Conteúdo

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 Geral da 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.

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.

Os requisitos para a proteção 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, 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 de 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:

I. Toda informação – online ou offline - que seja propriedade do Banco BIC, SA deve ser protegida de qualquer ameaça que possa comprometer sua confidencialidade, integridade ou disponibilidade;

II. No que tange à Cibersegurança e proteção de dados, o Banco BIC, SA, deve empregar esforços compatíveis com a natureza das operações e complexidade de seus produtos;

III. O Banco BIC, SA deve disseminar cultura de Cibersegurança e proteção de dados a todos seus stakeholders;

IV. O Banco BIC, SA deve adotar postura prospetiva no gerenciamento de Cibersegurança e proteção de dados, atuando com procedimentos e controles que reduzam sua vulnerabilidade a falhas e incidentes;

V. Independentemente da forma como é gerada, tratada ou compartilhada, toda informação sob propriedade da Banco BIC, SA deve ser utilizada unicamente para finalidade com a qual foi autorizada;

VI. O tratamento de incidentes relativos ao sistema cibernético e de dados deve obedecer, MANUAL DE PROCEDIMENTOS (Processo de Resposta e Reporte de Incidentes), e às disposições específicas nesta política;

VII. A Politica 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;

VIII. A contratação de serviços relevantes, fornecedores e terceiros que atuem no processamento e armazenamento de dados deve obedecer, além do estipulado na na política de segurança de informação, às disposições específicas desta política

2 DIRECTRIZES

Para assegurar que as informações e dados sob propriedade do Banco BIC, S. A estejam gerenciadas e protegidas contra roubo, fraude, espionagem, perda e quaisquer outras ameaças, tornam-se objetivos da cibersegurança:

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

2.1 UNIDADE RESPONSÁVEL

Fica eleito a unidade organizacional da DSI Infraestrutura como a 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 gestão de segurança da informação; realizar a gestão de controle, distribuição e instalação de softwares utilizados. A DSI Infraestrutura 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 Politica de Classificação da Informação, as informações e dados são classificados em:

I. **Pública**: é toda informação de propriedade do Banco BIC, SA oriunda de base pública e/ou com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional, sendo destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma;
II. **Pessoal**: é toda informação de propriedade do Banco BIC, SA relacionada a pessoa natural identificada ou identificável;
III. **Pessoal Sensível**: é toda informação de propriedade do Banco BIC, SA sobre 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;
IV. **Interna**: é toda informação de propriedade do Banco BIC, SA que esta não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos mínimos ou irrelevantes à imagem da Organização o que permite seu acesso sem restrições por todos os empregados e prestadores de serviços do Banco BIC, SA.
V. **Confidencial**: é toda informação de propriedade do Banco BIC, SA 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 empregados, clientes e/ou fornecedores.
VI. **Restrita**: é toda informação de propriedade do Banco BIC, SA que pode ser acessada somente por usuários desta Instituição explicitamente indicado pelo nome ou por 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 CIBERSEGURANCA

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 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, SA bem como atender às quaisquer solicitações desta instituição, inclusive de visitação, além de garantir sua capacidade de resposta a incidentes e 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, 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 Endpoint para fins de controle de ameaças eletrônicas, vírus, zero-day, ransonware.

2.3.2 REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente, com papéis de responsabilidade claramente definidos e registrados. 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 riscos e garantir os objetivos desta política.

2.3.3 AUTENTICAÇÃO E SENHA

O usuário (seja colaborador ou terceiro) é responsável por todos os atos executados com seu login e senha, sendo papel do usuário manter a confidencialidade de seus dados e alterar a senha periodicamente, utilizando combinações de qualidade e difícil adivinhação. Também é papel do usuário bloquear seu equipamento sempre que se ausentar.

2.3.4 MESA LIMPA E TELA LIMPA

O usuário deve adotar postura aderente as práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo.

2.3.5 BACKUP

Os backups devem ser automatizados por sistemas de agendamento e executados, preferencialmente, fora do horário comercial. As mídias de backup (como DAT, DLT, LTO) devem ser acondicionadas em local seco, climatizado, seguro (e 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, além do prazo recomendado pelo

fabricante, o parque de fitas deverá ser substituído no máximo após 2 anos de uso. É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

A unidade responsável pela gestão dos sistemas de backup deverá realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias e testes periódicos de restauração (restore) com prazo máximo de 120 dias, de acordo com a criticidade do backup.

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

2.3.6 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 usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários. 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.

2.3.7 VIOLAÇÃO DESTA POLÍTICA

Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis. O infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato e a Diretoria

2.5 CONTRATAÇÃO DE SERVIÇOS RELEVANTES, DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

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

I. Observar a contratação com aderência à estratégia, apetite e gestão de riscos e capital do Banco BIC, SA;
II. 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 processados ou armazenados;

III. 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 informações a serem processados ou armazenados;
IV. 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 controles adotados na prestação do serviço;
V. Assegurar que o potencial prestador de serviço demonstre a identificação e segregação dos dados dos clientes do Banco BIC, SA por meio de controles físicos ou lógicos, bem como a qualidade dos controles de acessos voltados à proteção de dados e informações dos clientes da instituição;
VI. Documentar a diligência realizada para contratação do prestador de serviço e disponibilizar tais relatórios à unidade responsável pela gestão de riscos e de capital;
VII. 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 controle de acesso para proteção de informações dos clientes do Banco BIC, SA;
VIII. 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 informações ao novo prestador de serviço bem como a exclusão dos mesmos após a transferência.

2.6 PLANO DE AÇÃO E RESPOSTA A INCIDENTES CIBERNÉTICOS

Fica autorizado a gestão específica e direcionada do Manual de procedimentos (Processo de Resposta e Reporte de Incidentes), que deve abranger:

I. Mapeamento dos principais incidentes, tanto observado em base histórica quanto incidentes de probabilidade significativa;
II. As rotinas, os procedimentos, os controles e a tecnologia empregada na prevenção e na resposta aos incidentes mapeados;
III. Produção de relatório anual onde conste os incidentes registrados e a efetividade das ações adotadas, os resultados obtidos e quaisquer mudanças necessárias para evolução da Cibersegurança.

2.7 DIVULGAÇÃO DA POLÍTICA DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

Esta política deve ser divulgada aos colaboradores, fornecedores e terceiros que atuem no Banco BIC, S.A com linguagem clara, acessível e compatível as funções desempenhadas.

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 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 BIC, 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

As situações de incumprimento com a presente politica, ainda que de forma tentada, poderão originar processos disciplinares, bem como ações de natureza cível ou penal, em conformidade com as leis aplicáveis.

5 HISTORICO DE ALTERAÇÂO

DATA DE CRIAÇÂO	10/12/2020	
DATA DE REVISAO	06/01/2021	
DATA APROVAÇÂO	21/01/2021	POR: DSI