Política de Segurança da Informação

Índice

1. OBJECTO 4

2. ÂMBITO E OBJECTIVO DA POLÍTICA 4

3. ENQUADRAMENTO LEGAL 5

4. DEFINIÇÕES 5

5. PRINCÍPIOS GERAIS 6

5.1 Definição de Segurança da Informação 6
5.2 Consciencialização Para a Segurança da Informação 8
5.3 Compromisso Para a Segurança da Informação 9
5.4 Tratamento de Não Conformidades 10
5.5 Tratamento de Excepções 10

6. ESTRUTURA ORGANIZACIONAL 11

6.1 Responsabilidades 11
6.2 Estrutura Documental 12

7. PRINCÍPIOS GERAIS 13

7.1 Propriedade da Informação 13
7.2 Tratamento da Informação 14
7.3 Tratamento de Incidentes de Segurança 14
7.4 Gestão de Riscos 15
7.5 Gestão de Continuidade 15
7.6 Auditoria e Conformidade 15
7.7 Controlos de Acesso 15
7.8 Utilização do Correio Electrónico 15
7.9 Acesso à Internet 16
7.10 Gestão de Alterações 16
7.11 Gestão de Activos de Informação 16
7.12 Dispositivos Móveis 16
7.13 Computação na Nuvem 16
7.14 Redes Sociais 17
7.15 Aquisição, Desenvolvimento e Manutenção de Sistemas 17
7.16 Preservação de Evidências 17
7.17 Criptografia 18

8. RESPONSABILIDADE DA POLÍTICA 18

9. INCUMPRIMENTOS 18

10. INTERPRETAÇÃO 18

11. DIVULGAÇÃO 18

12. ALTERAÇÕES E APROVAÇÕES 19

13. DOCUMENTOS RELACIONADOS..... 19

14. ANEXO I – MODELO ORGANIZACIONAL DA SEGURANÇA DA INFORMAÇÃO ERRO! MARCADOR NÃO DEFINIDO.

15. ANEXO II – ESTRUTURAS ORGANIZACIONAIS DA SEGURANÇA DA INFORMAÇÃO ..... ERRO! MARCADOR NÃO DEFINIDO.

16. ANEXO III – FRAMEWORK DE DOCUMENTAÇÃO DA SEGURANÇA DA INFORMAÇÃO ..... ERRO! MARCADOR NÃO DEFINIDO.

1. Objecto

A Política de Segurança da Informação (PSI) enquadra-se no nível estratégico da estrutura documental do Sistema de Gestão de Segurança da Informação (SGSI) do Banco Económico, define e promove a estratégia de Segurança da Informação. Adicionalmente, pretende dar suporte a tomada de decisões em âmbito através da determinação de prioridades.

Neste sentido, todos os documentos enquadrados nos níveis tático e operacional da estrutura documental (e.g., políticas específicas, normas, regulamentos, processos, procedimentos, modelos, evidências) devem ter como base o conteúdo vertido pelo presente documento e emanar as preocupações e considerações por ele estabelecidas.

2. Âmbito e Objectivo da Política

A Segurança da Informação é relevante para todos os tipos de informação e para todos os sistemas e aplicações que a armazenam, processam ou transferem, seja no contexto de simples sistemas de indexação e arquivo em papel ou em sistemas especializados e tecnologicamente avançados. A Segurança da Informação deverá ser ajustada, de forma proporcional, face à sua importância e valor.

Nesse sentido, o presente documento aplica-se directamente a todos os colaboradores do Banco Económico, independentemente da sua posição ou função, seja qual for o seu nível de responsabilidade e funções exercidas. Adicionalmente, também se aplica indirectamente a todos os parceiros, a todos os fornecedores e outras entidades ou utilizadores que tenham acesso a uma rede de comunicação ou sistema de informação gerido pelo Banco Económico.

