3.6. Deve ser preparada a documentação formal de exercícios, que lista as lições aprendidas e todas as medidas de mitigação de novos riscos. A gestão sénior deve homologar a documentação e concordar com a nova proposta de medidas de mitigação.

[16] Os backup sites são entendidos como sendo espaços alternativos tanto de processamento informático como de trabalho para os colaboradores de outras áreas de suporte e de negócio.

3.3.7. Testes adequadamente dimensionados e coordenados entre os principais provedores de serviços financeiros[17] públicos e as instituições servidas podem aumentar o nível de consciência e confiança nas operações de recuperação. Podem também aumentar a confiança no sector financeiro.

3.4. Princípio 4: As Instituições Devem Desenvolver as Suas Estratégias de Recuperação e Estabelecer Rto Para as Funções Críticas do Negócio

3.4.1. O estabelecimento de estratégias de recuperação permite às instituições executarem os seus BCP de forma organizada e previamente definida, minimizando interrupções e perdas financeiras. As estratégias de recuperação são a base para a definição de RTO de funções críticas do negócio. Sem estes marcos claros, os escassos recursos podem ser inadequadamente direccionados para actividades menos importantes. Isto pode afectar negativamente a reputação das instituições e a capacidade de sobrevivência.

Funções Críticas do Negócio

3.4.2. Diante de uma crise, pode não ser exequível recuperar todas funções do negócio em simultâneo. As instituições devem, portanto, identificar as funções críticas do negócio (incluindo operações de suporte e sistemas de TI relacionados) e as perdas potenciais (em termos monetários e não-monetários). Um processo comum de obtenção desta informação é a análise de impacto no negócio (BIA). Este processo serve também para destacar as prioridades relativas entre as diversas funções críticas e auxiliar as instituições a determinarem as suas estratégias de recuperação e RTO.

3.4.3. As funções críticas do negócio diferem consideravelmente de uma instituição para outra devido a diferenças no foco do negócio e expectativas de clientes. Algumas das funções críticas do negócio podem incluir: cumprimento de instruções de pagamento, compensação e liquidação de transacções, cumprimento de obrigações de financiamento e de garantias, gestão de posições de risco de clientes e manutenção da confiança de clientes, investidores e público.

Recovery Time Objectives

3.4.4. Os RTO podem variar de minutos a horas, sendo que, para alguns sectores e funções, podem ser ainda mais longos. Pelas razões anteriormente expostas, é importante que as Instituições Significativamente Importantes ("ISI")[18] recuperem e retomem as suas funções críticas do negócio mais rapidamente que as instituições que delas dependem.

3.4.5. A transparência e partilha de RTO podem ajudar a melhorar as expectativas do nível de serviço e compreensão entre instituições e contribuir para o aprimoramento da mitigação de riscos de interdependência.

Determinação de RTO para Funções Críticas do Negócio

3.4.6. As instituições são responsáveis por determinar as respectivas funções críticas do negócio, estratégias de recuperação e os correspondentes RTO compatíveis com a natureza, dimensão e complexidade das suas funções e obrigações.

3.4.7. É pouco provável que todas funções críticas do negócio partilhem o mesmo RTO. Os RTO das diferentes funções do negócio devem ser proporcionais às obrigações da instituição em relação ao mercado, clientes e indústria.

3.5. Princípio 5: As Instituições Devem Perceber e Adequadamente Mitigar os Riscos de Interdependências das Funções Críticas do Negócio

3.5.1. Há uma tendência crescente, por parte das instituições, para partir e redistribuir os riscos e processos local, regional ou globalmente, levando a uma maior dependência de entidades internas e externas. Qualquer má gestão dessas dependências e dos riscos que elas incorporam podem desencadear ineficiências operacionais ou sistémicas, conduzindo a potenciais fracassos.

3.5.2. Ao planear para a continuidade de funções críticas do negócio, as instituições devem considerar as interdependências dessas funções e aferir em que medida elas dependem doutras entidades. As instituições devem também compreender os processos do negócio das entidades que suportam as suas funções críticas, incluindo o grau de preparação de continuidade do negócio e prioridades de recuperação.

3.5.3. Exemplos das referidas dependências:

a) Unidades dentro da instituição (ex., tesouraria, serviços de custódia, etc.);

b) Provedores de serviços financeiros públicos (ex., provedores de serviços de compensação e liquidação, etc.);

c) Fornecedores (ex., provedores de serviços de TI ou de recuperação de desastres, etc.);

d) Provedores de infra-estruturas (ex., serviços de telecomunicações, etc.).

3.5.4. As instituições devem mitigar os riscos decorrentes das dependências, tanto quanto possível e considerar tais dependências nas suas estratégias de recuperação e RTO.

3.5.5. Pese embora a mitigação integral de alguns riscos de interdependências estar fora do controlo directo das instituições (ex., indisponibilidade de redes de telecomunicações, etc.), isso não pode diluir as expectativas dos seus clientes e contrapartes sobre os serviços e obrigações das instituições. É responsabilidade das instituições tomarem medidas razoáveis (ex., iniciar discussões com provedores de serviços de telecomunicações sobre capacidades de redundância, etc.) para assegurar que os seus principais provedores de serviços são capazes de suportar os seus negócios, mesmo mediante interrupções.

3.5.6. Antes da contratação de provedores de serviços externos, as instituições devem certificar-se de que o risco resultante da terceirização mantém-se dentro dos níveis permitidos por suas políticas de gestão de risco operacional e não compromete a preparação relativa à continuidade do negócio. Devem garantir que os seus provedores possuem BCP iguais ou melhores que os seus. Adicionalmente, as instituições devem proactivamente procurar assegurar-se de que os BCP dos seus provedores são testados regularmente.

3.5.7. É fundamental que as instituições monitorizem continuamente a sua situação financeira e obtenham experiências do mercado que lhes permitam detectar sinais de alerta de potenciais problemas.

3.5.8. As instituições devem mitigar o risco de cessação ou liquidação imprevista dos seus principais provedores de serviços, dos quais as suas funções críticas do negócio dependem. Esta situação prende-se com o facto de as instituições poderem levar bastante tempo para implementar soluções alternativas. Para o efeito, devem tomar medidas razoáveis para manter um nível adequado de controlo e reservarem-se o direito de intervir com medidas apropriadas para continuar as suas operações críticas do negócio.

3.5.9. Em última análise, o risco de interdependência permanece com as instituições e essa responsabilidade não pode ser delegada. As instituições são ainda responsáveis por encontrar

[17] Provedores de serviços financeiros públicos são organizações que prestam serviços financeiros especializados, tais como compensação de cheques e liquidação.

[18] Para o propósito destas directrizes, são ISI aquelas de que outras instituições de crédito do sistema financeiro nacional dependem, a ponto de que suas dificuldades de recuperação de eventos adversos podem contribuir para a amplificação do risco sistémico.

equilíbrio entre riscos e custos, tratar os riscos devidamente e tomar medidas proporcionais à criticidade de funções do negócio, bem como com o tamanho e natureza de operações.

3.6. Princípio 6: As Instituições Devem Planear Interrupções de Vastas Áreas

3.6.1. O incidente de 11 de Setembro de 2001 demonstrou que as instituições devem planear interrupções que afectem uma vasta área/zona. Devido à diversidade de factores, como diferentes tamanhos e complexidade de operações do negócio entre instituições do sistema financeiro, não seria adequado, nem prático, padronizar um critério que defina uma "zona" para aplicação uniforme em todo o sector financeiro.

3.6.2. O Banco de Moçambique espera das instituições a demonstração de terem planeado e tomado providências na sua gestão da continuidade do negócio relativamente a interrupções abrangendo vastas áreas. Alguns parâmetros de planeamento que as instituições podem considerar são: a concentração geográfica de instituições, actividades de processamento transaccional e dependências de provedores de serviços internos e externos.

3.6.3. Dependendo da configuração operacional das instituições, as interrupções abrangendo vastas áreas podem ampliar os riscos de interdependência entre funções críticas e provedores de serviços dentro de uma mesma zona. Isto pode dever-se a interrupção generalizada de serviços críticos tais como falha de telecomunicações ou inacessibilidade de pessoal crítico. Tais riscos devem ser mitigados adequadamente.

3.6.4. As instituições são responsáveis por decidir sobre a necessidade de atender a múltiplos cenários de interrupção, considerando as suas actividades críticas e políticas de gestão de risco. Adicionalmente, elas devem considerar a expansão e aprofundamento do escopo da sua gestão de continuidade do negócio para atender a rupturas operacionais prolongadas.

