Quinta-feira, 2 de Abril de 2020 I Série – N.º 41

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 680,00

SUMÁRIO

COMANDANTE-EM-CHEFE DAS FORÇAS ARMADAS ANGOLANAS

Ordem do Comandante-Em-Chefe n.º 5/20

de 2 de Abril

O Presidente da República determina, nos termos da alínea e) do artigo 122.º e do n.º 4 do artigo 125.º, ambos da Constituição da República de Angola, conjugados com o artigo 30.º da Lei n.º 24/19, de 23 de Setembro — sobre o Estatuto dos Magistrados Judiciais Militares, e alínea d) do n.º 2 do artigo 10.º da Lei n.º 2/93, de 26 de Março — Lei de Defesa Nacional e das Forças Armadas, ouvido o Conselho de Segurança Nacional, o seguinte:

1. É promovido ao Posto Militar de Tenente-General o Brigadeiro (NIP 40307192) Celestino Manuel, Juiz Conselheiro do Supremo Tribunal Militar.

ARTIGO 24.°
(Norma revogatória)

Fica revogado o Aviso n.° 25/12, de 20 de Agosto, e toda a regulamentação que contrarie o disposto no presente Aviso.

ARTIGO25.°
(Dúvidas e omissões)

As dúvidas e omissões resultantes da interpretação e aplicação do presente Aviso são resolvidas pelo Banco Nacional de Angola.

ARTIGO 26.°
(Entrada em vigor)

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

Publique-se.

Luanda, aos 16 de Março de 2020.

O Governador, *José de Lima Massano*.

Aviso n.° 8/20
de 2 de Abril

Considerando a necessidade de se estabelecer regras sobre a componente de segurança cibernética, bem como os termos e condições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas Instituições Financeiras sob a supervisão do Banco Nacional de Angola;

Havendo igualmente a necessidade de se definir os mecanismos de prestação de informação respeitantes a quaisquer situações com impacto significativo na estabilidade do Sistema Financeiro Angolano, nomeadamente eventos com potencial impacto negativo nos resultados ou capital próprio das Instituições Financeiras, incluindo incidentes de índole operacional, num contexto de importância crescente do risco operacional associado às tecnologias de informação e comunicação;

Nestes termos, ao abrigo das disposições combinadas da alínea j) do n.° 1 do artigo 90.° da Lei n.° 12/15, de 17 de Junho — Lei de Bases das Instituições Financeiras e da alínea f) do n.° 1 do artigo 21.° e do artigo 51.°, ambos da Lei n.° 16/10, de 15 de Julho — Lei do Banco Nacional de Angola, determino:

CAPÍTULO I
Disposições Gerais

ARTIGO 1.°
(Objecto)

O presente Aviso estabelece as regras sobre a política de segurança cibernética e os termos e condições de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas Instituições Financeiras autorizadas a funcionar pelo Banco Nacional de Angola.

ARTIGO 2.°
(Âmbito)

O presente Aviso é aplicável às Instituições Financeiras sob supervisão do Banco Nacional de Angola, adiante abreviadamente, designadas, por Instituições, nos termos e condições previstos na Lei de Bases das Instituições Financeiras.

ARTIGO 3.°
(Definições)

Para efeitos do presente Aviso, entende-se por:

a) *Segurança Cibernética*: conjunto de políticas e controlos, meios e tecnologias que visam proteger programas, computadores, redes e dados de intrusão ilícita ou ataques digitais que provoquem danos aos mesmos;

b) *Computação em Nuvem*: modelo que permite o acesso e o fornecimento de forma conveniente e directa a um conjunto de recursos computacionais configuráveis e armazenamento de dados que podem ser rapidamente aprovisionados e acessíveis com o mínimo esforço de gestão ou interacção entre os prestadores de serviços;

c) *Infra-Estrutura Tecnológica Crítica*: sistemas e activos de informação, sejam físicos, virtuais e vitais para o funcionamento normal das Instituições Financeiras, cuja incapacidade ou destruição acarreta um elevado impacto na operacionalidade das Instituições.

CAPÍTULO II
Política de Segurança Cibernética

ARTIGO 4.°
(Implementação da política de segurança cibernética)

1. As Instituições devem definir, implementar e manter uma política de segurança cibernética, com base em padrões, princípios e directrizes internacionalmente aceites, que visam assegurar a confidencialidade, integridade e a disponibilidade das redes, dados e dos sistemas de informação utilizados.

