BANCO SOL
O banco de todos nós

NORMA DE APLICAÇÃO PERMANENTE

POLÍTICA DE GESTÃO DO RISCO OPERACIONAL

NAP – DGR/05/2026

Publicado em:

03-02-2026

NORMA DE APLICAÇÃO PERMANENTE – POLÍTICA DE GESTÃO DO RISCO OPERACIONAL

1. DISPOSIÇÕES GERAIS

No presente capítulo, apresentam-se as disposições gerais referentes à Norma de Aplicação Permanente da Política de Gestão do Risco Operacional:

1.1. Histórico de actualizações e revogações de Normativos Internos;
1.2. Enquadramento legal e Normativos Internos associados;
1.3. Objectivo e Âmbito;
1.4. Conceitos, abreviaturas e nomenclaturas;
1.5. Órgãos de estrutura responsáveis;
1.6. Conteúdos regulamentados.

1.1. Histórico de Actualizações e Revogações de Normativos

1.1.1. Histórico de Actualizações

VERSÃO	DATA DE PUBLICAÇÃO	AUTOR	PRINCIPAIS ALTERAÇÕES
1	01/06/2022	Direcção de Organização e Qualidade	Primeira publicação da Política de Gestão do Risco Operacional
2	03/02/2026	Direcção de Organização e Qualidade	Actualização a nível do Enquadramento Legal e Procedimentos e inclusão dos pontos 2.8 e 2.9.

1.1.2. Revogações de Normativos

A presente Norma de Aplicação Permanente vem regulamentar a Política de Gestão do Risco Operacional, revogando a versão anterior de 01/06/2022.

1.2. Enquadramento Legal e Normativos Internos

Consideram-se relevantes para a presente Norma de Aplicação Permanente os seguintes diplomas externos:

- **Aviso n.º 01/2022, de 28 de Janeiro –** Sistema Financeiro - Governo societário das instituições financeiras;
- **Aviso n.º 08/2021, de 05 de Julho –** Sistema Financeiro - Requisitos de Fundos Próprios – Processo de Supervisão e Gestão de Risco- Disciplina do Mercado;
- **Instrutivo n.º 13/2021, de 27 de Setembro –** Sistema Financeiro - Cálculo e Requisito de Fundos Próprios Regulamentares para Risco Operacional e Respectiva Prestação de Informação Periódica;
- **Instrutivo n.º 3/2022, de 29 de Março –** Testes de Esforço;
- **Instrutivo n.º 28/2016, de 16 de Novembro –** Governação do Risco Operacional.

1.3. Objectivo e Âmbito

A presente Norma de Aplicação Permanente tem como objectivo definir, os principais riscos operacionais susceptíveis de originar perdas directas ou indirectas, bem como danos à reputação do Banco, resultantes da inadequação ou falhas de processos, sistemas, pessoas, da possibilidade de ocorrência de fraudes bem como de eventos externos.

No âmbito do risco operacional, assumem particular relevância os seguintes riscos específicos:

- O risco de Compliance: risco de violação ou incumprimento de leis, regras, disposições regulamentares, contratos, práticas prescritas e padrões éticos.
- O risco de sistemas de informação: risco de inadequação das tecnologias de informação quanto ao respectivo processamento, integridade, controlo, disponibilidade e continuidade (proveniente de concepções ou utilizações erradas).
- O risco de reputação: risco adicional que se sobrepõe, por deficit de gestão ou de tempestividade, a um evento ou eventos de risco de diversas naturezas, prejudicando a imagem do Banco junto de *stakeholders* e público em geral.

A gestão do risco operacional tem um carácter essencialmente preventivo visando, designadamente:

- A promoção de boa conduta ética e integra por parte dos colaboradores;
- A garantia da continuidade do negócio / operações;
- A fiabilidade e qualidade da informação prestada às entidades externas e internas;
- O cumprimento da lei e regulamentação em vigor;
- A prevenção do branqueamento de capitais e do financiamento do terrorismo;
- A segurança de pessoas, sistemas e instalações.