3.7. Princípio 7: As Instituições Devem Estabelecer uma Política de Segregação para Mitigar o Risco de Concentração nas Funções Críticas do Negócio

3.7.1. A centralização de funções críticas do negócio e de suporte, tais como tesouraria, *back-office*, TI e centros de dados, traz benefícios económicos. Contudo, as instituições arriscam-se a perder a capacidade de recuperar estas funções na eventualidade de um incidente ou desastre.

3.7.2. O pessoal e informações críticas são activos importantes que são difíceis de substituir rapidamente. Muitas instituições assumem que o mesmo leque de pessoal estará disponível para recuperar as suas funções críticas do negócio, mas essa suposição nem sempre é verdadeira, pois as rupturas podem resultar na indisponibilidade do pessoal crítico. Por outro lado, identificar alternativas ao pessoal crítico nem sempre reduz o risco, especialmente se ambos, pessoal crítico e alternativo, estiverem alojados no mesmo local ou zona.

3.7.3. É importante, portanto, encontrar o equilíbrio certo entre a mitigação do risco de concentração e a preservação de eficiências obtidas da centralização de processos do negócio e do pessoal crítico. Para mitigar o risco de concentração de funções críticas do negócio, as instituições podem considerar as seguintes abordagens:

a) Separação do local primário e secundário: ao separar em diferentes zonas os locais primário e secundário de funções críticas do negócio pode-se mitigar o risco de perda de ambos os locais na eventualidade de ruptura que abranja uma vasta área.

b) Separação de funções críticas do negócio e separação intra-função: ao separar as funções críticas do negócio em diferentes zonas pode-se mitigar o risco de perda de múltiplas funções críticas devido a ruptura numa zona. Igualmente, ao diversificar por localizações as funções críticas do negócio, garantindo que o outro grupo de trabalho seja capaz de assumir as funções durante as rupturas, pode-se eliminar a dependência de um único grupo de trabalho.

3.7.4. Estas abordagens têm diferentes implicações de custos e, ainda que estes sejam um factor importante, as instituições devem desenhar e determinar a abordagem mais adequada ou combinar as abordagens para melhor balancear os custos e exposição a riscos, de modo a prover um adequado nível de conforto e garantia. A solução de mitigação deve ser proporcional à natureza, dimensão e complexidade das funções do negócio.

3.7.5. As instituições são encorajadas a serem inovadoras e a explorarem as diversas possibilidades de mitigação da concentração de risco.

IV Apêndices

4.1. Apêndice A: Estorvo de Ataques do Tipo *Man-In-The-Middle*

4.1.1. Como parte da infra-estrutura de autenticação de dois factores, as instituições de crédito devem também considerar e, se julgado apropriado, implementar os seguintes controlos e medidas de segurança para minimizar a exposição a ataques do tipo *man-in-the-middle*:

a) OTP específicos para a adição de novos beneficiários:
Cada novo beneficiário deve ser autorizado pelo cliente com base numa OTP de um segundo canal que, igualmente, mostre os detalhes do beneficiário ou a assinatura manuscritas do cliente, verificada na instituição de crédito a partir de um procedimento manual.

b) OTP individuais para transacções de valores (pagamentos e transferência de fundos):
Cada transacção de valor ou uma lista aprovada de transacções de valores acima de um certo limite determinado pelo cliente deve requerer um novo OTP. Todos os pagamentos e transacções de transferência de fundos devem ser encriptados na camada da aplicação.

c) Janela de tempo de OTP:
OTP *challenge-based* e *time-based* fornecem melhor segurança, porque o seu período de validade é inteiramente controlado pela instituição de crédito e não depende do comportamento do utilizador. Devido aos problemas de sincronização temporal, a utilização de OTP time-based requer uma janela de tempo do lado do servidor. As instituições de crédito não devem permitir que a janela de tempo de OTP exceda 100 segundos. Quanto menor a janela de tempo, menor o risco de abuso do OTP.

d) Segurança de pagamentos e transferências de fundos:
Podem ser utilizadas assinaturas digitais e códigos baseados em chave para autenticação de mensagem (KMAC[19]), com vista à detecção de modificações não autorizadas ou de injecção de dados transaccionais em ataques do tipo *man-in-the-middle*. Para que esta solução de segurança funcione efectivamente, um cliente utilizando token de *hardware* deve poder

[19] KMAC: *key-based message authentyication codes*.

distinguir o processo de geração de OTP do processo de assinatura digital de uma transacção. O que o cliente assina digitalmente também deve ser significativo para si. Isto significa que os *tokens* devem, no mínimo, mostrar de forma explícita o número de conta do beneficiário e o montante de pagamento, a partir do qual um valor *hash* pode ser derivado com o propósito de criar uma assinatura digital. Chaves criptográficas diferentes devem ser usadas para gerar OTP e para assinar transacções.

e) Notificação/confirmação por segundo canal:

A instituição de crédito deve notificar o cliente, através de um segundo canal, em relação a todos os pagamentos ou transacções de transferência de fundos acima de um determinado valor especificado pelo cliente.

f) Tempo limite de sessão:

Uma sessão online deve ser terminada após um período fixo de tempo, a não ser que o cliente seja re-autenticado para que a actual sessão seja mantida. Isto previne que um atacante possa manter uma sessão de internet banking activa indefinidamente.

g) Aviso de certificado de servidor SSL:

Clientes de *internet banking* devem ser consciencializados e instruídos sobre como reagir ao aviso de certificado de servidor SSL. Eles devem terminar a sessão de *login* se o certificado SSL não pertencer à instituição de crédito e um aviso deve ser dado para o efeito. Os clientes devem informar a instituição de crédito imediatamente após o *log off*.

4.2. Apêndice B: Teste de Segurança de Sistema

4.2.1. O teste de segurança de sistema deve incluir as seguintes especificações:

a) Fuga de informação:

A colecta de informação sobre um sistema é normalmente o primeiro passo que um *hacker* toma através do scanning e sondagem do perímetro da rede e dos limites do sistema. À sua disposição estão os motores de busca públicos, *scanners* de rede e mensagens especialmente criadas, que podem ser utilizadas para descobrir brechas ou vulnerabilidades de segurança que possam ser exploradas para aceder ao sistema. Devem ser conduzidos testes para detectar prolixidade e promiscuidade nos sistemas de rede.

b) Lógica do negócio:

Erros cometidos na implementação da lógica do negócio podem conduzir a brechas de segurança, pelas quais usuários podem executar funções não autorizadas. Por exemplo, uma operação de transacção deve ser executada numa sequência, mas o utilizador pode ignorar os controlos através do baralhamento da sequência de passos de entrada.

c) Autenticação:

O exemplo mais comum de um esquema de autenticação é o processo de logon utilizando *passwords* estáticas ou dinâmicas. O teste de autenticação deve assegurar que os requisitos de segurança (expiração de credenciais, revogação, reutilização, etc.) são correctamente implementados e que a protecção de funções de segurança e de chaves criptográficas é robusta.

d) Autorização:

Após autenticação de um usuário e o consequente acesso ao sistema, a autorização ajuda a garantir que a um determinado usuário somente lhe seja permitido visualizar, escrever, executar, modificar, criar e/ou apagar dados e invocar as funções dentro das suas permissões. Devem ser conduzidos testes para verificar se a matriz de acesso de segurança funciona correctamente em várias permutações.

e) Validação de entrada de dados:

A fraqueza mais comum nas aplicações é a falha de validação apropriada de entrada de dados dos usuários. Esta fraqueza pode criar maiores vulnerabilidades tais como injecção de scripts e *overflows* de *buffer*. Uma validação apropriada de dados deve incluir o seguinte:

i. Todas as entradas numa aplicação devem ser validadas;

ii. Todas as formas de dados (tais como caixas de texto, caixas de selecção e campos ocultos) devem ser verificadas;

iii. O tratamento de dados de entrada nulos ou incorrectos deve ser verificado;

iv. A formatação de conteúdos deve ser verificada;

v. O tamanho máximo de cada campo de entrada deve ser validado.

f) Tratamento de excepções/erros:

O tratamento rigoroso de excepções/erros pode facilitar o processamento livre de falhas numa situação de vários erros e em condições de excepção. A fuga de informação sensível não deve ser resultado duma falha de sistema.

g) Gestão de sessão:

A manipulação da gestão de sessão de aplicações pode conduzir a problemas de segurança. Para assegurar uma gestão segura de sessão, as seguintes condições devem ser observadas:

i. As informações sensíveis passadas através de *cookies* devem ser encriptadas;

ii. O identificador de sessão deve ser aleatório e único;

iii. A sessão deve expirar após um tempo pré-determinado.

h) Criptografia:

A criptografia deve ser empregue para proteger dados sensíveis. A resistência da criptografia não só depende do algoritmo e tamanho da chave, mas também da sua implementação. Deste modo, a implementação deve ser rigorosamente testada, cobrindo todas as funções criptográficas (encriptação, desencriptação, *hashing*, assinatura) e procedimentos chave de gestão (geração, distribuição, instalação, renovação, revogação e expiração).

i) *Logging*:

O *logging* deve ser correctamente implementado para evitar defeitos de segurança, assim como para facilitar investigações de acompanhamento

e troubleshooting quando ocorre um incidente de sistema. Devem ser aplicados os seguintes requisitos e especificações:

i. Dados sensíveis como *passwords* e credenciais de autenticação não devem ser registados em ficheiros de transacção ou de actividade do sistema;

ii. A extensão máxima de dados para o *logging* deve ser pré-determinada;

iii. Devem ser registadas todas tentativas de autenticação, tenham elas sido bem ou mal sucedidas;

iv. Devem ser registados todos os eventos de autorização, tenham eles sido bem ou mal sucedidos.

j) Desempenho e estabilidade:

O desempenho e a estabilidade de um sistema em condições irregulares, tais como rácios anormais de tráfego ou reboots frequentes, devem ser verificados. Devem ser conduzidos testes de esforço para além dos limites estabelecidos nos sistemas, para assegurar que a aplicação mantém um funcionamento correcto, embora com níveis de serviço degradados.

