POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Informação sobre o documento			
Data do documento	Fevereiro 2023	**Responsável pela política**	DGR
Data de revisão	03/02/2023	**Aprovado por**	C.A
Número de páginas	34	**Número da versão**	6.0/2023

Controlo de versões		
Versão	**Descrição**	**Data**
05	Revisão	2019
04	Revisão	2017
03	Revisão	2013
02	Revisão	2009
01	Aprovação	2006

Índice

1. INTRODUÇÃO

Sendo a informação uma das variáveis determinantes na composição da oferta de produtos e serviços destinada aos seus clientes e colaboradores, através da Política de Segurança da Informação o Banco está comprometido em proteger a integridade, confidencialidade e disponibilidade dos seus sistemas de informação, das informações que estes sistemas manuseiam, a privacidade dos seus clientes e colaboradores, bem como no cumprimento de requisitos legais vigentes enquanto fornece de uma maneira eficiente e efectiva a gestão desta informação e do negócio.

Com efeito, a **Política de Segurança da Informação** rege-se pelas melhores práticas sobre a matéria bem como pelos normativos vigentes, tais como Aviso 08/2020 do Banco Nacional de Angola.

A presente política serve de base à implementação de Regras e Normas que permitem protecção dos dados e informação nos sistemas sobre a Instituição, seus Clientes, nas Transacções Financeiras, Registo e Pagamento do Pessoal, Processos e Balanços Financeiros.

Esta política aplica-se a todos os Colaboradores e demais intervenientes nos Sistemas de Informação do Banco e visa a preservação dos activos de informação do Banco quanto a:

- **Integridade:** garantia de que à informação seja mantida em seu estado original, visando protegê-la contra alterações indevidas, intencionais ou acidentais tanto na guarda como na transmissão;
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Disponibilidade**: garantia de que os utilizadores autorizados tenham acesso a informação sempre que necessário.

Deste modo, neste documento descrevem-se as formas de evitar e responder às ameaças à informação e aos sistemas de informação, incluindo o acesso não autorizado, divulgações, modificações, destruição, perdas e uso incorreto.

2. Referências Normativas e Cruzadas

Na elaboração da presente política foram consideradas a legislação vigente sobre a matéria, o código de conduta do Banco e as boas práticas nacionais e internacionais reconhecidas ao nível dos sectores de actuação do Banco, nomeadamente:

- ISO/IEC 27001:2013 - Information Security Management
- ISO/IEC 27002:2022 - Code of Practice for Information Security Controls
- Aviso 08/2020 Política de Segurança Cibernética e Adopção de computação em nuvem, de 16 de Março;
- Lei nº 7/2017; Lei de Proteção das Redes e Sistemas Informáticos;
- Lei 22/11 de 17 de junho – Lei da Proteção de Dados (Angola)

3. Glossário

Ameaça - como qualquer factor ou açção capaz de interferir e causar danos à integridade, à confidencialidade, à autenticidade e à disponibilidades de dados e informações da empresa.

Activo - Qualquer componente (seja humano, tecnológico, *software*, entre outros) que suporte um ou mais processos de negócio de uma unidade ou área de negócio.

Capacitação em Segurança de Informação - Capacitar as diferentes áreas da organização, em segurança da informação, no sentido de proteger activos valiosos e contribuir para um ambiente mais seguro e que respeita a privacidade dos clientes.

Confidencialidade - Propriedade que garante que a informação não está disponível ou é divulgada a indivíduos ou entidades não autorizadas.

Controlo de Acesso - Conjunto de procedimentos e meios utilizados com a finalidade de permitir ou bloquear um acesso quer físico, quer virtual a activos de informação.

Disponibilidade - Propriedade que garante que a informação esteja disponível sempre que necessário, para acesso de utilizadores autorizados.

Estrutura de Gestão da Segurança da Informação - Órgãos e Direcções responsáveis pela definição, gestão e execução da segurança da informação.

Gestão de Activos - Processo de identificação, actualização e manutenção dos activos de informação que suportam os processos de negócio e de suporte do Banco**.**

Gestão de Continuidade de Negócio - compreende o conjunto integrado de políticas e procedimentos que visam assegurar o funcionamento contínuo da Instituição, ou a recuperação atempada da sua actividade, no caso de ocorrência de eventos susceptíveis de perturbar o normal desenrolar do negócio.

Gestão de Risco de Sistemas de Informação - Processo que permite identificar, implementar e posteriormente acompanhar, as medidas necessárias para minimizar ou eliminar os riscos a que estão sujeitos os activos de informação do Banco.

Incidente - Qualquer evento que possa comprometer a disponibilidade, confidencialidade e integridade da informação ou serviços do Banco (e.g. um utilizador não autorizado consegue ter acesso a um sistema crítico ao negócio).

Infra-estrutura de Tecnologias de Informação - As instalações, aplicações de negócio, infra-estrutura tecnológicas (equipamentos e *hardware* fixo e portátil necessário à gestão funcional da rede) e sistemas de armazenamento e recuperação de dados (arquivos e armazenamento).

Integridade - Propriedade que garante que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Quebra de segurança - Acção ou omissão, intencional ou acidental, que resulta no comprometimento da informação.

Risco de Sistemas de Informação - Possibilidade de exploração dos activos de informação por parte de uma ou várias ameaças, com impacto negativo para o Banco. Resulta da combinação entre a probabilidade de um evento ocorrer e o seu impacto.

Segurança da informação - diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança dinformação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Segurança física e do ambiente de Sistemas de Informação - Processo que trata da protecção de todos os activos físicos do Banco. Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, algo que possa danificar a parte física da segurança, acesso indevido de estranhos (controlo de acesso), forma inadequada de tratamento e manuseio dos veículos.

Sistema de Gestão da Segurança da Informação - Políticas, normas e processos que definem a forma como o Banco gere a segurança da informação.

Sistemas estruturantes - Aplicações de negócio (*hardware* e *software* base e aplicacional) e infra-estrutura tecnológicas (equipamentos e *software* fixos e portáteis necessários para a LAN e WAN e equipamentos de impressão e equipamentos para o utilizador).

Terceiros - Quaisquer pessoas físicas ou entidades jurídicas externas ao Banco.

Tratamento da informação - Conjunto de acções referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controlo da informação.

Tratamento de incidentes/ocorrências - Processo que consiste em identificar, analisar e responder às solicitações e alertas, e realizar as análises aos incidentes/ocorrências de segurança, procurando extrair informações que permitam impedir a continuidade da acção maliciosa e também identificar tendências.

Vulnerabilidade - Fragilidade do activo de informação e da sua utilização que pode ser explorada por uma ou mais ameaças.

4. Intervenientes

Conselho de Administração (CA): Órgão de administração responsável no âmbito das suas atribuições por assegurar a aprovação e implementação das políticas.

Comissão Executiva (CE) – Órgão de Administração, encarregue da gestão corrente do Banco responsável, bem como deliberar sobre decisões relevantes, nomeadamente, as que tenham impacto na Arquitectura e Segurança das TSI nos termos estabelecidos no respectivo regulamento.

Departamento de Segurança da Informação (DSI) – Departamento responsável pela definição, actualização, monitorização e divulgação das Políticas de Segurança da Informação junto dos colaboradores do Banco e pela execução de auditorias periódicas por forma a avaliar a adequação e eficácia das Políticas de Segurança da Informação.

Direcção de Gestão de Risco (DGR) – Unidade responsável pela gestão, acompanhamento e supervisão dos riscos associados à segurança da informação de forma transversal à actividade do Banco. No âmbito da gestão de riscos de segurança da informação, compete igualmente à DGR a prestação de assessoria em contexto de CSI.

