BDA

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

1. Introdução
2. Glossário
3. Intervenientes
4. Âmbito
5. Princípios de Segurança e Cibersegurança
6. Objectivos de Segurança e Cibersegurança
7. Política de Computação em Nuvem: Visão das Actividades
8. Modelo de Governo
9. Descrição das Actividades
10. Classificação
11. Responsabilidades
12. Obrigação de Notificação de Incidentes
13. Alterações
14. Papéis, Responsabilidades e Autoridades
15. Entrada em Vigor e Revisão

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;

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;

SGSI – Sistema de Gestão de Segurança de Informação e Cibersegurança;

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. Intervenientes

Conselho de Administração (CAD) – Órgão de governo responsável pela aprovação da Política de Segurança Cibernética e Adopção de Computação em Nuvem.

Comissão Executiva (CEX) – Órgão de gestão corrente responsável, no âmbito das suas funções, pela coordenação e acompanhamento da implementação da presente política.

Comité de Organização e Tecnologias (POT) – Órgão com competências delgadas para supervisão da implementação da presente política.

Direcção de Administração Geral (DAG) – Unidade de estrutura responsável por todos os serviços relativos à logística, instalações, gestão de economato, entre outros.

Direcção de Tecnologias de Informação e Comunicação (DTI) – Unidade de estrutura responsável pelos sistemas de informação que suportam toda a operação do Banco.

Gabinete de Auditoria Interna (GAI) – Gabinete responsável, no âmbito das suas funções, pela execução de auditorias periódicas por forma a avaliar a adequação e eficácia dos serviços e sistemas tecnológicos e de informação do BDA. O GAI, em função da natureza ou especificidade da ocorrência ou do evento, pode socorrer-se de entidades externas sobre a sua supervisão.

Gabinete de Gestão de Risco (GGR) – Unidade de estrutura responsável pela análise e monitorização do risco de exposição do BDA, em particular, os riscos associados as tecnologias de informação.

Gabinete de Organização e Sistemas de Informação (GOI) – Unidade de estrutura responsável pela definição, actualização, manutenção da presente política.

Gabinete de Segurança de Informação e Cibersegurança (GSI) – Unidade de estrutura responsável pela implementação da presente política.

4. Âmbito

A presente política aplica-se a todos os colaboradores 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.

5. 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.

Os princípios da política de segurança da informação, compreendendo a prevenção e recuperação, são os seguintes:

- As informações devem ser protegidas contra acesso não autorizado, sendo prevenidas utilizações indevidas (fuga de informação);
- A confidencialidade da informação deve ser garantida de forma continuada;
- A integridade das informações deve ser assegurada e protegida;

- Eventuais falhas na segurança detectadas ou sob suspeita devem ser analisadas;
- A resposta operacional a eventuais incidentes deve estar formalizada, estando estabelecidas as equipas competentes para o efeito;
- 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.

Para o efeito, o BDA deve definir um Sistema de Gestão da Segurança da Informação e Cibersegurança (SGSI) que compreende esta política, bem como outras políticas, procedimentos e normas destinadas a manter, rever e melhorar os controlos de segurança da informação, com uma abordagem orientada para o risco e com sentido de proporcionalidade.

6. Objectivos de Segurança e Cibersegurança

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

a) Desenvolver normas de segurança da informação alinhadas com os requisitos do BDA, boas práticas, leis e regulamentos aplicáveis;

b) Assegurar que os activos de informação recebam um nível de protecção adequado, de acordo com sua classificação;

c) Garantir o devido controlo de acesso e registo dos utilizadores, sob o princípio do acesso mínimo e essencial para a função, revisto regularmente;

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

e) Prevenir a exploração de vulnerabilidades técnicas, monitorizando de forma sistemática os recursos críticos;

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

g) Assegurar uma abordagem consistente na gestão de incidentes de segurança;

h) Acompanhar continuamente o nível de protecção dos sistemas, dados e aplicações, envolvendo as várias partes interessadas;

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

j) Garantir os requisitos de segurança no plano de continuidade de negócio; e

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

7. Política de Computação em Nuvem: Visão das Actividades

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.

Deste modo, a política de computação em nuvem estabelece os seguintes requisitos: (a) pré-contratação dos serviços, (b) na contratação, (c) durante a contratação, (d) na eventual pós-contratação.

a) Pré-contratação dos serviços

- Planeamento: avaliação da criticidade dos dados e classificação da informação em causa.
- Análise do risco: análise do risco potencial envolvido e critérios de mitigação para colocação do mesmo a um nível aceitável.

b) Na contratação dos serviços

- Selecção do fornecedor;
- Inclusão de controlos no contrato.

c) Durante a vigência do acordo de serviços

- Monitorização dos controlos.

d) Na pós-contratação

- Acompanhamento da transição de serviço.