Aviso n.º 5/GBM/2013

de 18 de Setembro

Havendo necessidade de actualizar os anexos 1 e 2 do Regulamento do Sistema de Operações de Mercado aos Mercados Monetário e Cambial Interbancários, o Banco de Moçambique, no uso das competências que lhe são conferidas pelo n.º 1 do artigo 21 da Lei n.º1/92, de 3 de Janeiro – Lei Orgânica do Banco, determina:

1. É aprovado o Regulamento do Sistema de Operações de Mercado, que constitui o anexo deste Aviso faz parte integrante do mesmo.

2. O presente Aviso entra em vigor na data da sua publicação e revoga o Regulamento aprovado pelo Aviso n.º 2/GBM/2009, de 26 de Fevereiro.

As dúvidas que surgirem na interpretação e aplicação do presente Aviso deverão ser submetidas ao Departamento de Mercados do Banco de Moçambique.

Banco de Mo;ambique, em Maputo, 6 de Junho de 2013. – O Governador, *Ernesto Gouveia Gove*.

Regulamento do Sistema de Operações de Mercado

ARTIGO 1

Objecto

1. O Sistema de Operações de Mercado, adiante designado por SOM, é composto por um conjunto de normas e procedimentos a observar pelo Banco de Moçambique e pelas instituições autorizadas a participar no Mercado Cambial Interbancário e no Mercado Monetário Interbancário, doravante designados por MCI e MMI, respectivamente, relativamente às operações realizadas nesses mercados.

2. As comunicações entre o Banco de Moçambique e as instituições participantes no SOM são, em geral, estabelecidas por via electrónica, através de uma aplicação informática (*Meticalnet*) que funciona "on line" ou outro meio de comunicação que venha a ser indicado pelo Banco de Moçambique.

3. O Banco de Moçambique emite comprovativos das operações realizadas.

ARTIGO 2

Instituições participantes

Podem participar no SOM as instituições que, para o efeito, forem autorizadas pelo Banco de Moçambique.

ARTIGO 3

Requisitos de adesão ao SOM

São requisitos de adesão ao SOM:

a) Estar vinculado ao regime de constituição de reservas obrigatórias;

b) Subscrever o Código de Conduta dos Mercados Interbancários.

ARTIGO 4

Procedimentos para adesão ao SOM

1. A autorização para utilizar o SOM e intervir nos diversos segmentos dos mercados deve ser solicitada através de carta dirigida ao Departamento de Mercados do Banco de Moçambique.

2. O Departamento de Mercados deve comunicar da decisão sobre os pedidos a que se refere o número anterior no prazo máximo de 5 dias úteis, a contar da data de recepção dos mesmos.

3. As entidades aderentes ao SOM devem solicitar ao Banco de Moçambique, através do Departamento de Assuntos Jurídicos, a actualização das fichas de abertura de contas, de forma a fazerem constar das mesmas os nomes das pessoas com poderes para movimentar as contas, no âmbito das operações realizadas no MCI e MMI, observando o modelo que consta no Anexo 1.

4. No anexo referido na parte final do número anterior, as entidades aderentes ao SOM devem mencionar o nome das pessoas autorizadas a efectuar as operações a realizar no MCI e MMI.

5. Para efeitos de realização das operações por via electrónica, através da aplicação informática do MCI e MMI, o Banco de Moçambique comunica a cada instituição os códigos de acesso a atribuir às pessoas referidas nos n.os 3 e 4 deste artigo.

ARTIGO 5

Dever das Instituições participantes

As entidades aderentes devem respeitar as normas relativas aos mercados em que participem, bem como as normas operativas estabelecidas quanto ao funcionamento do SOM.

ARTIGO 6

Forma que revestem as operações no SOM

1. As operações realizadas através do SOM que tenham por objecto Bilhetes do Tesouro ou títulos emitidos pelo Banco de Moçambique, sob forma escritural, estão isentas de número de ordem e são materializadas pela sua mera inscrição em contas-título abertas no Banco de Moçambique em nome dos respectivos titulares.

2. De modo a reflectir as diversas situações patrimoniais dos títulos registados em cada conta-título, podem ser abertas tantas sub-contas quantas se mostrarem necessárias.

3. Nas contas-título, e sub-contas referidas neste artigo, e proceder-se ao lançamento das operações de que tais títulos forem objecto e registar-se, através de Inscrições, o exercício de direitos de conteúdo patrimonial.

4. As inscrições são canceladas pelo reembolso ou pela venda total ou parcial dos títulos por elas abrangidos; neste último caso, o cancelamento é realizado de acordo com a quantidade de títulos vendidos.

ARTIGO 7

Forma de comunicação

1. As instituições participantes devem transmitir por via electrónica, utilizando a aplicação informática, ou por outro meio de comunicação que seja indicado pelo Banco de Moçambique, os elementos relativos às operações que pretendam realizar através do SOM.

2. O Banco de Moçambique utiliza os mesmos meios de comunicação referidos no número anterior para anunciar as operações que se propõe realizar e para transmitir os respectivos resultados.

ARTIGO 8

Elementos a comunicar

1. O Banco de Moçambique indica, em regulamentação específica, os elementos que identificam a operação, os quais devem ser comunicados pelas instituições participantes.

2. Os códigos das operações constam do Anexo 2 ao presente Regulamento.

ARTIGO 9

Confirmação das operações

1. As operações realizadas por meio de comunicação electrónica por via da aplicação informática devem ser confirmadas pelo usuário com o perfil de Aprovador, através da alteração do Status da Transmissão de "Verificado" para "Aprovado".

2. A confirmação das operações referidas no número anterior autoriza, de forma irreversível, os movimentos nas contas de depósito à ordem abertas no Banco de Moçambique em nome das instituições, bem como nas respectivas contas-título, quando for o caso.

ARTIGO 10

Funcionamento

1. O SOM funciona no Departamento de Mercados, todos os dias úteis, no horário que for estabelecido pelo Banco de Moçambique.

2. As operações realizadas entre instituições participantes podem ser transmitidas durante todo o período de funcionamento do SOM.

3. As demais operações previstas nas instruções que regulam o MCI e o MMI devem ser transmitidas nos períodos que, para o efeito, forem anunciados pelo Banco de Moçambique.

ARTIGO 11

Sanções

O Banco de Moçambique poderá excluir do acesso a todos ou parte dos serviços prestados pelo SOM as entidades que, por incumprimento do preceituado neste regulamento ou por negligência grave, ocasionarem perturbações ao normal funcionamento do SOM ou por qualquer forma colocarem em perigo a sua segurança.

Anexo 1

Departamento de Assuntos Jurídicos

Banco de Moçambique

Av. 25 de Setembro, 1679

Maputo

Assunto: Aprovadores e comunicadores das operações do MCI e MMI.