Direcção de Tecnologias de Informação (DTI) – Direcção, que no âmbito das suas funções, zela pela protecção da informação (confidencialidade, integridade e disponibilidade) que é armazenada, transmitida e processada nos sistemas, redes e comunicações do Banco. Responsável, por assegurar que as políticas e procedimentos de governação das TSI – Tecnologias de Segurança de Informação, estão implementadas e alinhadas com a visão e objectivos gerais corporativos do Banco, bem com, em articulação com a DSI, pela definição, implementação, gestão e monitorização dos respectivos

controlos de segurança da informação.

Gabinete de Compliance (GCO) - Gabinete, que no âmbito das suas funções, é responsável pelo acompanhamento e supervisão do cumprimento das Políticas de Segurança da Informação, gerir os incumprimentos identificados e propor a instauração de processos disciplinares resultantes do incumprimento das mesmas.

Gabinete Jurídico e Contencioso (GJC) – Função responsável por controlar o cumprimento das obrigações em matéria de protecção de dados pessoais, cooperando com a Agência de Protecção de Dados (APD) e servindo como ponto de contacto entre o Banco e a autoridade de controlo e para os titulares dos dados pessoais.

Unidades de Estrutura – Órgãos a quem compete, por intermédio dos respectivos responsáveis, assegurar que os colaboradores que estão sob a sua responsabilidade, bem como as entidades externas/terceiros com quem estabelecem relações, conhecem, compreendam e apliquem as Políticas de Segurança da Informação. Compete ainda às Unidades de Estrutura, e sempre que aplicável, garantir e controlar a aplicação destas políticas na sua área funcional.

Utilizadores de Informação – Todos os Colaboradores, que no âmbito das suas funções, zelam pelo cumprimento escrupuloso da Políticas de Segurança da Informação.

5. Destinatários

O presente documento aplica-se a todos os colaboradores do Banco, bem como 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. Responsabilidades e Atribuições

De forma a ser eficaz, a segurança de informação deve ser um esforço de equipa, envolvendo a participação e apoio de todos os colaboradores do Banco Comercial Angolano que lidam com a informação e com os sistemas de informação. Reconhecendo a necessidade do trabalho em equipa, esta política esclarece as responsabilidades dos utilizadores e dos passos que eles devem tomar para ajudar o Banco Comercial Angolano a proteger a sua informação e os seus sistemas de informação.

6.1. Entidades envolvidas na "guarda" da Informação

Responsabilidades dos Utilizadores - Os Utilizadores têm a responsabilidade de se familiarizarem e respeitarem todas as políticas, procedimentos e normas do Banco sobre a segurança de Informação. Quaisquer perguntas ou dúvidas concernentes ao tratamento de um tipo específico de informação devem ser encaminhadas para o Zelador ou para o Detentor da informação em questão.

Responsabilidades dos Detentores - Os Detentores da Informação são os Responsáveis de Direcções, Gabinetes e Departamento. Toda a informação produzida pelos sistemas aplicacionais tem de ter um detentor designado. Todos os tipos de informação devem ser alvo de uma classificação por parte dos seus Detentores em função da sua sensibilidade. Os Detentores da informação devem também definir quais são os utilizadores com acesso à informação, e aprovar pedidos inerentes às várias maneiras em que a informação será utilizada.

Responsabilidades dos Zeladores - Os zeladores são aqueles que têm em sua posse física ou lógica informação do Banco Comercial Angolano ou informação que foi confiada ao Banco. Embora os elementos da Direção de Tecnologia de Informação sejam obviamente zeladores, os administradores de sistemas locais também o são. Para os sistemas centrais, os técnicos da Direção de tecnologia de Informação devidamente identificados como zelador. Sempre que a informação é conservada apenas num computador pessoal, o Utilizador desse computador pessoal também passa a ser zelador. Cada tipo de informação contido no sistema de informação de uma aplicação de produção tem de ter um ou mais zeladores designados. Os Zeladores são responsáveis pela salvaguarda da informação, incluindo a implementação de sistemas de controlo de acesso que visam evitar as disseminações inapropriadas, e a realização de cópias de segurança (backup), com o intuito de impedir que a informação crítica não seja perdida. Cabe, ainda, aos Zeladores, implementar, acçionar e manter as medidas de segurança definidas pelos Detentores da informação.

A Direção de TI deverá possuir informação / inventário de todos os ativos (físicos, serviços, sistemas, aplicações, etc.) de TI do Banco bem como os seus Zeladores e Detentores.

7. Política de Segurança de Informação

7.1. Introdução

O Conselho de Administração (CA) 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. Por este motivo, e conforme indicado anteriormente, o CA do Banco entendeu definir um conjunto de **politicas de segurança de informação** (PSI), de modo a assegurar a protecção da informação de uma forma transversal, bem como dos SI que lhe estão associados. Estas políticas regem-se pela regulamentação vigente e pelas boas práticas sobre a matéria e visam 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.

7.2. Definição

As directrizes das PSI constituem os principais pilares da gestão de segurança da informação. A esse respeito, a normalização da segurança da informação do Banco é definida em três níveis hierárquicos:

- **Políticas de Segurança da Informação**: estabelecem a estrutura, objectivos, directrizes e as obrigações de carácter geral (a PGSI definida no presente documento) ou específico (PSI complementares) referentes à segurança da informação;

- **Normas de Segurança da Informação:** definem os requisitos e planos de acção em maior nível de detalhe, através dos quais as tecnologias e procedimentos devem ser implementados em toda a organização, por forma a suportar os objectivos e linhas orientadoras definidos pela PSI; e

- **Procedimentos de Segurança da Informação:** descrevem detalhadamente um conjunto de acções, passo-a-passo, necessárias à implementação de um mecanismo, controlo ou solução de segurança específico. O propósito dos procedimentos é assegurar a integridade dos processos de negócios, de modo que as actividades sejam desenvolvidas em conformidade com as políticas e normas definidas. Estes, tipicamente, destinam-se a uma audiência limitada e com foco alinhado com as funções desempenhadas.

Podem existir, ainda, um conjunto de documentação adicional que pretende complementar as políticas, normas e procedimentos (e.g. documentação de processos).

7.3. Princípios Orientadores da Segurança da Informação

Por forma a assegurar que as PSI se encontram devidamente alinhadas e suportam, na sua totalidade, os objectivos para a segurança da informação definidos pelo Banco (apresentados neste documento), são estabelecidos os seguintes princípios orientadores, que deverão ser considerados na definição e implementação das demais PSI.

No que respeita à **protecção da informação e SI associados**:

A informação, os sistemas e os serviços utilizados pelos colaboradores são de exclusiva propriedade do Banco, não podendo ser interpretados como de uso pessoal;

- Toda a informação do Banco deve ser protegida de riscos e ameaças que possam comprometer a sua **confidencialidade**, **integridade** e **disponibilidade**. Para tal, deve assegurar-se:
    - O nível de **confidencialidade** adequado para a informação, garantindo que a mesma apenas está acessível a quem esteja autorizado. Para mais informações, consultar a **Política de Classificação de Informação** e a **Política de Controlo de Acessos e Gestão de Utilizadores**;
    - A **integridade** da informação, na sua totalidade e exactidão, procurando que a mesma seja mantida quer na forma como foi criada pelo seu autor, quer no conteúdo e que não existem alterações indevidas, intencionais ou acidentais; e
    - A **disponibilidade** da informação sempre que necessária, por quem está autorizado, de acordo com o perfil de acesso.
- É **proibida** a divulgação, duplicação, modificação, destruição, uso inadequado, roubo e acesso não autorizado à informação pertencente ao Banco, a clientes e outras entidades que lhe tenham confiado informação;
- Toda a informação do Banco, independentemente da forma, deve ser utilizada unicamente para a **finalidade** para que foi criada e devidamente autorizada;
- Todo o **acesso** à informação e aos SI associados deve ser previamente autorizado, efectuado de forma controlada e devidamente monitorizada, respeitando os princípios do **privilégio mínimo** e **necessidade de saber**; e
- O **envolvimento e responsabilização** de todos os órgãos e Direcções da estrutura do Banco deve ser assegurado relativamente à protecção da informação.

