

## A POLITICA DE SEGURANÇA CIBERNÉTICA DO BANCO VTB-AFRICA, S.A.

### 1. INTRODUÇÃO.

A Política de Segurança Cibernética é um documento interno orientador sobre as responsabilidades do Banco VTB Africa (Banco) para efeitos de cumprimento dos requisitos do Aviso n.º 08/2020, de 02 de Abril e Instrutivo n.º 10/2020, de 29 de Maio.

1.1. **A dimensão, o perfil de risco e o modelo de negócio do Banco** no actual contexto, do sistema financeiro angolano, se insere no grupo dos bancos de media dimensão e, em termos de tomada de riscos, o Banco segue um padrão conservador, porém, um dos principais objectivos passa pela necessidade de proceder a monitorização dos riscos de forma a obter indicadores que permitam detectar e quantificar o impacto dos riscos relevantes.

O Modelo de Negócio do Banco assenta na oferta de produtos e serviços aos clientes corporativos.

1.2. **A natureza das operações e a complexidade dos produtos, serviços, actividades, processos da Instituição.**

O Banco tem, no seu portfólio, operações com as seguintes naturezas:

I. Operações próprias do Sector Bancário – tais como depósitos, créditos, transferências, pagamentos;

II. Operações do sector de Mercado de Capitais – tais como compra, venda e custódia de títulos da dívida publica.

Os produtos, serviços, actividades e processos do Banco não se revelam complexos.

1.3. **A sensibilidade dos dados e das informações sob responsabilidade do Banco.**

Os dados sob tutela do Banco, em tudo quanto se referir a dados pessoais, dados patrimoniais, informação financeira e histórico transaccional de clientes são considerados de sensibilidade crítica e sujeito as medidas de segurança previstas na presente política bem como na Regulamentação e Legislação aplicável ao Sector.

2. **ÂMBITO** A presente política aplica-se a todas áreas do Banco, com principal enfoque à Área de IT, tendo todos os colaboradores do Banco a responsabilidade de serem diligentes no cumprimento das directrizes definidas pela presente. Em cumprimento do artigo 7º do Aviso 08/2020, o Banco tem, na sua organização interna, uma estrutura/equipa dentro de área de IT, dedicada à política de segurança cibernética, sendo esta área responsável pela política de segurança cibernética e pela execução do plano de acção e de resposta a incidentes.

3. **PRINCÍPIOS.** A Segurança da Informação e Cibernética é baseada nos seguintes princípios:

**Confidencialidade** - Somente o Usuário da Informação, que esteja devidamente autorizado pelo Gestor da Informação, deve ter acesso às Informações respeitando os critérios de segregação de funções pré-definidos;

**Integridade** - Garantir que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo Gestor da Informação;

**Disponibilidade** - Deve garantir que as Informações estejam sempre disponíveis para o Usuário da Informação;

**Autenticidade** - Garante a identidade de quem está enviando a Informação, ou seja, gera o não-repúdio que se dá quando há garantia de que o emissor não pode se esquivar da autoria da mensagem.

#### **4. DIRECTRIZES GERAIS E CONTROLOS ADOPTADOS PARA GARANTIR OS OBJETIVOS DE SEGURANÇA CIBERNÉTICA.**

É de extrema importância a disseminação da cultura de segurança cibernética para garantir a integridade, confiabilidade e disponibilidade das informações. Para garantir o cumprimento dos princípios dispostos acima, o Banco utiliza diversos meios como as políticas internas, instruções normativas, comunicados e a realização de treinamentos periódicos, de segurança da informação, centradas no seguinte:

i. **Autenticação** – o Banco adota os seguintes meios: login e senha, certificados e biometria, token. A escolha do procedimento de validação observa a especificidade do acesso e o grau de confidencialidade da informação.

ii. **Autorização** – deve ser garantida que todos tenham apenas acesso a informação que estejam autorizados. Por outro lado, o acesso as áreas de Backup, servidores e bastidores, deve ser protegido contra acesso não autorizado de colaboradores.

iii. **Criptografia** – utilizada para a protecção de informações que circulam no ambiente digital, devendo seguir os requisitos descritos nos documentos do BNA e padrões internacionais.