Exmo. Senhor,

Em aditamento à ficha de abertura de contas em poder dessa instituição, vimos, pelo presente meio e em obediência ao estabelecido no n.º 3 do artigo 4 do Regulamento do SOM, solicitar que tomem boa nota de que estão autorizadas por esta instituição, na qualidade de aprovador, a movimentar electronicamente, através do sistema informático, contas do ..... (nome da instituição), nomeadamente para efeitos de aprovação das operações a serem realizadas em todos os segmentos do MCI e MMI a que tenhamos acesso, as seguintes pessoas:

Cargo	Nome	Apelido	Assinatura

Esta instituição obriga-se pelas assinaturas de _____ aprovador(es) nas operações transmitidas por via electrónica, através da aplicação informática. Nas operações transmitidas por fax ou outro meio de comunicação, esta instituição obriga-se pela assinatura de _____ aprovador(es), cessando, assim, para este efeito, as seguintes assinaturas:

_____

_____

_____

_____

_____

_____

_____

Aproveitamos a ocasião para informar que são nomeados comunicadores desta instituição, para efeitos do estabelecido no n.º 4 do supracitado artigo 4, as seguintes pessoas:

Cargo	Nome	Apelido

Sem outro assunto, de momento, (fecho)

O representante com poderes legais para o acto

_____

Anexo 2

Códigos das Operações Realizadas no Âmbito do Mercado Monetário Interbancário

AFPD – Absorção de liquidez no âmbito da facilidade permanente de depósito

AFPDV – Vencimento de absorção de liquidez no âmbito da facilidade permanente de depósito

BTAR – Facilidade permanente de cedência de liquidez, tendo bt's como colateral

BTCV – Vencimento de facilidade permanente de cedência de liquidez, tendo bt's como colateral

BTPR – Emissão de bilhetes do tesouro

OTAR – Facilidade permanente de cedência de liquidez, tendo ot's como colateral

OTCV – Vencimento de facilidade permanente de cedência de liquidez, tendo ot's como colateral

REEMBTAM – Vencimento de títulos de autoridade monetária

REEMBTS – Reembolso de bilhetes do tesouro

REPOBT – Compra de bilhetes do tesouro, com acordo de revenda

REPOBTR – Venda de bilhetes do tesouro, com acordo de recompra

REPOBTCV – Vencimento de acordo de revenda de *bt's* Vencimento de acordo de recompra de bt's

REPOOT – Compra de ot's, com acordo de revenda

REPOOTR – Venda de ot's, com acordo de revenda

REPOOTCV – Vencimento de acordo de recompra de *ot's*

REPOTAM – Compra de títulos de autoridade monetária, com acordo de revenda

REPOTAMR – Venda de títulos de autoridade monetária, com acordo de revenda

REPOTAMCV – Vencimento de acordo de revenda de tam's

REPOTAMCVR – Vencimento de acordo de recompra de tam's

TAMAR – Facilidade permanente de cedência, tendo *tam's* como colateral

TAMCV – Vencimento de facilidade permanente de cedência de liquidez, tendo *tam's* como colateral

TAMPR – Emissão de títulos de autoridade monetária

TIPCD – Transferência de liquidez entre as instituições participantes, sem garantia de títulos

TIPCV – Vencimento de transferência de liquidez entre as instituições participantes, sem garantia

TIPGCD – Transferência de liquidez entre as instituições participantes, com garantia de títulos

TIPGCV – Vencimento de transferência de liquidez entre as instituições participantes, com garantia

---

Aviso n.º 6/GBM/2013

de 18 de Setembro

Havendo necessidade de garantir fluidez na realização de operações com acordo de recompra e revenda de títulos do Mercado Monetário Interbancário, o Banco de Moçambique, no uso das competências que lhe são conferidas pelo n.º 1 do artigo 21 da Lei n.º 1/92, de 3 de Janeiro, - Lei Orgânica do Banco - determina:

1. É aprovado o Regulamento sobre Operações com acordo de recompra e revenda de Títulos de Renda Fixa, que constitui o anexo e faz parte integrante do presente Aviso.

2. O presente Aviso entra em vigor na data da sua publicação e revoga o Aviso n.º 11/GBM/2007, de 11 de Julho.

As dúvidas que surgirem da interpretação e aplicação do presente Aviso deverão ser submetidas ao Departamento de Mercados do Banco de Moçambique.

Banco de Moçambique, em Maputo, 6 de Junho de 2013. – O Governador, *Ernesto Gouveia Gove*.

Regulamento Sobre Operações com Acordo de Recompra e Revenda de Títulos de Renda Fixa

CAPÍTULO I

Disposições Gerais

ARTIGO 1

Objecto

O presente Regulamento tem por objecto estabelecer o regime das operações com acordo de recompra e revenda de Títulos de Renda Fixa do Mercado Monetário Interbancário.

ARTIGO 2

Definições

Para efeitos do presente Regulamento, entende-se por:

a) Bilhetes do Tesouro (BT) – os valores mobiliários escriturais representativos de empréstimo de curto prazo da República de Moçambique, denominados em moeda nacional;

b) Grande Risco - o risco assumido por uma instituição de crédito quando o seu valor, isoladamente ou em conjunto com os outros vigentes respeitantes ao mesmo cliente, represente pelo menos 10% dos fundos próprios da instituição;

c) Mercado Monetário Interbancário (MMI) – o segmento do mercado monetário do Metical, regulamentado, no qual as instituições autorizadas permutam fundos representados por saldos das suas contas de depósito à ordem no Banco de Moçambique ou valores mobiliários desmaterializados inscritos em contas-título neste mesmo Banco, visando equilibrar os excedentes e necessidades de moeda primária entre as instituições monetárias. Neste segmento, o Banco de Moçambique pode intervir absorvendo ou cedendo liquidez, através da compra, venda ou emissão de títulos.

d) Meticalnet – o sistema informático do Banco de Moçambique;

e) Operações com acordo de recompra – venda de títulos com acordo de recompra assumido pelo vendedor, conjugadamente com acordo de revenda assumido pelo comprador, para liquidação em data pré--estabelecida;

f) Operações com acordo de revenda – compra de títulos com acordo de revenda assumido pelo comprador, conjugadamente com o acordo de recompra assumido pelo vendedor, para liquidação em data pré-estabelecida;

g) Risco - qualquer facilidade, utilizada ou não, concedida por uma instituição de crédito e traduzida, designadamente, na atribuição de crédito, ainda que sob forma de fiança, garantia bancária ou outra semelhante, e na aquisição ou detenção de participações financeiras ou de títulos de qualquer natureza emitidos pelo mesmo cliente;

h) Sistema de Operações de Mercado (SOM) – conjunto de normas e procedimentos observados pelo Banco de Moçambique e pelas instituições autorizadas a participar no Mercado Monetário Interbancário, relativamente às operações realizadas neste mercado;

i) Títulos da Autoridade Monetária (TAM's) – títulos de depósito utilizados pelo Banco de Moçambique com o objectivo de intervenção no mercado monetário;

j) Títulos de Renda Fixa - Activos que prevêem a correcção do seu valor nominal por uma rentabilidade definida ou um parâmetro de remuneração previamente estabelecido.

ARTIGO 3

Condições de acesso

As operações objecto do presente Regulamento somente podem ser realizadas entre as instituições participantes do Sistema de Operações do Mercado, nos termos estabelecidos no respectivo Regulamento aprovado pelo Aviso n.º 5/GBM/2013, de 6 de Junho de 2013.

CAPÍTULO II

TÍTULOS

ARTIGO 4

Títulos elegíveis

São elegíveis para as operações objecto do presente Regulamento os seguintes títulos:

a) Bilhetes do Tesouro;
b) Títulos da Autoridade Monetária;
c) Outros títulos que venham a ser autorizados pelo Banco de Moçambique.

ARTIGO 5

Registo

Os títulos a que se refere o artigo anterior só podem servir de base às operações objecto do presente Regulamento quando devidamente registados no Sistema de Registo, Liquidação e Custódia do Banco de Moçambique, designado Meticalnet ou em sistema de registo e de liquidação financeira de activos autorizado e/ou aceite pelo Banco de Moçambique.

ARTIGO 6

Venda de Títulos de Acordo de Revenda

Os títulos objecto de acordos de revenda podem ser vendidos em novas operações de acordo de recompra e revenda com data de recompra igual ou anterior à data da revenda.

ARTIGO 7

Prazo de garantia

Os títulos objecto de acordos de revenda somente podem servir de garantia em operações com acordo de recompra que tenham data de liquidação igual ou anterior à data de revenda.

CAPÍTULO III

Realização das operações

ARTIGO 8

Prazos das operações

As operações objecto do presente Regulamento não podem ser acordadas por prazos que excedam os de vencimento dos títulos que lhes servem de base.

ARTIGO 9

Preço e valor de liquidação

1. As operações objecto do presente Regulamento devem ser realizadas a preços fixos, negociados entre as partes, devendo o valor de liquidação ser previamente definido.

2. O preço e valor de liquidação das operações objecto do presente Regulamento devem ser calculados segundo a fórmula constante do anexo ao presente Regulamento.

ARTIGO 10

Liquidação financeira

1. A liquidação financeira das operações que não envolvem o Banco de Moçambique é efectuada, por débito ou crédito às contas de depósito à ordem tituladas no Banco de Moçambique, no mesmo dia da realização da operação, observado o princípio de entrega contra pagamento, através do Meticalnet.

