BancoBNI
Banco de Negócios Internacional

POLÍTICA DE SEGURANÇA CIBERNÉTICA PARA CLIENTES

www.bni.ao

ÍNDICE

1. Âmbito

No cumprimento dos normativos legais, regulamentares e das recomendações das entidades internacionais relevantes sobre a necessidade de se estabelecerem regras sobre a componente da Segurança Cibernética, termos e condições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas Instituições Financeiras sob supervisão do Banco Nacional de Angola (BNA), bem como nas boas práticas do mercado para a Gestão da Segurança da Informação, nomeadamente a norma ISO/IEC 27001 sobre a implementação de um Sistema de Gestão de Segurança da Informação, o BNI implementou um conjunto adequado de requisitos, dos quais políticas, processos, procedimentos, estruturas organizacionais e tecnologias, de forma a assegurar a confidencialidade, integridade e a disponibilidade das redes, dados e dos sistemas de informação.

2. Objectivo

A presente Política de Segurança Cibernética para os clientes do Banco tem como objectivo a prevenção, detecção e redução de vulnerabilidades e impactos gerados pelos incidentes relacionados ao ambiente cibernético que afectem a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação utilizados pelo Banco, de forma a:

a) Contribuir para a manutenção da confiança de clientes, colaboradores, accionistas, parceiros, *stakeholders* e entidades reguladoras, na capacidade do Banco em proteger os activos sob a sua responsabilidade contra ameaças acidentais ou intencionais que ocorram internamente ou externamente e que possam comprometer a sua confidencialidade, integridade e disponibilidade.

b) Cumprir com as obrigações legais, regulamentares e contratuais aplicáveis ao Banco.

c) Possibilitar a capacidade de detecção atempada de eventos que possam representar indícios de acções que visem o comprometimento dos activos do Banco.

d) Disponibilizar a capacidade de resposta eficaz e eficiente, em caso de ocorrência de incidentes de segurança da informação.

e) Operacionalizar a estratégia de segurança cibernética e da informação, considerando os desafios actuais e futuros a que o Banco tem de dar resposta, em função da evolução tecnológica.

3. Conceitos e definições

Os conceitos de seguida elencados devem prevalecer ao longo do texto desta política, com a definição que lhes é formulada:

f) Activos de informação: toda a informação com valor para a Organização, incluindo tecnologias de informação, instalações e pessoas que transmitam, armazenam e processam essa informação, independentemente do seu formato.

g) Ciclo de vida da informação: etapas relevantes da existência da informação, desde a criação, utilização, transporte até a destruição.

h) Computação em nuvem: modelo que permite o acesso e o fornecimento de forma conveniente e directa a um conjunto de recursos computacionais configuráveis e de armazenamento de dados que possam ser rapidamente aprovisionados e acessíveis com o mínimo esforço de gestão ou interacção entre os prestadores de serviços.

i) Confidencialidade: atributo de segurança da informação que assegura a acessibilidade da informação apenas para entidades autorizadas.

j) Disponibilidade: atributo de segurança da informação que assegura a disponibilidade atempada da informação sempre que solicitada por entidades autorizadas.

k) Formato da Informação: existência da informação em formato estruturado (em estruturas de dados, como base de dados) ou não estruturada (texto, conhecimento, voz), em formato electrónico (e.g. documento electrónico, aplicação) ou físico (e.g. impressa, manuscrita).

l) Incidente de Segurança da Informação: qualquer ocorrência que afecte ou venha a afectar a confidencialidade, integridade e/ou disponibilidade da informação ou das tecnologias de informação, com prejuízo financeiro, reputacional ou operacional para o Banco, incluindo qualquer acção ou omissão, deliberada ou não, que viole a regulação de segurança e privacidade da informação.

m) Infraestrutura tecnológica crítica: sistemas e activos de informação, sejam físicos, virtuais ou vitais para o bom funcionamento das Instituições Financeiras, cuja incapacidade ou destruição acarreta um elevado impacto na operacionalidade das Instituições.