2. A política de segurança cibernética referida no número anterior deve prever, no mínimo, o seguinte:

a) A dimensão, o perfil de risco e o modelo de negócio da Instituição;

b) A natureza das operações e a complexidade dos produtos, serviços, actividades, processos das Instituições; e

c) A sensibilidade dos dados e das informações sob responsabilidade das Instituições.

3. Os procedimentos e os controlos adoptados para reduzir a vulnerabilidade das Instituições a incidentes e atender aos demais objectivos da política de segurança cibernética, de acordo com as directrizes da ISO/IEC 27035 e da ISO 27001, respeitantes à gestão de incidentes de segurança de informação tecnológica e gestão da segurança da informação, respectivamente, devem comportar:

a) A autenticação, a autorização, a criptografia, a prevenção e a detecção de intrusão;

b) A prevenção de fuga de informações;

c) A realização periódica de testes e auditorias para detecção de vulnerabilidades;

d) A protecção contra softwares maliciosos;

e) O controlo de acesso e de segmentação da rede de computadores;

f) A manutenção de cópias de segurança dos dados e das informações;

g) Os controlos específicos para garantir a segurança das informações sensíveis, incluindo de rastreabilidade de informação;

h) Os procedimentos a adoptar para o registo, a análise da causa e do impacto, bem como, o controlo dos efeitos de incidentes para as actividades das Instituições;

i) Os mecanismos para disseminação, capacitação e avaliação periódica de pessoal para a elevação da cultura de segurança cibernética na Instituição;

j) A prestação de informações a clientes e utentes sobre precauções na utilização de produtos e serviços financeiros; e

k) O comprometimento do órgão da administração com a melhoria contínua dos procedimentos relacionados com a política de segurança cibernética.

4. As Instituições devem definir directrizes necessárias para:

a) A elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de tecnologia de informação e do negócio;

b) A definição de procedimentos e de controlos de prevenção e tratamento dos incidentes a serem adoptados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das actividades operacionais de Instituições;

c) Definição de parâmetros a serem utilizados na avaliação da relevância de incidentes; e

d) A classificação dos dados e das informações quanto à criticidade para o negócio da Instituição.

ARTIGO 5.º
(Dever de divulgação de políticas de segurança)

A política de segurança cibernética deve ser divulgada ao público, trabalhadores e empresas prestadoras de serviços, mediante a utilização de uma linguagem clara, objectiva e acessível, de acordo com os níveis de funções desempenhadas, bem como a sensibilidade das informações inerentes à referida política.

ARTIGO 6.º
(Plano de acção e de resposta a incidentes)

Para efeitos de implementação da política de segurança cibernética, as Instituições devem elaborar um plano de acção capaz de responder a incidentes, contendo, no mínimo, os seguintes requisitos:

a) Adequação das estruturas organizacionais e operacionais;

b) Rotinas, procedimentos, controlos e tecnologias a serem utilizadas na prevenção e resposta a incidentes, em conformidade com as directrizes da política de segurança cibernética;

c) Acções a serem desenvolvidas pelas Instituições para adequar às estruturas, organizacional e operacional, aos princípios e às directrizes da política de segurança cibernética;

d) Indicação da área responsável pelo registo, monitoramento e controlo de incidentes relevantes; e

e) Manual de procedimentos de política de segurança cibernética, aprovado pelo órgão da administração ou gerência, que deve ser revisto anualmente ou sempre que ocorram alterações relevantes na Instituição.

ARTIGO 7.º
(Institucionalização de estruturas de segurança)

As Instituições devem estabelecer uma estrutura ou equipa(s) dedicada(s) à política de segurança cibernética, responsável(eis) pela política de segurança cibernética e pela execução do plano de acção e de resposta a incidentes.

ARTIGO 8.º
(Obrigação de notificação de incidentes)

1. As Instituições devem comunicar, ao Banco Nacional de Angola, as violações das redes e dos sistemas de informação ou perdas de integridade com impacto significativo no funcionamento das referidas redes e serviços.

2. A comunicação prevista no número anterior deve acontecer obrigatoriamente após a detecção do incidente, seguindo-se de outras comunicações, com pontos de situação com intervalos de 4 horas, até à reposição normal dos serviços.

3. Sem prejuízo do dever de sigilo profissional e de livre concorrência, sempre que necessário, as Instituições devem desenvolver iniciativas para a partilha de informações, sobre os incidentes relevantes, visando a mitigação do impacto e reforço da resiliência do sistema financeiro a ataques cibernéticos.

