# Política de Segurança Cibernética

**Banco Angolano de Investimentos, S.A.| Sociedade Aberta**
Complexo Garden Towers, Torre BAI Travessa Ho Chi Minh, Maianga, Luanda-Angola
Tel: (+244) 222 693 800/693 899 •C.P.: 6022 •SWIFT: BAIPAOLU
Registo no BNA N.º 40 •Conservatória de Registo Comercial N.º 10/97 •NIF.: 5410000510
Capital Social integralmente realizado: Kz 157 545 000 000
www.bancobai.ao

Índice

Histórico de versões

| Versão | Data | Descrição das alterações | Aprovação |
|---|---|---|---|
| 1.0 | 24 de Julho de 2020 | - | Conselho de Administração (CA) |
| 1.1 | 28, 29 e 30 de Setembro de 2022 | **Informação adicionada e/ou actualizada**<br>Introdução (actualização do texto)<br>Âmbito e Aplicabilidade<br>Enquadramento Regulamentar<br>Objectivo<br>Responsabilidades<br>Princípios para Gestão da Segurança Cibernética (actualização do texto)<br>Incumprimento<br>Aprovação e Entrada em Vigor<br>Divulgação, Revisão e Actualização da Política<br><br>**Informação eliminada**<br>Introdução e Objectivo<br>Melhores Práticas<br>Atribuições e Responsabilidades<br>Gestão da Segurança Cibernética<br>Adopção da Computação em Nuvem<br>Disposições Finais | CA |
| 1.2 | 25, 26 e 27 de Janeiro de 2023 | Revisão efectuada, sem alterações identificadas. | CA |
| 1.3 | 22, 23 e 24 de Novembro de 2023 | Revisão efectuada, sem alterações relevantes identificadas. | CA |

## 1. Introdução

O BAI – Banco Angolano de Investimentos, S.A.| Sociedade Aberta (doravante "BAI" ou "Banco") institui a presente Política que define os princípios aplicáveis a segurança cibernética.

## 2. Âmbito e aplicabilidade

A presente Política é aplicável ao Banco.

## 3. Enquadramento legal e regulamentar

A presente política foi elaborada com base nos seguintes diplomas:

a) Aviso 08/2020 – Política de Segurança Cibernética e Adopção de Computação em nuvem, do Banco Nacional de Angola (BNA);

b) ISO/IEC 27001 – Sistemas de Gestão da Segurança da Informação;

c) ISO/IEC 27035 – Gestão de Incidentes de Segurança de Informação Tecnológica;

d) NIST *Cybersecurity Framework* V1.1;

e) CIS *Controls* V7.1;

f) ISO/IEC 27002:2022 – *Code of Practice for Information Security Controls*.

## 4. Objectivo

A presente Política tem como principais objectivos: (i) garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, empregados e fornecedores do Banco; (ii) proteger adequadamente os sistemas e informações do Banco; (iii) garantir a continuidade dos negócios do Banco, protegendo os processos críticos de interrupções; e (iv) garantir que sejam respeitadas as finalidades aprovadas pelo Banco durante a prestação de serviços de terceiros quando da contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

## 5. Responsabilidades

Sem prejuízo do previsto nos regulamentos, no âmbito das suas atribuições cabe:

a) ao Conselho de Administração (CA): definir e aprovar a presente Política, bem como supervisionar a sua eficácia;

b) à Comissão Executiva (CE): aprovar os normativos e outros instrumentos internos necessários à aplicação da Política.

## 6. Princípios

O Banco possui políticas e procedimentos para assegurar que as informações estejam adequadamente protegidas, baseadas nos requerimentos mínimos exigidos pelo BNA e nas melhores práticas reconhecidas pelo mercado.

### 6.1. Gestão de Activos da Informação

Os activos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, de eventuais adulterações de dados e ter documentação e planos de manutenção actualizados.

### 6.2. Classificação da Informação

a) As informações devem ser classificadas de acordo com a confidencialidade e as protecções necessárias, abrangendo inclusive a criptografia de dados e de acordo com a classificação dos níveis de relevância.

b) Para mais informações, consultar a Norma de Classificação de Informação e a Norma de Controlo de Acessos e Gestão de Utilizadores.

6.3. Gestão de Acessos

a) As concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso. Os acessos devem ser rastreáveis, a fim de garantir a identificação de acesso e transacção.

b) Os níveis de controlos aplicados na gestão de controlo de acessos do Banco variam de acordo com a classificação do activo, incluindo, dentre outros, os seguintes mecanismos de controlo:

i. controlos de autenticação;

ii. criptografia;

iii. controlos de autorização;

iv. segregação de funções; e

v. revisão periódica de acessos.

6.4. Gestão de Riscos Cibernéticos

Os riscos cibernéticos devem ser mapeados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os activos de informação do Banco, por forma a serem endereçadas as protecções adequadas.

6.5. Gestão da Continuidade de Negócios

a) Os controlos adoptados pelo Banco, na gestão de infraestrutura tecnológica, possuem como objectivo primário garantir que o Banco se mantenha operacional frente a ameaças cibernéticas, de modo a assegurar a confidencialidade, integridade e disponibilidade da informação.

b) O gerenciamento de riscos cibernéticos deve garantir a manutenção da continuidade dos negócios, abrangendo serviços relevantes e a capacidade de continuar a entrega de produtos ou serviços em um nível mínimo aceitável e previamente definido, quando da ocorrência de um evento que interrompa as operações do Banco.

c) Os seguintes controlos devem ser adoptados:

i. *Backup* (cópias de segurança) dos dados e das informações;

ii. Elaboração de cenários de incidentes considerados nos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos; e

iii. Os resultados dos testes de continuidade de negócios devem ser informados para elaboração do relatório sobre o plano de acção e de resposta a incidentes.