2. A liquidação financeira das operações que envolvem o Banco de Moçambique é efectuada, por débito ou crédito às contas de depósito à ordem tituladas no Banco de Moçambique, em contrapartida de uma conta específica do Banco de Moçambique, no mesmo dia da realização da operação, observado o princípio de entrega contra pagamento, através do Meticalnet.

CAPÍTULO IV

Limites operacionais

ARTIGO 11

Base de cálculo dos limites

Na realização das operações objecto do presente Regulamento, a base de cálculo para os limites operacionais da instituição são os respectivos fundos próprios nos termos definidos pelo Aviso n.º 5/GBM/2007, de 2 de Maio.

ARTIGO 12

Limites

1. As instituições habilitadas à realização de operações previstas neste Regulamento que tenham recebido títulos em contrapartida da cedência de recursos financeiros devem observar os seguintes limites:

a) Em relação a um só vendedor de títulos não devem realizar operações com acordo de revenda cujo valor, no seu conjunto, exceda 25% dos seus fundos próprios.
b) O valor agregado das compras de títulos classificados como grande risco não deve exceder oito vezes o valor dos fundos próprios.

2. O valor das vendas com acordo de recompra, em termos individual e agregado, com Bilhetes do Tesouro, Títulos da Autoridade Monetária e outros títulos que venham a ser autorizados pelo Banco de Moçambique,
independentemente das condições de remuneração e prazo, não deve exceder oito vezes o valor dos seus fundos próprios.

3. Quando um risco sobre uma entidade estiver garantido por um terceiro, de forma irrevogável e juridicamente vinculativa, considera-se que tal risco é assumido sobre esse terceiro e não sobre a entidade.

ARTIGO 13

Verificação

A verificação do cumprimento dos limites operacionais estabelecidos no artigo anterior efectua-se com base na computação dos valores efectivos da liquidação das operações.

CAPÍTULO V

Infracções e sanções

ARTIGO 14

Infracções

Constituem infracções ao presente Regulamento:

a) A realização de operações com acordo de recompra e revenda tendo por objecto outros títulos que não os referidos no artigo 4 do presente Regulamento;

b) A venda de títulos sem que o vendedor tenha, na ocasião, a propriedade dos títulos negociados;
c) A negociação de títulos a preço unitário manifestamente diferente do praticado no mercado ou, na ausência de publicação que informe o preço de mercado, a preço manifestamente diferente do valor nominal vigente;
d) A criação de condições artificiais de negociação ou manipulação de preços de títulos objecto de operações com acordo de recompra ou revenda;
e) A inobservância dos limites operacionais estabelecidos neste Regulamento;
f) O incumprimento da obrigatoriedade de remessa, nos prazos estabelecidos na regulamentação em vigor, das informações relativas às operações com acordo de recompra ou revenda de títulos;
g) A adopção de prática que, deliberadamente, implique apresentação de informações inexactas.

ARTIGO 15

Sanções

Sem prejuízo de outras sanções que ao caso possam caber, nos termos previstos em demais disposições legais ou regulamentares aplicáveis, a violação das normas previstas neste Regulamento e normativos complementares sujeita a entidade infractora à suspensão da realização de quaisquer dos tipos de operações com acordo de recompra ou revenda de títulos, por um período não inferior a seis meses contados da data da comunicação da respectiva decisão tomada pelo Banco de Moçambique.

CAPÍTULO VI

Disposições finais

ARTIGO 16

Dever de comunicação

As instituições autorizadas a realizar operações objecto do presente Regulamento são obrigadas a comunicar ao Banco de Moçambique todas as operações com acordo de recompra e revenda de títulos por elas realizadas, na forma, prazos e demais termos previstos nos Regulamentos do MMI e do SOM.

ARTIGO 17

Divulgação de Informações e Remessa de Documentos

O Banco de Moçambique comunica as condições de prestação e de divulgação de informações sobre as operações objecto do presente Regulamento.

ANEXO

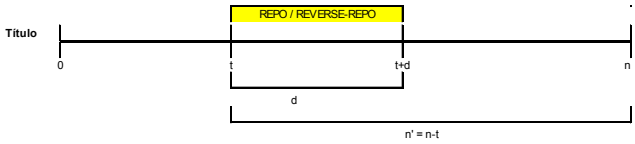
Fórmulas a Aplicar no Cálculo do Preço e Valor de Liquidação de Operações de Operações com Acordos de Recompra e Revenda de Títulos de Renda Fixa

1. Operação de Venda / Compra de Títulos com Acordo de Recompra/Revenda

Considere-se a seguinte terminologia:

VNu = Valor Nominal unitário do título = MZN 1.000,00.
Pu = Preço unitário actualizado/ descontado do título (preço de colateral = preço de venda / compra com acordo de recompra / revenda).
B = Base anual (365 dias, para efeitos do presente Regulamento).
i = taxa de juro de colateral.
t = Data-Valor da operação.
n = prazo do título (em dias).
n' = número de dias para o vencimento do título (n' = n-t, em dias).
QT = Quantidade de títulos a entregar/receber pela operação.
VN = Valor Nominal Total da operação.
r = taxa de juro da operação.
d = prazo da operação (em dias).
VT = Valor Total de Transacção da operação (capital financeiro).
VT' = Valor Total de Transacção ajustado da operação (capital financeiro ajustado).
VR = Valor total de reembolso da operação = Valor de Recompra/Revenda.
Pu' = Preço unitário de recompra/revenda.
JT = Juro Total da operação.
Ju = Juro unitário da operação.

Esquema da Operação



O preço unitário de um título em cada momento de sua vida útil é obtido a partir da seguinte fórmula:

$$(i) \qquad P_u = \frac{VN_u \times B}{B + i \times n'}$$

O resultado obtido na fórmula (*i*) deve ser arredondado a 5 casas decimais.

A quantidade de títulos que servirão para colaterizar a operação será obtida como resultado do quociente entre o valor de transacção da operação e o preço unitário:

$$(ii) \qquad QT = \frac{VT}{P_u}$$

Devendo o resultado obtido na fórmula (*ii*) ser um número inteiro arredondado sempre por excesso.

Na data-valor da contratação da operação, o capital a ser efectivamente transaccionado (VT) deverá ser ajustado por forma a compensar o efeito resultante do arredondamento efectuado na obtenção da quantidade total de títulos transaccionados. Assim, o valor de transacção ajustado (ou capital financeiro ajustado, VT') será obtido a partir da seguinte fórmula:

$$(iii) \qquad QT' = P_u \times VT$$

O valor nominal correspondente ao capital transaccionado na operação é obtido pelo produto entre a quantidade total de títulos e o valor nominal unitário de cada título.

$$(iv) \qquad VN = VN_u \times QT$$

O valor do juro total da operação é calculado por uma das fórmulas a seguir indicadas:

$$(iv) \qquad JT = VT' \times r \times \frac{d}{B} \text{ ou } JT = J_u \times QT$$

O valor do juro unitário da operação é calculado por uma das fórmulas a seguir indicadas:

$$(vi) \qquad J_n = P_u \times r \times \frac{d}{B} \text{ ou } J_u = \frac{JT}{QT}$$

O valor total de reembolso (recompra/revenda) na data de vencimento da operação é obtido por uma das seguintes fórmulas:

$$(vii) \qquad VR = VT' + JT \text{ ou } VR = P_u' \times QT$$

O preço unitário de recompra/revenda na data de vencimento da operação é obtido por uma das seguintes fórmulas:

$$(viii) \qquad P_u' = P_u + JT \text{ ou } P_u = \frac{VR}{QT}$$

1. Operação de Venda / Compra Definitiva de Títulos

Considere-se a seguinte terminologia:

VN_u = Valor Nominal unitário do título = MZN 1.000,00.

P_u = Preço unitário actualizado/ descontado do título (preço de venda / compra definitiva) no momento t.

$P_{u\ t-1}$ = Preço de Aquisição do título no momento t-1 (no mercado primário ou secundário). Sendo no mercado primário, Put-1 será igual ao preço de emissão do título; sendo no mercado secundário, será igual ao preço de venda / compra definitiva no momento anterior à operação corrente.

P_m = Preço de Mercado.

B = Base anual (365 dias, para efeitos do presente Regulamento).

t = Data-Valor da operação.

t' = Prazo (em dias) decorrido desde aquisição do título até a data-Valor da valorização.

n = prazo do título (em dias).

n' = número de dias para o vencimento do título (n' = n-t, em dias).

QT = Quantidade de títulos a entregar / receber pela operação.

VN = Valor Nominal Total da operação.

r = taxa de juro da operação

r_t = taxa de juro pela qual o título está sendo remunerada desde a aquisição até ao período t.

r_{t-1} = taxa de juro da operação no momento t-1. Pode ser idêntica a taxa de juros de emissão quando o período t-1 coincidir com o momento da emissão.