iv. **Prevenção e a detecção de intrusão** – o Banco detecta as tentativas de intrusão através do monitoramento do tráfego de rede, verificação de ataques de negação de serviço, varredura de portas ou quaisquer outras evidências

v. **A prevenção de fuga de informações** - seguindo as directrizes estabelecidas na Política de Segurança de Informação, a Equipa de Segurança Cibernética (area de IT) acompanha e monitoriza o fluxo de informação, por meio de ferramenta de protecção de dados em movimento, repouso ou memória, garantindo a rastreabilidade;

vi. **A realização periódica de testes para detecção de vulnerabilidades** – no intuito de identificar vulnerabilidades, riscos, falhas e incidentes seguindo os procedimentos, regras, comunicações e periodicidades descritas no Plano de Acção e Resposta à Incidentes de Segurança Cibernética e nos demais documentos internos orientadores;

vii. **A protecção contra softwares maliciosos** - Protecção contra Softwares Maliciosos deve ser garantida, utilizando software para definição de ameaças, periodicidade de avaliações e varreduras, bem como o registro, comunicação e tratamento de incidentes relevantes.

viii. **O controlo de acesso e de segmentação da rede de computadores** - pelo menos divididos entre homologação, pré-produção e produção, com firewall de acesso e diferenciação de VLANs para cada ambiente, seguindo as melhores práticas e o conceito de dados seguros. Além disso, o acesso de cada ambiente deve ser restrito às necessidades de suas utilizações e contratos preestabelecidos;

ix. **A manutenção de cópias de segurança dos dados e das informações** - com realização de backups automáticos e pré-programados, respeitando o grau de classificação da informação, realizados em conformidade com as leis e normas vigentes, incluindo descarte e restore;

2  
Ubaldo  
H →

x. **A prestação de informações a clientes e utentes sobre precauções na utilização de produtos e serviços financeiros:** O Banco na comercialização dos produtos e serviços, dedica numa secção própria das condições de adesão/utilização recomendações de segurança.

xi. **O comprometimento do órgão da administração** com a melhoria contínua dos procedimentos relacionados com a política de segurança cibernética: as directrizes sobre segurança cibernética, são ratificadas pela Administração do Banco, incluindo, detalhes sobre o orçamento anual, para efeitos de melhorar o sistema de ciber segurança do Banco.

xii. **Arquitectura de Segurança da Informação:** estabelecendo mecanismos de protecção contra a exploração de falhas sistémicas e vulnerabilidades, garantindo a segurança corporativa e conformidade às legislações e regulamentações aplicáveis, mediante o mapeamento de topologia e comunicações, o mapeamento de serviços e testes de segurança;

xiii. **Desenvolvimento Seguro de Software** – caso o Banco opte por desenvolver qualquer software, devem ser aplicadas práticas e técnicas para tornar as aplicações desenvolvidas internamente pela instituição livres de vulnerabilidade se dividindo em:

- Gerenciamento do Controle de Acessos;
- Autenticação e Gestão de Credenciais;
- Gestão de Sessão; e
- Validação das Informações: Código de entrada, criptografia e segurança em comunicações, protecção de dados, codificação dos dados de saída, configuração de sistema, banco de Dados, tratamento de Erros e Logs.

xiv. **Novas tecnologias** - devem ser testadas e validadas mediante eficiência de ferramenta e convergência com as estratégias de negócio e da infraestrutura da instituição, a fim de mitigar as ameaças nos ambientes cibernéticos.

xv. **Software Licenciados** – Os Software usados no banco deve estar licenciados.

## 5. CONTROLES ADOPTADOS PARA A SEGURANÇA DAS INFORMAÇÕES SENSÍVEIS

O Banco possui diversos controles e procedimentos para garantir a segurança das informações sensíveis, conforme descrito nos tópicos abaixo:

5.1. **Controlo de Acesso, Gerenciamento e Autorização.** A prática de Controle de Acesso e Gerenciamento tem o objectivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo assim a confidencialidade das informações. O Banco segue as boas práticas no sentido de orientar que todos os usuários devem possuir acesso à informação de acordo com as necessidades de negócio. O Banco elenca a descrição dos fluxos operacionais para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso.

