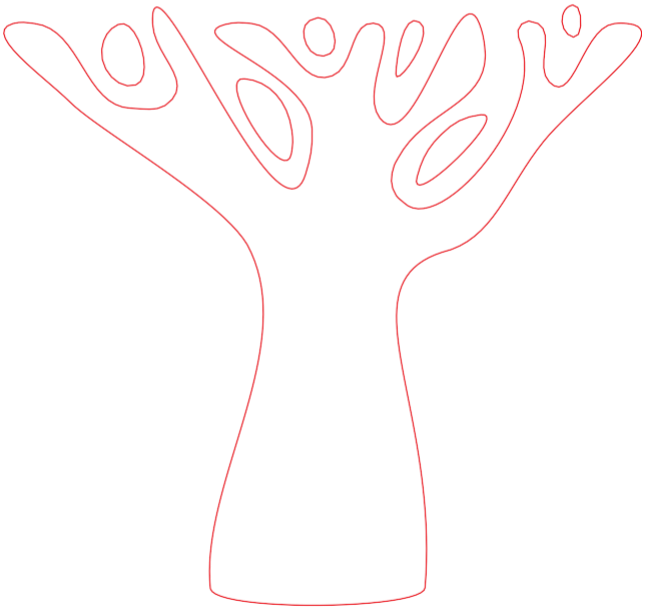
Política de Cibersegurança



BancoBIC

Crescemos Juntos

Índice

1. ASPECTOS GERAIS

1.1. Enquadramento

A Política de Uso Aceitável dos Sistemas de Informação do Banco BIC, formalizada neste documento - doravante designado por PoSI-PoCI – constitui uma Política específica alinhada com a Política de Segurança da Informação.

Qualquer alteração à presente Política tem efeito à data de entrada em vigor, que constar no documento que formalizar a referida alteração. Estas alterações são publicadas nos meios de comunicação estabelecidos pelo Banco BIC.

A presente Política também se alinha às regulamentações internacionais, incluindo o Regulamento Geral sobre a Proteção de Dados (RGPD) e as leis locais aplicáveis, para assegurar a proteção e privacidade dos dados dos nossos clientes e parceiros.

1.2. Âmbito

A PoSI-PoCI aplica-se a todos os colaboradores internos e entidades parceiras – doravante designados por colaboradores – que utilizem os Sistemas de Informação disponibilizados pelo Banco BIC, incluindo dispositivos móveis, computadores pessoais e plataformas de trabalho remoto.

Os requisitos para a Protecção dos dados e das informações do Banco BIC, conforme estabelecidos nesta Política, também devem ser estipulados e cumpridos sempre que parceiros externos e terceiros (inclusive consultores, trabalhadores contingentes, contratados ou prestadores de serviços) prestarem serviços para o Banco BIC, ou em seu nome.

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, e a Norma ISO/IEC 27035 que sistematiza as melhores práticas e orientações para a realização de uma abordagem eficaz à de gestão de incidentes, o Banco BIC 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.

1.3. Objetivos

A PoSI-PoCI para o Banco tem como objetivo a prevenção, deteção e redução de vulnerabilidades e impactos gerados pelos incidentes relacionados ao ambiente cibernético que afetem a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação utilizados pelo Banco, de forma a:

- Toda informação online ou offline que seja propriedade do Banco BIC deve ser protegida de qualquer ameaça que possa comprometer a sua confidencialidade, integridade ou disponibilidade;
- No que diz respeito a Cibersegurança e Protecção de Dados, o Banco BIC, deve empregar esforços compatíveis com a natureza das operações e complexidade dos seus produtos;
- O Banco BIC deve disseminar a cultura de Cibersegurança e Protecção de dados atodos os seus stakeholders;
- O Banco BIC deve adotar a postura prospectiva no gerenciamento de Cibersegurança e Proteção de Dados, atuando com Procedimentos e Controles que reduzam a sua vulnerabilidade a falhas e incidentes;
- Independentemente da forma como é gerada, tratada ou compartilhada, toda informação sob propriedade da Banco BIC deve ser utilizada unicamente para finalidade com a qual foi autorizada;
- A Política de Continuidade de Negócios (PCN) deve considerar o tratamento de incidentes cibernéticos e definir protocolos de ação para cenários de interrupção dos serviços de processamento e armazenamento de dados e de computação em nuvem;
- A contratação de serviços relevantes, fornecedores e terceiros que atuem no processamento e armazenamento de dados deve obedecer, além do estipulado na Política de Segurança de Informação, às disposições específicas desta Política.
- A Política de Cibersegrança tem como objetivo específico prevenir, detectar e mitigar ameaças emergentes como ataques de phishing e ransomware, garantindo a proteção contínua dos dados e sistemas de informação do Banco BIC.