CAPÍTULO III
Contratação de Serviços de Computação em Nuvem

ARTIGO 9.º
(Adopção da computação em nuvem)

1. A adopção de serviços na nuvem pelas Instituições implica a adequação de políticas, estratégias e estruturas para gestão de riscos inerentes à terceirização dos referidos serviços.

2. Na avaliação da relevância do serviço a ser disponibilizado na nuvem, a Instituição deve considerar a criticidade e a sensibilidade dos dados e das informações suportadas pelo referido serviço, de acordo com a sua classificação, bem como o risco associado em caso de acesso indevido.

3. As Instituições devem garantir a capacitação dos seus recursos humanos para a correcta gestão dos serviços implementados, visando assegurar a autonomia interna para o acesso e utilização da tecnologia de nuvem.

4. Sempre que se verificar a impossibilidade de manutenção do contrato de prestação de serviços, as Instituições devem garantir a gestão de continuidade dos serviços contratados em nuvem.

ARTIGO 10.º
(Comunicação da adopção da computação em nuvem)

1. A intenção de contratação de serviços com o suporte de computação em nuvem deve ser comunicada ao Banco Nacional de Angola, com antecedência mínima de 60 (sessenta) dias da referida contratação para efeitos de apreciação e aprovação, a qual deve conter a seguinte informação detalhada:

a) A empresa a ser contratada;
b) O plano de continuidade de negócio;
c) Os serviços a serem prestados;
d) O local ou país de «hospedagem ou alojamento» da infra-estrutura, sistemas e processamento;
e) Tipo de informação a migrar para a nuvem;
f) Indicação da lei que rege o contrato que se pretende celebrar;
g) Demonstração de competências e recursos necessários para manter e monitorizar o serviço que pretende contratar; e
h) Disponibilidade do prestador de serviços de computação em nuvem de cooperar com as autoridades nacionais que supervisionam a Instituição.

2. Sempre que se verificar alterações contratuais, as Instituições devem, igualmente, comunicar tal ocorrência ao Banco Nacional de Angola, num período não inferior a 90 (noventa) dias, podendo esse período ser inferior, em casos excepcionais, desde que devidamente justificado, quando comprometam o pleno funcionamento das Instituições;

3. As Instituições devem, ainda, criar condições que assegurem a continuidade de negócio.

4. Para os serviços já contratados a comunicação ao Banco Nacional de Angola deve acontecer no período máximo de 30 (trinta) dias após a publicação do presente normativo.

ARTIGO 11.º
(Contratação de serviços em nuvem)

1. Previamente à contratação de serviços de computação em nuvem, as Instituições devem verificar e documentar a capacidade do potencial prestador de serviço em assegurar o cumprimento dos seguintes aspectos:

a) A confidencialidade, integridade, disponibilidade e recuperação de dados e de informações processados ou armazenados pelo prestador de serviço;
b) O acesso das Instituições aos dados e às informações a serem processados ou armazenados pelo prestador de serviços, bem como o provimento de informações e de recursos de gestão adequados à monitorização dos serviços a serem prestados; e
c) A disponibilização dos relatórios elaborados por empresa de auditoria especializada e independente, relativos aos procedimentos e aos controlos utilizados na prestação de serviços.

2. Na contratação de serviços de computação em nuvem, as Instituições devem observar, no mínimo, os seguintes requisitos:

a) Práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;
b) Verificação da capacidade do potencial prestador de serviço;
c) Licença e certificação de prestadores de serviço de computação em nuvem, cujo local de alojamento do datacenter deve estar em conformidade com as boas práticas do mercado;
d) Idoneidade, disponibilidade, experiência profissional e capacidade financeira, nos termos da legislação vigente do País;
e) As Instituições devem avaliar a relevância dos serviços e classificação da informação, nos termos do anexo do presente Aviso;
f) Centros de dados de suporte, que garantam a recuperação dos mesmos, em caso de desastre e acesso a backup (cópia de segurança) em situações de anormalidade;
g) Suporte técnico na modalidade 24/7 (vinte e quatro horas por dia e sete dias na semana);
h) Medidas de segurança adoptadas para a transmissão e armazenamento dos dados, segregação de dados, lógico e físico, e adequação do controlo de acesso para protecção de informação;
i) Comunicação prévia 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;
j) Transferência de dados ao novo prestador de serviços ou às Instituições Contratantes, em caso resolução do contrato, e, consequentemente, a eliminação dos dados pela empresa contratada substituída, após a confirmação da integridade e da disponibilidade de dados recebidos pela contratante;
k) Permissão de acesso pelas Instituições às informações e recursos de gestão adequados à monitorização de serviços a serem fornecidos pela empresa contratada, visando a verificação do cumprimento do disposto na alínea f) do n.º 2 do presente artigo; e
l) Acesso à documentação e às informações referentes aos serviços prestados pelas Instituições Contratantes, designadamente, dados armazenados e processados, cópias de segurança e códigos de acesso.