No que respeita à **gestão da segurança da informação**:

- O Banco deve ter uma organização interna de **gestão da segurança da informação** e um sistema de gestão de riscos, adequados à dimensão e à complexidade do seu negócio, que garanta uma gestão efectiva da segurança da informação. Nesse sentido, deve adopter uma abordagem que integre:
    - O planeamento da segurança da informação, o controlo da implementação, o tratamento de incidentes e o cumprimento sistemático das PSI;
    - O alinhamento dos Planos e Processos do Banco com as directrizes das PSI; e
    - A monitorização e avaliação da eficácia da aplicação das PSI deverá ser realizada de forma independente, e enquadrada num processo de melhoria contínua.
- Os controlos de segurança implementados com vista ao cumprimento dos princípios previstos nas PSI são definidos com base num processo de **análise do risco**.

No que respeita à **definição** e **cumprimento das PSI**:

- O Banco deve seguir as **boas práticas** de segurança da informação previstas nas normas ISO/IEC 27001:2013 e ISO/IEC 27002:2022, CIS Controls e SWIFT CSP devidamente adaptadas ao seu negócio e dimensão;
- O Banco deverá cumprir com as regras de **formalização** do Sistema de Controlo Interno que compreendem todas as políticas desenvolvidas no âmbito da segurança da informação;
- O Banco deve **comunicar** as PSI a todos os colaboradores e entidades que acedem e utilizam a sua informação, por forma a assegurar que estes as conhecem, compreendem e aplicam devidamente; e
- As **consequências** e **penalidades** provenientes do **incumprimento** ou violação das PSI devem ser definidas e devidamente comunicadas pelo Banco.

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.

7.4. Gestão da Segurança da Informação

A gestão da segurança da informação do Banco assenta no o modelo PDCA (*plan*, *do*, *check*, *act*) previsto na norma ISO/IEC 27002:2022 e compreende quatro fases:

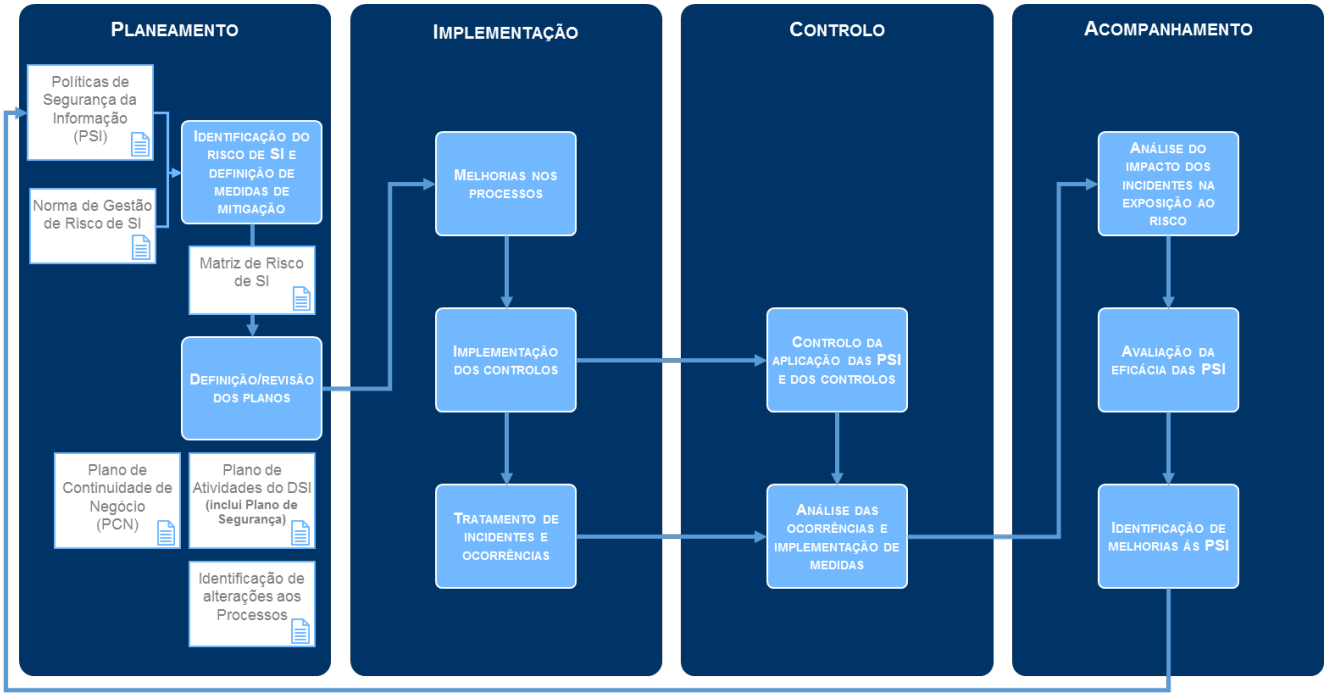
- **Planeamento da segurança da informação** – Tem por objectivo identificar periodicamente o risco de SI e planear as medidas de mitigação, de acordo com as orientações da **Norma de Gestão de Risco de Sistemas de Informação**;

- **Implementação** - Tem por objectivo adequar e aplicar a PSI aos processos do Banco, implementar as medidas de mitigação do risco e tratar os incidentes de segurança da informação;

- **Controlo** - Tem por objectivo assegurar que a política de segurança e que os processos e controlos definidos são aplicados; e

- **Acompanhamento** - Tem por objectivo acompanhar de forma sistemática a adequação e a eficácia das PSI.

Apresenta-se abaixo o esquema geral da gestão integrada da segurança da informação:



7.5. 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 ao CA, 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.

Nesse sentido, apresenta-se de seguida a estrutura de gestão de segurança de informação definida, bem como as responsabilidades de cada órgão da estrutura do Banco.

Conselho de Administração

Tem as seguintes atribuições:

- Aprovar as PSI, estratégias, normas de gestão de risco relacionadas (os planos e processos relacionados podem ser aprovados apenas pela (CE);

- Definir o nível de tolerância aos riscos de segurança da informação e os princípios orientadores relativamente à segurança da informação;

- Assegurar que a monitorização das PSI é efectuada de forma independente e sujeita a revisões periódicas;

- Delegar responsabilidades específicas na gestão da segurança da informação e assegurar que essas funções têm a autoridade, o conhecimento e os recursos materiais e humanos necessários para assegurar o cumprimento das PSI;

Comissão Executiva

Tem a responsabilidade última pela segurança da informação do Banco e, neste âmbito, tem as seguintes atribuições:

- Assegurar que as políticas e procedimentos de governação das TSI estão implementadas e alinhadas com a visão e objectivos gerais corporativos do Banco;

- Deliberar sobre decisões relevantes, nomeadamente, as que tenham impacto na Arquitectura e Segurança das TSI nos termos estabelecidos no respectivo regulamento

- Avaliar periodicamente a eficácia das PSI, através de análises independentes, recorrendo ao apoio especializado externo, se necessário. Esta análise tem por objectivo identificar desvios

em relação às PSI e normas de segurança da informação aprovados, devendo o Banco adoptar, posteriormente, as acções correctivas necessárias;

- Decidir sobre as propostas de melhoria e necessidades de mudança nas PSI;

- Tomar as decisões sobre a aplicação de medidas disciplinares referentes aos casos de incumprimento das PSI, normas e/ou de procedimentos de segurança da informação; e

- Autorizar a divulgação da PGSI a todos os colaboradores e entidades relacionadas com o Banco, assim como qualquer uma das demais PSI, normas e procedimentos complementares, de acordo com o seu perfil de responsabilidade.

