POLÍTICA DE SEGURANÇA CIBERNÉTICA

Uso Interno

Informação sobre o Documento			
Data do documento	3 de Fevereiro de 2023	**Responsável pela política**	DGR
Data de revisão		**Aprovado por**	C.A
Número de páginas	13	**Número da versão**	1.0/2023

Controlo de Versões		
Versão	**Descrição**	**Data**
1.1	Aprovado	3.02 2023

Índice

1. Disposições Iniciais 3
2. Âmbito da Política ..... Erro! Marcador não definido.
3. Objectivos da Política ..... Erro! Marcador não definido.
4. Referências utilizadas ..... Erro! Marcador não definido.
5. Disponibilidade da política 5
6. Revisão da Política 6
7. Aprovação da Política 6
8. Acções pelo Não Cumprimento 6
9. Governação da Política 6
9.1. Estrutura de Governação 6
9.2. Atribuições e Responsabilidades 6
9.2.3. Unidades de Negócio 7
9.2.4. Colaboradores 7
9.2.5. Direcção de Gestão de Risco (DGR) 8
9.2.6. Direcção de Tecnologias de Informação (DTI) 8
9.2.7. Departamento de Segurança da Informação (DSI) 8
9.2.8. Departamento de Compliance (DCO) 9
9.2.9. Gabinete de Organização, Políticas e Procedimentos 9
9.2.10. Direcção de Capital Humano (DCH) 9
10. Gestão da Segurança Cibernética 9
10.1. Gestão de Activos da Informação 9
10.2. Classificação da Informação 10
10.3. Gestão de Acessos 10
10.4. Gestão de Riscos Cibernéticos 10
10.5. Gestão da Continuidade de Negócios 10
10.6. Gestão de Segurança das Aplicações e Adopção de Novas Tecnologias 11
10.7. Testes de Segurança Cibernética 11
10.8. Gestão de Incidentes de Segurança de Informação 11
10.9. Monitoramento de segurança da informação e prevenção contra ciberataques 12
10.10. Sensibilização sobre Segurança Cibernética 13
11. Adopção da Computação em Nuvem 13
12. Disposições Finais 13

1. Disposições Iniciais

Sendo a informação uma das variáveis determinantes na composição da oferta de produtos e serviços destinados aos seus clientes e colaboradores, através da **Política de Segurança Cibernética** o Banco está comprometido em garantir a integridade, confidencialidade e disponibilidade da informação dos seus sistemas de informação, da privacidade dos seus clientes e colaboradores, do cumprimento de requisitos legais vigentes fornecendo de uma maneira eficiente e efectiva a gestão desta informação e do negócio.

A Política de Segurança Cibernética, que é revista anualmente, abrange controlos para assegurar a confidencialidade, integridade e disponibilidade de informações, assim como medidas preventivas e corretivas, voltadas ao controlo do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de pontos de vulnerabilidades. Entre os principais controlos adoptados pelo Banco, destacam-se os seguintes:

- Autenticação;
- Criptografia;
- Prevenção e detecção de invasão;
- Prevenção de fuga de informações;
- Realização periódica de testes e varreduras para detecção de vulnerabilidades;
- Protecção contra softwares maliciosos;
- Estabelecimento de mecanismos de rastreabilidade da informação;
- Controlos de acesso e de segmentação da rede de computadores;
- Manutenção de cópias de segurança dos dados e das informações;
- Desenvolvimento seguro;
- Gestão de incidentes;
- Sensibilização de utilizadores, clientes e fornecedores:
    - Iniciativas de sensibilização da cultura de segurança cibernética, incluindo a implementação de programas de treinamento e de avaliação periódica da sensibilização de colaboradores;
    - Iniciativas de sensibilização sobre segurança cibernética para clientes, empresas terceiras e prestadores de serviços relevantes.

Com efeito, a Política de Segurança Cibernética rege-se pela regulamentação e melhores práticas sobre a matéria bem como pelos normativos vigentes.

Esta política aplica-se a todos os Colaboradores e demais intervenientes nos Sistemas de Informação do Banco.

Conceitos e Definições

Definições:

a) Segurança Cibernética

A Segurança Cibernética é o 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

A Computação em Nuvem é o 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) Infraestrutura Tecnológica Crítica

A Infraestrutura Tecnológica Crítica são 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.

d) Vulnerabilidades

As vulnerabilidades são quaisquer condições que, quando exploradas por um terceiro mal intencionado, possam resultar em violações de segurança cibernética, tais como falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede, desatualização ou ausência de mecanismos de segurança cibernética. Um ataque de exploração de vulnerabilidades ocorre quando um atacante tenta executar acções maliciosas, como por exemplo: invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar uma aplicação ou serviço indisponível.

e) Incidentes cibernéticos

Os incidentes cibernéticos são todo e qualquer evento não esperado que gere algum tipo de instabilidade, quebra de política ou que possa causar danos ao Banco.

f) Ataque cibernético

O ataque cibernético é a exploração por parte de um agente malicioso para tirar proveito de ponto(s) fraco(s) com a intenção de alcançar um impacto negativo no alvo. Os atacantes podem ter como alvo os clientes, fornecedores e parceiros do Banco para causar impacto significante para o Banco.