Adicionalmente, os procedimentos de Concessão e Alteração de acessos a informação sensível, devem ser aprovados/autorizados pelo Administrador do Pelouro após solicitação do responsável da area. O Banco realiza periodicamente a revisão de acessos, conforme política, que tem como objectivo a actualização dos acessos e permissões, procedimento este, que é coordenado pela Equipa de Segurança da Informação (área de IT).

5.2. **Gerenciamento de Riscos e Tecnologia da Informação.** O Banco verifica periodicamente o controle de acessos à internet e controla os aplicativos instalados nos computadores. Nenhum usuário possui acesso de administrador local, impossibilitando a instalação de qualquer aplicativo, que somente podem ser

ulhal  <sup>2</sup>  
H. J. >

instalados aplicativos previamente testados e autorizados, bem como obedecerem a todos os critérios legais e regulamentares. O Banco realiza o monitoramento da rede por meio de software específico.

5.3. **Segurança de Rede.** A segurança é realizada através da monitorização da infraestrutura, sendo que todo acesso às redes internas e acessos à internet são controlados por Tecnologia e softwares adequados as melhores praticas do mercado.

5.4. **Segurança e gerenciamento de Activos de Sistemas.** Quando disponível, o acesso aos sistemas de informação do Banco é integrado com o AD (Active Directory). Para os Sistemas de Informação que não estão integrados com AD, existe um pré-requisito mínimo para as parametrizações de senhas definido em política própria. Referente ao gerenciamento das parametrizações de segurança, somente a área de Segurança da Informação tem acesso para alterar as configurações de acesso e segurança nos Sistemas de Informação.

5.5. **Gestão de Ameaças e Vulnerabilidades de T.I.** O ambiente possui instalado software de antivírus para a protecção contra vírus, arquivos e softwares maliciosos, actualizados periodicamente (antivírus). Todas as actualizações de segurança do Windows são gerenciadas e actualizadas frequentemente.

5.6. **Dispositivos e Controles de DVD e USB.** Somente pessoas previamente autorizadas pela Comissão Executiva tem acesso aos dispositivos móveis e acessos ao leitor de DVD e USB do computador.

5.7. **Segurança Física.** Os recursos e instalações de processamento de informações críticas para as actividades do Banco são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos para controle de acesso. Os equipamentos críticos possuem protecção contra desastre físico e recursos para combate a incêndio. O Banco possui sistema para controle do acesso dos colaboradores, prestadores de serviços ou fornecedores aos locais restritos, que são monitorados por câmaras de vigilância, permitindo identificar quem teve acesso aos espaços.

## **6. REGISTO, ANÁLISE DA CAUSA E DO IMPACTO, BEM COMO, O CONTROLO DOS EFEITOS DE INCIDENTES PARA AS ACTIVIDADES DO BANCO.**

O registo, a análise da causa e do impacto dos incidentes são actividades cruciais para minimizar impactos negativos para o Banco VTB África, a nível operacional e reputacional. Os eventos de TI e Segurança cibernética são registados em software próprios. Sempre que ocorra um incidente cibernético, para além do seu registo o Banco, analisa as causas do mesmo, no sentido de minimizar a possibilidade de novas ocorrências por essas mesmas causas. É feita também a análise sobre os impactos presente e futuros de todos os incidentes cibernéticos que ocorram, sendo esta análise levada a conhecimento (por escrito) da Comissão Executiva do Banco.

O Banco se preocupa com as empresas que prestam serviços para o mesmo. As informações recebidas por estas empresas são objecto de NDA (Non Disclosure Agreement), contempladas em registo específico e objecto de análise complementar no que se refere a impactos dos efeitos de incidentes e vulnerabilidades. O Banco entende que é de extrema importância a existência de um procedimento que possibilita a detecção tempestiva e a pronta comunicação de incidentes e vulnerabilidades, assegurando assim, a eficácia das medidas a serem tomadas na sequência. O Banco possui os controlos que permitem detectar e identificar os incidentes e vulnerabilidades que afectam o ambiente de Segurança Cibernética, bem como, permitam controlar e minimizar os efeitos desses mesmos incidentes.