A política **aplica-se a todas as unidades orgânicas, colaboradores, prestadores de serviços e terceiros relevantes**.

1.4. Conceitos, Abreviaturas e Nomenclaturas

Apresenta-se em seguida a lista de siglas e conceitos utilizados ao longo da presente Norma de Aplicação Permanente:

- **CA** – Conselho de Administração;
- **CE** – Comissão Executiva;
- **BNA** – Banco Nacional de Angola;
- **DGR -** Direcção de Gestão de Risco;
- **DTI -** Direcção de Tecnologia e Sistemas de Informação;
- **PCN –** Plano de Continuidade de negócios,
- **BIA –** Business *Impact Analysis;*
- **KRI –** *Key RisK Indicators;*
- **LD –** Linha de Defesa;
- ***Stakeholders*** - Partes interessadas.
- **Risco Bruto** – Risco identificado antes da aplicação de medidas de mitigação;
- **Risco Residual** – Risco remanescente após a aplicação das medidas de mitigação.

1.5. Órgãos de Estrutura Responsáveis

A Direcção de Gestão de Risco é responsável pela permanente actualização da presente Norma de Aplicação Permanente.

É da responsabilidade dos Líderes, assegurar que o conteúdo da presente política seja levado ao conhecimento dos seus Liderados.

1.6. Conteúdos Regulamentados

Encontram-se estabelecidas na presente Norma de Aplicação Permanente as regras e princípios orientadores, no que se refere a:

CAPÍTULO	NOME DO CAPÍTULO
2	Política de Gestão do Risco Operacional
3	Outorgamento

2. POLÍTICA DE GESTÃO DO RISCO OPERACIONAL

Encontram-se regulamentados no presente capítulo os seguintes temas:

2.1. Requisitos de Estrutura e Meios;
2.2. Hierarquia de Tomada de Decisões e Delegação de Competências;
2.3. Requisitos de Identificação e Avaliação do Risco;
2.4. Mitigação do Risco Operacional;
2.5. Monitorização e Controlo do Risco Operacional;
2.6. Testes de Esforço;
2.7. Requisitos de Prestação de Informação;
2.8. Incumprimento;
2.9. Aprovação e Revisão.

2.1. Requisitos de Estrutura e Meios

1. No Banco Sol a gestão do risco operacional atravessa toda a organização não só por decorrência da adopção do sistema governativo das 3 linhas de defesa como também por via da nomeação de "responsáveis por risco operacional" ao nível das unidades orgânicas e processos críticos.

2. Centralmente o risco operacional é conduzido e controlado na Direcção de Gestão de Risco, cuja intervenção se estende a vários domínios específicos da gestão deste tipo de risco.

3. A relação entre os papéis assumidos por áreas de negócio e suporte como 1ª linha de defesa e a Direcção de Gestão de Risco como 2ª linha de defesa estão representados na matriz seguinte:

Intervenção das Linhas de Defesa 1 e 2	LD1	LD2
Auto-avaliação de riscos e controlos	Descreve os riscos e controlos associados aos principais processos do Banco	Revê criticamente, para um conjunto de processos críticos, a inventariação dos riscos e a adequação dos controlos
Cenários de risco operacional	Constrói cenários de risco operacional para efeitos de testes de esforço	Revê criticamente os cenários e resultados
Eventos de risco	Regista os eventos de risco e absorve as respectivas perdas	Classifica os eventos de risco
Indicadores de risco (KRI)	Define e acompanha KRI no seu domínio	Monitoriza KRI e agrega os respectivos resultados no perfil de risco operacional do Banco
Tecnologia e sistemas	Inventaria os riscos de IT e segurança informática e estabelece os controlos julgados adequados	Revê criticamente o perfil de risco informático e os controlos estabelecidos.
Compliance	Estabelece um programa de cumprimento dos requisitos regulamentares em vigor	Revê criticamente o perfil de risco de *compliance* e os controlos estabelecidos
Novos produtos e mercados	Propõe novos produtos e mercados e prepara respectiva ficha	Verifica alterações ao perfil de risco do Banco e seu enquadramento na apetência ao risco
Modelos	Inventaria e classifica os modelos ao seu serviço; propõe novos modelos, seguindo os procedimentos adequados ao nível (de complexidade e materialidade) do modelo	Revê a classificação dos modelos; executa ou subcontrata protocolos de validação
Outsourcing / fornecedores (contratos com terceiros)	Inventaria e classifica os contratos com terceiros da sua esfera de actuação; propõe novos contratos - e eventualmente novos fornecedores - seguindo os procedimentos adequados ao nível (de complexidade e materialidade) de cada contrato	Revê a classificação os contratos; executa ou subcontrata protocolos de validação