2. Âmbito da Política

Esta Politica define o âmbito de actuação perante os os potenciais riscos cibernéticos na garantia dos 3 pilares da segurança: confidencialidade, integridade e disponibilidade.

A presente política define igualmente directrizes às Unidades de Estrutura e Colaboradores, assim como os critérios na gestão da Informação e seus activos.

3. Natureza da Instituição Financeira

Sendo o BCA uma instituição bancária, a presente polítiva visa dar cumprimento intermo as disposições do da Lei 22/11 de 17 de Junho – Lei da Protecção de Dados de Angola, relativamente à sensibilidades dos dados e das informações sob sua responsabilidade, bem com os normativos do Banco Nacional de Angola sobre a matéria, em especial o Aviso n.º 8/2020.

4. Objectivos da Política

Os objectivos principais da Política de Segurança Cibernética são os eguintes :

i. Garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, colaboradores 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;
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 núvem;
v. Responder aos pontos identificados no artigo 4º, nº2 alíneas a), b) e c) do Aviso 8/2020 - Política de Segurança Cibernética e Adopção de Computação em Nuvem.

5. Referências utilizadas

- ISO/IEC 27001:2013 - Information Security Management
- ISO/IEC 27002:2022 - Code of Practice for Information Security Controls
- Lei 22/11 de 17 de Junho – Lei da Protecção de Dados de Angola
- Lei 14/21 de 19 de Maio – Lei do Regime Geral das Instituições Financeiras

- Capitulo II, Artº 4 nº2 a), b) e C) do Aviso 08/2020 do Banco Nacional de Angola
- Norma de Gestão de Risco do BCA
- Politica de Segurança da Informação do BCA
- Processo de Gestão de Incidentes de Segurança da Informação do BCA

6. Disponibilidade da política

A Política é aplicável a todo o Banco, com especial relevo para o Conselho de Administração (CA), a Comissão Executiva (CE), a Comité de Controlo Interno e Auditoria (CCIA), a Direcção de Gestão de Risco (DGR), o Gabinete de Auditoria Interna (GAI) e as unidades operacionais do Banco.

7. Revisão da Política

A Política deverá ser revista numa base anual, ou sempre que necessário, de forma a garantir a respectiva actualização face a eventuais alterações legais, e/ou regulamentares, e às evoluções do negócio do Banco. A DGR coordenará a revisão regular da Política conforme recomendação da Comité de Controlo Interno e Auditoria (CCIA).

8. Aprovação da Política

Esta política é aprovada pelo Conselho de Administração, mediante recomendação do Comite de Controlo Interno e Auditoria, devendo a Direcção de Gestão de Risco assegurar e coordenar a sua implementação.

9. Acções pelo Não Cumprimento

Todos os casos de violação da presente política serão devidamente comunicados, nos termos dos processos de gestão e do controlo de riscos.

10. Governação da Política

10.1. Estrutura de Governação

O Modelo de Governo utilizado nesta política assenta na estrutura da organização e na atribuição de Responsabilidades com base nas Funções que cada Unidade de estrutura desempenha no Banco.

10.2. Atribuições e Responsabilidades

Para estabelecer o processo de Gestão da Segurança Cibernética é necessário determinar as atribuições e responsabilidades dos responsáveis e co-responsáveis pelos controlos internos de tecnologia e segurança da informação.

10.2.1. Conselho de Administração (CA): Órgão de administração responsável no âmbito das suas atribuições por assegurar a aprovação das políticas e suas revisões.

10.2.2. Comissão Executiva (CE): Órgão de administração, responsável, no âmbito das suas atribuições, por assegurar que as políticas e procedimentos de governação das TSI – Tecnologias de Segurança de Informação, estão implementadas e alinhadas com a visão e objectivos gerais corporativos do Banco, bem como deliberar sobre decisões relevantes da gestão corrente, nomeadamente, as que tenham impacto na Arquitectura e Segurança das TSI nos termos estabelecidos nos regulamentos do Banco.

10.2.3. Unidades de Negócio

- Cumprir e fazer cumprir a Política e os Procedimentos de Segurança da informação bem como as disposições legais e regulamentares vigentes sobre Segurança da Informação;
- Assegurar que as suas equipas tenham acesso e conhecimento da Política e dos Procedimentos de Segurança da informação;
- Garantir que todos os colaboradores têm acesso à Política e Procedimentos de Segurança da Informação;
- Comunicar imediatamente à DGR eventuais casos de violação de segurança da informação pelos canais indicados nesta política (ver "Incidentes de Segurança de Informação").

