Âmbito de distribuição: **Público**

Política de Segurança da Informação

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** Introdução Âmbito e Aplicabilidade Enquadramento Regulamentar Objectivo Responsabilidades Princípios Incumprimento Aprovação e Entrada em Vigor Divulgação, Revisão e Actualização da Política **Informação eliminada** Introdução e Objectivo Princípios Orientadores Gestão da Segurança da Informação Divulgação e Acesso Incumprimento Anexo	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 da informação.

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 do Banco Nacional de Angola – Política de Segurança Cibernética e adopção de computação em nuvem;

b) Instrutivo 10/2020 do Banco Nacional de Angola – Reporte de Incidentes de Segurança Cibernética;

c) Lei nº 7/2017 – Lei de Protecção das redes e dos sistemas Informáticos;

d) Lei 22/11 de 17 de Junho – Lei da Protecção de Dados (Angola);

e) ISO/IEC 27001:2013 – *Information Security Management;*

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

g) Regulamento Geral da Protecção de Dados da União Europeia – Directiva 95/46/CE;

h) CIS *Controls* V8;

i) SWIFT CSP.

4. Objectivo

A presente Política tem como objectivo:

a) Assegurar que o Banco dispõe e promove processos adequados na protecção dos dados e informação nos sistemas de acordo com o previsto na regulamentação acima, que permitam o cumprimento das suas obrigações perante terceiros, incluindo as obrigações de reporte às autoridades de supervisão;

b) Garantir o acompanhamento e a avaliação regular da eficácia dos procedimentos adoptados para a sua implementação e a correcção atempada de eventuais deficiências detectadas.

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

a) Por forma a assegurar que as Normas de Segurança da Informação (NSI) se encontram devidamente alinhadas e suportam, na sua totalidade, os objectivos para a segurança da informação definidos pelo Banco, são estabelecidos os seguintes princípios orientadores, que deverão ser considerados na definição e implementação das demais NSI;

b) No que respeita à protecção da informação e SI associados:

   i. A informação, os sistemas e os serviços utilizados pelos colaboradores são de exclusiva propriedade do Banco BAI, não podendo ser interpretados como de uso pessoal;

ii. Toda a informação do Banco deve ser protegida de riscos e ameaças que possam comprometer a sua confidencialidade, integridade e disponibilidade. Para tal, deve assegurar-se:

- O nível de confidencialidade adequado para a informação, garantindo que a mesma apenas está acessível a quem esteja autorizado. Para mais informações, consultar a Norma de Classificação de Informação e a Política de Controlo de Acessos e Gestão de Utilizadores;
- A integridade da informação, na sua totalidade e exactidão, procurando que a mesma seja mantida quer na forma como foi criada pelo seu autor, quer no conteúdo e que não existem alterações indevidas, intencionais ou acidentais; e
- A disponibilidade da informação sempre que necessária, por quem está autorizado (e de acordo com o perfil de acesso).

iii. Está proibida a divulgação, duplicação, modificação, destruição, uso inadequado, roubo e acesso não autorizado à informação pertencente ao Banco BAI, a clientes e outras entidades que lhe tenham confiado informação;

iv. Toda a informação do Banco BAI, independentemente da forma, deve ser utilizada unicamente para a finalidade para que foi criada e devidamente autorizada;

v. Todo o acesso à informação e aos SI associados deve ser previamente autorizado, efectuado de forma controlada e devidamente monitorizada, respeitando os princípios do privilégio mínimo e necessidade de saber (ver a Norma de Controlo de Acessos e Gestão de Utilizadores); e

vi. O envolvimento e responsabilização de todos os órgãos e Direcções da estrutura do Banco BAI deve ser assegurado relativamente à protecção da informação.

c) No que respeita à gestão da segurança da informação:

i. O Banco BAI deve ter uma organização interna de gestão da segurança da informação e um sistema de gestão de riscos, adequados à dimensão e à complexidade do seu negócio, que garanta uma gestão efectiva da segurança da informação. Nesse sentido, deve seguir uma abordagem que integre:

- O planeamento da segurança da informação, o controlo da implementação, o tratamento de incidentes e o cumprimento sistemático das NSI;
- O alinhamento dos Planos e Processos do Banco BAI com as directrizes das NSI; e
- A monitorização e avaliação da eficácia da aplicação das NSI deverá ser realizada de forma independente, e enquadrada num processo de melhoria contínua.

ii. Os controlos de segurança implementados com vista ao cumprimento dos princípios previstos nas NSI são definidos com base num processo de análise do risco.

d) No que respeita à definição e cumprimento das NSI:

i. O Banco deve seguir as boas práticas de segurança da informação previstas nas normas ISO/IEC 27001:2013 e ISO/IEC 27002:2022, CIS *Controls* e SWIFT CSP devidamente adaptadas ao seu negócio e dimensão;

ii. O Banco deverá cumprir com as regras de formalização do Sistema de Controlo Interno que compreendem todas as políticas desenvolvidas no âmbito da segurança da informação;

iii. O Banco deve comunicar as NSI a todos os colaboradores e entidades que acedem e utilizam a sua informação, por forma a assegurar que estes as conhecem, compreendem e aplicam devidamente; e

iv. As consequências e penalidades provenientes do incumprimento ou violação das NSI devem ser definidas e devidamente comunicadas pelo Banco BAI.

6.1. Gestão da Segurança da Informação

a) A gestão da segurança da informação do Banco BAI assenta numa abordagem de acordo com o modelo PDCA (*plan*, *do*, *check*, *act*) previsto na norma ISO/IEC 27002:2022 e compreende quatro fases:

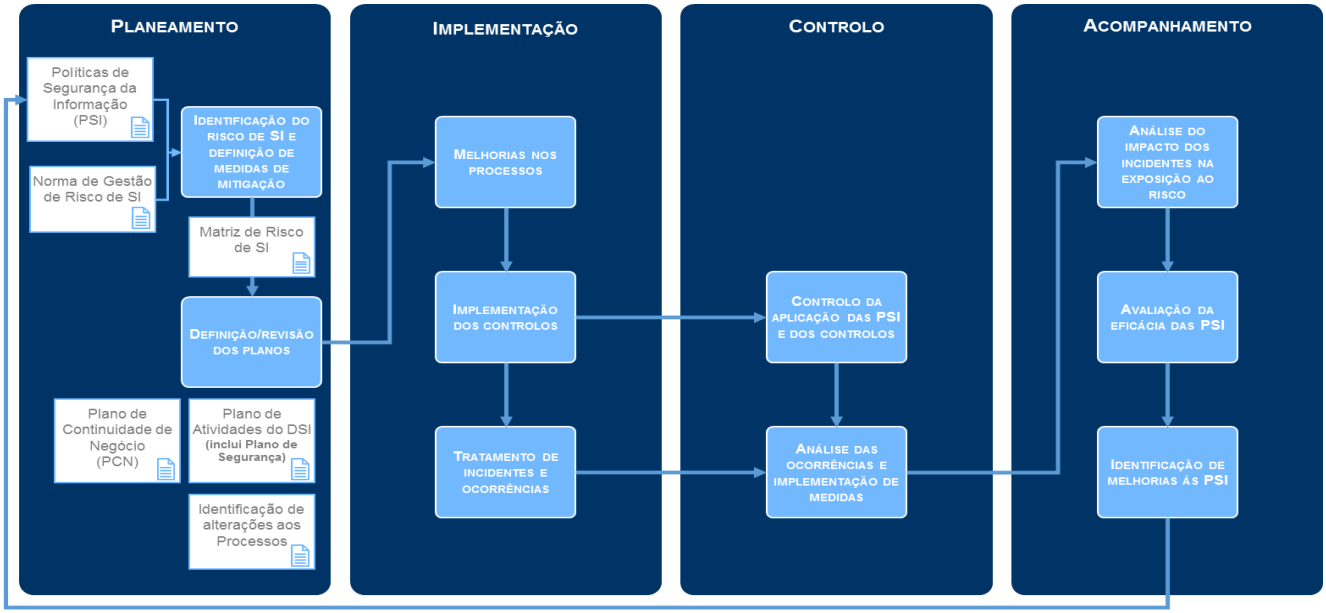
i. Planeamento da segurança da informação – Tem por objectivo identificar periodicamente o risco de SI e planear as medidas de mitigação, de acordo com as orientações da Norma de Gestão de Risco de Sistemas de Informação;

