**Aviso N.º…… /GBM/2024**

**Maputo, … de Novembro de 2024**

|  |  |
| --- | --- |
| **ASSUNTO:** | **REGRAS SOBRE PROCESSAMENTO E ARMAZENAMENTO DE DADOS DAS INSTITUIÇÕES DE CRÉDITO E SOCIEDADES FINANCEIRAS** |

Mostrando-se necessário rever os requisitos de processamento e armazenamento de dados observados pelas instituições de crédito e sociedades financeiras, o Banco de Moçambique, à luz da alínea d) do n.º 2 do artigo 3, conjugada com a alínea d) do n.º 2 do artigo 37 da Lei n.º 1/92, de 03 de Janeiro e artigo 56 da Lei n.º 20/2020, de 31 de Dezembro determina:

**CAPÍTULO I**

**DISPOSIÇÕES GERAIS**

**Artigo 1**

**Objecto**

O presente Aviso estabelece os requisitos de processamento e armazenamento de dados a serem observados pelas instituições de crédito e sociedades financeiras.

**Artigo 2**

**Âmbito de aplicação**

O presente Aviso aplica-se às instituições de crédito e sociedades financeiras, doravante designadas por “instituições”.

**Artigo 3**

**Definições**

Os termos e expressões usados no presente Aviso são definidos no Glossário, em anexo, que é dele parte integrante.

**CAPÍTULO II**

**CENTROS DE PROCESSAMENTO DE DADOS E SERVIÇOS DE COMPUTAÇÃO EM NUVEM**

**Artigo 4**

**Domicílio de sistemas informáticos**

1. As instituições devem ter os seus sistemas informáticos implementados em centros de processamento de dados (CPD) sediados em território nacional.
2. Exceptuam-se do previsto no número anterior os sistemas periféricos e os sistemas fornecidos de acordo com as políticas de provedores que actuam a nível global, em relação aos quais as instituições devem obter autorização prévia do Banco de Moçambique para alojamento fora de território nacional.

**Artigo 5**

**Requisitos para implementação e funcionamento de centros de processamento de dados**

1. Os CPD primários devem possuir condições físicas e ambientais adequadas por forma a garantir a qualidade dos serviços de tecnologias de informação prestados.
2. As instituições devem possuir políticas e procedimentos para garantir a integridade dos CPD, estabelecendo responsabilidades para a sua gestão.

**Artigo 6**

**Instalações de Réplica**

1. As instituições devem estar dotadas de instalações de réplica, que assegurem a continuidade de negócio e recuperação de dados, em caso de falhas ou desastres.
2. As instalações de réplica devem estar equipadas de meios semelhantes aos dos CPD primários, podendo os mesmos ser instalados em território nacional ou no estrangeiro, desde que se assegure a inexistência de conflitos legais.
3. A domiciliação e activação de instalações de réplica dos CPD primários no estrangeiro carecem de autorização prévia do Banco de Moçambique.
4. As instalações de réplica devem estar situadas a uma distância que assegure exposição a riscos físicos distintos dos aplicáveis aos CPD primários.

**Artigo 7**

**Computação em nuvem**

1. Sem prejuízo do previsto no artigo 4 do presente Aviso, é permitida a contratação de serviços de computação em nuvem para sistemas principais e periféricos, nas seguintes condições:
2. Contratação de serviços de computação em nuvem para sistemas principais apenas em território nacional, sujeita à autorização prévia pelo Banco de Moçambique; e
3. Contratação de serviços de computação em nuvem para sistemas periféricos em território nacional ou estrangeiro.
4. A contratação de serviços de computação em nuvem para sistemas periféricos, fora do território nacional, está sujeita a autorização pelo Banco de Moçambique.
5. A contratação de serviços de computação em nuvem para sistemas periféricos exclusivamente em território nacional, está sujeita a comunicação prévia ao Banco de Moçambique com antecedência mínima de 15 dias.