Departamento de Segurança da Informação

Departamento da DGR que tem a função de Gestor da Segurança da Informação e Cibersegurança, com as seguintes responsabilidades:

- Definir e propor ao CA uma estratégia de segurança da informação, que apoie e esteja em alinhamento com a visão da CA e dos demais *stakeholders*;

- Definir e propor ao CA uma estratégia e uma estrutura de governança da Segurança da Informação transversal ao Banco, através da definição de princípios orientadores, políticas e normas;

- Preparar os planos estratégicos, tácticos e operacionais de suporte à segurança da informação;

- Elaborar e propor as PSI a aprovar pelo CA e, sempre que necessário, propor as revisões das mesmas, promovendo o envolvimento das Direcções e outras unidades de estrutura relevantes;

- Supervisionar e monitorizar a devida aplicação/adesão às PSI por parte dos colaboradores do Banco, avaliar a eficácia dos controlos implementados e promover a melhoria contínua dos mesmos;

- Gerir todos os aspectos de Segurança da Informação transversais ao Banco (tecnologias, pessoas e processos), de forma a assegurar a adequada protecção dos activos (salvaguardar a confidencialidade, integridade e disponibilidade) em função do nível da criticidade dos mesmos;

- Promover a realização de acções de sensibilização no que diz respeito à segurança da informação para todos os colaboradores (para mais informações, consultar a **Norma de Segurança de Recursos Humanos**);

- Planear as actividades de segurança da informação e apoiar a CE na tomada de decisão neste âmbito (e.g. estratégia de segurança da informação e transformação digital, planos de investimento, identificação de tecnologias, obrigações legais e regulamentares);

- Garantir que as actividades de segurança da informação são realizadas em conformidade com as PSI, executando os controlos necessários para o efeito;

- Garantir o tratamento de situações de incumprimento das PSI, promovendo o envolvimento de todas as Unidades de Estrutura relevantes ao apuramento das causas e responsabilidades, tratamento e reporte das mesmas.

- Assegurar o tratamento de incidentes de segurança da informação e analisar o respectivo impacto na exposição ao risco de segurança da informação, propondo, quando aplicável e conjuntamente com o Gabinete(s) da(s) Direcção(ões) relevantes, medidas correctivas e/ou preventivas. Para mais informações, consultar a **Norma de Gestão de Incidentes de Segurança da Informação**;

- Divulgar internamente a PSI, após aprovação pelo CE e obter a assinatura da Declaração de Conhecimento e Aceitação dos colaboradores, na qual os mesmos se comprometem a cumprir e respeitar esta Política, normas e os procedimentos de segurança da informação, arquivando-a em conjunto com a respectiva documentação individual;

- Arquivar e tornar disponível aos destinatários de cada política, as versões das PSI mais recentes;

- Solicitar testes de segurança e análise de risco à infra-estrutura dos SI a fim de certificar que as vulnerabilidades e os riscos destas são adequadamente identificados e mitigados;

Direcção de Gestão de Risco

No âmbito da segurança da informação, a DGR é responsável por:

- Rever o Plano de Continuidade de Negócio (PCN), com base nos riscos de sistemas de informação; e

- Supervisionar a função de Segurança de Informação no tratamento de incidentes de segurança da informação, com foco no apuramento do risco dos mesmos para o Banco.

Direcção de Tecnologias de Informação

No âmbito da segurança da informação, a DTI é responsável por:

- Identificar anualmente, ou sempre que uma alteração significativa do contexto o justifique, os activos que são críticos para os processos de negócio e determinar as ameaças e vulnerabilidades a que estão expostos;

- Identificar e rever, pelo menos anualmente, ou sempre que uma alteração significativa do contexto o justifique, o risco de SI e planear e propor os controlos e medidas de mitigação do mesmo;

- Assegurar a gestão dos activos de informação, infra-estruturas e tecnologias de informação, bem como dos controlos de segurança mais adequados;

- Definir as autorizações de acesso, para toda a informação sob sua responsabilidade, relacionando cargos e funções com as autorizações de acesso atribuídas, nomeadamente na Matriz de Acessos e Matriz de Segregação de Funções;

- Manter o registo e controlo actualizado de todos os acessos concedidos, determinando, sempre que necessário, a pronta suspensão ou alteração, bem como o cancelamento de acessos concedidos não necessários;

- Reavaliar, sempre que necessário, as autorizações de acesso concedidas e revogando aquelas que não são necessárias;

- Monitorizar os acessos às redes, SI e informação associada;

- Em articulação com a DSI, executar testes de segurança e análise de risco à infra-estrutura de rede e SI, no âmbito das suas actividades ou por solicitação da GAI – Departamento de Auditoria Interna, a fim de certificar que as vulnerabilidades e os riscos destas são adequadamente identificados e tratados;

- Tomar parte na investigação de incidentes de segurança relacionados com a informação sobre sua responsabilidade (ver a **Norma de Gestão de Incidentes de Segurança da Informação**).

Gabinete de Auditoria Interna

No âmbito da segurança da informação, o GAI é responsável por:

- Executar auditorias periódicas, se necessário recorrendo a entidades externas credenciadas para o efeito, para avaliar a adequação e eficácia das PSI, por forma a identificar e avaliar sistematicamente os riscos relacionados com a segurança da informação;

- Assegurar que o registo de todos os acessos concedidos é alvo de revisão periódica, determinando, sempre que necessário, a alteração, suspensão ou cancelamento (nas situações em que estes já não sejam necessários);

- Tomar parte na investigação de incidentes de segurança relacionados com a informação sobre sua responsabilidade; e

- Acompanhar a realização de auditorias externas aos SI.

Gabinete de Compliance

No âmbito da segurança da informação, o GCO é responsável por:

- Assegurar que as PSI, normas e procedimentos, cumprem as obrigações legais e/ ou regulamentares (ver a **Norma de Compliance da Segurança da Informação)**;

- Informar as diversas áreas envolvidas na gestão de segurança da informação sobre eventuais alterações legais e/ou regulamentares que impliquem responsabilidade e/ou acções referentes à segurança da informação, a análise e na elaboração de contratos (e.g. o Termo de Responsabilidade a ser assinado por fornecedores), sempre que necessário, cláusulas específicas relacionadas com a segurança da informação, com o objectivo de proteger os interesses do Banco;

- Propor à CE a instauração de processos disciplinares, que se verifiquem necessários, ao abrigo do disposto na PGSI, e no Código de Conduta em vigor; e

- Avaliar, quando solicitado, a conformidade legal dos procedimentos de segurança da informação em vigor.