2.2. Hierarquia de Tomada de Decisões e Delegação de Competências

1. **Conselho de Administração**

Compete ao Conselho de Administração:

a) Definir o apetite ao risco operacional;
b) Supervisionar o perfil de risco operacional do Banco.

2. **Comissão Executiva**

Compete à Comissão Executiva:

a) Implementar a Política aprovada;
b) Garantir a eficácia dos controlos internos;
c) Acompanhar os relatórios de risco operacional.

3. **Comité de Gestão Risco**

Compete ao Comité de Risco:

a) Acompanhar a exposição ao risco operacional;
b) Avaliar eventos relevantes;
c) Monitorizar planos de ação.

4. **Direção de Risco**

Compete à Direção de Risco:

a) Desenvolver metodologias de gestão do risco operacional;
b) Consolidar e analisar eventos de risco;
c) Produzir relatórios periódicos;
d) Assegurar conformidade com Basileia e BNA.

5. **Direções Operacionais**

Compete às Direções Operacionais:

a) Identificar e reportar eventos de risco operacional;
b) Implementar controlos e planos de mitigação;
c) Cooperar com a Direção de Risco.

A Auditoria Interna, enquanto terceira linha de defesa, é responsável pela avaliação independente da adequação e eficácia do sistema de gestão do risco operacional.

Na gestão de novas situações identificadas em auto-avaliações, eventos de risco e recomendações de auditoria esta política define classes de materialidade e competências para a mitigação do risco e para a aceitação do risco.

As classes de materialidade são quatro - risco muito elevado, risco elevado, risco médio e risco baixo - definindo-se severidade como a estimativa da perda por materialização do risco em causa.

1. Na mitigação do risco distinguem-se diferentes planos de actuação:

    a) Alteração de processos sem custos ou envolvendo custos pouco significativos (inferiores a 30% da severidade do risco);
    b) Alteração de processos envolvendo custos significativos (não inferiores a 30% da severidade do risco);
    c) Partilha do risco com terceiros (por alteração de formatos de contratação ou transferência de risco para empresas seguradoras, por exemplo).

2. A aceitação do risco é o processo formal através do qual o Banco estabelece e documenta a sua preferência por não mitigar um determinado risco (por exemplo em situações nas quais o custo de mitigação se sobrepõe às correspondentes vantagens).

3. A hierarquia e delegação de competências na mitigação e aceitação de riscos operacionais é apresentada no quadro a seguir:

SEVERIDADE DO RISCO:	MITIGAÇÃO DE CUSTO NÃO SIGNIFICATIVO (*)	MITIGAÇÃO DE CUSTO SIGNIFICATIVO (*)	REPARTIÇÃO DO RISCO	ACEITAÇÃO DO RISCO
RISCO MUITO ELEVADO	Comissão Executiva	Conselho de Administração	Conselho de Administração	Conselho de Administração
RISCO ELEVADO	Administrador do Pelouro	Conselho de Administração	Conselho de Administração	Conselho de Administração
RISCO MÉDIO	Administrador do Pelouro	Comissão Executiva	Comissão Executiva	Conselho de Administração
RISCO BAIXO	Administrador do Pelouro	Comissão Executiva	Comissão Executiva	Comissão Executiva

(*) Pressupõe cabimento orçamental

2.3. Requisitos de Identificação e Avaliação do Risco

1. O processo de identificação e avaliação de riscos de natureza operacional é sustentado na própria moldura de controlo interno e as respectivas disciplinas de (a) repetitiva (anual) auto-avaliação de processos, identificação de riscos e desenho e implementação dos controlos julgados adequados na gestão desses riscos e de (b) resolução de recomendações de auditoria.