**Artigo 8**

**Avaliação para contratação de serviços de processamento e armazenamento de dados**

1. Para a contratação de serviços de processamento de dados, no país ou no estrangeiro, as instituições devem adoptar os seguintes procedimentos:
2. Prossecução de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e
3. Verificação da capacidade do prestador de serviço de assegurar:
4. O cumprimento da legislação e da regulamentação em vigor;
5. As certificações relevantes para a prestação do serviço;
6. O acesso pelas instituições aos dados a serem processadas ou armazenadas pelo prestador de serviços;
7. O provimento de informações e de recursos de gestão adequados à monitorização dos serviços a serem prestados;
8. A confidencialidade, integridade, disponibilidade e a recuperação dos dados processados ou armazenadas pelo prestador de serviço; e
9. O acesso pelas instituições aos relatórios de auditoria e/ou certificações acreditadas, contratadas pelo prestador de serviço.
10. As instituições devem definir processos de gestão que permitam identificar os riscos envolvidos e implementar controlos adequados que estejam em conformidade com o apetite ao risco.
11. Para efeitos do disposto no número anterior, os factores a considerar incluem, mas não se limitam, a:
	* + 1. Continuidade de negócio;
			2. Protecção e confiabilidade dos dados;
			3. Integridade e rastreabilidade dos dados;
			4. Conformidade prudencial e regulamentar; e
			5. Garantia do exercício de funções por parte das autoridades de supervisão.

**Artigo 9**

**Pedido de autorização para a contratação de prestadores de serviços de processamento e armazenamento de dados**

As instituições devem, no âmbito do pedido de autorização para a terceirização dos serviços de processamento e armazenamento de dados, submeter os seguintes elementos:

1. Descrição completa do prestador de serviço a contratar, incluindo a respectiva proposta de contrato;
2. Demonstração da necessidade de adoptar o serviço terceirizado e de informação sobre custos, taxas associadas e a metodologia de actualização;
3. Informação detalhada do conjunto de dados que a solução proposta irá recuperar, processar, manter e divulgar, incluindo os sistemas de origem e de destino, bem como os respectivos pormenores do armazenamento;
4. Provas de diligência sobre a capacidade do prestador de serviços com base no previsto no artigo 8 do presente Aviso, que devem incluir igualmente:
	1. Medidas de segurança de protecção de dados em trânsito e em repouso, incluindo cifragem, autenticação multifactor, identificação e correcção de vulnerabilidades e controlos de acesso;
	2. Capacidade para gerir o volume de trabalho exigido pelas instituições;
	3. Capacidade para oferecer um elevado nível de apoio técnico e de serviço ao cliente, com pessoal de apoio dedicado para dar suporte na resolução de quaisquer problemas;
	4. Capacidade de personalizar e adaptar os seus serviços para satisfazer as necessidades específicas da instituição.

**Artigo 10**

**Cláusulas mínimas dos contratos de prestação de serviços de processamento e armazenamento de dados**

Os contratos de prestação de serviços de processamento e armazenamento de dados devem prever no mínimo:

1. Indicação dos países e da região onde os serviços serão prestados e os dados armazenados, processados e geridos;
2. Acordos de níveis de serviços com parâmetros e níveis específicos para cada elemento fornecido, devendo cobrir, dentre outros, os aspectos seguintes: disponibilidade, tempo de resposta, desempenho, segurança e tempo para correção de erros e resolução de incidentes;
3. Práticas de governança corporativa e de gestão proporcionais ao serviço a ser contratado e aos riscos a que estejam expostos;
4. Centros de réplica que garantam a recuperação dos dados, em caso de falhas ou desastres;
5. Suporte técnico na modalidade 24/7 (vinte e quatro horas por dia e sete dias por semana);
6. Medidas de segurança adoptadas para a transmissão, armazenamento e segregação de dados, lógica e física;
7. Direito de auditar, incluindo auditorias remotas pelas instituições, por auditores externos, pelo Banco de Moçambique, ou por qualquer entidade expressamente designada pelo Banco de Moçambique;
8. Acesso ilimitado pelas instituições, pelos seus auditores externos, pelo Banco de Moçambique, ou por qualquer entidade expressamente designada pelo Banco de Moçambique, a relatórios de auditoria e relatórios de testes do prestador de serviços efectuados por entidades independentes;
9. Comunicação prévia, de pelo menos 90 (noventa) dias, às instituições sobre a subcontratação de serviços a prestar e eventuais limitações que possam afectar a prestação de serviços ou o cumprimento da legislação e da regulamentação em vigor;
10. Condições específicas para a resolução de litígios;
11. Processo de gestão de incidentes, incluindo funções e responsabilidades de cada parte;
12. Garantia de que a informação só será utilizada para efeitos do contrato;
13. Obrigatoriedade, em caso de extinção do contrato, de:
14. transferência de dados a um novo prestador de serviços ou à instituição;
15. eliminação dos dados, de forma segura e irreversível, pelo prestador de serviços contratado substituído, após a confirmação da integridade e da disponibilidade de dados recebidos pela instituição.
16. O acesso das instituições à:
17. Informações fornecidas pelo prestador de serviço contratado;
18. Informações relativas a certificações;
19. Informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados.
20. Permissão de acesso do Banco de Moçambique aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre o seu processamento bem como às cópias de segurança dos dados;
21. Adopção de medidas pelas instituições, em decorrência de determinações do Banco de Moçambique;
22. Obrigação de o prestador de serviço contratado manter a instituição permanentemente informada sobre eventuais limitações que possam afectar a prestação dos serviços ou o cumprimento da legislação e da regulamentação aplicável.

