BANCO DE DESENVOLVIMENTO DE ANGOLA

Uma visão de futuro.

Política de Cibersegurança e de Adopção de Computação em Nuvem

NORMA DE SERVIÇO N.º 701/22	Entrada em vigor 30/12/2022
Política de Cibersegurança e de Adopção de Computação em Nuvem	Data da publicação 30/12/2022

ÍNDICE

Modelo 02

1. Introdução

O Banco de Desenvolvimento de Angola (BDA) está totalmente empenhado em salvaguardar a confidencialidade, integridade e disponibilidade da informação sob sua responsabilidade. Com foco na informação dos seus clientes, parceiros, colaboradores e na sua própria informação corporativa classificada, o BDA assume o compromisso com os requisitos legais relativos à segurança e cibersegurança, aplicando um conjunto de medidas técnicas e organizativas visando proteger os activos e recursos de informação.

A política em apreço tem em consideração o contexto do negócio, a relação com outras entidades, a complexidade dos produtos e operações, com uma orientação ao risco e aplicando as medidas proporcionais e mais adequadas. O presente documento estabelece também a política e o processo de Computação em Nuvem do Banco de Desenvolvimento de Angola (BDA), em linha com os requisitos legais aplicáveis, nomeadamente com o Aviso n.º 08/2020, de 02 de Abril.

2. Glossário

Activo de Informação – Um activo de software ou de hardware que se encontra no ambiente empresarial;

Apetite ao Risco – Os tipos de risco e o seu nível agregado que os prestadores de serviços de pagamento e as instituições financeiras bancárias estão dispostas a assumir no contexto da sua capacidade de risco, de acordo com o seu modelo de negócio, para alcançar os seus objectivos estratégicos;

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;

Incidente Operacional ou de Segurança – um único evento ou uma série de eventos conexos e imprevistos pela Instituição Financeira Bancária que tem, ou poderá vir a ter, um impacto negativo na integridade, disponibilidade, confidencialidade e/ou autenticidade dos serviços;

Infraestrutura 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;

Segurança Cibernética / Cibersegurança – 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.

Segurança Física – Conjunto de mecanismos que visam prevenir o acesso não autorizado a equipamentos, instalações, materiais ou documentos da instituição;

Segurança Lógica – Conjunto de mecanismos que visam controlar o acesso a aplicativos, dados, sistemas operacionais, senhas e arquivos de log, por meio de hardwares e softwares, criptografia e diversas aplicações contra-ataques de cibercriminosos e possíveis invasores às fontes da instituição;

Riscos Associados às TICs e à Segurança Cibernética – O risco de perdas por violação da confidencialidade, falta de integridade de sistemas e dados, inadequação ou indisponibilidade de sistemas e dados ou incapacidade para alterar as tecnologias da informação (TI) num período de tempo e custos razoáveis quando o ambiente ou os requisitos empresariais se alteram, inclui riscos de segurança resultantes de eventos externos ou processos internos inadequados ou deficientes, incluindo ataques cibernéticos ou uma segurança física inadequada.

3. Âmbito

A presente política aplica-se a todos os colaboradores e fornecedores do BDA, e em especial a aqueles com responsabilidades directa relacionada a Segurança Cibernética e Adopção de Computação em Nuvem, quer do ponto de vista técnico/operacional, quer na óptica da gestão da conformidade.

4. Princípios de Segurança e Cibersegurança

No contexto de ameaças à segurança de informação e cibersegurança, torna-se imperativo a aplicação de medidas técnicas e organizativas de forma a salvaguardar e a perda ou roubo de informação, acessos não autorizados, assegurar a continuidade e disponibilidade, manter a qualidade da informação, adoptando um sistema de gestão e uma revisão contínua dos seus controlos.

- Todas as leis e regulamentos aplicáveis devem ser respeitados;
- A formação e sensibilização do capital humano são promovidas regularmente, conducente ao reforço continuado de uma cultura de segurança da informação e cibersegurança.

5. Objectivos de Segurança e Cibersegurança

São listados de seguida os objectivos de segurança e Cibersegurança fixados:

a) Prevenir o acesso físico não autorizado, danos e interferências nas informações e nos recursos de processamento de dados;

b) Garantir que a segurança da informação seja projectada desde logo no desenho das aplicações e implementada ao longo do seu ciclo de vida;

c) Garantir os requisitos de segurança e de gestão relativamente à computação em nuvem;

d) Contribuir para uma cultura de segurança da informação, numa lógica de melhoria contínua, contemplando a cooperação com as entidades do ecossistema do BDA.

6. Política de Computação em Nuvem

A adopção da política de computação em nuvem no BDA obedece a um processo estruturado, implicando o planeamento e avaliação de viabilidade, análise do risco inerente, selecção da terceirização dos referidos serviços através de critérios formais, aplicação dos controlos de mitigação do risco e monitorização da adequação das medidas técnicas e organizativas aplicáveis.

7. Selecção do Fornecedor

Na avaliação dos atributos dos fornecedores para a sua selecção, serão considerados critérios da sua qualificação técnica, de *compliance* e risco, para além do valor financeiro associado.

Como orientação, recomenda-se que os fornecedores de computação em nuvem (CSP – *Cloud service providers*) tenham aderido ao referencial da CSA (*Cloud Security Alliance*), boa prática nesta matéria, consultável em www.clousecurityalliance.org.

A qualificação (e a comparação) dos fornecedores deverá basear-se no referencial da CSA, acima citada, nomeadamente no CCM – *Could Controls Matrix*, sempre que for aplicável aos fornecedores em apreço.

8. Responsabilidades

Os colaboradores, bem como terceiros, que de alguma forma possam interagir com as informações dos clientes e do BDA, são obrigados a apoiar e executar todas as regras de segurança da informação, devendo reportar imediatamente qualquer evento que possa causar um incidente de segurança, comunicando através do canal institucionalizado para o efeito.

Os colaboradores, bem como terceiros, podem ser responsabilizados em caso de incumprimento das políticas e normas de segurança da informação do BDA.

9. Obrigação de Notificação de Incidentes

O BDA irá activamente contribuir para uma cultura de segurança e controlo dos riscos, através de iniciativas de comunicação e cooperação com partes interessadas, numa lógica de parceria. O objectivo de manter a segurança e cibersegurança num ambiente complexo e conflitual é um desafio que apela à cooperação institucional e a um esforço colectivo. Adicionalmente, a adopção da política de computação em nuvem no BDA obedece ainda a um processo de comunicação ao BNA.

10. Entrada em Vigor e Revisão

A presente Política foi publicada à 30 de Dezembro de 2022, e entra em vigor na data da sua publicação.

PRESIDENTE DO CONSELHO DE ADMINISTRAÇÃO

_____