Serve o presente documento para explanar a estrutura da Segurança da Informação do Banco Económico, de modo a atingir os seguintes objectivos:

- Definir a estratégia para a Segurança da Informação, alinhada com o Modelo Organizacional da mesma;
- Fomentar uma cultura de segurança entre todo o universo Banco Económico;
- Sensibilizar os utilizadores para a importância da Segurança da Informação e para a literacia neste âmbito; e
- Promover a Segurança da Informação como um propósito indispensável a alcançar.

3. Enquadramento Legal

A instituição da presente Política obedece a exigência do quadro legal aplicável, composto, essencialmente pelos seguintes diplomas:

- Resolução n.º 33/19, de 09 de julho (União Africana) aprovada pela Assembleia Nacional aos 23 de maio de 2019 - Convenção da União Africana sobre CiberSegurança e Protecção de Dados Pessoais, e tem por objectivo combater as Violações da Privacidade através da recolha, tratamento, transmissão, armazenamento e utilização de dados pessoais;
- Lei n.º 7/17, de 16 de fevereiro (Assembleia Nacional) - Lei de Protecção das Redes e Sistemas Informáticos, que estabelece o regime jurídico sobre as medidas de Protecção das Redes e Sistemas Informáticos;
- Lei n.º 22/11, de 17 de junho (Assembleia Nacional) - Lei da Protecção de Dados Pessoais, que estabelece as regras jurídicas aplicáveis ao tratamento de dados pessoais, com o objectivo de garantir o respeito pelas liberdades públicas e os direitos e garantias fundamentais das pessoas singulares;
- Aviso n.º 08/2020, de 02 de abril (Banco Nacional de Angola) – estabelece regras sobre a componente de segurança cibernética, bem como os 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 a supervisão do Banco Nacional de Angola; e
- Instrutivo n.º 10/2020, de 29 de maio (Banco Nacional de Angola) – estabelece o dever de comunicação de incidentes de segurança cibernética ao Banco Nacional de Angola.
- Directiva 05/DSB/DRO2022, de 02 de junho (Banco Nacional de Angola) – Gestão de Riscos Associados às Tecnologias de Informação e Comunicação e à Segurança Cibernética.

4. Definições

Neste documento são referidos diversos conceitos, relacionados com a Segurança da Informação, que importa definir previamente, nomeadamente:

- **Activo**: qualquer bem, tangível ou intangível, que agrega valor para o Banco;
- **Activo de Informação**: representação de conhecimento que agrega valor para o negócio e para a actividade operacional do Banco Económico, independentemente do tipo de suporte e forma utilizados para o seu tratamento;
- **Controlo de Segurança**: uma salvaguarda ou medida prescrita para um sistema de informação e comunicação projectada para proteger a confidencialidade,

integridade e disponibilidade da informação. Os controlos podem ser de vários tipos, como por exemplo físicos, administrativos ou tecnológicos;

- **Governance**: garantia de que a Segurança da Informação se encontra alinhada com os objectivos de negócio, através do desenvolvimento de processos de gestão eficientes e eficazes que suportem a tomada de decisão;
- **Incidente de Segurança da Informação**: qualquer evento adverso, confirmado ou sob suspeita, que impacte a confidencialidade, integridade e disponibilidade dos activos de informação do Banco Económico;
- **ISO/IEC 27000:** família de normas internacionais que fornecem recomendações no sentido de auxiliar as organizações a estabelecer, e melhorar continuamente, a Segurança da Informação. Esta série de normas compreendem um conjunto de melhores práticas sobre gestão de Segurança da Informação e gestão de risco, no contexto de um Sistema de Gestão de Segurança da Informação;
- **Sistema de Gestão de Segurança da Informação**: abordagem sistemática para gerir e proteger os activos de informação do Banco Económico, sendo materializado por um conjunto de políticas, normas e procedimentos, bem como os controlos que definem toda a estratégia e operacionalização da Segurança da Informação. Os tipos de controlos que devem ser implementados são maioritariamente determinados com base nos resultados de avaliações de risco, mas também pelas exigências das partes interessadas, definidas pelo contexto do próprio Banco; e
- **Sistema de Informação e Comunicação**: grupo de componentes inter-relacionados que trabalham colectivamente para executar acções de recolha, armazenamento e processamento, com o objectivo de converter dados em activos de informação que podem ser utilizados para dar suporte a tomada de decisão e a actividade operacional do Banco.