3. As Instituições Contratantes de serviços de computação em nuvem são responsáveis por garantir a segurança dos serviços contratados, bem como pelo cumprimento da legislação em vigor.

ARTIGO 12.º
(Classificação da informação a migrar para a nuvem)

1. As Instituições devem classificar as informações consideradas imprescindíveis à segurança da sociedade, dos seus clientes e do Estado, em grau de sigilo da informação em muito confidencial, confidencial, reservada, interna e pública.

2. Para o efeito de classificação da informação, as Instituições Financeiras devem considerar os requisitos constantes no Anexo, que constitui parte integrante do Aviso.

3. A classificação da informação descrita no número anterior deve estar em conformidade com as disposições constantes na Lei n.º 22/11, de 17 de Junho, Lei da Protecção de Dados Pessoais, conjugadas com a Lei n.º 7/17, de 16 de Fevereiro, Lei de Protecção das Redes e Sistemas Informáticos, bem como com o disposto nos artigos 76.º e 77.º, ambos da Lei n.º 12/15, de 17 de Junho, Lei de Bases das Instituições Financeiras.

4. As Instituições, em função da classificação atribuída a cada tipo de informação, determinam a que é elegível para migrar para a nuvem, tendo em conta cada modelo de implementação em nuvem disponíveis, designadamente:

a) Serviços em nuvem prestados dentro de uma organização e que oferecem todas as funções básicas da computação em nuvem, respeitante ao aumento da produtividade, flexibilidade e escalabilidade, acesso remoto restrito a apenas uma organização, sem partilha de recursos de tecnologia de informação com outras organizações ou utilizadores fora do ambiente organizacional;

b) Serviço prestado por um provedor a utilizadores comuns ou organizações, ficando esse provedor de serviços com a responsabilidade de implementação de mecanismos de protecção, hospedagem, manutenção e gestão de dados, cobrando desses apenas os recursos utilizados, sejam eles de infra-estrutura aplicacional, infra-estrutura física ou *softwares*;

c) Serviço baseado na partilha da infra-estrutura de tecnologia de informação por várias organizações que partilham as mesmas preocupações como a missão, requisitos de segurança, políticas, entre outros, podendo ser administrada pelas próprias organizações ou por um terceiro, podendo existir no ambiente da organização ou fora dela; e

d) Serviço baseado num ambiente de computação que combina nuvem pública e nuvem privada, permitindo que os dados e aplicações sejam partilhados entre elas.

CAPÍTULO IV
Disposições Finais

ARTIGO 13.º
(Sanções)

O incumprimento do disposto no presente Aviso constitui contravenção prevista e punível nos termos da Lei n.º 12/15, de 17 de Junho, Lei de Bases das Instituições Financeiras.

ARTIGO 14.º
(Dúvidas e omissões)

As dúvidas e omissões resultantes da interpretação e aplicação do presente Aviso são resolvidas pelo Banco Nacional de Angola.

ARTIGO 15.º
(Norma revogatória)

Fica revogada toda a disposição que contrarie o disposto no presente Aviso.

ARTIGO 16.º
(Entrada em vigor)

O presente Aviso entra em vigor 30 (trinta) dias após a data da sua publicação.

Publique-se.

Luanda, aos 16 de Março de 2020.

O Governador, *José de Lima Massano*.

ANEXO

Para efeitos de classificação da informação pelas Instituições Financeiras, há a necessidade de medidas de tratamento especial, tendo em conta as implicações e responsabilidades associadas a esta classificação.

As Instituições Financeiras devem classificar a informação de acordo com os seguintes critérios:

1. Informação Muito Confidencial

1.1 É toda informação associada a interesses relevantes da Instituição. Se revelada, pode trazer sérios prejuízos financeiros, enorme impacto ao negócio ou repercussões para a imagem da Instituição ou do Governo de Angola. Estas informações requerem medidas excepcionais de controlo e protecção contra acessos não-autorizados.