2. A recolha sistemática de informação sobre eventos de risco, perdas verificadas e perdas potenciais complementa a identificação de risco em auto-avaliações e em processos de auditoria. Esta política determina que todos os eventos de risco operacional com perdas reais ou potenciais, devam ser formalmente identificados e catalogados de acordo com a categorização vigente.

3. O valor das perdas em causa deve ser estimado na unidade de 1ª linha que identifica o evento de risco e subsequentemente validado na Direcção de Gestão de Risco.

4. As categorias do risco operacional são as seguintes:

   a) **Risco de fraude interna** – Risco associado à desonestidade de conduta por parte de colaboradores do Banco – por exemplo falsificação, corrupção, ocultação maliciosa, conluio, prática de actividades vedadas, roubo, quebra propositada de confidencialidade; em determinadas circunstâncias os eventos desta natureza podem traduzir-se em riscos de Compliance.

   b) **Risco de fraude externa** – Risco associado à desonestidade de conduta por parte de entidades exteriores ao Banco – por exemplo, as fraudes no universo dos cartões, cheques, transacções, apresentação de dados.

c) **Risco de clientes, produtos e práticas de negócio** – Riscos relacionados com situações de negócio como o lançamento de novos produtos, o tratamento de informação de clientes, a autorização de pagamentos e outras transacções, a aceitação de fundos em depósito, o manuseamento de informação confidencial.

d) **Risco de execução, entrega e gestão de processos** – Resultam de erros de metodologia, do próprio processo operacional e dos colaboradores que o executam incluindo, por exemplo, a submissão de informação errónea, o incumprimento de requisitos contratuais, a manipulação deficiente de aplicativos informáticos.

e) **Risco de perturbação das actividades de negócio e quebra de sistemas** – Resultam de eventos e anomalias com efeito nos sistemas e aplicações do Banco e, consequentemente, na capacidade de acção das suas áreas comerciais, suporte e controlo.

f) **Risco relacionado com práticas de emprego e segurança no trabalho** – Materializam-se em situações de improdutividade e desmotivação da força de trabalho, levando por vezes à litigação e resignação de colaboradores valiosos, e resultam da adopção de práticas ineficientes na admissão, compensação, e gestão de carreiras dos empregados; inclui também os riscos relacionados com a saúde e segurança no trabalho.

g) **Risco de ocorrência de danos em activos físicos** – Riscos de danificação ou destruição de activos físicos do Banco como resultado de acidentes, causas naturais, confrontações e motins, actos de terrorismo e sabotagem, etc.

As auto-avaliações de risco operacional devem ser realizadas, no mínimo, com periodicidade anual e sempre que ocorram alterações relevantes nos processos, sistemas, produtos ou enquadramento regulamentar.

Devem igualmente ser considerados riscos emergentes, resultantes de mudanças tecnológicas, regulamentares, de mercado ou estratégicas.

2.4. Mitigação do Risco Operacional

1. A mitigação do risco operacional baseia-se na boa prevenção e controlo do risco ao nível de todas as áreas do Banco Sol que encontra sustentação e consistência nos princípios da presente política, na moldura de controlo interno estabelecida e na própria cultura de risco que o Conselho de Administração tem vindo a disseminar.

2. A Política de Gestão do Risco operacional contempla orientações de política quanto a aspectos específicos da vida do Banco: a aprovação de novos produtos e mercados, a moldura de sistemas de informação e tecnologia, o plano de continuidade de negócios, o risco de modelo, a gestão de outsourcing e fornecedores.

3. Para cada risco material identificado devem ser definidos planos de acção formalizados, com indicação clara das medidas de mitigação, responsáveis, prazos de implementação e mecanismos de acompanhamento.