**CAPÍTULO III**

**DISPOSIÇÕES FINAIS**

**Artigo 11**

**Regime sancionatório**

O incumprimento do previsto no presente Aviso constitui contravenção punível nos termos da Lei das Instituições de Crédito e Sociedades Financeiras.

**Artigo 12**

**Revogação**

 É revogado o Aviso n.º 4/GGBM/2003, de 10 de Setembro, sobre Centros de Processamento de Dados das Instituições de Crédito e Sociedades Financeiras.

**Artigo 13**

**Entrada em vigor**

O presente Aviso entra em vigor 120 dias a contar da data da sua publicação.

**Artigo 14**

**Esclarecimento de dúvidas**

As dúvidas na interpretação e aplicação do presente Aviso devem ser submetidas ao Departamento de Supervisão Prudencial do Banco de Moçambique.

**ANEXO**

**GLOSSÁRIO**

**C**

**Centro de Processamento de Dados (CPD)** - compreende o conjunto de infraestruturas de comunicações, de armazenamento e recursos computacionais, que incluem os servidores e as respectivas aplicações que asseguram o processamento de dados e a interconectividade entre os diversos componentes de todo o sistema informático.

**Computação em Nuvem (*Cloud computing*)** - modelo que permite o acesso e o fornecimento de forma conveniente, sob demanda a um conjunto de recursos computacionais configuráveis (redes, servidores, aplicativos e serviços) e armazenamento de dados que podem ser rapidamente aprovisionados e acessíveis com o mínimo de esforço de gestão ou interacção com os prestadores de serviços.

**S**

**Sistema periférico** refere-se ao sistema informático que não é essencial para as operações principais das instituições, sendo este importante para o negócio, mas não crítico para a sua capacidade de funcionar e servir ao cliente, permitindo que as instituições desempenhem funções como *marketing* e vendas, gestão de recursos humanos, orçamento e colaboração, entre outras.

**Sistema principal (*core*)** é todo aquele sistema informático que é essencial para as operações da instituição e que em caso de falha ou interrupção têm um impacto significativo no negócio. Estes são baseados em quaisquer componentes tecnológicos (*software*, *hardware*, base de dados, processos, aplicações, entre outros) para a execução de funções como gestão de operações financeiras, gestão de cartões bancários, canais digitais e gestão de transacções em mercados financeiros.

**Sistemas que actuam a nível global,** compreende o conjunto de Sistemas de transferências internacionais, Serviços de informação sobre mercados, infra-estruturas de redes globais de gestão de cartões bancários, infra-estruturas de suporte para operações de compensação e liquidação entre câmaras de compensação, contrapartes centrais e instituições de liquidação e seus membros, serviços de correspondente bancário e remessas de valores, e sistemas de monitoria de combate ao branqueamento de capitais e ao financiamento do terrorismo (AML/CFT), entre outros.