2. DIRECTRIZES

Para assegurar que as informações e os dados sob propriedade do Banco BIC estejam gerenciados e protegidos contra roubo, fraude, espionagem, perda e quaisquer outras ameaças,

tornam-se objetivos da Cibersegurança:

- **Confidencialidade**: é a garantia que as informações e os dados sejam acessíveis somente ao pessoal especificamente autorizado;
- **Integridade**: é a garantia de exatidão e inteireza das informações e dos dados, sem modificações indevidas (sejam intencional ou não);
- **Disponibilidade**: é a garantia que as pessoas autorizadas a tratar as informações e os dados tenham acesso ao seu conteúdo e possam consultá-las a qualquer momento;

2.1. Unidade Responsável

A Direcção da DSI é responsável pela gestão de Cibersegurança e Proteção de Dados, tendo como atuação a proposição de ajustes, melhorias, aprimoramentos, validações e modificações desta Política:

- Executar todas as atividades para a gestão de Segurança da Informação;
- Realizar a gestão de controlo, distribuição e instalação de softwares utilizados.

Esta Direcção também é responsável por colaborar juntamente à unidade organizacional responsável pela gestão de riscos e de capital para melhoria contínua da operação de gestão de risco e evolução de sua governança corporativa.

2.2. Classificação da Informação

Em conformidade com a Política de Classificação da Informação, as informações e dados são classificados em:

- **Pública**: é toda informação de propriedade do Banco BIC oriunda de base pública e/ou com linguagem e formato dedicado à divulgação ao público em geral, sendo o seu caráter informativo, comercial ou promocional, destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma;
- **Pessoal**: é toda informação de propriedade do Banco BIC relacionada a pessoa natural identificada ou identificável;
- **Pessoal Sensível**: é toda informação de propriedade do Banco BIC sobre a origem racial ou étnica, convicção religiosa, opinião Política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Interna**: é toda informação de propriedade do Banco BIC que esta não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado.

Caso esta informação seja acedida indevidamente, poderá causar danos mínimos ou irrelevantes à imagem da Organização o que permite seu acesso sem restrições por todos os colaboradores e prestadores de serviços da instituição.

- **Confidencial**: é toda informação de propriedade do Banco BIC considerada crítica para os negócios da instituição e cuja divulgação não autorizada pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por colaboradores, clientes e/ou fornecedores.
- **Restrita**: é toda informação de propriedade do Banco BIC que pode ser acedida somente por utilizadors desta Instituição explicitamente indicado pelo nome ou pela área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

2.3. Procedimentos de Cibersegurança

2.3.1. Requisitos de Segurança do Ambiente Físico

Os servidores que armazenam os sistemas devem ser hospedados em Data Centers que possua, acessos controlados e monitorados, bem como que garantam disponibilidade dos ativos informacionais a esta Instituição com perenidade, inclusive quando acionados os protocolos de Continuidade de Negócio.

Os Data Centers devem aderir às Políticas pertinentes do Banco BIC bem como atender a quaisquer solicitações desta instituição, além de garantir a capacidade de resposta a incidentese a Continuidade de Negócio.

Já as máquinas e estações de trabalhos dos colaboradores e terceiros, devem ser protegidos contra danos ou perdas, bem como o acesso, o uso ou exposição indevidos. Observa-se que estes ativos físicos devem utilizar apenas softwares licenciados ou autorizados pela unidade responsável, bem como é obrigatório o uso de software de Anti-virus com Endpoint Detection e Response e Endopoint Protection para fins de controlo de ameaças eletrónicas, vírus, zero-day e ransonware.

Os servidores devem ser hospedados em Data Centers com monitoramento contínuo por câmeras de segurança e controle de acesso através de autenticação biométrica, garantindo a proteção física e a integridade dos dados armazenados.

2.3.2. Requisitos de Segurança do Ambiente Lógico

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir o acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registadas continuadamente, com papéis de responsabilidade claramente definidos eregistados. Os dados, as informações e os Sistemas de Informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir os riscos e garantir os objetivos desta Política.