n) Informação: entende-se por informação, todo e qualquer dado de qualquer natureza incluindo relactivos às actividades do Banco e de terceiros com quem se relacione, ou que a organização coloque à disposição dos seus colaboradores e de entidades externas, e que estes possam vir a ter conhecimento ou acesso no exercício das suas funções.

o) Integridade: atributo de segurança da informação, que assegura que a informação é alterada ou suprimida de forma autorizada.

p) Segregação de Funções: separação efectiva entre actividades incompatíveis ou conflituantes entre si (e.g. autorização e execução), com o intuíto de assegurar que nenhum colaborador tem controlo exclusivo sobre um Activo ou processo associado.

q) Segurança Cibernética: 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.

r) Tecnologias de Informação: qualquer combinação de dispositivos, equipamentos de rede, plataformas, processos, aplicações, interativos ou não, total ou parcialmente automatizados, que utilizem, armazenem, transportem ou transformem informação.

4. Aplicabilidade

1. Nos termos e para os efeitos decorrentes da presente Política, designadamente no que respeita aos poderes e responsabilidades que nela estão previstos, considera-se que o *Chief information security officer* ("CISO") é o responsável pela Seguraça da Infomação.

2. Esta Política estabelece o enquadramento das áreas de segurança da informação e *cibersegurança* do Banco e aplica-se a:

   a) Activos publicados externamente que se encontrem sob a responsabilidade do Banco ao longo das diferentes etapas do seu ciclo de vida;

   b) Clientes;

   c) Fornecedores, *stakeholders*, parceiros, organismos privados e/ou públicos, com quem o Banco estabele uma relação de cooperação e potencializa a troca de informação.

3. Apresente política estabelece as linhas orientadoras por forma a garantir a utilização de mecanismos, metodologias, processos e procedimentos de resposta a incidentes de

segurança, que permitam gerir, controlar, monitorizar e reportar incidentes de segurança sob diferentes vectores de actuação originados externamente ao Banco.

5. Implementação da Política

5.1 Modelo de gestão

1. A missão, a visão, os valores e a política do Banco, bem como o bem-estar, a segurança das pessoas, da Informação, dos activos e das instalações são factores chave para o sucesso do Negócio.
2. O Banco está consciente de que a Informação sensível dos seus clientes e do negócio, deve ser tratada de forma a assegurar a credibilidade junto dos clientes e dos colaboradores, devendo:
   a) Manter o comprometimento com a Segurança da Informação.
   b) Garantir e reforçar a conformidade com a regulamentação e exigências legais em vigor.
   c) Assegurar a integridade, a confidencialidade e a disponibilidade da Informação.
   d) Estabelecer um padrão de qualidade consistente com a dimensão e importância da organização.
   e) Manter o conhecimento e recursos adequados a garantir capacidade em responder e mitigar incidentes de segurança.

5.2 Principio gerais da Segurança e *Cibersegurança*

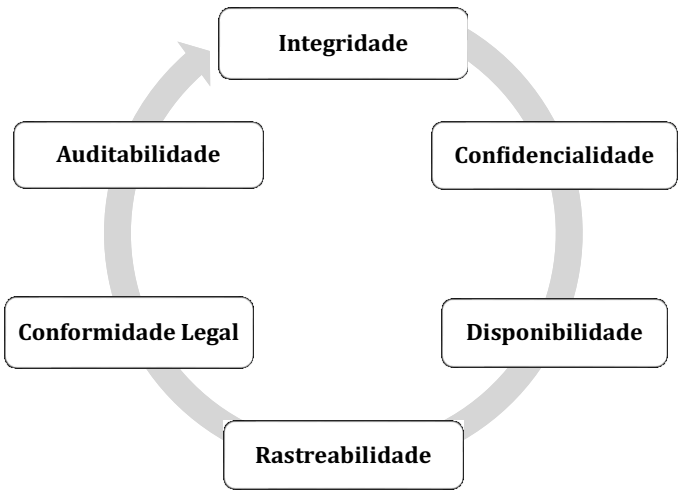
O Banco compromete-se em:

a) Seguir e implementar os princípios descritos na presente política, politicas associadas, divulgando recomendações actualizadas aos seus clientes e parceiros.
b) Manter uma infraestrutura organizacional de suporte, garantindo a sustentabilidade e as evidências necessárias, de forma a garantir a confidencialidade, integridade, autenticidade, o não repudio da informação por nós recebida, processada ou transmitida.
c) Definir a estratégia e as politicas que devem ser aplicadas no âmbito da gestão de Segurança da Informação e da Cibersegurança.
d) Proceder ao relato regular e transparente do seu desempenho na matéria da Segurança da Informação e da Cibersegurança.
e) Manter as melhores recomendações ou guias de segurança para com os clientes, de modo a permitir que estejam actualizados, face as melhores práticas para utilização dos serviços *web* disponibilizados pelo Banco.

5.3 Segurança da informação e *Cibersegurança*

1. A Segurança da Informação protege a informação contra uma multiplicidade de ameaças, visando designadamente, assegurar a continuidade do negócio, minimizar os efeitos negativos no mesmo, maximizar a rentabilização dos investimentos e melhorar a qualidade do serviço prestado. A cibersegurança, exige a necessidade de protecção dos activos de informação, por meio do tratamento de ameaças que põem em risco a informação que é processada, armazenada e transmitida pelos sistemas de informação que estão interligados.
2. A informação é um activo crítico de extrema importância e pertença do Banco. São igualmente considerados activos da organização, todos os recursos informáticos de *software* e *hardware* utilizados na administração e gestão da Informação, independentemente da sua situação em termos de propriedade legal.

3. Adicionalmente, considera-se de importância estratégica a existência de uma "cultura de Segurança e de Cibersegurança", que propicie a todos os clientes um panorama claro das suas responsabilidades no âmbito da Segurança da Informação.
4. Nos meandros da organização, são aplicados a cada activo os seguintes valores:
    a) Confidencialidade: garantir que a Informação não é divulgada e acedida de forma inadequada por entidades ou processos.
    b) Integridade: garantir a prevenção contra a modificação e/ou destruição não autorizada de Informação.
    c) Disponibilidade: garantir o acesso à informação onde e quando necessário, sem atraso.
    d) Rastreabilidade: evidências para assegurar a capacidade de recuperação do histórico das acções concretizadas, através de um registo actualizado e disponível em qualquer momento.
    e) Conformidade Legal: respeito pelas leis civis e criminais, regulamentações ou obrigações contratuais e requisitos de Segurança de Informação.
    f) Auditabilidade: auditabilidade por parte dos auditores internos ou fornecedores externos, de modo a testar a veracidade dos dados e informação corporativa e/ou de negócio, que são registados, compilados e analisados.



5. É obrigação legal e ética do Banco garantir os valores anteriores junto de qualquer cliente/entidade com a qual é mantido algum tipo de relacionamento, nomeadamente clientes, parceiros, fornecedores, e organismos oficiais competentes.

5.4 Procedimentos e controlos

De acordo as directrizes da ISO/IEC 27001, ISO/IEC 27005 e ISO/IEC 27035º, o Banco estabeleceu os seguintes mecanismos de forma a garantir a segurança e Cibersegurança, nomeadamente:

a) Procedimentos de autenticação, autorização e auditoria para garantir a identidade digital do utilizador de um sistema, garantir que o utilizador é autenticado e que somente tenha acesso aos recursos autorizados e, por fim, a colecta de informações sobre o uso dos recursos de um sistema pelos seus clientes, respetivamente.

b) Utilização de criptografia, visa codificar a informação de forma que só o cliente e o Banco consiga decifrá-la.

c) Detecção e prevenção de intrusões, combinação de vários sistemas para a detecção e prevenção de intrusão baseado em redes e em *hosts*, tratando o Banco como complementares de acordo com a necessidade e criticidade de proteção exigidas pelo negócio.

d) Prevenção de fuga de dados e de informações, através da identificação de pontos críticos, mapeamento de todos os pontos de vulnerabilidades, devendo definir as prioridades de cada um destes pontos críticos e aplicar as devidas protecções, sustentada em 3 (três) pilares:

    i) proteção dos dados sensíveis;

    ii) proteção da rede e sistemas do Banco;

    iii) *awareness* a colaboradores e clientes do Banco.