4. Este ponto inclui ainda uma súmula de orientações de mitigação do risco de reputação.

2.4.1. Orientações quanto à Aprovação de Novos Produtos e Mercados

1. É indiscutível que a aprovação de novos produtos e mercados exige uma disciplina e um governo que proteja o Banco de incorrer em riscos excessivos. Entende-se por *novos* produtos aqueles que diferem substancialmente dos existentes, no seu desenho e complexidade e nos riscos que fazem emergir.

2. Um novo produto, ou uma proposta para desenvolver actividades num novo mercado, começam numa ficha de produto / mercado na qual se inventariam:

    a) As características intrínsecas do produto ou mercado;

    b) O respectivo enquadramento legal e regulamentar;

    c) A estratégia de comunicação;

    d) Os meios humanos, materiais e tecnológicos necessários ao seu desenvolvimento e lançamento;

    e) O plano de negócios (business case) evidenciando a rendibilidade do projecto e os seus impactos em custos e proveitos e no balanço do Banco;

    f) O perfil de risco do produto ou mercado para os principais tipos de risco relevantes;

    g) As decorrentes alterações ao perfil de risco do Banco, contrastando-o com a apetência ao risco do Banco.

3. Com excepção do último ponto, que será da competência da Direcção de Gestão de Risco e redigida em nota autónoma, a ficha é preparada por quem toma a iniciativa sobre o novo produto ou mercado, tipicamente áreas de negócio em conjunto com a Direcção de Marketing e Inovação, para cobrir de forma sistemática os aspectos essenciais na discussão aberta que se almeja. Funciona como um guião para uma revisão colectiva envolvendo as áreas de Risco, Compliance, Financeira, Sistemas de Informação, Operações, Jurídica e Marketing e Inovação.

4. Ainda que parte da discussão se possa (e deva) efectuar trocando emails e reunindo ad hoc e mesmo em sede de Comité de Estratégia e Negócios, cabe à Direcção de Marketing e Inovação coordenar com a Direcção de Gestão de Risco a decisiva apresentação do novo produto / mercado no Comissão Executiva.

5. A comissão Executiva tomará uma de três posições:

    a) Acolhimento da ideia e consideração de que os trabalhos preparatórios são suficientes e plenamente satisfatórios (endossando a aprovação ao Conselho de Administração).

    b) Acolhimento da ideia, mas considerando que os trabalhos preparatórios são insuficientes e, portanto, não satisfatórios (remetendo o dossier aos originadores e outras Direcções com indicação das condições adicionais que deve satisfazer e marcando um prazo para nova apresentação na Comissão Executiva).

    c) Rejeição da ideia (dando conhecimento dessa posição e sugerindo a recusa ao Conselho de Administração).

6. Posteriormente à aprovação definitiva do produto ou mercado e respectivo lançamento efectivo os benefícios, custos e riscos verificados são comparados com as expectativas do business case. Esta análise comparativa deverá ser apresentada nos Comités de Gestão de Risco e de Estratégia e Negócios podendo, perante a evidência de incumprimento daquelas expectativas, recomendar-se ao Conselho de Administração a suspensão ou descontinuação da actividade em causa.

2.4.2. Orientações quanto à Moldura de Sistemas de Informação e Tecnologia

1. A tecnologia e os sistemas de informação devem estar ao serviço da prossecução dos objectivos estratégicos do Banco.

2. Essa consistência é garantida, em primeiro lugar, através da participação da Direcção de Tecnologia e Sistemas de Informação (DTI) nos trabalhos do planeamento estratégico e do plano anual de

actividades, mas também através das reuniões regulares das Direcções de Tecnologia e Sistemas de Informação e de Operações com os Administradores dos Pelouros.