Gabinete Jurídico e Contencioso (GJC)

No âmbito da segurança da informação e protecção dos dados pessoais, o GJC tem as seguintes principais responsabilidades:

- Informar e aconselhar os responsáveis pelo tratamento ou subcontratantes, bem como os colaboradores que tratem dados, a respeito das suas obrigações;

- Monitorizar e controlar a conformidade com a Lei 22/11 de 17 de junho;

- Prestar aconselhamento no que respeita à avaliação de impacto sobre a protecção de dados, e controlar a sua realização;

- Cooperar com a APD (Agência de Proteção de Dados) na sua actuação como ponto de contacto no âmbito da protecção de dados;

- Actuar como ponto de contacto para os titulares dos dados, no que respeita ao tratamento de dados, e outros esclarecimentos relacionados;

- Adoptar uma abordagem baseada no risco, no que diz respeito às operações de tratamento; e

- Acompanhar a conservação do registo de actividades de tratamento.

- Instruir e supervisionar os processos disciplinares instruídos em virtude da violação do disposto nas politicas de SI.

Responsáveis das Unidades de estruturas

Os responsáveis das Unidades de Estrutura utilizadores de informação devem, no âmbito da segurança da informação:

- Integrar as orientações da PSI e as medidas de mitigação do risco de SI na definição dos processos de negócio pelos quais são responsáveis;

- Cumprir e fazer cumprir as PSI, normas e procedimentos de segurança da informação;

- Assegurar que as suas equipas e entidades externas, enquanto seus prestadores de serviço, têm acesso e conhecimento das PSI, normas e procedimentos de segurança da informação, de acordo com o seu perfil de responsabilidade, garantido a sua aceitação;

- Obter das entidades externas a assinatura do Termo de Responsabilidade, na qual as mesmas se comprometem a cumprir e respeitar esta Política e os procedimentos de segurança da informação, entregando-as à DSI para arquivo

- Contribuir para o processo de classificação da informação, sendo responsável pela identificação, classificação e etiquetagem da informação do qual é dono (proprietário da informação);

- Definir os perfis de acesso à informação para os colaboradores da sua área;

- Informar, prontamente, a DTI, de todas as suspensões, demissões e modificações ao quadro do Banco, para a devida actualização do sistema de acesso; e

- Apoiar a DSI na definição de medidas correctivas e/ou preventivas.

Unidades de estruturas (internos e externos)

No âmbito da segurança da informação, os utilizadores da informação são responsáveis por:

- Conhecer e cumprir fielmente a PGSI, bem como, as restantes PSI, normas e procedimentos de segurança da informação aplicáveis, de acordo com o seu perfil de responsabilidade;
- Solicitar orientação ao superior hierárquico em caso de dúvidas relacionadas com a segurança de informação;
- Proteger a informação contra acesso, modificação, destruição ou divulgação não autorizados pelo Banco;
- Assinar a Declaração de Conhecimento e Aceitação (colaboradores) e assinatura de Termo de Responsabilidade e Acordo de Confidencialidade (utilizadores externos), formalizando a aceitação das PSI partilhadas (incluindo a presente política) e assumindo a responsabilidade pelo seu cumprimento;
- Cumprir as leis e as normas que regulam aspectos de propriedade intelectual; e
- Alertar e reportar, ao responsável da sua Direcção e à DSI, incidentes/ocorrências de segurança da informação, incluindo situações de inconformidade.

7.6. Critérios de Concessão de Acessos / Necessidade de conhecer

O acesso à informação em posse ou sob o controlo do Banco Comercial Angolano deve ser facultado com base na 'necessidade de conhecer'.

O acesso à informação deve ser permitido apenas às entidades que precisam da informação para fins comerciais legítimos. Ao mesmo tempo, os Colaboradores do Banco não devem sonegar informação naquelas situações em que os Detentores da informação concedam instruções para partilha da informação.

De maneira a implementar o conceito 'necessidade de conhecer', o Banco Comercial Angolano adoptou um processo que envolve o pedido de acesso e a autorização dos detentores da informação. Os colaboradores do Banco não devem tentar aceder à informação sensível, a não ser que o detentor relevante lhe tenha autorizado direitos de acesso.

Quando a relação jurídica laboral de um Colaborador do Banco sofre alterações como: despedimento, transferência, promoção ou licença temporária – o seu responsável direto, bem como a Direção de

Capital Humano deve informar de imediato o " Servicedesk BANCO" da Direcção de Tecnologias de Informação.

Os privilégios concedidos aos colaboradores devem ser periodicamente revistos (e actualizados se for o caso) pelos Detentores e Zeladores da informação para garantir que apenas aqueles com actual 'necessidade de conhecer' tenham acesso à informação.

7.7. Identificadores de Utilizador ("Username") e Palavra Passe ("Password")

De formas a implementar o processo de 'necessidade de conhecer', o Banco exige que todos os colaboradores que tenham acesso aos sistemas de informação possuam um identificador de utilizador único e uma palavra de passe privada (credenciais de acesso). Estes identificadores de utilizador devem ser empregues com o propósito de limitar os privilégios associados aos sistemas com base em funções e responsabilidades. Cada colaborador é responsável pelo uso dos seus credenciais de acesso.

Identificadores de Utilizador Anónimos - Com a excepção dos placards informativos electrónicos, sites da Internet, sites da intranet, e outros sistemas em que a intenção é que os utilizadores sejam anónimos, os utilizadores estão proibidos de entrar anonimamente em qualquer rede ou sistema informático do Banco Comercial Angolano. O acesso anónimo pode, por exemplo, contar com o uso de identificadores de utilizador "convidados". Quando os utilizadores utilizam comandos de sistema que lhes permitam mudar os identificadores de utilizador activo para adquirir certos privilégios, devem ter entrado inicialmente no sistema através de identificadores de utilizador que indiquem claramente as suas identidades.
A palavra passe dos identificadores instalados por defeito pelos sistemas ou aplicações devem ser alteradas.

Palavras de passe difíceis de adivinhar - Os utilizadores devem escolher palavras de passe que sejam difíceis de adivinhar. Isto quer dizer que, as palavras passe não devem estar relacionadas com o emprego ou vida pessoal dos colaboradores. Por exemplo, não se deve usar o número da matrícula de um automóvel, o nome de um cônjuge ou fragmentos de uma morada residencial. Isto quer também dizer que a palavra passe não deve constituir palavras que se encontram em dicionários ou categorias gramaticais. Por exemplo, não se deve usar nomes próprios, nomes de locais, termos técnicos e calão.

Dicas para escolher palavras de passe

Palavras de Passe Fáceis de Recordar - Os utilizadores devem escolher palavras de passe fáceis de recordar, mas que terceiros não autorizados terão dificuldade em adivinhar. Como fazê-lo?

- Junte palavras diferentes
- Permute letras minúsculas e maiúsculas
- Troque as letras que compõem uma palavra vulgar
- Transforme uma palavra comum seguindo um método específico
- Combine a pontuação ou números com uma palavra vulgar
- Crie acrónimos a partir de uma canção ou de um poema
- Soletre mal e deliberadamente uma palavra, combinando com essa técnica um número ou uma cor.

Padrão de Palavras Passe Repetidas - Os utilizadores não devem construir palavras passe com uma sequência básica de letras que possa ser subsequentemente ou parcialmente alterada, com base numa data ou outro fator previsível. Os utilizadores não devem construir palavras passe que sejam idênticas ou parecidas com palavras passe anteriormente empregues.