2.3.3. Autenticação e Autorização

Autenticação é o processo de verificação das credenciais que um utilizador fornece, com aquelas armazenadas em um sistema para provar que a autenticidade do Utilizador. A Autenticação pode ser de factor único ou de múltiplo factor.

Autorização é o processo de verificar se este utilizador tem permissão para aceder uma área de uma aplicação ou executar ações específicas, com base em determinados critérios e condições estabelecidos pela aplicação, e designado de matriz de acesso ou controle de privilégio. A autorização pode conceder ou negar permissão para realizar tarefas ou acessar áreas de uma aplicação.

O utilizador (colaborador ou terceiro) é responsável por todos os actos executados com as suas credenciais de login, devendo manter a confidencialidade dos seus dados e alterar a password periodicamente, utilizando combinações de qualidade e difícil enigma. Também deve o utilizador bloquear o seu equipamento sempre que se ausentar.

2.3.4. Criptografia

A Política de Cibersegurança está em conformidade com a Política de Criptografia do Banco BIC - PoSI-PoCr, que constitui uma Política específica alinhada com a PoSI.

2.3.5. Postura de trabalho

O utilizador deve adotar postura aderente às boas práticas relacionadas, e assegurar que as informações sensíveis, tanto em formato digital, quanto físico e ativos (ex.: portáteis, celulares, tablets e outros) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa a sua área de trabalho, mesmo que seja por um curto período.

Os colaboradores devem adotar práticas de segurança para assegurar que informações sensíveis não sejam deixadas desprotegidas em espaços de trabalho compartilhados, ou durante o trabalho remoto, incluindo o uso de telas de privacidade e o bloqueio de dispositivos.

2.3.6. Backup

Os backups devem ser automatizados por sistemas de agendamento e executados, preferencialmente, fora do horário laboral. As mídias de backup (como DAT, DLT, LTO) devem ser acondicionadas em local seco, climatizado, seguro (sempre que possível em salas cofres e/ou cofres corta-fogo segundo as Normas de Segurança) e fora do site de produção. Já as fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome com etiquetas não manuscritas.

O tempo de vida, qualidade e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, definido no prazo recomendado pelo fabricante, com substituição periódica.

A unidade responsável pela gestão dos sistemas de backup deverá realizar e documentar testes periódicos de restauro de acordo com a criticidade do backup, mediante as boas práticas, para garantir a integridade e a disponibilidade contínua dos dados críticos do Banco.

Os elementos descritos acima estão indicados na PoSI-PoSRD-Política de Salvaguarda e Restauro de Dados.

2.3.7. VPN

O uso do acesso via VPN deve ser restrito e utilizado para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades, sendo vetado aos utilizadors do serviço, compartilhar credenciais de acesso via VPN com quem quer que seja, ou de aceder ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros colaboradores. Todo acesso por meio de VPN deverá ser antecedido pela formalização do pedido de acesso, seguido da finalidade e período necessário para a realização da tarefa, após o período de liberação o mesmo deverá ser bloqueado. Os elementos descritos acima estão indicados na PoSI-PoGIA - Política de Gestão de Identidades e Acessos.

Todo acesso via VPN será monitorado continuamente e sujeito a auditorias regulares para garantir que apenas atividades autorizadas sejam realizadas e para detectar qualquer uso indevido ou tentativa de acesso não autorizado.

2.3.8. Contratação e Serviços Relevantes, de Processamento e Armazenamento de Dados e de Computação em Nuvem

A contratação de serviços relevantes para o processamento e armazenamento de dados e de computação em nuvem são solicitadas através da unidade responsável pela Cibersegurança, que deve:

- Observar a contratação com aderência à estratégia, apetite e gestão de riscos e capital do Banco BIC;
- Assegurar que o potencial prestador de serviço tenha capacidade de fornecer o produto/serviço dentro das especificações técnicas bem como garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e informações processadas ou armazenadas;
- Assegurar que o potencial prestador de serviço esteja em condições de cumprir a legislação vigente e fornecer, a qualquer tempo, o acesso aos dados e as informações a serem processadas ou armazenadas;
- Assegurar que o potencial prestador de serviço seja devidamente certificado para a prestação do serviço e disponibilizar relatórios de auditoria independente – contratada pelo prestador – a respeito dos procedimentos e controlos adotados na prestação do serviço;
- Assegurar que o potencial prestador de serviço demonstre a identificação e segregação dos dados dos clientes do Banco BIC por meio de controlos físicos ou lógicos, bem como a qualidade dos controlos de acessos voltados à proteção de dados e as informações dos clientes da instituição;
- Documentar a diligência realizada para contratação do prestador de serviço e disponibilizar tais relatórios à unidade responsável pela gestão de riscos e de capital;
- Garantir que o contrato firmado entre as partes, apresente de maneira clara a adoção de medidas de segurança para transmissão e armazenamento de dados, além da manutenção da segregação de dados e controlo de acesso para proteção de informações dos clientes do Banco BIC;
- Comunicar ao BNA a respeito das possíveis contratações de serviços relevantes de processamento e armazenamento de dados, conforme o AVISO N.º 08/2020.
- Garantir que o contrato firmado entre as partes apresente de maneira clara as cláusulas, em caso de extinção, que versam sobre a transferência de dados e as informações ao novo prestador de serviço bem como a exclusão dos mesmos após a transferência.
- Os prestadores de serviços de processamento e armazenamento de dados devem estar em conformidade com normas de segurança reconhecidas internacionalmente, como ISO/IEC 27017 e ISO/IEC 27018, garantindo a segurança e privacidade dos dados.

2.3.9. Plano de Ação e Resposta a Incidentes Cibernéticos

A Administração do Banco BIC estabelecerá uma Equipe de Resposta a Incidentes (IRT) dedicada, responsável pela coordenação e resposta a incidentes de Cibersegurança, seguindo um plano de ação predefinido, que deve abranger:

- Mapeamento dos principais incidentes, tanto observado em base histórica quanto incidentes de probabilidade significativa;
- As rotinas, os procedimentos, os controlos e a tecnologia implementada na prevenção e na resposta aos incidentes mapeados;
- Produção de Relatório anual onde conste os incidentes registados e a efetividade das ações adotadas, os resultados obtidos e quaisquer mudanças necessárias para evolução da Cibersegurança.
- Serão realizadas simulações periódicas de incidentes cibernéticos para treinar a equipe e validar os procedimentos de resposta, garantindo a prontidão e eficácia em situações reais de emergência.

2.3.10. Divulgação a Política De Cibersegurança e Proteção de Dados

Esta Política deve ser divulgada a todos os que atuem no Banco BIC com linguagem clara, acessível e compatível as funções desempenhadas.

A Política de Cibersegurança e proteção de dados será continuamente divulgada aos colaboradores, fornecedores e terceiros por meio de formações regulares e campanhas de conscientização, para assegurar a compreensão e a adesão às práticas estabelecidas.

3. TERMOS E DEFINIÇÕES

- **Colaboradores:** Funcionários, fornecedores, consultores, incluindo os colaboradores de entidades externas ou outras entidades e/ou pessoas que acedam à informação e/ou aos Sistemas de Informação do Banco BIC;
- **Confidencialidade:** Atributo de Segurança da Informação que assegura que a informação é acessível apenas por entidades autorizadas;
- **Disponibilidade:** Atributo de Segurança da Informação que assegura que a informação está disponível, atempadamente, sempre que solicitado por entidades autorizadas;
- **Incidente de Segurança da Informação:** Qualquer ocorrência que afete ou possa afetar a confidencialidade, integridade e/ou disponibilidade da informação ou dos Sistemas de Informação do Banco BIC, com prejuízo financeiro, reputacional ou operacional para o

Banco, incluindo qualquer ação ou omissão, deliberada ou não, que viole a regulação de segurança e privacidade da informação;

- **Integridade:** Atributo de segurança da informação que assegura que a informação é alterada ou suprimida de forma autorizada;
- **Posto de Trabalho:** Equipamento disponibilizado aos colaboradores para o exercício das suas funções, podendo incluir computadores do tipo Desktop bem como equipamentos portáteis (e.g. Laptops, Tablets);
- **Sistemas 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. SANÇÕES

Nos casos em que houver violação desta Política, sanções administrativas e/ou legais poderão ser adotadas sem prévio aviso, podendo culminar com eventuais processos se aplicáveis, com a notificação do infrator.

Qualquer violação desta Política deve ser comunicada imediatamente através dos canais designados, incluindo opções de denúncia anônima, e será tratada conforme os procedimentos internos de investigação e resolução de incidentes.

---

5. HISTÓRICO DE APROVAÇÃO

Data	Descrição	Aprovador
28.03.2024	Aprovação da Política	Conselho de Administração