3. Cabe à DTI propor a Comissão Executiva documentos de enunciação de princípios de tecnologia e sistemas e de princípios de segurança informática contemplando, entre outros, os seguintes aspectos:

   a) Tecnologia e Sistemas:

   i. Modelo tecnológico do Banco Sol;
   ii. Princípios operacionais: disponibilidade, *backups*, gestão de sistemas, recuperação, mudança (*change management*);
   iii. Plano de continuidade de sistemas (integrando o plano de continuidade de negócios do Banco);
   iv. Leque de produtos;
   v. Tarefas e responsabilidades do *staff;*
   vi. Formação.

   b) Segurança Informática:

   i. Políticas de segurança informática;
   ii. Produtos de segurança (e.g firewalls) e anti-virus;
   iii. Programa de testes de segurança;
   iv. Controlo de acessos;
   v. Gestão de incidentes;
   vi. Revisões de rotina;
   vii. Formação.

4. Na formulação desses princípios a DTI terá em conta as prioridades dos sistemas de informações visando proteger o Banco de interrupções prolongadas de conectividade/acesso, quebras graves afectando serviços e clientes, corrompimento de informação e dados e quebras de segurança informática.

2.4.3. Orientações sobre o Plano de Continuidade de Negócios

1. A continuidade normal das operações e negócios do Banco pode colocar-se em causa por motivos diversos, incluindo incidentes, desastres naturais e acções de terrorismo e sabotagem.

2. Na presente Política a Administração do Banco define os seguintes princípios reguladores do plano de continuidade de negócios (PCN):

   a) O PCN é aprovado no Conselho de Administração;

   b) O PCN é desenvolvido com a contribuição de um conjunto de áreas do Banco coordenado pelas Direcções de Gestão do Risco, Tecnologias de Informação, Património e Serviços;

   c) O PCN integra três componentes nucleares: (i) análise de impacto (business impact analysis ou BIA), que quantifica os impactos da descontinuidade nas diversas áreas do Banco; (ii) objectivos temporais de recuperação (em linha com o BIA); e (iii) procedimentos de emergência e de comunicação;

d) Para além dos componentes enunciados acima, o PCN deve incluir uma descrição técnica das acções de recuperação subjacentes ao restabelecimento da normal operação do Banco;

e) O PCN integra um protocolo de testes periódicos.

2.4.4. Orientações sobre Risco de Modelo

1. São evidentes as vantagens da utilização de modelos: facilitam a nivelação / padronização e a rapidez da decisão; permitem tratar questões tecnicamente exigentes; potenciam poupanças de custos. Mas são igualmente evidentes os riscos gerados por uma utilização disseminada e frequente de modelos.

2. Um modelo é um sistema que aplica determinadas técnicas e teorias de forma a obter resultados (ou estimativas da realidade). O risco de modelo materializa-se na *utilização de um modelo inadequado* e na *utilização deficiente de um modelo adequado*.

3. A gestão do risco de modelo no Banco Sol pressupõe:

   a) A inventariação dos modelos em utilização no Banco;
   b) A classificação dos modelos quanto a complexidade e materialidade (em termos de impacto dos erros causados por deficiente modelização ou utilização);
   c) A subsequente distribuição dos modelos por níveis, como se apresenta a seguir:
      i. Nível 1 – elevada materialidade x elevada complexidade;
      ii. Nível 2 – elevada materialidade x baixa complexidade;
      iii. Nível 3 – baixa materialidade x elevada complexidade;
      iv. Nível 4 – baixa materialidade x baixa complexidade.

4. A definição de requisitos de aprovação, documentação, teste, validação prévia e periodicidade de validação de acordo com os níveis supra enunciados.

REGRAS DE GESTÃO / REQUISITOS DE ACORDO COM O NÍVEL (COMPLEX. / MATERIAL.) DO MODELO

	1	2	3	4
Aprovação do modelo	CA	CE	CE	LD1 (*)
Requisitos especiais de documentação *(a)*	S	S		
Requisitos de teste *(b)*	S	S		
Validação pré-utilização *(c)*	S	S	S	
Periodicidade de validação regular *(d)*	Anual	Anual	Anual	Tri-anual

(*) assumindo cabimento orçamental

(a) Definição de propósito e uso; metodologia e abordagem técnica, limitações do modelo, relevância dos dados disponíveis, testes de aceitação

(b) testes em situações extremas

(c) validação prévia executada ou subcontratada pela DGR e formalmente aceite pela LD1

(d) a validação regular inclui a monitorização de qualidade de dados, a análise de excepções, a validação da estabilidade e desempenho do modelo, a sua calibragem e back-testing.