Os Constrangimentos das Palavras Passe - As palavras passe devem estar constituídas por pelo menos 8 caracteres, devendo conter pelo menos um carácter maiúsculo, um carácter minúsculo, um número e um carácter especial. As palavras passe devem ser mudadas de 30 em 30 dias ou mesmo em intervalos mais frequentes, dependendo do nível de sensibilidade da informação que é acedida. Os sistemas deverão acautelar para que o utilizador não possa usar as 8 password anteriores e garantir um período de utilização da senha de ao menos um dia. Em caso de tentativas de acesso com senha errada, o sistema deve bloquear o perfil de acesso, ao menos na Quinta tentativa. Caso um colaborador suspeite que a sua palavra passe é do conhecimento de outra pessoa, ele deverá mudá-la imediatamente.

Os Sistemas / aplicações deverão ser parametrizados em conformidade com as recomendações de segurança dos fabricantes, sem prejuízo desta política.

Armazenamento das Palavras Passe - As palavras passe não devem ser armazenadas em ficheiros de forma legível, guiões de abertura de sessão, teclas funcionais, computadores sem sistemas de controlo ao acesso ou noutros locais onde pessoas não autorizadas as poderiam descobrir. As palavras passe não devem ser apontadas numa forma fácil de decifrar e deixadas num lugar onde pessoas não autorizadas as poderiam descobrir.

Partilha das Palavras Passe - Caso os colaboradores do Banco precisem de partilhar dados armazenados num computador, devem recorrer ao correio eletrónico, às bases de dados, aos diretórios

públicos existentes nos servidores e a outros mecanismos. As palavras passe nunca devem ser reveladas a outras pessoas. Os administradores de sistemas e o outro pessoal dos sistemas de informação técnica não devem nunca solicitar a um colaborador para revelar a sua palavra passe pessoal. Uma palavra passe apenas pode ser do conhecimento de outra pessoa, na altura em que for emitida. ***Estas palavras passe temporárias devem ser alteradas a primeira vez que o utilizador autorizado aceder ao sistema.*** Se um utilizador suspeite que o seu identificador de utilizador e palavra de passe estão a ser usados por outra pessoa, ele deve logo notificar o administrador de sistemas.

As palavras passe padrão das aplicações / sistemas devem ser imediatamente alteradas após instalação do sistema / aplicação.

As palavras passe temporária deverá ser única para cada colaborador e não deverão ser fáceis de adivinhar.

Credenciais de acesso de colaboradores temporário – Os Perfis de acesso de consultores, estagiários, prestadores de serviços deverão estar habilitadas apenas no período que decorrer a sua intervenção, devendo estar definida a data de expiração definida (em conformidade com a data do final da intervenção) sempre que habilitada.

Declaração de Cumprimento - Todos os colaboradores que usam os sistemas de informação do Banco Comercial Angolano têm de assinar uma declaração de cumprimento antes que lhes seja emitido um identificador de utilizador [veja anexo B]. Para os utilizadores que já têm identificadores de utilizador, tais assinaturas têm que ser obtidas antes ser accionada a sua renovação anual. A assinatura desta declaração de cumprimento indica que o utilizador em questão compreende, e compromete-se a respeitar, as políticas e procedimentos informáticos do Banco Comercial Angolano, incluindo as instruções contidas nesta política.

Divulgação de Informação a Terceiros - A menos que tenha sido declarada como sendo de índole pública, toda a informação interna do Banco deve ser protegida, impedindo-se assim a sua divulgação a terceiros. Terceiros podem, contudo, ter acesso à informação interna do Banco quando existir uma necessidade imprescindível de divulgação, ou, no caso em que o Banco tenha assinado um acordo não divulgação, o Detentor dessa informação autorizar expressamente a sua divulgação. Se a informação sensível for perdida, divulgada a partes não autorizadas, ou se suspeite que estes dois casos tenham ocorrido o Detentor da Informação e/ou ” Servicedesk” da Direção de Tecnologias de Informação devem ser informados imediatamente.

Meios de Segurança Física para Controlar Acesso à Informação - O acesso a todos os escritórios, à sala dos computadores, e a outras áreas de trabalho que contêm informação sensível, deve ser

fisicamente limitado àquelas pessoas que têm a necessidade de conhecer ou precisam de ter acesso. Quando não estiver a ser usada, a informação sensível deverá ser sempre protegida contra o perigo de uma divulgação não autorizada.

A menos que a informação esteja a ser activamente usada por pessoas autorizadas, as secretárias dos colaboradores do Banco devem permanecer desobstruídas e limpas fora do horário de expediente, de maneira a evitar o acesso não autorizado a dita informação. Os colaboradores do banco devem colocar os ecrãs dos seus computadores de maneira a que as pessoas não autorizadas não consigam ver a informação sensível exibida.

O acesso ao "Data Center" deverá ser restringido ao pessoal da Direção de Tecnologias de Informação e a Segurança Interna do Banco através de um sistema de autenticação forte (exemplo: biométrico), devendo ser salvaguardado o registo de entradas.

Os prestadores de Serviços / consultores que por razões objetivas precisem ter acesso ao "Data Center" poderão fazê-lo na presença permanente de um colaborador da Direção de TI do Banco.

Não é permitida a entrada de nenhum tipo de alimento, bebida ou qualquer produto inflamável no "Dada Center"

A entrada ou remoção de qualquer equipamento no Data Center deverá obedecer a autorização formal do Director de Tecnologias de Informação.

7.8. COMPUTADORES, RECURSOS DE TECNOLÓGICOS E SERVIÇOS

Os equipamentos disponibilizados aos colaboradores são de propriedade do Banco, cabendo a cada colaborador utilizá-los e manuseá-los corretamente para as actividades do interesse da instituição cumprindo as recomendações dessa política e procedimentos operacionais a respeito.

Software

Os computadores e redes do Banco Comercial Angolano não devem trabalhar com software não provenientes dos Departamentos do Banco, grupos de utilizadores conhecedores e fiáveis, entidades conhecidas e que dominam o campo da segurança de sistemas, ou vendedores oficiais de software informático.

O software de fontes duvidosas não deve ser usado, a menos que tenha sido sujeito a uma prova rigorosa e aprovada pela DTI.

A instalação ou remoção de software é uma actividade exclusiva do pessoal de TI sendo proibida a instalação de software ilegal e/ou não autorizada.

Todo o software desenvolvido pelo pessoal interno do Banco e que visa processar informação Banco crítica ou sensível, deve ter uma especificação escrita e formal. Esta especificação deve incluir uma discussão dos riscos e controlos de segurança, incluindo os sistemas de controlo ao acesso e planos de contingência. A especificação deve fazer parte integrante de um acordo entre o Detentor da informação e o desenvolvedor de sistemas.

Os macros nas folhas de cálculo e nos documentos de processamento de texto, não são considerados como software.

Todo software aplicacional ou de Sistemas, antes do início da sua utilização no Banco ou mudança substancial deverá passar apenas a produção, depois de devidamente testado em qualidade, e com a devida aprovação do Director de TI. Este requisito aplica-se tanto aos computadores pessoais como aos sistemas maiores.

Todo o desenvolvimento de software de produção e todas as actividades de manutenção de software levadas a cabo pelo pessoal interno, devem seguir as políticas, normas e procedimentos vigentes no Banco, assim como outras convenções do desenvolvimento de sistemas. Estas convenções incluem testes, formação e documentação convenientes.

Os utilizadores não devem copiar o software ou códigos fonte fornecidos pelo Banco para qualquer suporte de memória, transferi-los para outro computador não pertencente ao Banco, ou divulgar o software ou código fonte a partes externas, sem o consentimento prévio do seu supervisor hierárquico - excepção autorizada feita a esta política, no caso das cópias de segurança normais.