ii. Implementação – Tem por objectivo adequar e aplicar a NSI aos processos do Banco BAI, implementar as medidas de mitigação do risco e tratar os incidentes de segurança da informação;

iii. Controlo – Tem por objectivo assegurar que a política de segurança e que os processos e controlos definidos são aplicados; e

iv. Acompanhamento – Tem por objectivo acompanhar de forma sistemática a adequação e a eficácia das NSI.

b) De seguida, apresenta-se o esquema geral da gestão integrada da segurança da informação:



6.2. Monitorização e Controlo

a) A utilização da informação e dos SI do Banco BAI deve ser monitorizada e registada para detecção de incumprimentos das NSI, normas e procedimentos de segurança da informação e, consoante o caso, servir como evidência em processos administrativos, disciplinares e/ou legais;

b) A análise/avaliação de riscos de segurança da informação pode ser aplicada à totalidade do Banco BAI, partes do Banco BAI, um SI específico, ou apenas componentes de um sistema específico, entre outros;

c) A análise dos riscos deve constituir ferramenta de orientação, nomeadamente:

i. Na identificação dos riscos em função do potencial impacto e probabilidade;

ii. Na identificação de medidas de mitigação dos riscos aos quais a informação está exposta; e

iii. Na priorização de acções para mitigação dos riscos identificados, tais como implementação de novos controlos, regras, procedimentos e reformulação de sistemas, entre outros.

d) A autorização de acesso à informação deve ser determinada com base na necessidade de saber e do privilégio mínimo, associada às funções do colaborador ou entidade, assim como esta deve ser objecto de aprovação e controlo;

e) Os acessos aos SI devem ser definidos segundo uma lógica de segregação de funções (evitando acumulação de funções potencialmente conflituosas), ao nível da utilização, operação, manutenção e outras actividades envolvendo a informação, em conformidade com a Matriz de Acessos em vigor;

f) Em caso de necessidade de acesso por terceiros aos SI do Banco BAI, deve ser analisado o respectivo risco e este deve ser sujeito a aprovação prévia e a controlo;

g) O acesso e utilização da informação deve ser feito com recurso a um identificador único de utilizador, de forma a permitir que este seja controlado e auditado, assegurando a responsabilização inequívoca de cada utilizador pelas suas acções;

h) A concessão e revogação de autorização de acesso aos SI devem ser efectuadas de acordo com os procedimentos de segurança em vigor;

i) Devem ser removidas, imediatamente, autorizações dadas a colaboradores demitidos ou suspensos;

j) As autorizações dos colaboradores que tenham mudado de função devem ser revistas e alteradas em conformidade;

k) As autorizações concedidas bem como as regras de atribuição, manutenção e uso de palavra-passe devem ser revistas, pelo menos, anualmente; e

l) A informação e os SI devem ter a sua exposição, a ameaças naturais e outros riscos físicos relevantes, mitigada por intermédio de controlos de acessos físicos, vigilância dos espaços (e.g. meios humanos ou sistemas de vídeo vigilância), monitorização e controlo de condições climatização, falhas e estabilização de energia, detecção e supressão de incêndios e inundações.

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.