2.4.5. Orientações sobre Risco de Outsourcing e Fornecedores

1. A utilização de um serviço de terceiros tem por base uma escolha que reflectirá a ponderação de critérios de conveniência económica e de especialização. Por princípio o Banco adjudica a terceiros os serviços em que não é suficientemente eficiente nem pretende sê-lo.

2. A gestão do risco de outsourcing e fornecedores no Banco Sol pressupõe:

    a) A inventariação dos serviços prestados por terceiros no Banco;
    b) A classificação desses serviços quanto a complexidade e materialidade;
    c) A subsequente distribuição dos serviços por níveis, como se apresenta a seguir:
        i. Nível 1 – elevada materialidade x elevada complexidade;
        ii. Nível 2 – elevada materialidade x baixa complexidade;
        iii. Nível 3 – baixa materialidade x elevada complexidade;
        iv. Nível 4 – baixa materialidade x baixa complexidade.

REGRAS DE GESTÃO / REQUISITOS DE ACORDO COM O NÍVEL (COMPLEX. / MATERIAL.) DO SERVIÇO PRESTADO

	1	2	3	4
Aprovação da prestação do serviço	CA	CE	CE	LD1 (*)
Visita de auditoria / análise de risco ao prestador *(a)*	S			
Análise patrimonial e da exploração do prestador *(b)*	S	S		
Ficha do prestador e sócios *(c)*	S	S	S	
Análise sumária da experiência do prestador *(d)*	S	S	S	S

(*) Assumindo cabimento orçamental

(a) Inspecção a realizar pela auditoria do Banco a fim de validar o risco de entrega e execução do prestador

(b) verificação do balanço e demonstração de resultados do prestador na busca de situações de desequilíbrio, sobreendividamento, etc. que possam comprometer a prestação.

(c) questionário completo sobre a experiência do prestador de serviços e respectivos sócios.

(d) questionário simples sobre a experiência do prestador de serviços no ramo.

3. A definição de requisitos de aprovação, selecção, documentação e seguimento variam de acordo com os níveis supra enunciados.

2.4.6. Mitigação do Risco de Reputação

6. Conforme definido supra, o risco de reputação "é o risco adicional que se sobrepõe, por deficit de gestão ou de tempestividade, a um evento ou eventos de risco de diversas naturezas, prejudicando a imagem do Banco junto de stakeholders e público em geral". Trata-se, assim, de um risco de segunda vaga, emergente após a ocorrência de um risco primário não adequadamente gerido.

7. Em termos práticos, diversas situações adversas - como interrupções de actividade, sanções regulamentares, cassação de licença bancária no estrangeiro, etc. – ordem, pela sua gravidade e impacto, gerar danos reputacionais relevantes.

8. A gestão do risco de reputação assenta no princípio de que uma resposta tempestiva, assertiva e bem estruturada a qualquer situação adversa conduz a uma forte redução do potencial de emergência daquele risco (como segunda vaga do risco original materializado).

9. Como princípios de gestão deste risco o Banco Sol estabelece:

    a) Imediata comunicação à Administração de qualquer evento adverso ou situação de risco com gravidade elevada;

    b) Constituição de um gabinete de crise, quando aplicável, composto por Directores com competências ajustadas à natureza do evento;

    c) Análise célere da situação, definição de contra-medidas e envio de uma comunicação preliminar e sintética a entidades estratégicas (regulador, accionistas, corpo directivo), informando que nova comunicação mais detalhada será emitida brevemente;

    d) Comunicação pública subsequente, com carácter proactivo, dirigida a clientes, fornecedores e ao público em geral, clarificando a origem do evento, as consequências e as acções adoptadas ou em curso;

    e) Ao longo de todo o processo, demonstração clara de liderança, domínio da situação e responsabilidade institucional.