Mudanças efectuadas aos recursos de TI / Controlo de Mudanças formais

Com exceção de situações de emergência, todas as mudanças ecfetuadas aos recursos de TI do Banco Comercial Angolano (incluindo as realizadas por entidades externas) devem ser documentadas num pedido de Mudança, aprovadas antecipadamente pelo Diretor de TI, através de um rigoroso procedimento para o efeito, evitando por via disso que mudanças inesperadas levem à interrupção involuntária da prestação de serviços, a divulgação não autorizada de informação, e outros incidentes ou problemas.

O referido procedimento de controlo deve ser usado no caso das mudanças significativas feitas ao software de sistemas, hardware e ligações de comunicação tanto para computadores pessoais que operam sistemas de produção e aos sistemas multiutilizador mais alargado.
As mudanças deverão apenas ser efectuadas por colaboradores da Direcção TI do Banco ou por parceiros (prestadores de serviços, consultores, etc.) devidamente autorizados pela Direcção de TI.
As mudanças, actualizações e correcções de segurança dos sistemas ou aplicações apenas deverão ocorrer depois da testado no devido ambiente para o efeito, sempre que aplicável.

Detecção / Erradicação de vírus Informáticos

Os sistemas e computadores do Banco deverão ter aplicação de Antivírus instalado e actualizados permanentemente com gestão central sob responsabilidade da Direção de TI.

Se os Colaboradores suspeitarem da existência de uma infecção por vírus informático, devem deixar logo de usar o computador em questão e pedir auxílio a Direcção de Tecnologias de Informação. Até que o vírus tenha sido erradicado com êxito, PEN drives ou outro suporte de memória usados no computador infectado não devem ser reutilizados. O computador infectado deve ainda ser imediatamente isolado da rede. Os utilizadores não devem tentar erradicar os vírus sem o suporte da DTI. É o pessoal da Direcção de Tecnologias de Informação que deve efectuar esta tarefa, de maneiras a minimizar tanto a destruição de dados como o tempo de inactividade do sistema.

Os utilizadores não devem cancelar os processos de software automáticos que actualizam as assinaturas dos vírus. O software de detecção de vírus informáticos deve ser usado para analisar todos ficheiros de dados provenientes de terceiros. Este processo deve ser levado a cabo antes de se abrir ficheiros de dados novos e antes de se executar software novo. Os colaboradores do Banco não devem omitir ou desligar os processos de verificação capazes de impedir a transmissão de vírus informáticos.

Ligações de Rede Interna

Todos os computadores do Banco que estejam permanentes ou intermitentemente ligados a rede interna de computadores, têm de possuir um sistema de controlo de acesso com base em nome de utilizador & palavras passe, criado pela Direcção de Tecnologias de Informação.

Os Sistemas multiutilizadores usados em todo Banco devem utilizar sistemas de bloqueio ou desconexão automática da sessão de um utilizador após um período de 10 minutos de inactividade ou inferior.

Os utilizadores deverão bloquear a sessão de login do sistema ao se ausentarem da estação de trabalho.

Ligações de Rede Externa

Todas as ligações de sessão direcionadas aos computadores do Banco Comercial Angolano, a partir de redes externas, devem estar protegidas por VPN (Rede Privada Virtual) ou outra ligação segura. Deve evitar-se o referido acesso usando computadores públicos.

Autorização para acesso remoto a infraestrutura por VPN deve ser autorizada pelo supervisor directo e baseia-se numa lista de verificação de factores relevantes.

Correio Eletrónico (email)

Aos colaboradores do Banco que usam computadores no seu dia-a-dia de serviço, serão providenciados um endereço eletrónico e os respetivos privilégios.

Toda comunicação de serviço deve ser enviada através do endereço eletrónico do Banco. Os endereços de correio eletrónico pessoais não devem ser utilizados para tratar de assuntos oficiais do Banco, a menos que o colaborador em questão tenha obtido permissão da Direção de Gestão de Risco.

Todos os correios eletrónicos devem assumir uma aparência e tom profissionais.

Os colaboradores do Banco Comercial Angolano devem abster-se de enviar números de cartão de crédito, palavras passe, ou outra informação sensível que possa ser intercetada.

Todos os colaboradores do Banco devem ainda utilizar uma assinatura de e-mail padronizada, a qual inclui nome completo, cargo, endereço de serviço, extensão e número telefónico de serviço

Antes de abrir um email deverá confirmar que o remetente é conhecido ou pelo menos não se trate de uma fonte suspeita.

Nunca deverá abrir anexos de correios cujas fontes não sejam conhecidas.

Não responder mensagem de “spam”. Deverá sim apagá-las.

Sendo a solicitação de “password” proibida por essa política, não responda positivamente a correios dessa natureza independentemente da origem da solicitação

Proíbe-se:

- O envio de e-mail não solicitados a clientes e a potencial clientes,
- O envio de mensagens emocionais,

- O sobrecarregamento de caixas de correio eletrónico, com mensagens de material de campanha política, religiosas, ou outras,
- Transmitir material censurável (exemplo: pornografia, “booling”, etc.) ou outro material não relacionada com as atividades comerciais do Banco.

Serviços de Internet

Os Colaboradores do Banco têm acesso à Internet para desempenharem as suas funções, mas este acesso pode ser retirado a qualquer momento, à discrição do supervisor do colaborador. O acesso à Internet é monitorizado para garantir que os colaboradores não naveguem por sites não relacionados com as suas funções e, ainda, para assegurar que as deliberações da política de segurança sejam respeitadas.

Os colaboradores do Banco devem ter um cuidado especial para garantir que não representem o Banco em grupos de discussão na Internet, nem noutros fóruns públicos, a não ser que tenham recebido uma autorização prévia da Direção de Gestão de Risco do Banco para fazê-lo.

Toda a informação recebida da Internet deve ser considerada como suspeita, até que tenha sido confirmada por fontes fiáveis.

Os colaboradores do Banco não devem colocar qualquer tipo de material da instituição em qualquer sistema informatizado de acesso público, tal como a Internet, a menos que a colocação da mesma tenha sido autorizada pela Direção de Tecnologia de Informação ou a Direção de Gestão de Risco.

Prevenção de Roubos

Todos os computadores e equipamento de rede do Banco Comercial Angolano situados em escritórios abertos devem dispor de dispositivos antirroubo. Os servidores LAN e outros sistemas multiutilizador devem ser colocados em armários trancados ou em salas de computador trancadas.

Os computadores portáteis devem dispor de cabos anti roubo, ser colocados em armários trancáveis, ou quando não em uso activo, mas situados em escritórios abertos, devem dispor de outros tipos de sistema anti roubo. Os computadores e o equipamento inerente às redes informáticas não podem ser removidos dos escritórios do Banco Comercial Angolano, a menos que a pessoa em questão tenha obtido um passe do gerente do edifício bancário.

7.9. Cópias de Segurança / Backups

Responsabilidades pelas Cópias de Segurança– A Direcção de Tecnologias de Informação deve instalar, ou disponibilizar a assistência técnica necessária para permitir a instalação de cópias de segurança / Backups.

Todas as cópias de segurança com informação crítica ou sensível devem ser armazenadas num local fora do Banco e devem caracterizar-se por controlos ao acesso físico e por um sistema de encriptação.

No caso das aplicações que processam a informação de produção crítica, deve preparar-se um plano de contingência.

É responsabilidade do detentor da informação garantir que este plano foi adequadamente desenvolvido, é atualizado regularmente e sujeito periodicamente a prova.

