POLÍTICA DE PREVENÇÃO DE FUGA DE INFORMAÇÃO

Informação sobre o documento			
Data do documento	Dezembro 2022	**Responsável pela política**	DTI
Data de revisão	03/02/2023	**Aprovado por**	CA
Número de páginas	11	**Número da versão**	1.0/2022

Controlo de versões		
Versão	**Descrição**	**Data**

Índice

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 Prevenção de Fuga de Informação o Banco está envolvido em garantir a integridade, confidencialidade e disponibilidade da informação dos seus sistemas de informação, da privacidade dos seus clientes e colaboradores, no cumprimento de requisitos legais vigentes fornecendo de uma maneira eficiente e efectiva a gestão desta informação e do negócio, minimizando assim a fuga de informações que possam colocar o Banco numa situação desfavorável perante os seus Clientes, Administradores e Reputação Institucional.

A fuga de informação sensível pode ser prejudicial e em simultâneo um "trunfo" para os concorrentes, que poderão até se apoderar dessa informação utilizando-a para seu benefício. Para isso, a informação deve ser transmitida de forma íntegra entre computadores e dispositivos protegidos para que só as pessoas autorizadas tenham acesso. Devem ainda ser implementadas e cumpridas regras de boas práticas para a segurança da informação, nas quais os colaboradores possam basear as suas ações.

2. Âmbito da Política

A presente política, centra-se nas soluções que façam face a fuga de informação (Postos de Trabalho) e infraestruturas tecnológicas (Sistemas Informático e de comunicação) ou à incapacidade generalizada de controlar a informação que circula dentro e fora do Banco Comercial Angolano, adiante designado como Banco ou BCA. Assim, o âmbito da aplicação desta política estende-se as questões associadas à prevenção e segurança da informação, ainda que incidentes possam evoluir para um impacto grave da segurança da informação.

3. Objectivos da Política

O objectivo da política de prevenção de fuga de informação é definir as linhas de orientação para a implementação capaz de minimizar o risco, perante um incidente que afete o negócio, e seja capaz de garantir o seguinte:

- Garantir a segurança da informação e de sistemas;
- Garantir a salvaguarda de dados e informações de Clientes e do Banco;
- Reduzir a exposição do Banco aos efeitos potenciais de um evento de fuga de informação e/ ou mitigar o seu impacto;
- Mitigar, em situações de incidente, os riscos para a segurança da informação do Banco.

4. Referências utilizadas

Na elaboração da presente política, foram consideradas a legislação, regulamentação, códigos de conduta e outras boas práticas nacionais e internacionais reconhecidas ao nível dos sectores de actuação do Banco, como, por exemplo:

- ISO/IEC 27001:2013 - Information Security Management
- ISO/IEC 27002:2022 - Code of Practice for Information Security Controls
- ISO 15443 – Information Technology – Security Techniques
- Lei nº 7/17 de 16 de Fevereiro – Lei de Proteção das Redes e Sistemas Informáticos;
- Lei nº 22/11 de 17 de junho – Lei da Proteção de Dados Pessoais
- Política de Segurança de Informação do Banco.

5. Disponibilidade da política

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

É também extensivel a todas as entidades externas, incluindo entidades terceiras com quem o Banco tem contratos e acordos celebrados, que utilizem ou acedam à informação e Sistemas de Informação (SI) do Banco.

Para uma adequada gestão da segurança da informação é fundamental que os destinatários cumpram com o dever de sigilo e adoptem um comportamento seguro, aceitável e consistente na sua actividade diária, visando a protecção da informação e do negócio do Banco.

As políticas, normas e procedimentos de segurança da informação são de cumprimento obrigatório para todos os que intervêm, directa ou indirectamente, no acesso e uso da informação e SI do Banco.

6. 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).

7. Aprovação da Política

Esta política é recomendada pelo Comité de Controlo Interno e Auditoria (CCCIA) e aprovada pelo Conselho de Administração (CA).

8. Implementação da Política

A Direcção de Gestão de Risco facilitará e assegurará a coordenação da implementação da presente política.

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. Politica de Prevenção de Fuga de Informação

10.1. Introdução

A Comissão Executiva (CE) do Banco considera que toda a informação e os sistemas de informação (SI) que lhe estão associados constituem activos essenciais ao funcionamento e desenvolvimento do negócio.