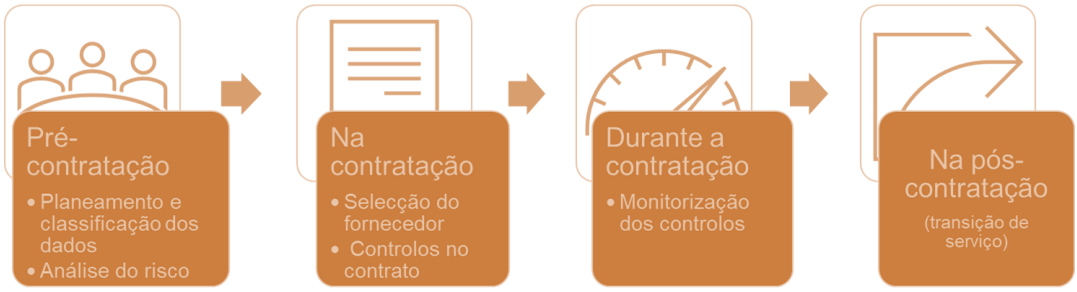

Figura 1 – Actividades da Computação em Nuvem.

8. Modelo de Governo

A Política de Cibersegurança e Adopção de Computação em Nuvem, faz parte do conjunto de normas que definem a estratégia de tecnologias de informação, que visam em articulação com as demais políticas da instituição, assegurar adopção das melhores práticas nacionais e internacionais a nível Cibersegurança e computação em nuvem.

O Gabinete de Segurança de Informação e Cibersegurança é responsável pela implementação da presente política, submetendo sempre que necessário à CEX as situações que possam comprometer os serviços e sistemas do BDA.

Adicionalmente, compete ao Gabinete de Gestão de Risco a monitorização, controlo e supervisão sobre a implementação e operacionalização da presente política, enquanto segunda linha de defesa.

9. Descrição das Actividades

As actividades descritas anteriormente são agora, de forma individual, sumariamente desenvolvidas.

9.1. Planeamento e Classificação da Informação

Na avaliação da relevância do serviço a ser disponibilizado na nuvem, o BDA deve considerar a criticidade e a sensibilidade dos dados e das informações a suportar pelo serviço. Neste particular, devem ser verificados:

a) Face ao grau de criticidade dos dados, alinhar o modelo de serviço de computação em nuvem mais indicado (ex*:* nuvem pública ou privada);

b) Face ao risco potencial, projectar os requisitos de segurança e de protecção e privacidade de dados (ex: encriptar os dados; controlo da localização dos dados).

Em função da criticidade poderá ser aplicado:

Modelo aplicável de computação em nuvem	Descrição
Computação em nuvem no modelo privado	Dados sensíveis, categorias especiais de dados; Requisitos específicos de Clientes em caso de computação em nuvem; Situações de risco potencial extremamente elevado.
Computação em nuvem no modelo público	Dados confidenciais, dados pessoais. Nota: desde que mantidos com medidas de protecção de segurança adequadas. Dados não críticos para o negócio ou sem impactos significativos em termos de privacidade.

9.2. Análise do risco do potencial serviço em nuvem

O BDA deve ainda avaliar os riscos associados ao potencial serviço em nuvem, visando a implementação dos controlos compensatórios adequados na fase seguinte de selecção de fornecedores. Os riscos potenciais a ponderar (e a mitigar), entre outros, contemplam:

- Acessos indevidos;
- *Compliance* (ex: localização dos dados);
- Dependência de fornecedor (*lock in);*
- Eventual falha no isolamento dos dados;
- Protecção dos dados e continuidade;
- Ameaças internas no fornecedor do serviço;
- Eliminação de dados ou devolução na transição do serviço.

Nota 1: Antes da contratação do serviço, a informação a migrar para este ambiente tecnológico deverá ser classificada, sendo que as regras específicas do seu manuseamento devem ser aplicadas. Por exemplo, dados confidenciais devem ser encriptados, na comunicação e quando arquivados, no ambiente de computação em nuvem.

Nota 2: Antes do processo de migração deve ser ponderado e decidido a metodologia de garantir a continuidade de IT:

- Suportado apenas na continuidade de IT do fornecedor de serviço;
- Suportado por um outro fornecedor, em redundância;
- Suportado por sistemas próprios do BDA, em complementaridade da continuidade do fornecedor de serviços.

Esta decisão deve ser ponderada tendo em consideração o risco potencial dos dados a migrar e os processos suportados por esta infraestrutura.

9.3. 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.

9.3.1. Qualificação de Fornecedores

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.

9.3.2. Requisitos Mínimos

De qualquer modo, previamente à contratação de serviços de computação em nuvem, o BDA deve verificar e documentar a capacidade do potencial prestador de serviço em assegurar o cumprimento dos seguintes aspectos:

Os pontos de controlo mínimo serão:

- A confidencialidade, integridade, disponibilidade e recuperação de dados e de informações processados ou armazenados pelo prestador de serviço;
- O acesso do BDA 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;
- A disponibilização dos relatórios elaborados por empresa de auditoria especializada e independente, relativos aos procedimentos e aos controlos utilizados na prestação de serviços.