10.2.4. Colaboradores

- Cumprir, fielmente, a Política e os Procedimentos de Segurança de Informação em vigor, incluindo o Regulamento Interno do Colaborador, o Código de Conduta, o Guia de Referência Rápida de Segurança da Informação e outros normativos aplicáveis;
- Procurar orientação junto do Superior Hierárquico directo em caso de dúvidas relacionadas com a segurança da informação;
- Assinar o Termo de Confidencialidade da Informação concordando com a Política e os Procedimentos de Segurança de Informação em vigor, bem como assumir responsabilidade pelo seu cumprimento;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo Banco;
- Assegurar que os recursos informáticos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Banco;
- Cumprir as leis e as normas que regulamentam os aspectos de carácter intelectual;
- Comunicar de imediato ao Superior Hierárquico sobre qualquer incumprimento ou violação desta Política e dos Procedimentos definidos.

10.2.5. Direcção de Gestão de Risco (DGR)

- Autorizar o acesso à informação devendo observar o definido na Matriz de Acessos e na Política e Procedimentos de Segurança da Informação;
- Cumprir com o estipulado na Política de Classificação da Informação em vigor no Banco.

10.2.6. Direcção de Tecnologias de Informação (DTI)

- Manter o registo e controlo actualizado de todos os acessos concedidos, determinando, sempre que necessário, a pronta suspensão, alteração ou cancelamento de acessos que não sejam necessários;
- Reavaliar, sempre que necessário, as autorizações de acesso concedidas, cancelando aquelas que não forem necessárias;
- Observar o cumprimento de normas de protecção e processamento de dados, bem como as normas inerentes à destruição de documentos;
- Participar da investigação de incidentes de segurança relacionados com a informação sob sua responsabilidade;
- Realizar testes na implementação de novas tecnologias e sistemas de informação antes de serem implementados e colocados em produção na infra-estrutura informática.

10.2.7. Departamento de Segurança da Informação (DSI)

- Identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações;
- Rever, actualizar e divulgar a Matriz de Acessos;
- Verificar, regularmente, os acessos implementados nos sistemas de informação para garantir a conformidade com as políticas (perfis de acessos) definidas na Matriz de Acessos;
- Avaliar as notificações de incidentes de segurança electrónica e da informação remetidos pelas áreas e colaboradores;
- Acompanhar a investigação de incidentes de segurança relacionados com a informação sob sua responsabilidade;
- Participar, nas reuniões da CE, prestando os esclarecimentos solicitados;
- Identificar e avaliar sistematicamente os riscos relacionados à segurança electrónica e da Informação;
- Solicitar testes e análise de risco na infra-estrutura dos sistemas de informação a fim de certificar que as vulnerabilidades e os riscos dos sistemas de informação são adequadamente resolvidos;

- Efectuar, periodicamente, controlos às Políticas de Segurança da Informação aprovadas para assegurar a sua conformidade.

10.2.8. Gabinete de Compliance (GCO)

- Manter as unidades de estrutura informadas sobre eventuais alterações legais e/ou jurídicas que impliquem responsabilidade e/ou acções envolvendo a gestão de segurança da informação;
- Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objectivo de proteger os interesses do Banco;
- Avaliar, quando solicitada, os Procedimentos de Segurança da Informação em vigor.

10.2.9. Gabinete de Organização, Políticas e Procedimentos

- Documentar e arquivar as versões aprovadas da Política e dos Procedimentos de Segurança da Informação bem como da documentação relacionada.

10.2.10. Direcção de Capital Humano (DCH)

- Dar a conhecer aos novos colaboradores a Política de Segurança da Informação e obter a assinatura do Termo de Confidencialidade da Informação;
- Informar prontamente, à DTI a admissão e demissão de colaboradores para que possam ser cadastrados ou excluídos do quadro funcional do Banco;
- Disponibilizar mensalmente, a lista de colaboradores suspensos, admitidos e demitidos, incluindo estagiários e transferências de áreas, para que a DTI possa estar informada e proceder à devida actualização no sistema de acesso;
- Adoptar medidas disciplinares necessárias em caso de incumprimento do estabelecido na presente política e normativos relacionados aplicáveis.

11. Gestão da Segurança Cibernética

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

11.1. 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 atualizados.

11.2. Classificação da Informação

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

- Confidencial;
- Restrita;
- Uso Interno; e
- Pública.

11.3. Gestão de Acessos

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

- Controlos de autenticação;
- Criptografia;
- Controlos de autorização;
- Segregação de funções; e
- Revisão periódica de acessos.

11.4. 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, para que sejam endereçadas as proteções adequadas.