1.2 As informações muito confidenciais são, em geral, restritas ao Conselho de Administração, Directores com função de gestão relevante, gerentes e empregados previamente designados que, pela natureza da função que exercem, são obrigados a conhecê-las.

1.3 Toda informação muito confidencial deve possuir controlo rigoroso quanto a sua divulgação, bem como registos históricos com a identificação inequívoca dos utilizadores que tiveram acesso a ela.

1.4 As cópias de documentos muito confidenciais devem ser pré-aprovadas pelo seu proprietário (quem deu origem ao documento) e possuir uma identificação única.

1.5 A informação muito confidencial deve ser guardada em local com acesso controlado e possuir medidas de segurança física para o seu transporte, sendo necessária a autorização do proprietário para o seu transporte para fora da Instituição.

1.6 Para a transmissão electrónica de informações muito confidenciais é obrigatório o uso de criptografia, em qualquer meio de comunicação, interno ou externo à Instituição.

2. Informação Confidencial

2.1 É toda informação cujo conhecimento deve ficar limitado a um número reduzido de pessoas autorizadas. Se revelada, pode trazer grande impacto ao negócio ou repercussões para a imagem da Instituição, embaraços administrativos com funcionários ou trazer vantagens a terceiros. Estas informações requerem um alto grau de controlo e protecção contra acessos não-autorizados.

2.2 Incluem-se nesta classificação: as informações que garantem à Instituição a obtenção de vantagens competitivas, as que descrevem uma parte significante dos negócios da Instituição, as que contêm estratégias operacionais de longo prazo, as que são importantes para o sucesso técnico ou financeiro de um produto e aquelas que têm um impacto potencialmente sério nas políticas e práticas da área de Recursos Humanos.

2.3 As informações confidenciais são, em geral, restritas aos gestores da Instituição e empregados previamente designados que, pela natureza da função que exercem, são obrigados a conhecê-las.

2.4 A divulgação interna de uma informação confidencial para empregados que não pertencem à mesma função de quem a recebeu, bem como as cópias de documentos confidenciais, devem ser pré-aprovadas pelo proprietário.

2.5 Toda informação confidencial deve ser guardada em local com acesso controlado e possuir medidas de segurança física para o seu transporte, sendo necessária a autorização do proprietário para o seu transporte para fora da Instituição.

2.6 Para a transmissão electrónica de informações confidenciais é obrigatório o uso de criptografia.

3. Informação Reservada

3.1 É toda informação cujo conhecimento e uso deve estar restrito a um grupo específico de empregados ou áreas da Instituição. Não deve ser divulgada, publicada e estar acessível a qualquer empregado ou não-empregado.

3.2 As informações reservadas são, em geral, limitadas a uma unidade ou grupo de trabalho e empregados que, pela natureza da função que exercem, são obrigados a conhecê-las.

3.3 Na classificação de uma informação como reservada deve-se explicitar para que grupo ou propósito a informação é reservada.

3.4 É permitida a divulgação interna de uma informação reservada, bem como a cópia de documentos reservados, para outros empregados, que deles necessitem para a realização de suas tarefas.

3.5 Toda informação reservada deve ser guardada em local com acesso controlado, sendo necessária a autorização do proprietário para o seu transporte para fora da Instituição.

4. Informação Interna

4.1 É toda informação cujo conhecimento e uso está restrito exclusivamente ao âmbito interno e propósitos da Instituição, estando disponível para todos os empregados, e não-empregados autorizados a circular em suas dependências. Só devem ser reveladas ao público externo mediante autorização.

4.2 Incluem-se nesta classificação: as informações relativas ao desenvolvimento de programas internos da empresa; listas para localização dos empregados na empresa, etc.

5. Informação Pública

5.1 É toda informação que pode ou deve ser divulgada para o público externo à Instituição.

5.2 Incluem-se nesta classificação: as informações de carácter informativo a serem publicadas e as informações, que a Instituição é obrigada a divulgarem em função da legislação vigente.

5.3 Toda informação pública deve receber tratamento especial quanto à sua apresentação e conteúdo, de modo a não prejudicar a imagem da Instituição.

O Governador, *José de Lima Massano.*

O. E. 0549 - 4/41 - 150 ex. - I.N.-E.P. - 2020