Divulgação Externa de Informação acerca da Segurança de Informação - Informação sobre as medidas de segurança de computadores e sistemas computorizados e de rede do Banco Comercial Angolano é confidencial e não deve ser divulgada a pessoas que não sejam utilizadores autorizados dos sistemas envolvidos, salvo se a autorização da Direção de Gestão de Risco tenha sido obtida. Por exemplo, a publicação dos números telefónicos dos modems ou outra informação referente a informação de acesso, contida em diretórios, é proibida. A divulgação de moradas de e-mail é permissível.

Direitos de Propriedade sobre o Material Desenvolvido - Enquanto a serviço do Banco, os colaboradores do banco têm de conceder ao Banco os direitos exclusivos advindos das patentes, direitos de autor, invenções ou outra propriedade intelectual por eles elaborados ou desenvolvidos. Todos os programas informáticos e documentação gerados ou providenciados por colaboradores do Banco para benefício do Banco Comercial Angolano são propriedade do Banco. O Banco Comercial Angolano reivindica os direitos de propriedade sobre o conteúdo de todos os sistemas de informação sob seu controlo. O Banco Comercial Angolano reserva o direito de aceder a esta informação e de usá-la sempre que achar conveniente.

Direito de Revistar e Monitorizar - A Administração do Banco reserva-se ao direito de, em qualquer altura, monitorizar, inspeccionar ou revistar os sistemas de informação do Banco. Esta inspecção pode ocorrer com ou sem o consentimento, presença ou conhecimento dos colaboradores envolvidos. Os sistemas de informação sujeitos a revisões incluem as áreas de armazenamento de ficheiros,

sistema(s) de e-mail, etc. Todas as buscas desta natureza devem ser conduzidas após se ter obtido autorização do Gabinete Jurídico e/ou Direção de Gestão de Risco.

Visto os computadores e redes do Banco Comercial Angolano serem disponibilizados apenas para fins comerciais, os colaboradores do banco não devem ter qualquer expectativa de privacidade no que concerne à informação armazenada nestes sistemas de informação, ou através deles, enviada. A Administração do Banco através da Direção de Tecnologias de Informação, reserva o direito de remover dos seus sistemas de informação qualquer material que achar ser ofensivo ou potencialmente ilegal.

7.10. Uso Pessoal dos Sistemas de TI

Os sistemas de informação do Banco Comercial Angolano destinam-se apenas ao uso comercial.

O uso pessoal da **Internet** é permissível, desde que o mesmo não consuma recursos que, de outra forma, poderiam ser usados para fins comerciais. Isto é, não interfira com a produtividade do Banco e/ou não se sobreponha a qualquer actividade comercial.

Os jogos de computador que vêm com os sistemas operativos podem ser desenvolvidos durante o(s) intervalos laborais previstos (exemplo durante a hora do almoço), considerando não interferir com a produtividade dos colaboradores do Banco. Os jogos que tomem a forma de um conjunto de programas separado são proibidos.

Comportamento Impróprio - A Administração do Banco Comercial Angolano reserva-se ao direito de, em qualquer altura, anular os privilégios oferecidos pelo sistema aos utilizadores. Um comportamento que interfira com o funcionamento normal e característico dos sistemas de informação do Banco, que afecte de modo adverso a capacidade de outros usarem estes sistemas de informação, ou que prejudique ou ofenda os outros, não é permitido.

Ferramentas que podem Comprometer a Segurança A menos que especificamente autorizado pela Direcção de Tecnologias de Informação, os colaboradores do Banco não devem adquirir, possuir ou utilizar ferramentas de hardware ou software que possam ser empregues para avaliar ou comprometer a segurança dos sistemas de informação.

Exemplos de tais ferramentas incluem: aquelas que descobrem as palavras de passe secretas ou as vulnerabilidades do sistema.

Actividades Proibidas - A pirataria informática, as tentativas de adivinhar as palavras passe, a descodificação de ficheiros, as tentativas de instalar software pirateado ou outras tentativas similares que possam comprometer as medidas de segurança serão consideradas como sendo infrações graves da política interna do Banco. Proíbe-se o acesso directo que contorne as medidas de segurança do sistema e as partidas e brincadeiras que comprometam as medidas de segurança dos sistemas.

Aplicações Informáticas dos Utilizadores Finais - Todas as Aplicações Informáticas dos utilizadores finais, tais como as folhas de cálculo elaboradas pelos próprios utilizadores ou as bases de dados usadas como aplicações comerciais críticas, devem ser colocadas sob uma gestão formal. Os controlos chave que devem ser implementados são a proteção das palavras de passe, o controlo do acesso aos sistemas, o planeamento das cópias de segurança e da continuidade das actividades comerciais do Banco. Deve ter-se o cuidado de indigitar um sucessor para o operador principal, no caso de ele não estar disponível.

7.11. Aprovação e Revisão

As PSI são aprovadas pela CE, comprometendo-se o mesmo também a instruir a sua divulgação, no todo ou em parte, as PSI, normas e processos, a todos os colaboradores internos e a terceiros.

A actualização das PSI (incluindo a PGSI) é proposta pelo DSI, revista pelo GCO e DGR e é aprovada pela CA. Esta revisão tem por objectivo melhorar a eficácia da segurança da informação, sendo efectuada com base nos seguintes elementos de análise:

- Alterações no contexto externo ou interno que alterem o perfil de risco (e.g. alterações significativas no ambiente de SI);
- Relatórios de auditoria internas e externas;
- Incidentes de segurança ocorridos no período;
- Acções preventivas e correctivas; e
- Alterações à regulamentação externa e normativos internos.

As PSI deverão ser revistas numa base anual, salvo necessidade extraordinária que justifique a revisão antecipada.

7.12. Divulgação e Acesso

A PGSI 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 aos destinatários relevantes.

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

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.

7.13. Incumprimento

Qualquer incumprimento ou violação das políticas de segurança da informação deve ser imediatamente reportado à DGR sendo da competência deste 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 de nível grave para o Banco, deverá reportar a DGR deverá apresentar, de imediato, o caso para apreciação em sede da CE e 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, o 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.

7.14. 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 análise dos riscos deve constituir ferramenta de orientação, nomeadamente:

    a) Na identificação dos riscos em função do potencial impacto e probabilidade;

    b) Na identificação de medidas de mitigação dos riscos aos quais a informação está exposta; e

    c) Na priorização de acções para mitigação dos riscos identificados, tais como implementação de novos controlos, regras, procedimentos e reformulação de sistemas, 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 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.

7.15. Excepções

No caso de impossibilidade de implementação de qualquer das orientações de controlo previstas nas PSI, normas e procedimentos, 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.

8. Denuncias

Denúncias Obrigatórias - Todas as suspeitas de contravenções de política, presença de vírus informáticos e outras condições que possam comprometer a informação ou os sistemas de informação do Banco Comercial Angolano, devem ser imediatamente denunciadas a Direção de Tecnologia de Informação.

9. Código Disciplinar de Práticas e Litígios

O Banco Comercial Angolano encara a implementação desta política seriamente e não hesitará em agir em caso de não cumprimento. A recusa de um colaborador do Banco em cumprir com esta política pode ser considerada como uma infracção grave, resultando na instauração de um processo disciplinar cuja sanção será o despedimento.

Os requisitos legais, de acordo com o acordo formal entre o Banco Comercial Angolano e Terceiros deverão estar alinhados a essa política.

10. Directrizes de Implementação

Esta política deve ser comunicada através de todos os canais disponíveis aos respectivos supervisores directos que, por sua vez, deveriam comunicá-la a todos os seus subordinados. Onde aplicável, devem definir-se processos específicos com vista à implementação dos controlos requeridos por esta política.

11. Vigência

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