11.5. Gestão da Continuidade de Negócios

Os controlos adoptados pelo Banco, na gestão de infraestrutura tecnológica, possuem como objetivo primário garantir que o Banco se mantenha operacional face a ameaças cibernéticas, de modo a assegurar a confidencialidade, integridade e disponibilidade da informação.
A gestão 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 a um nível mínimo aceitável e previamente definido, aquando da ocorrência de um evento que interrompa as operações do Banco.
Os seguintes controlos devem ser adotados:

- Backup (cópias de segurança) dos dados e das informações;

- Elaboração de cenários de incidentes considerados nos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos; e
- Os resultados dos testes de continuidade de negócios devem ser registados e compilados para a elaboração do relatório sobre o plano de ação e de resposta a incidentes.

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

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

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

- A adopção de novas tecnologias também deve ser submetida 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 correções ou adequações antes de serem disponibilizadas no ambiente produtivo;
- Controlos e mecanismos de rastreabilidade das informações;
- Testes de segurança, como testes de penetração e testes de código seguro, também devem ser executados para os serviços relevantes antes da implementação no ambiente de produção;
- Testes de segurança da informação gerais (como, por exemplo, análise de código seguro);
- Controlos para assegurar a segregação entre os ambientes de desenvolvimento, homologação/teste e produção, com o objetivo de reduzir os riscos de acessos não autorizados ou alterações indevidas no ambiente operacional, banco de dados e/ou aplicações.

11.7. Testes de Segurança Cibernética

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

- Testes de segurança cibernética para novas aplicações;
- Testes de segurança cibernética para aplicações existentes;
- Testes de segurança cibernética para a infraestrutura de rede;
- Acompanhamento de correções de segurança de falhas identificadas durantes os testes; e
- Execução de novos testes de segurança cibernética para confirmação de que as falhas foram corrigidas.

11.8. Gestão de Incidentes de Segurança de Informação

A gestão e plano de resposta 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:

- Plano de Ações de Resposta a Incidentes;
- Medidas preventivas e mitigantes de incidentes relacionados com o ambiente cibernético;
- Processos e ferramentas utilizados na prevenção e resposta a incidentes;
- Designação de área responsável pelo registo e controlo dos efeitos de incidentes relevantes;
- Registo de incidentes, com informações sobre papéis e responsabilidades;
- Classificação do incidente cibernético;
- Análise de causa e impacto;
- Recebimento de informações de fornecedores, relacionadas com incidentes com impacto na prestação de serviços relevantes;
- Definição de mecanismos para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
- Elaboração do relatório anual sobre o plano de ação e de resposta para incidentes;
- Iniciativas para compartilhamento de informações sobre os incidentes cibernéticos relevantes com outras instituições financeiras autorizadas pelo Banco Nacional de Angola ocorridos no BCA e/ou comunicados pelos prestadores de serviços relevantes; e
- Comunicação tempestiva ao Banco Nacional de Angola das ocorrências de incidentes cibernéticos relevantes e das interrupções de serviços relevantes.

11.9. Monitoramento de segurança da informação e prevenção contra ciberataques

O processo de monitoramento de segurança da informação e prevenção contra ciberataques do Banco consistem num conjunto de controlos e medidas correctivas, com o objetivo de evitar a concretização de ameaças cibernéticas, as quais se destacam:

- Aplicação de atualizações e correções de segurança;
- Monitoramento contra ataques cibernéticos e prevenção contra invasões;
- Verificação de conformidade de requisitos de segurança cibernética;
- Realização periódica de testes e varredura de vulnerabilidades;
- Monitoramento de status das ferramentas de anti-vírus e de alertas gerados;
- Protecção contra softwares maliciosos;
- Prevenção de fuga de dados.

11.10. Sensibilização sobre Segurança Cibernética

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

12. Adopção da Computação em Nuvem

O Banco, em caso de utilização de serviços em nuvem, atenderá aos critérios previstos no Aviso 08/2020 do Banco Nacional de Angola, 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.

Na gestão de seus fornecedores de serviços em nuvem, o Banco procura 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 atividades do Banco. Os referidos controlos devem ser compatíveis com os processos e mecanismos de segurança cibernética adoptados pelo próprio Banco.

13. Disposições Finais

1. O incumprimento das disposições definidas na presente política é passível de aplicação de medidas disciplinares. A aplicação de medidas disciplinares não exclui a aplicação, pelas autoridades competentes, de outras sanções legais.
2. O DSI – Departamento de Segurança da Informação e o Gabinete de Auditoria Interna (GAI) devem monitorar o nível de observância das disposições definidas nesta norma devendo, sempre que necessário, efectuar as recomendações que julgarem pertinentes e comunicar os casos de incumprimento à Direcção de Capital Humano (DCH).
3. O DSI deve acompanhar e arquivar os processos disciplinares instaurados ao abrigo do disposto no número anterior.