## **7.DIRETRIZES ESPECÍFICAS.**



7.1. **Teste de Continuidade de Negócios.** O Banco assume o compromisso de manter a continuidade dos negócios em caso de incidentes que possam comprometer o funcionamento normal de suas actividades, através do Plano de Gestão de Continuidade de Negócios (PGCN), sendo constantemente revisado com o objectivo contínuo de melhoria. O programa possui o objectivo de identificar e elaborar os cenários que possam comprometer a continuidade da sua actividade, analisar o seu impacto e promover a resiliência organizacional, dotando a organização da capacidade de prevenir ou, na sua impossibilidade, responder de forma eficaz a estes eventos.

O PGCN é constituído por quatro (04) fases:

- 1ª – Planeamento;
- 2ª - Operação;
- 3ª – Avaliação e Revisão;
- 4ª - Melhoria contínua.

Estas fases contemplam todas as responsabilidades dos órgãos responsáveis pela coordenação do plano, as responsabilidades das áreas envolvidas, os procedimentos para a realização da avaliação/revisão do programa, como testes e relatórios de reporte.

7.2. **Prestadores de Serviços de Tecnologia.** Os procedimentos e controlos voltados à prevenção e ao tratamento de incidentes em relação aos prestadores de serviço de Tecnologia são, previamente, definidos em contratos, especificamente, em relação aos fornecedores de Infraestrutura e software. O Banco recebe mensalmente relatórios com os incidentes ocorridos e, em caso de necessidade, é elaborado um plano de acção, que é acompanhado pela área de Tecnologia até o seu encerramento.

7.3. **Classificação da criticidade dos Incidentes.** Os incidentes relacionados à Segurança Cibernética podem seguir os factores de criticidade: i. Significativos; ou ii. Muito significativos

Para efeitos da classificação conforme acima referido, o Banco usa os dados e informações recolhidas no âmbito da avaliação de risco cibernético, que engloba, também, o impacto derivado dos mesmos, sendo que os parâmetros identificados (significativos e muito significativos) devem estar alinhados entre a área de tecnologias de informação e de negócio, visando essencialmente evitar danos económicos e financeiros, sociais e reputacionais decorrentes destes incidentes.

7.3.1. **Plano de Acção de Resposta a Incidentes.** A elaboração e acompanhamento do plano de acção são coordenados pela Equipa de Segurança Cibernética (Área de IT), com participação de outras áreas do Banco sempre que necessário. O plano de Acção deve englobar:

- a) Adequação das estruturas organizacionais e operacionais;
- b) Rotinas, procedimentos, controlos e tecnologias a serem utilizadas na prevenção e resposta a incidentes, em conformidade com as directrizes da política de segurança cibernética;
- c) Acções a serem desenvolvidas pelas Instituições para adequar às estruturas, organizacional e operacional, aos princípios e às directrizes da política de segurança cibernética;
- d) Indicação da área responsável pelo registo, monitoramento e controlo de incidentes relevantes;
- e) Manual de procedimentos de política de segurança cibernética, aprovado pelo órgão da administração ou gerência, que deve ser revisto anualmente ou sempre que ocorram alterações relevantes na Instituição.

7.3.2. **Classificação da Informação.** O Banco classifica a informação da seguinte maneira:

- a) Informação Muito Confidencial;
- b) Informação Confidencial;
- c) Informação Reservada;

E



- d) Informação Interna;
- e) Informação Pública.

Os detalhes sobre a que se refere cada um dos tipos de informação encontra-se vertido no documento interno.