VT = Valor Total de Transacção da operação (capital financeiro).

VT' = Valor Total de Transacção ajustado da operação (capital financeiro ajustado).

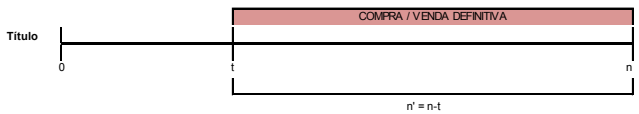
JT = Juro Total da operação (para o comprador).

Ju = Juro unitário da operação (para o comprador).

Gc = Ganho de Capital (para o vendedor).

Pc = Perda de Capital (para o vendedor).

Esquema da Operação



O preço unitário de um título em cada momento de sua vida útil é obtido a partir da seguinte fórmula:

$$(ix) \qquad P_{u_t} = \frac{VN_u \times B}{B + r \times n'}$$

O resultado obtido na fórmula (ix) deve ser arredondado a 5 casas decimais.

A quantidade de títulos que servirão para colaterizar a operação será obtida como resultado do quociente entre o valor de transacção da operação e o preço unitário:

$$(x) \qquad QT = \frac{VT}{P_{u_t}}$$

Devendo o resultado obtido na fórmula (x) ser um número inteiro arredondado sempre por excesso.

Na data-valor da contratação da operação, o capital a ser efectivamente transaccionado (VT) deverá ser ajustado de forma a compensar o efeito resultante do arredondamento efectuado na obtenção da quantidade total de títulos transaccionados. Assim, o valor de transacção ajustado (ou capital financeiro ajustado, VT') será obtido a partir da seguinte fórmula:

$$(xi) \quad VT' = P_{u_t} \times QT$$

O valor nominal total correspondente ao capital transaccionado na operação é obtido pelo produto entre a quantidade total de títulos e o valor nominal unitário de cada título.

$$(xii) \quad VN = VN_u \times QT \text{, sendo que } VN_u = MZN\ 1.000,00.$$

O valor do juro total da operação, a ser recebido pelo comprador do título no fim da vida útil do mesmo, é calculado pela fórmula:

$$(xiii) \quad JT = VN - VT'$$

Ganhos de Capital e Perdas de Capital

Os ganhos de capital (G_c) e perdas de capital (P_c) serão determinados pela fórmula seguinte:

$$(xiv) \qquad G_c, P_c = P_{u_t} - P_{u_{t-1}}$$

Sendo que o vendedor irá obter um ganho de capital se o resultado for maior que zero; e terá uma perda de capital se o resultado for inferior a zero.

Onde o $P_{u_{t-1}}$ é calculado pela fórmula $P_{u_{t-1}} = \frac{VN_u \times B}{B + r_{t-1} \times n}$

Mais-Valias e Menos-Valias

Na efectivação da venda definitiva do título, o vendedor poderá realizar mais-valia ou menos-valia, que resulta da diferença entre o preço efectivo da venda do título (P_{u_t}), e o preço ao qual o mesmo título está sendo valorizado no mercado.

O preço de mercado (P_m) é calculado pela seguinte fórmula:

$$(xv) \qquad P_m = \frac{VN_u \times B}{B + i_m \times n}$$, onde teremos:

• Mais Valia, se $P_{u_t} > Pm$

• Menos Valia, se $P_{u_t} < Pm$

Flutuação de Valores

Nos termos das Normas Internacionais do Relato Financeiro (NIRF´s) em vigor os títulos que forem detidos para a negociação estão sujeitos a necessidade de valorização a mercado (marcação a preços de mercado). A diferença entre o preço de mercado (P_m) e o Preço Contabilístico (P_{cont}) resulta na flutuação de valores dos títulos, que pode ser negativa ou positiva. O preço Contabilístico é calculado pela seguinte fórmula:

$$(xvi) \quad P_{Cont} = P_{t-1}(1 + \frac{t' \times r_t}{B})$$

• Flutuação negativa $P_{t-1} > P_m$

• Flutuação positiva $P_{t-1} < P_m$

Aviso n.º 7/GBM/2013

de 18 de Setembro

Havendo necessidade de actualizar o quadro normativo que regula o Mercado Monetário Interbancário, o Banco de Moçambique, no uso das competências que lhe são conferidas pelo n.º 1 do artigo 21 da Lei n.º 1/92, de 3 de Janeiro – Lei Orgânica do Banco, determina:

É aprovado o Regulamento do Mercado Monetário Interbancário, em anexo, que faz parte integrante deste Aviso.

O presente Aviso entra em vigor na data da sua publicação e revoga o Aviso n.º 1/GBM/2009, de 26 de Fevereiro.

As dúvidas que surgirem na interpretação e aplicação do presente Aviso deverão ser submetidas ao Departamento de Mercados do Banco de Moçambique.

Banco de Moçambique, em Maputo, 6 de Junho de 2013. – O Governador, *Ernesto Gouveia Gove*.

Regulamento do Mercado Monetário Interbancário

CAPÍTULO I

Mercado Monetário Interbancário

ARTIGO 1

Conceito e objectivos do MMI

1. O Mercado Monetário Interbancário, doravante designado por MMI, é um segmento regulamentado do mercado monetário do Metical, no qual as instituições autorizadas permutam fundos representados por saldos das suas contas de depósito à ordem no Banco de Moçambique ou valores mobiliários desmaterializados inscritos em contas-título neste mesmo Banco, visando equilibrar os excedentes e necessidades de moeda primária entre as instituições monetárias.

2. O Banco de Moçambique pode intervir no MMI, absorvendo ou cedendo liquidez, através da compra, venda ou emissão de títulos.

ARTIGO 2

Montante mínimo das operações do MMI

Os montantes das operações realizadas no MMI são expressos em milhões de meticais, sendo que:

a) O valor de cada operação da iniciativa do Banco de Moçambique não deve ser inferior a 5 milhões de meticais;

b) O valor de cada operação da iniciativa dos Bancos comerciais não deve ser inferior a 1 milhão de meticais.

CAPÍTULO II

Operações de transferência de liquidez entre as instituições participantes

ARTIGO 3

Cedência e obtenção de fundos

1. As instituições financeiras previamente autorizadas pelo Banco de Moçambique podem ceder, na base da confiança, fundos detidos nas respectivas contas de depósito à ordem no Banco de Moçambique a outras instituições autorizadas a participar no MMI.

2. Nos termos do Regulamento sobre as operações com acordo de recompra e revenda de títulos de renda fixa, as instituições referidas no número 1 do presente artigo podem obter fundos sob a forma de depósitos à ordem no Banco de Moçambique, cedendo a outras instituições participantes no mercado títulos desmaterializados inscritos em contas-título no Banco de Moçambique, nomeadamente, Bilhetes do Tesouro (BT),Títulos da Autoridade Monetária (TAM) e outros títulos que vierem a ser autorizados pelo Banco de Moçambique.

ARTIGO 4

Requisitos a observar nas operações

As instituições devem negociar as operações, observando o seguinte:

a) Os montantes das operações são estipulados com observância do disposto no artigo 2 do presente regulamento;

b) As operações são realizadas a prazo certo, o qual não pode exceder um ano;

c) Sempre que a data de vencimento das operações não coincidir com um dia útil, o prazo é considerado terminado no dia útil imediatamente anterior;

d) As taxas de juro são expressas até à centésima de ponto percentual;

e) As operações contratadas de acordo com o n.º 1 do artigo 3 são realizadas pelo montante negociado;

f) Os montantes negociados, relativos às operações contratadas de acordo com o n.º 2 do artigo 3 do presente Regulamento, referem-se ao valor dos títulos, calculado segundo a fórmula constante do Anexo ao Regulamento sobre Operações com Acordo de Recompra e Revenda e de Títulos de Renda Fixa, aprovado pelo Aviso n.º 6/GBM/13, de 6 de Junho de 2013.

ARTIGO 5

Necessidade de comunicação ao BM

1. As operações devem ser comunicadas ao Banco de Moçambique imediatamente após terem sido negociadas, por ambas as partes contratantes, nos termos do disposto no Regulamento do Sistema de Operações de Mercados, daqui em diante designado por SOM.

2. Devem ser comunicadas ao Banco de Moçambique as operações do mercado monetário, a qualquer prazo até um ano, declarado em dias, com data-valor:

a) Do próprio dia;
b) Do dia útil imediatamente seguinte; e
c) Do segundo dia útil seguinte.

3. Se até à hora de fecho do mercado se verificar a existência de operações que por falta de comunicação de uma das partes ou por qualquer outro motivo, não tenham sido "processadas", o Banco de Moçambique procede à sua rejeição.