6.6. Gestão de Segurança das Aplicações e Adopção de Novas Tecnologias

As principais premissas aplicáveis à gestão de segurança das aplicações e adopção de novas tecnologias pelo Banco devem incluir:

a) O desenvolvimento de novas aplicações de serviços relevantes deve estar alinhado com as melhores práticas de segurança cibernética recomendadas por padrões internacionais e pelas políticas do Banco, específicas para desenvolvimento seguro;

b) Na adopção de novas tecnologias também deve ser submetido a controlos de segurança cibernética proporcionais à classificação de criticidade do activo, sendo que estas passam por processos de classificação, avaliação de riscos e implementação de correcções ou adequações antes de serem disponibilizadas no ambiente produtivo;

c) Controlos e mecanismos de rastreabilidade das informações;

d) Testes de segurança, como teste de penetração e teste de código seguro, também devem ser executados para os serviços relevantes antes da implementação no ambiente de produção;

e) Testes de segurança da informação gerais (como, por exemplo, análise de código seguro);

f) Controlos para assegurar a segregação entre os ambientes de desenvolvimento, homologação/teste e produção, com o objectivo de reduzir os riscos de acessos não autorizados ou alterações indevidas no ambiente operacional, banco de dados e/ou aplicações.

6.7. Testes de Segurança Cibernética

A gestão de testes de segurança cibernética do Banco inclui os seguintes mecanismos de controlo:

a) Testes de segurança cibernética para novas aplicações;

b) Testes de segurança cibernética para aplicações existentes;

c) Testes de segurança cibernética para a infraestrutura de rede;

d) Acompanhamento de correcções segurança de falhas identificadas durante os testes; e

e) Execução de novos testes de segurança cibernética para confirmação de que as falhas foram corrigidas.

6.8. Gestão de Incidentes de Segurança de Informação Tecnológica

A gestão e plano de respostas a incidentes cibernéticos para serviços relevantes do Banco, inclusive os ocorridos em sistemas operados ou instalados em empresas contratadas que prestam serviços relevantes, deve ser executado considerando as análises de causa, impacto e efeito dos incidentes, bem como deve incluir, dentre outros, os seguintes controlos:

a) Plano de Acção de Resposta a Incidentes;

b) Medidas preventivas e mitigantes de incidentes relacionados com o ambiente cibernético;

c) Processos e ferramentas utilizados na prevenção e resposta a incidentes;

d) Designação de área responsável pelo registo e controlo dos efeitos de incidentes relevantes;

e) Registo de incidentes, com informações sobre papéis e responsabilidades;

f) Classificação do incidente cibernético;

g) Análise de causa e impacto;

h) Recebimento de informações de fornecedores, relacionadas com incidentes com impacto na prestação de serviços relevantes;

i) Definição de mecanismos para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;

j) Elaboração do relatório anual sobre o plano de acção e de resposta para incidentes;

k) Iniciativas para compartilhamento de informações sobre os incidentes cibernéticos relevantes com outras instituições financeiras autorizadas pelo BNA ocorridos no Banco e/ou comunicados pelos prestadores de serviços relevantes do Banco; e

l) Comunicação tempestiva ao BNA das ocorrências de incidentes cibernéticos relevantes e das interrupções de serviços relevantes.

6.9. Monitoramento de segurança da informação e prevenção contra ciberataques

O processo de monitoramento de segurança da informação e prevenção contra ciberataques do Banco deve ter um conjunto de controlos e correctivos, com o objectivo de evitar a concretização de ameaças cibernéticas, dentre os quais destacam-se:

a) Aplicação de actualizações e correcções de segurança;

b) Monitoramento contra-ataques cibernéticos e prevenção contra invasões;

c) Verificação de conformidade de requisitos de segurança cibernética;

d) Realização periódica de testes e varredura de vulnerabilidades;

e) Monitoramento de status das ferramentas de antivírus e de alertas gerados;

f) Protecção contra softwares maliciosos;

g) Prevenção de fuga de dados.

6.10. Sensibilização sobre Segurança Cibernética

O Banco deve garantir a disseminação dos princípios e directrizes de Segurança Cibernética por meio de programas de sensibilização e capacitação, fortalecendo a cultura de segurança cibernética e informação, em todos os níveis operacionais.

6.11. Adopção da computação em nuvem

a) O Banco, quando da utilização de serviços em nuvem, atenderá aos critérios previstos no Aviso n.º 08/2020, do BNA, considerando 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;

b) Na gestão dos seus fornecedores de serviços em nuvem, o Banco busca principalmente garantir a execução de controlos para prevenção de incidentes a serem adoptados por fornecedores que manuseiam dados sensíveis ou que sejam relevantes para as actividades do Banco. Os referidos controlos devem ser compatíveis com os processos e mecanismos de segurança cibernética adoptados pelo próprio Banco.

## 7. Incumprimento

As excepções à presente Política requerem a aprovação prévia do CA.

## 8. Aprovação e entrada em vigor

A presente Política foi aprovada pelo CA, entrando em vigor a partir da data da sua publicação, podendo ser alterada por deliberação deste órgão.

## 9. Divulgação, revisão e actualização

a) A presente Política encontra-se disponível para consulta no sítio de *Intranet* e *Internet* do Banco;

b) Esta Política deve ser revista anualmente ou sempre que se verifiquem alterações que justifiquem a sua revisão.