Em particular, os SI são recursos críticos para a produção, processamento, transmissão e armazenamento da informação e devem acompanhar a evolução do negócio permitindo melhorias na eficácia e eficiência da sua gestão. Caso contrário, podem ocorrer incidentes com origem em erros, falhas, fraudes, intrusões, entre outros, que afectam a integridade, a disponibilidade e a confidencialidade dos activos do Banco. Estas ocorrências podem resultar em impactos negativos, tanto ao nível da fiabilidade, da operacionalidade ou qualidade dos serviços prestados, como das oportunidades de negócio, da imagem ou da capacidade de cumprir requisitos do âmbito contratual, legal ou regulamentar, entre outros riscos relevantes.

O crescente nível de risco dos activos de informação, assim como, a maior complexidade dos SI que conduz ao aparecimento de novos riscos para a informação, requerem níveis de controlo e protecção cada vez mais exigentes. Esta política rege-se pela regulamentação vigente e pelas boas práticas sobre a matéria e visa proteger e salvaguardar a informação e os SI de eventos adversos que possam causar impacto significativo, contribuindo para um controlo interno mais efectivo e para a redução do risco operacional, reputacional e de conformidade.

10.2. Definição

As medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam informações confidenciais.
Têm como propósito detectar e impedir a divulgação e extração não autorizada de informações por indivíduos ou sistemas.

10.3. Princípios Orientadores Da Segurança Da Informação

A organização deve considerar o seguinte para reduzir o risco de fuga de informação:

a) Identificação e classificação de informações para proteção contra vazamento (por exemplo, informações pessoais, modelos de preços e designs de produtos);
b) Canais de monitoramento de vazamento de Informação e dados (por exemplo, e-mail, transferências de arquivos, dispositivos móveis e dispositivos de armazenamento portáteis);
c) Agir para evitar o vazamento de informações (por exemplo, e-mails de quarentena contendo informações confidenciais).

As ferramentas de prevenção de fuga de informação e dados devem ser usadas para:

a) Identificar e monitorar informações confidenciais em risco de divulgação não autorizada (por exemplo, em dados não estruturados no sistema de um utilizador);
b) Detectar a divulgação de informações confidenciais (por exemplo, quando as informações são carregadas em serviços de nuvem de terceiros não confiáveis ou enviadas por e-mail);
c) Bloquear ações do utilizador ou transmissões de rede que exponham informações confidenciais (por exemplo, impedindo a cópia de entradas de bases de dados num formulário).

No que respeita à **gestão de fuga de informação** o Banco deve:

- Determinar se é necessário restringir a capacidade de um utilizador de copiar e colar ou fazer upload de dados para serviços, e dispositivos de armazenamento fora da organização;
- Se for esse o caso, deve implementar tecnologia como ferramentas de prevenção de fuga de Informação (DLP) ou a configuração de ferramentas existentes que permitam aos utilizadores visualizar e manipular a informação e os dados mantidos remotamente, mas evitar copiar e colar fora do controlo da organização;
- Se a exportação da informação ou dados for necessária, o proprietário deve ter permissão para aprovar a exportação e responsabilizar os utilizadores pelas suas acções;
- Configurar o Privilégio de Acesso predefinido para documentos guardados no servidor de documentos (exemplo Sharepoint) e ter mecanismos de IAM – Identity Access Management e IRM – Information Rights Management para gerir o acesso à Informação por parte dos Colaboradores;
- Capturas de tela ou fotografias da tela devem ser abordadas por meio de termos e condições de uso, formação e auditoria;

- No backup da informação, deve-se tomar cuidado para garantir que as informações confidenciais sejam protegidas usando medidas como criptografia, controlo de acesso e proteção física da base de armazenamento que contém o backup;
- A prevenção de fuga de informação também deve ser considerada para proteger contra as ações de inteligência de um adversário em obter informações confidenciais ou secretas (geopolíticas, humanas, financeiras, comerciais, científicas ou qualquer outra) que possam ser de interesse para espionagem ou críticas para a comunidade;
- As ações de prevenção de fuga de informação devem ser orientadas para confundir as decisões do adversário, por exemplo, substituindo informações autênticas por informações falsas, seja como uma ação independente ou como resposta às ações de inteligência do adversário;

No que respeita a outras medidas de prevenção de fuga de informação:

- As ferramentas de prevenção de fuga de informação devem ser projectadas para identificar a informação, monitorar o uso e o movimento da informação e tomar medidas para evitar a fuga de informação (por exemplo, bloquear a transferência de informação para dispositivos de armazenamento portáteis);
- A prevenção de fuga de informação envolve a monitorização das comunicações e atividades online dos colaboradores e, por extensão, das mensagens de terceiros;
- A prevenção de fuga de informação pode ser suportada por controlos de segurança padrão, como políticas específicas de tópicos sobre controlo de acesso, Classificação da informação e gestão segura de documentos;
- Restringir o método para especificar destinos no scanner para evitar o envio de dados para um endereço não desejado, ou para for a da organização sem controlo;
- Desativar a porta USB e a slot do cartão SD na parte lateral do painel de controlo para guardar dados digitalizados e evitar fuga de dados;
- Evitar deixar documentos impressos na impressora, e evitar deixar endereços na memória da impressora pois permitem aceder ao spooler até 24h;
- Colocar marcas de água com IP do utilizador e data / hora da impressão ou da digitalização do documento;
- A Informação e os dados no disco rígido podem ser encriptados ou os dados temporários podem ser eliminados por substituição, para evitar a reposição e alteração dos mesmos.

Nota:

Existe uma variedade de legislação relativa à privacidade, proteção de dados e informação, interceptação de informação e telecomunicações, que é aplicável ao monitoramento e processamento da informação no contexto da prevenção de fuga de informação.

No que respeita a **assistência técnica por parte de fornecedores**:

- Restringir as Operações do Técnico de Assistência sem Supervisão do Administrador do Equipamento;
- Restringir o acesso a zonas de Data Center para substituição ou manutenção de equipamentos sem a supervisão de um colaborador do Banco;
- Não permitir a retirada de equipamentos do Banco sem primeiro verificar a informação contida nos mesmos, no caso de discos rígidos deve ser garantida que a informação que estava armazenada já não se encontra disponível para ser acedida;
- Em situações de necessidade de acesso remoto, deve ser garantida a supervisão desses acessos por forma a garantir que não existe fuga de informação ou acesso indevido por parte do fornecedor / técnico de assistência.

No que respeita às **obrigações legais e regulamentares**:

- O Banco deve assegurar a conformidade com **as normas legais** e **regulamentos**, especialmente os relativos ao tratamento de dados de carácter pessoal, informação privilegiada e salvaguarda do sigilo bancário, levando a cabo as medidas necessárias para o efeito.

10.4. Responsabilidades

A segurança da informação é garantida pelos vários órgãos de estrutura do Banco. As responsabilidades pela Gestão da Segurança da Informação e Cibersegurança são asseguradas pelo Departamento de Segurança da Informação (DSI).

Compete à DTI, enquanto proprietário da informação, indicar as áreas responsáveis pela gestão da informação de acordo com as necessidades do negócio e da gestão da infra-estrutura IT de suporte.

10.5. Divulgação e Acesso

Esta política deve ser divulgada a todos os colaboradores do Banco e entidades externas relevantes e estar acessível para que o seu conteúdo possa ser consultado a qualquer momento. As restantes PSI, normas e processos deverão ser igualmente disponibilizadas, mediante a audiência a que estas se destinem.

A responsabilidade pela divulgação interna das PSI e futuras revisões, compete ao DSI a todos os órgãos e a Direcções do Banco.

A responsabilidade pela divulgação das PSI a terceiros, no que for aplicável, é dos responsáveis das Unidades de Estrutura que gerem a relação com essas entidades.

Adicionalmente, devem ser realizadas acções de formação e sensibilização adequadas, a todos os colaboradores e entidades externas, enquanto prestadoras de serviços, salvaguardando a actualização necessária às PSI, normas e procedimentos de segurança de informação em vigor.