4. O Banco de Moçambique tem a responsabilidade de, diariamente, divulgar, às instituições participantes, informação relativa aos montantes e às taxas de juro mínima, máxima e média das operações contratadas, de acordo com a data-valor das operações e para os diversos prazos, podendo estes ser agrupados em classes estatísticas representativas do mercado.

5. As instituições participantes do MMI devem, sempre que solicitadas pelo Banco de Moçambique, fornecer informação relativa ao mercado.

CAPÍTULO III

Operações de regulação da liquidez realizadas pelo banco de Moçambique com as instituições participantes

ARTIGO 6

Absorção e cedência de liquidez por iniciativa do BM

1. O Banco de Moçambique realiza, com as instituições autorizadas, operações de compra, venda ou emissão de títulos, por sua iniciativa, visando a regulação da liquidez do sistema bancário e a manutenção das taxas de juro em níveis adequados ao equilíbrio dos diferentes mercados.

2. As operações de absorção ou de cedência de liquidez, em contrapartida da venda/emissão ou compra de títulos, têm carácter regular ou ocasional e são realizadas nas condições que o Banco anunciar através do SOM.

ARTIGO 7

Anúncio das condições, prazos de diferimento e vencimento

1. O Banco de Moçambique anuncia, através do SOM, as condições de realização das operações, nomeadamente, montantes, taxas, prazos, datas-valor, títulos aceites para a transacção e horas limite de apresentação de propostas.

2. A data de pagamento, por débito ou crédito da(s) conta(s) de depósitos da(s) instituição(ões) adquirente(s) ou cedente(s) de títulos pode ter um diferimento de um ou mais dias úteis relativamente à data de contratação das operações, sendo tal facto anunciado através do SOM.

3. Sempre que a data de vencimento das operações não coincidir com um dia útil, o prazo é considerado terminado no dia útil imediatamente anterior.

ARTIGO 8

Propostas

1. As operações de absorção e de cedência de liquidez realizadas pelo Banco de Moçambique no MMI têm por base as propostas apresentadas pelas instituições, através do SOM.

2. Quando as operações são anunciadas na modalidade de leilão de taxa de juros, com ou sem fixação de montante, as instituições podem apresentar até 6 propostas, às quais serão aplicadas as seguintes regras:

a) As propostas são satisfeitas a partir das que apresentem taxas para compra ou venda de títulos mais baixas ou altas, sucessivamente, até se perfazer o montante proposto pelo Banco de Moçambique ou até se atingir a taxa que este considere como limite para realizar as operações;

b) O montante a transaccionar à última das taxas que satisfizer os requisitos da alínea anterior é, quando necessário, rateado na proporção dos montantes propostos pelas instituições participantes na referida taxa.

3. Nas propostas, as taxas de juro devem ser expressas até à centésima de ponto percentual e os montantes devem corresponder a múltiplos de um milhão de meticais, não podendo cada proposta ser inferior ao montante estabelecido na alínea *a*) do artigo 2 do presente Regulamento.

4. O Banco de Moçambique comunica a cada uma das instituições proponentes, através do SOM, o valor de reembolso e o montante líquido do desconto respeitantes aos títulos comprados e/ou vendidos à instituição e ao conjunto de instituições, bem como a taxa média ponderada das transacções realizadas, sempre que a taxa das operações for determinada em sistema de leilão, e outras informações que entenda transmitir ao mercado.

ARTIGO 9

Absorção e cedência de liquidez por iniciativa das instituições participantes

1. As operações de absorção e cedência de liquidez da iniciativa das instituições são realizadas obedecendo o estabelecido no Regulamento sobre as operações com acordo de recompra e revenda de títulos de renda fixa.

2. O Banco de Moçambique realiza, com as instituições autorizadas, operações de absorção de liquidez através de aceitação de depósitos, por iniciativas destas, visando a regulação da liquidez do sistema bancário.

3. Ainda por iniciativas das instituições autorizadas, o Banco de Moçambique realiza operações de cedência, em contrapartida da compra de títulos, visando solver uma eventual escassez de liquidez.

4. As operações de absorção e cedência de liquidez da iniciativa das instituições autorizadas têm carácter permanente e são realizadas

com data-valor do próprio dia e à taxa de juro previamente anunciada pelo Banco de Moçambique, através do SOM.

5. As operações relativas às facilidades permanentes de depósito e cedência de liquidez vencem no dia útil imediatamente seguinte ao das suas datas-valor.

6. O Banco de Moçambique reserva-se o direito de suspender, por tempo indeterminado e mediante comunicação prévia, as facilidades permanentes de depósito e cedência de liquidez.

CAPÍTULO IV

Títulos transaccionáveis

ARTIGO 10

Garantia

Nas operações de transferência de liquidez entre instituições participantes com garantia de títulos e nas de regulação de liquidez realizadas pelo Banco de Moçambique com as instituições participantes, podem ser utilizados, como garantia, BT, TAM e outros títulos que o Banco de Moçambique autorizar como sendo transaccionáveis no MMI.

ARTIGO 11

Valor dos Títulos a transaccionar

1. Os títulos são transaccionados em lotes de valor nominal múltiplo de mil Meticais e num valor mínimo estabelecido no artigo 2 do presente regulamento.

2. As transacções são, em regra, realizadas pelo valor actual dos títulos.

3. As emissões de títulos são realizadas pelo valor descontado dos mesmos, segundo a fórmula constante no Anexo.

4. A compra com acordo de revenda ou a venda com acordo de recompra de títulos cuja emissão haja sido feita a desconto é feita pelo valor actual dos títulos, calculado segundo os critérios estabelecidos pelo normativo que regula as operações com acordo de recompra e revenda de títulos de renda fixa.

ARTIGO 12

Transferência de propriedade

A efectivação de operações com contrapartida da compra ou venda de títulos, incluindo as realizadas pelo Banco de Moçambique, pressupõe a transferência de propriedade dos títulos objecto de transacção.

ARTIGO 13

Inscrições

As operações que tenham por objecto títulos representados escrituralmente, nomeadamente, sob a forma de BT e TAM, materializados pela sua inscrição em contas-título abertas no Banco de Moçambique em nome dos respectivos titulares, são registadas em contas-título das instituições adquirentes e/ou cedentes dos títulos, através das respectivas inscrições ou seus cancelamentos.

CAPÍTULO V

Disposições gerais

ARTIGO 14

Prova

O Banco de Moçambique, na data-valor das operações e na data de vencimento, procede à movimentação das contas de depósito à ordem das

instituições intervenientes e emite comprovativos de Débito e/ou de Crédito, os quais constituem prova bastante da efectivação das operações.

ARTIGO 15

Juros

O pagamento dos juros é processado com o reembolso dos montantes das operações, nas datas dos respectivos vencimentos.

ARTIGO 16

Sanções

O Banco de Moçambique poderá excluir da realização de todas ou parte das operações previstas no MMI as entidades que, por incumprimento do preceituado neste regulamento ou por negligência grave, ocasionarem perturbações ao normal funcionamento do mercado.

ANEXO

Fórmula a aplicar no cálculo do valor de transacção nas emissões dos bilhetes do tesouro e de títulos da autoridade monetária

a) Na data de realização da operação

$$VT = \frac{VN\ 36\ 500}{36\ 500 + t.n}$$

em que:

VT – valor a debitar às instituições adquirentes

VN – valor nominal

t – taxa de juro da operação em base anual, expressa em pontos percentuais e arredondada até à centésima de ponto percentual

n – prazo da operação em dias

a) Na data de vencimento da operação

Valor de reembolso = Valor nominal

Aviso n.º 8/GBM/2013

de 18 de Setembro

Havendo necessidade de adequar as normas que regulam a colocação dos Bilhetes do Tesouro ao actual estágio de desenvolvimento do sistema financeiro moçambicano e do Mercado Monetário Interbancário.

O Banco de Moçambique, no uso das competências que lhe são conferidas pelo artigo 21 da Lei n.º 1/92 - Lei Orgânica do Banco – de 3 de Janeiro, determina:

1. É aprovado o Regulamento sobre a Emissão e Transacção de Bilhetes do Tesouro, que faz parte integrante do presente Aviso.

2. O presente Aviso entra em vigor na data da sua publicação e revoga o Aviso n.º 10/GGBM/2005, de 19 de Outubro.

As dúvidas que surgirem da interpretação e aplicação do presente Aviso deverão ser submetidas ao Departamento de Mercados do Banco de Moçambique.

Banco de Moçambique, em Maputo, 6 de Junho de 2013. – O Governador, *Ernesto Gouveia Gove*.

Regulamento Sobre a Emissão e Transacção de Bilhetes do Tesouro

CAPÍTULO I

Disposições gerais

ARTIGO 1

Definição

Os Bilhetes do Tesouro, doravante designados BT, são valores mobiliários escriturais representativos de empréstimos de curto prazo da República de Moçambique, denominados em moeda nacional.