## **8. OS MECANISMOS PARA DISSEMINAÇÃO, CAPACITAÇÃO E AVALIAÇÃO PERIÓDICA DE PESSOAL PARA A ELEVAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA NA INSTITUIÇÃO.**

A Cultura de Segurança Cibernética é disseminada internamente através de programas de capacitação ministrados, periodicamente, para todos os colaboradores, garantindo, assim, que todos estejam cientes das possíveis ameaças e vulnerabilidades que ocorrerem no âmbito da Segurança Cibernética, bem como, quais são os procedimentos que devem ser adoptados em casos de incidentes, sendo obrigatória uma Avaliação dos colaboradores para aferir o seu conhecimento em relação a segurança cibernética. O Banco tem consciência que as actividades no âmbito de Segurança Cibernética, estão em constante evolução, sendo assim, os procedimentos e controles relacionados com o tema, devem ser revistos com periodicidade adequada, promovendo uma melhoria contínua do ambiente de Segurança Cibernética do Banco.

## **9.COMUNICAÇÕES DE INCIDENTES.**

**9.1. Comunicação de Incidentes ao BNA.** O Banco comunica ao Banco Nacional de Angola, as violações das redes e dos sistemas de informação ou perdas de integridade com impacto significativo no funcionamento das referidas redes e serviços. A comunicação acima referida acontece de acordo com os normativos vigentes do BNA.

**9.2. Comunicação de Incidentes ou ataques contra o Banco.** A todos colaboradores do Banco que tomem conhecimento de algum incidente de segurança cibernética a ocorrer ou em preparação devem comunicar de imediato ao banco (equipa de segurança cibernética, area de IT).

## **10.CONTRATAÇÃO DE SERVIÇOS E DE COMPUTAÇÃO DE NUVEM.**

Para efeitos de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o Banco procede conforme estabelecido no Aviso n.º 08/2020, adoptando as seguintes directrizes:

I. - Adequação de políticas, estratégias e estruturas para gestão de riscos inerentes à terceirização dos referidos serviços.

II. - Na avaliação da relevância do serviço a ser disponibilizado na nuvem, o Banco deve considerar 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.

III. - O Banco deve garantir a capacitação dos seus recursos humanos para a correcta gestão dos serviços implementados, visando assegurar a autonomia interna para o acesso e utilização da tecnologia de nuvem.

IV. - Sempre que se verificar a impossibilidade de manutenção do contrato de prestação de serviços, o Banco deve garantir a gestão de continuidade dos serviços contratados em nuvem.

**10.1. Comunicação da Adopção da Computação em Nuvem.** 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, a qual deve conter a seguinte informação detalhada:



- a) A empresa a ser contratada
- b) O plano de continuidade de negócio;
- c) Os serviços a serem prestados;
- d) O local ou país de “hospedagem ou alojamento” da infraestrutura, sistemas e processamento;
- e) Tipo de informação a migrar para a nuvem;
- f) Indicação da lei que rege o contrato que se pretende celebrar;
- g) Demonstração de competências e recursos necessários para manter e monitorizar o serviço que pretende contratar; e
- h) Disponibilidade do prestador de serviços de computação em nuvem de cooperar com as autoridades nacionais que supervisionam o banco.

Sempre que se verificar alterações contratuais aos serviços de computação na nuvem contratados, o banco deve, 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, quando comprometam o pleno funcionamento das Instituições, devendo o Banco ainda, criar condições que assegurem a continuidade de negócio.

#### **11. RELATÓRIOS.**

A Equipa Responsável pela Segurança Cibernética (Área de IT) elabora 1 relatório semestral (até 15 de Agosto) e outro anual (até 28 de Fevereiro) sobre a implementação do plano de acção de respostas a incidentes, com data base de 31 de Dezembro do ano anterior ao relatório, contendo:

- A efectividade da implementação das acções a serem desenvolvidas pela instituição para adequar suas estruturas aos princípios e às directrizes da política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes ocorridos no período;
- Resultado dos testes de continuidade de negócios.

#### **12. CONTROLO INTERNO.**

Os procedimentos e a Política de Segurança Cibernética estão sujeitos à avaliação das áreas de controlo interno do Banco.

#### **13. ENTRADA EM VIGOR, REVISÃO E ACTUALIZAÇÃO DA POLÍTICA.**

A presente Política entra em vigor depois de aprovada e divulga a todos os colaboradores e deve ser revista sempre que se verifiquem alterações que justifiquem a sua revisão, a nível da Legislação, Regulamentação e Regras Internacionais.