Nota: será valorizado a adesão ao referencial CSA e ao programa STAR onde existe, em sede de registo público, o repositório das certificações e auditorias aplicáveis ao fornecedor de serviços.

9.4. Controlos no Contrato

Na contratação de serviços de computação em nuvem, O BDA deve 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) 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;

c) Idoneidade, disponibilidade, experiência profissional e capacidade financeira, nos termos da legislação vigente do país;

d) Garantir que os requisitos técnicos de segurança que foram identificados no Planeamento constam no contrato;

e) Assegurar que os Centros de dados de suporte garantem a recuperação dos mesmos, em caso de desastre e acesso a backup (cópia de segurança) em situações de anormalidade;

f) Assegurar um Suporte técnico na modalidade 24/7 (vinte e quatro horas por dia e sete dias na semana);

g) Assegurar que constam as 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;

h) Incluir a definição dos SLA (níveis de serviço) a garantir pelo Fornecedor (ex: disponibilidade, capacidade, elasticidade e gestão dos recursos);

i) Permissão de acesso ao BDA às informações e recursos de gestão adequados à monitorização de serviços a serem fornecidos pela empresa contratada;

j) Incluir a descrição do modo de eliminação de dados ou devolução de forma segura;

k) Incluir a definição do processo de transição de serviço. Isto é, a transferência de dados ao novo prestador de serviços ou ao BDA, 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.

Adicionalmente, deverão ser cumpridos os requisitos definidos na gestão de fornecedores, como por exemplo:

l) Comunicação prévia ao BDA sobre eventual subcontratação de serviços a prestar e eventuais limitações que possam afectar a prestação de serviços.

O fornecedor de serviços deverá assumir a sua disponibilidade em cooperar com as entidades e organismos de supervisão relativamente ao BDA.

10. Classificação da Informação

O Gabinete de Segurança de Informação e Cibersegurança deve assegurar a definição da classificação de toda informação de circulação do Banco.

11. Responsabilidades

No âmbito da gestão da segurança de informação e cibersegurança, o órgão máximo do Banco é a Comissão Executiva, a quem compete:

- Garantir que o sistema de gestão da segurança de informação e cibersegurança esteja incorporado em todos os processos do Banco e que os riscos tecnológicos sejam geridos e monitorizados;

- Manter formalmente um Comité de Organização e Tecnologias de Informação e Comunicação, com as responsabilidades, entre outras, de analisar o nível do risco, aprovar e supervisionar um plano de tratamento dos riscos;

- Enquadrar na estrutura o Gabinete de Segurança de Informação e Cibersegurança (GSI), que será o responsável pelo Sistema de Gestão da Segurança da Informação e Cibersegurança (SGSI) do BDA;

- O GSI irá trabalhar em colaboração com outras áreas internas, nomeadamente com a Direcção de Tecnologias de Informação, visando planear, implementar e acompanhar um conjunto de normas específicas, comunicando e sensibilizando toda a Organização para a relevância do tema e para a adopção de práticas seguras.

Todos os responsáveis da instituição devem estar sensíveis aos requisitos de conformidade dos processos e com as normas de segurança da informação do BDA, bem como contribuir, nas suas áreas operacionais, para os controlos técnicos, organizacionais e humanos aplicáveis.

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 endereço de correio electrónico: infosec@bda.ao

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

12. 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, nomeadamente:

a) 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;

b) A comunicação deverá conter a seguinte informação detalhada:

- A empresa a ser contratada;
- O plano de continuidade de negócio;
- Os serviços a serem prestados;
- O local ou país de "hospedagem ou alojamento" da infra-estrutura, sistemas e processamento;
- Tipo de informação a migrar para a nuvem.

Esta informação e estes dados serão agilizados sempre que tecnicamente viável e em linha com os normativos internos do BDA, visando cumprir a finalidade de comunicação.

13. Alterações

Quando se verificar alterações contratuais substantivas, o BDA deverá, 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.

14. Papéis, Responsabilidades e Autoridades

São formalmente fixadas através da tabela seguinte as actividades relacionadas com esta política:

Actividade	POT	GSI	DTI	Outras Unidades
Planeamento	R	A/C	A/C	
Análise do Risco	R	A	C	
Selecção	C/I	A	R/A	I
Contratação (inclusão de controlos)		A	R/A	
Monitorização do contrato	I	R/A	C/I	
Comunicação ao BNA	C/I	A	C	

Legenda: R: responsável | **A**: *accountable* (responsável por executar) | **C**: consultado | **I**: informado

15. Entrada em Vigor e Revisão

A presente Política foi aprovada na 14.ª Secção Extraordinária do Conselho de Administração, realizada à 28 de Dezembro de 2022, e entra em vigor na data da sua publicação.

A presente política deve ser revista anualmente, ou sempre que necessário.