ARTIGO 2

Características

1. O valor nominal mínimo de cada BT é de mil Meticais.

2. Os Bilhetes do Tesouro são títulos desmaterializados, amortizáveis a prazo não superior a 1 ano.

3. A emissão dos BT é paga abaixo do par pelo montante correspondente à diferença entre o valor nominal e a importância dos juros correspondentes a cada subcrição.

CAPÍTULO II

Mercado primário

ARTIGO 3

Condições de Acesso

Têm acesso ao mercado primário de BT as seguintes instituições:

a) As instituições monetárias participantes da câmara de compensação;

b) Outras instituições financeiras previamente autorizadas pelo Banco de Moçambique.

ARTIGO 4

Sessões de Mercado e Anúncio das Condições de Colocação

1. Os BT são colocados em sessões de mercado.

2. As condições de colocação de BT, nomeadamente, datas de colocação e emissão, tipo de montante (fixo ou indicativo), taxa de juros e prazo, são anunciadas por via electrónica ou outro meio de comunicação a ser indicado pelo Banco de Moçambique.

3. A colocação dos BT procede-se como se segue:

a) A data de colocação pode coincidir ou anteceder, em um ou mais dias úteis, a data da tomada de fundos por parte da entidade emitente;

b) As sessões de colocação são anunciadas através do Sistema de Operações de Mercado (doravante SOM), aprovado pelo Aviso n.º 5/GBM/2013, de 6 de Junho de 2013, no próprio dia da colocação ou com antecedência de um ou mais dias úteis, sendo mencionadas as datas de colocação, entrega de propostas e tomada de fundos, bem como as condições dos BT a colocar.

ARTIGO 5

Subscrição de Propostas de Compra

1. A colocação de BT é feita com base nas propostas de compra emitidas ou subscritas pelas instituições com acesso ao mercado primário.

2. As propostas de compra de BT´s devem ser transmitidas pelas instituições participantes ao Banco de Moçambique, nos termos estabelecidos no n.º 1 do Artigo 7 do Regulamento do SOM, aprovado pelo Aviso n.º 5/GBM/2013, de 6 de Junho de 2013.

3. Para cada espécie de BT, segundo o prazo, podem ser apresentadas por cada instituição até 6 propostas de compra com indicação da taxa, expressa em pontos percentuais e arredondada até à centésima de ponto percentual, e do montante pretendido, não podendo a soma das propostas exceder o montante de cada emissão.

4. O montante a subscrever é expresso em múltiplos de 1 milhão de Meticais, não podendo cada proposta ser inferior a 5 milhões de Meticais.

ARTIGO 6

Desconto e Valor da Transacção

Os BT são colocados a desconto sendo o valor da transacção determinado nos termos do Anexo ao presente Regulamento.

ARTIGO 7

Critérios de Selecção de Propostas

1. A colocação dos BT pode ser feita com base no leilão de taxas de juro ou à taxa de juro pré-fixada.

2. No caso da colocação de BT por leilão de taxas de juro, a procura é satisfeita de acordo com as seguintes regras:

a) São eliminadas as propostas com taxas de juro superiores à taxa máxima a que a entidade emissora está disposta a remunerar;

b) As restantes propostas são satisfeitas começando por aquelas que apresentam taxas de juro mais baixas e seguindo, sucessivamente, até se atingir o montante de colocação;

c) Havendo propostas de compra à mesma taxa de juro pretendida, igual ou inferior à taxa máxima referida em *a*), que, conjugadamente com as propostas a taxas inferiores já satisfeitas, impliquem um excesso de procura relativamente à oferta, a distribuição de BT disponíveis para aquisição entre os proponentes subscritores à referida taxa é feita proporcionalmente, em função dos montantes propostos.

3. No caso da colocação de BT à taxa de juro pré-fixada, a procura é satisfeita de acordo com as propostas apresentadas, sem prejuízo de, caso estas propostas impliquem um excesso de procura relativamente à oferta, se proceder à distribuição proporcional dos BT disponíveis entre os proponentes subscritores.

ARTIGO 8

Comunicação de Elementos Relativos aos Títulos Adquiridos

1. O Banco de Moçambique transmite a cada uma das entidades adquirentes, por via electrónica ou outro meio de comunicação a ser indicado, o valor nominal e o montante líquido do desconto, respeitantes aos BT que lhe tenham sido atribuídos, bem como a taxa média ponderada da colocação e o montante global colocado.

2. Na data de emissão, o Banco de Moçambique transmite, por via electrónica ou outro meio de comunicação a ser indicado, confirmativos da efectivação da compra dos BT.

3. Na data referida no número precedente, o montante líquido dos BT, é debitado nas contas de depósito à ordem das instituições adquirentes, abertas em seu nome no Banco de Moçambique, considerando-se, para todos os efeitos legais, que a submissão da proposta de aquisição vale como consentimento tácito deste movimento.

ARTIGO 9

Reembolso

1. Os BT colocados no mercado primário gozam de garantia de reembolso integral, pelo valor nominal, na data do seu vencimento.

2. O reembolso às instituições e entidades com acesso ao mercado primário dos BT é efectuado pelo Banco de Moçambique.

3. No reembolso referido no número anterior, o Banco de Moçambique suporta o capital e juros relativos ao uso dos títulos para fins de política monetária e o Estado, o capital e juros da parte que tiver utilizado para financiamento do défice da sua Tesouraria.

4. As importâncias reembolsadas são levadas a crédito, sob aviso, das contas de depósitos à ordem das instituições portadoras dos BT, nas datas dos respectivos vencimentos.

CAPÍTULO III

Mercado secundário

ARTIGO 10

Transacções das Instituições entre si e com o Banco de Moçambique

1. As instituições com acesso ao mercado primário de BT podem efectuar entre si ou com o Banco de Moçambique, operações de compra e venda, temporárias ou definitivas,

de BT, obedecendo ao estabelecido no Aviso n.º 6/GBM/2013, de 6 de Junho de 2013.

2. As operações efectuadas ao abrigo deste artigo devem ser comunicadas ao Banco de Moçambique, nos termos estabelecidos no n.º 1 do artigo 7 do Regulamento do SOM, aprovado pelo Aviso n.º 5/GBM/2013, de 6 de Junho de 2013.

3. Com base nas comunicações referidas no número anterior, o Banco de Moçambique procede à actualização das contas-título, cancelando os anteriores registos de propriedade em nome das entidades cedentes.

ARTIGO 11

Transacções com o público

1. Os BT adquiridos pelas instituições com acesso ao mercado primário podem ser vendidos ao público, a título temporário ou definitivo, mediante a abertura de contas-título em nome dos seus clientes.

2. Para efeitos do presente Aviso, consideram-se transacções com o público as que não forem realizadas exclusivamente entre entidades com acesso ao mercado primário.

3. As instituições que tenham vendido BT procedem ao seu reembolso na data do vencimento destes ou na data eventualmente estabelecida no acordo de recompra.

4. As operações realizadas ao abrigo deste artigo devem ser comunicadas ao Banco de Moçambique, no dia de realização da transacção, nos termos estabelecidos no n.º 1 do artigo 7 do Regulamento do SOM, aprovado pelo Aviso n.º 5/GBM/2013, de 6 de Junho 2013.

5. Com base nas comunicações referidas no número anterior, o Banco de Moçambique procede à actualização das contas-título, cancelando os anteriores registos de propriedade em nome das entidades cedentes.

ANEXO

Fórmula a aplicar no cálculo do valor de transacção dos bilhetes do tesouro, no mercado primário

$$VT = \frac{VN\ 36\ 500}{36\ 500 + t.n}$$

em que:

VT – valor a debitar às instituições adquirentes

VN – valor nominal

t – taxa de juro da operação em base anual, expressa em pontos percentuais e arredondada até à centésima

n – prazo da operação em dias

Aviso n.º 9/GBM/2013

de 18 de Setembro

Tornando-se necessário proceder ao preenchimento dos órgãos de gestão do Fundo de Garantia de Depósitos, ao abrigo do disposto no artigo 17 do Decreto n.º 49/2010, de 11 de Novembro, o Banco de Moçambique designa:

José Frederico da Cruz Viola Cabral, Presidente da Comissão Directiva do Fundo de Garantia de Depósitos.

O presente Aviso entra em vigor na data da sua publicação.

As dúvidas que surgirem na interpretação e aplicação do presente Aviso serão esclarecidas pelo Gabinete do Governador do Banco de Moçambique.

Banco de Moçambique, em Maputo, 10 de Junho de 2013. – O Governador, *Ernesto Gouveia Gove*.

Preço — 93,93 MT

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.