10.6. Incumprimento

Qualquer incumprimento ou violação das políticas de segurança da informação deve ser imediatamente reportado ao DSI, sendo da competência desta assegurar o seu tratamento.
A este respeito, e sempre que se justifique, o DSI deverá levar a cabo todas as diligencias necessárias, comunicar e envolver as Direcções e entidades que considere relevantes ao apuramento das causas e responsabilidades, tratamento, e reporte dos mesmos:

- Deverão ser envolvidas as Direcções e funções responsáveis;
- Deverá ser envolvida a DTI sempre que envolva responsabilidades no âmbito das Tecnologias e Sistemas de Informação;
- Deverá reportar o incumprimento ou violação ao DSI sempre que se verifique, após análise, que o incumprimento é passível de reporte à supervisão do compliance; e
- Sempre que o incumprimento ou violação represente risco não negligenciável para o Banco, deverá reportar:
    - Caso o incumprimento seja de nível grave, a DGR deverá apresentar, de imediato, o caso para apreciação em sede do CE.
- Deverá despoletar o processo de gestão de incidentes de segurança da informação (ver a **Norma de Gestão de Incidentes de Segurança de Informação**) sempre que necessário;

Caso se verifique que o incumprimento ou violação do disposto na presente política resulte igualmente na violação do Código de Conduta por parte de um colaborador do Banco, a DSI após o reporte, deve avaliar a situação e verificar se a mesma é passível de resultar na instauração de um processo disciplinar, de acordo com o disposto na presente política.

Caso um colaborador tome conhecimento de um possível incidente de segurança da informação é sua responsabilidade comunicá-lo imediatamente, de acordo com o procedimento de reporte de incidentes de segurança da informação instituído **(conforme definido na Norma de Gestão de Incidentes de Segurança de Informação)**.

No que respeita a prestadores de serviços externos, a violação das políticas de segurança da informação pode resultar no imediato cancelamento das respectivas autorizações de utilização dos SI e/ou na suspensão ou termo da respectiva relação contratual, sem prejuízo de indeminizações a accionar.

10.7. Monitorização e Controlo

- A utilização da informação e dos SI do Banco deve ser monitorizada e registada para detecção de incumprimentos das PSI, normas e procedimentos de segurança da informação e, consoante o caso, servir como evidência em processos administrativos, disciplinares e/ou legais;
- A análise/avaliação de riscos de segurança da informação pode ser aplicada à totalidade do Banco, partes do Banco, um SI específico, ou apenas componentes de um sistema específico, entre outros;
- A autorização de acesso à informação deve ser determinada com base na necessidade de saber e do privilégio mínimo, associada às funções do colaborador ou entidade, assim como esta deve ser objecto de aprovação e controlo;
- Os acessos aos SI devem ser definidos segundo uma lógica de segregação de funções (evitando a acumulação de funções potencialmente conflituosas), ao nível da utilização, operação, manutenção e outras actividades envolvendo a informação, em conformidade com Matriz de Acessos em vigor;
- Em caso de necessidade de acesso por terceiros aos SI do Banco, deve ser analisado o respectivo risco e este deve ser sujeito a aprovação prévia e a controlo;
- O acesso e utilização da informação deve ser feito com recurso a um identificador único de utilizador, de forma a permitir que este seja controlado e auditado, assegurando a responsabilização inequívoca de cada utilizador pelas suas acções;
- A concessão e revogação de autorização de acesso aos SI devem ser efectuadas de acordo com os procedimentos de segurança em vigor;
- Devem ser removidas, imediatamente, autorizações dadas a colaboradores demitidos ou suspensos;
- As autorizações dos colaboradores que tenham mudado de função devem ser revistas e alteradas em conformidade;
- As autorizações concedidas bem como as regras de atribuição, manutenção e uso de palavra-passe devem ser revistas, pelo menos, anualmente; e

- A informação e os SI devem ter a sua exposição, a ameaças naturais e outros riscos físicos relevantes, mitigada por intermédio de controlos de acessos físicos, vigilância dos espaços (e.g. meios humanos ou sistemas de vídeo vigilância), monitorização e controlo de condições climatização, falhas e estabilização de energia, detecção e supressão de incêndios, e inundações.

10.8. Excepções

No caso de impossibilidade de implementação de qualquer das orientações de controlos previstos nesta política, deverão ser definidos controlos adicionais no processo respectivo.

Os controlos adicionais em relação à segurança da informação devem ser validados pelo responsável do processo, devidamente documentados, e, após parecer favorável da DSI e da DGR (caso se traduza numa alteração da exposição do Banco ao risco), devem ser aprovados por dois administradores executivos.

10.9. Vigência

A presente política entra em vigor à data de emissão, após a sua aprovação por parte do CA.

11. Relação com Outros Documentos

Normas vigentes na instituição.