e) Realização periódica de testes e auditorias para a detecção de vulnerabilidades, garantir a gestão do risco operacional envolvido e avaliando a adequação das tecnologias e sistemas de informação utilizados no Banco através da revisão e avaliação dos controlos, desenvolvimento de sistemas, procedimentos de *TI*, infraestrutura, operação, desempenho e segurança da informação que envolve o processamento de informações críticas para a tomada de decisão.

f) Protecção contra *software* malicioso e tentativas de vectores de ataques, através do bloqueio ou diminuição da exposição do risco, face aos ataques (qualquer tentativa de expor, alterar, desa ctivar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um activo do Banco).

g) Controlo de acesso e de segmentação de redes de computadores: através da classificação dos itens como aplicações, utilizadores, dispositivos, serviços específicos e em utilizar o catálogo dessa classificação de acordo com as necessidades de acesso.

h) Realização periódica de testes e auditorias para a detecção de vulnerabilidades, garantir a gestão do risco operacional envolvido e avaliando a adequação das tecnologias e sistemas de informação utilizados no Banco, através da revisão e avaliação dos controlos, desenvolvimento de sistemas, procedimentos de *IT*, infraestrutura, operação, desempenho e segurança da informação que envolve o processamento de informações críticas para a tomada de decisão.

i) Controlos específicos, garantir a segurança das informações sensíveis, incluindo de rastreabilidade de informação através de coleta constante e análise, em tempo real, dos milhares tipos de eventos de segurança gerados pelos activos da rede, análise e *Threat Intelligence* para a efectiva detecção e resposta as ameaças, através da priorização dos incidentes de segurança para a necessária e efectiva reacção por parte do Banco.

j) Prestação de informações a clientes e utentes sobre precauções na utilização de produtos e serviços financeiros, assentes nas recomendações publicadas pelo Banco, através dos canais de comunicação definidos.

6. Disposições Finais

6.1 Revisão e actualização

1. A presente política deve ser revista sempre que necessário ou sempre que se verifiquem alterações relevantes ou num período mínimo, de a cada dois anos, de forma a garantir a sua actualização.

2. Cabe à Direcção de *Compliance* (DCP) solicitar alteração a política sempre que:

    a) ocorram alterações relevantes no mercado, na orientação estratégica do Banco e/ou na regulamentação emitida pelos órgãos de supervisão ou outras legislações a que o Banco está sujeito, desde que tais alterações afectem a conformidade necessária ao abrigo de todas as políticas.

    b) sejam adoptadas alterações relevantes à estrutura orgânica ou funcional do Banco, com impacto nas funções relevantes para o Sistema de Gestão da Qualidade.

3. Compete à DCP, sob a orientação do CISO, elaborar e manter actualizada a presente Política, sujeitando-a à apreciação do Comité de Inovação, Tecnologias e Segurança da Informação (CITSI), ficando este responsável pela submissão da Política e das suas propostas de revisão à aprovação do Conselho de Administração (CA).

6.2 Divulgação e Acesso

1. A publicação desta Política, visa contribuir para o estabelecimento de um ambiente de rigor e controlo eficaz na operacionalização dos processos relacionados com a prevenção, detecção, redução de vulnerabilidades e impactos gerados pelos incidentes relacionados ao ambiente cibernético e que afectam a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pelo Banco.

2. A presente Política deve ser divulgada em ficheiro electrónico e disponível no ***site*** Institucional do Banco para que o seu conteúdo possa ser consultado pelos clientes, parceiros, *stakeholders* e organismos externos, de acordo com a classificação dos respectivos documentos e autorização de acesso.

3. Todos os exemplares impressos são consideradas cópias não controladas.

6.3 Monitorização e Entrada em Vigor

1. Compete à DCP monitorar o cumprimento das regras da presente Política e demais normativos internos complementares em termos de matérias éticas, deontológicas e prudencial, tais como o código de conduta e o normativo sobre a actividade de intermediação financeiro.