2.5. Monitorização e Controlo do Risco Operacional

1. A monitorização do risco operacional assenta num conjunto estruturado de indicadores de risco (key risk indicators ou KRI) cuja definição é da competência das unidades orgânicas e dos responsáveis por processos críticos do Banco.

2. Mapeados sobre o organograma do Banco e o seu sistema de processos críticos, os KRI devem ser inteligíveis e representativos, concebidos sobre os riscos identificados e os controlos desenhados para a sua mitigação. Assim, fará sentido ter KRI que medem risco bruto (por exemplo, a percentagem de propostas fraudulentas em propostas de empréstimos pessoais) e KRI que medem a eficácia de controlos que mitigam o risco original (por exemplo, a percentagem de tentativas de fraude identificadas numa 2ª verificação do universo de propostas).

3. Na sua acção de agregação do risco para efeitos de monitorização no plano mais geral (da ligação ao perfil de risco do Banco) a Direcção de gestão de risco incluirá também indicadores de natureza global abordando temas como a resolução das recomendações de auditoria e das deficiências de controlo interno, os resultados de testes de esforço e validações conduzidos na própria DGR, os resultados dos testes de contingência, e a ligação dos resultados de risco ao desempenho das linhas de negócio do Banco.

4. Os KRIs devem incluir limites e níveis de tolerância previamente definidos, bem como mecanismos de escalonamento e reporte sempre que esses limites sejam ultrapassados.

2.6. Testes de Esforço

1. Com periodicidade semestral e anual serão conduzidos testes de esforço de risco operacional, sob articulação metodológica e coordenação da Direcção de Gestão de Risco.

2. Sem prejuízo da adopção de outras metodologias devem ser incluídos testes baseados na análise de cenários concretos com relevância na esfera do risco operacional.

3. Os cenários combinarão situações de natureza global e externa com situações idiossincráticas do Banco Sol e deverão abranger situações passíveis de materialização, ainda que improváveis.

2.7. Requisitos de Prestação de Informação

1. A informação de gestão do risco operacional tem como objectivos: (i) o cumprimento dos requisitos legais e regulamentares em vigor e (ii) o cumprimento de requisitos adicionais da gestão interna do Banco.

2. Deve basear-se, na essência, em dados residentes nos sistemas do Banco e manipulados automaticamente, através das suas aplicações. Sem embargo, a informação produzida central e automaticamente pode e deve ser complementada por análises suportadas por aplicações periféricas ou folhas de cálculo, quando tal se revele adequado.

3. Os requisitos de extracção e cálculos da gestão do risco operacional integram o modelo de dados da gestão do risco do Banco Sol.

2.8. Incumprimento

O incumprimento das regras descritas na presente Política pelos Colaboradores do Banco é considerado violação grave de deveres de conduta, consequentemente pode dar lugar à aplicação de medidas disciplinares.

2.9. Aprovação e Revisão

A presente Política entrará em vigor na data da sua aprovação pelo Conselho de Administração, devendo ser revista anualmente ou, extraordinariamente quando justificável, mantendo o histórico das versões, de forma a possibilitar a consulta das alterações efectuadas.

3. OUTORGAMENTO

O Conselho de Administração

António André Lopes
Presidente do Conselho de Administração

Osvaldo Salvador de Lemos Macaia
Presidente da Comissão Executiva

Ema Carla Lemos Coelho Gonçalves
Administradora Executiva

Paula Maria Tavares Monteiro
Administradora Executiva

Sandro Geovaldo Nogueira Fernandes da Silva
Administrador Executivo

Samahina de Sousa da Silva Saúde
Administrador Executivo

Vladmir Patrício Castelo Branco da Cunha
Administrador Executivo

Viriato Diaguenda Fernandes Capita
Administrador Executivo

Luís Reis Paulo Cuanga
Administrador Independente

Tatiana Olívia da Cunha dos Anjos
Administradora Independente

António Daniel Pereira dos Santos
Administrador Independente

Noé José Baltazar
Administrador Não-Executivo

Francisco Domingos Fortunato
Administrador Não-Executivo