5. Princípios Gerais

5.1 Definição de Segurança da Informação

A Segurança da Informação é fundamental, fruto do ambiente do negócio e dos avanços tecnológicos. A informação e respectivos repositórios são activos relevantes e críticos para o Banco Económico. Independentemente da forma e do meio de aquisição, armazenamento, tratamento e transmissão de activos de informação, estes devem ser adequadamente protegidos. A Segurança da Informação endereça a protecção dos activos de informação de um amplo conjunto de ameaças através de um processo de gestão de

risco, garantindo a continuidade da actividade operacional por forma a maximizar o retorno em investimentos efectuados.

De acordo com o seu Aviso n.º 08/2020, o Banco Nacional de Angola estabelece que as Instituições devem definir e implementar um conjunto de políticas, procedimentos e controlos de segurança, baseados em normas e boas práticas internacionalmente aceites, que "visam assegurar a confidencialidade, integridade e a disponibilidade das redes, dados e dos sistemas de informação utilizados".

Nesse sentido, e tendo por base a série de normas internacionais ISO/IEC 27000, a Segurança da Informação do Banco Económico é formalmente definida como a preservação da **confidencialidade**, **integridade**, **disponibilidade** da informação.

Figura 1 - Pilares da Segurança da Informação

Para um melhor entendimento importa esclarecer que os três pilares basilares da Segurança da Informação para o Banco Económico, são propriedades da informação nas seguintes medidas:

- **Confidencialidade**: Garantia de que a informação é acedida apenas por pessoas que têm autorização para tal;
- **Integridade**: Salvaguarda da exactidão da informação e dos métodos de processamento; e
- **Disponibilidade**: Garantia de que os utilizadores autorizados têm acesso à informação e activos correspondentes sempre que necessário.

Estes conceitos são complementares e devem ser entendidos como um todo. Assim, só garantindo que a informação é acessível apenas por aqueles que têm autorização para o fazer, que a sua integridade e completude é rigorosa e que, quando necessário, todos os

utilizadores autorizados têm-lhe acesso, é que podemos afirmar que a Segurança da Informação é eficaz.

Adicionalmente, o Banco Económico tem em consideração outras propriedades e conceitos relativamente à Segurança da Informação, nomeadamente:

- **Autenticidade**: que assegura que a informação é da fonte anunciada, não sofrendo alterações do seu conceito básico ou do seu significado. Aplica-se também ao processo através do qual é validada a identidade de um utilizador;
- **Não Repudiação**: que garante que uma transacção é reconhecida, ou seja, que não pode ser negada pelo emissor e/ou recetor; e
- **Privacidade**: Salvaguarda de um direito fundamental de cada pessoa singular que deve ser assegurado pelo Banco Económico, aquando do tratamento de dados pessoais.

5.2 Consciencialização Para a Segurança da Informação

A Segurança da Informação diz respeito a todos os níveis do Banco Económico, estando a respetiva eficácia dependente da interiorização e consciencialização por todo o seu universo, dos seguintes princípios:

- **Sensibilização**: O universo Banco Económico deve ser conhecedor da necessidade da existência de infraestruturas e sistemas de informação e comunicação seguros, e de qual poderá ser o seu papel na manutenção e incremento dessa segurança;
- **Responsabilidade**: Todo o universo Banco Económico deve conhecer e respeitar todas as normas de Segurança da Informação do Banco Económico;
- **Equanimidade**: todas as políticas, normas e regras de Segurança da Informação devem ser obedecidas por todos, sem distinção de cargo ou função;
- **Celeridade**: O universo Banco Económico deve agir de maneira célere e cooperativa para prevenir, detectar e responder a incidentes de Segurança da Informação;
- **Ética**: O universo Banco Económico deverá respeitar os legítimos interesses dos demais;
- **Gestão de Risco**: Devem ser conduzidas análises de risco, de forma a identificar ameaças e vulnerabilidades e, consequentemente, ser assegurado um nível aceitável de risco para o Banco Económico;
- **Desenho, Desenvolvimento e Implementação Segura**: A segurança deve ser incorporada como um elemento imprescindível nos processos de aquisição,

desenvolvimento e manutenção de todos os sistemas de informação e comunicação do Banco Económico;

- **Gestão de Segurança**: Deve ser adotada uma abordagem global e detalhada à gestão da Segurança da Informação, envolvendo todo o universo Banco Económico de forma coordenada e integrada, de forma a atingir os objectivos delineados pelo seu SGSI;
- **Proteção de Dados Pessoais e Privacidade:** Deve ser adotada uma abordagem de proteção de dados pessoais por forma a garantir a salvaguarda dos mesmos ao longo de todo o seu ciclo de vida. A privacidade dos dados pessoais deverá ser considerada enquanto salvaguarda de um direito fundamental cada pessoa singular;
- **Revisão e Reavaliação**: Periodicamente, deve ser revista e reavaliada a segurança da infraestrutura, sistemas e informação modificando-se, sempre que necessário, qualquer requisito estabelecido pelo SGSI; e
- **Transparência**: Deve haver transparência no tratamento da informação, observando os critérios legais. Devem divulgar-se, atempadamente, a todos os colaboradores do Banco Económico todas as políticas, normas, regulamentos, processos e procedimentos de Segurança da Informação.

5.3 Compromisso Para a Segurança da Informação

A visão estratégica da Segurança da Informação no Banco Económico vai para além da implementação de controlos pontuais. Como tal, todas as acções devem ser alinhadas com os princípios e objectivos vertidos no Modelo Organizacional de Segurança da Informação e geridas de forma integrada.

Para assegurar o cumprimento dos seus objectivos estratégicos, o Banco Económico assume o compromisso de:

- Assegurar o cumprimento dos princípios e deveres da legislação aplicável no âmbito da Segurança da Informação;
- Garantir o alinhamento das acções de Governance, gestão e operação dos sistemas de informação e comunicação do Banco Económico com o Modelo Organizacional de Segurança da Informação; e
- Estabelecer, implementar e continuamente melhorar a Segurança da Informação como um todo e, em particular, o seu SGSI.

Os benefícios do estabelecimento da Segurança da Informação traduzem-se na redução dos riscos para a actividade operacional, bem como no aumento da conformidade para

com a legislação e regulamentação aplicável, na protecção da reputação da instituição, na maior confiança por parte dos seus Clientes e partes interessadas e numa gestão eficaz dos seus recursos.

A operacionalização desta política deve ter em conta a formalização e aprovação do Modelo Organizacional de Segurança da Informação, do qual é emanada a premissa de que a PSI figura como pilar orientador do desenvolvimento de qualquer documento do nível tático e operacional.

5.4 Tratamento de Não Conformidades

Os colaboradores que tenham acesso a informações do Banco Económico sujeitam-se às diretrizes e requisitos definidos por esta política, bem como pela restante documentação de Segurança da Informação, e são responsáveis por garantir a segurança das informações a que tenham acesso, no decorrer das suas funções.

As acções que violem a PSI, bem como as normas, regulamentos, processos, procedimentos e regras, que quebrem os controlos de Segurança da Informação podem ser passíveis da aplicação de sanções disciplinares, civis e/ou penais em conformidade com a legislação aplicável.

As sanções disciplinares têm em conta a proporcionalidade e especificidade da acção praticada. Estas estão em conformidade com os procedimentos definidos nos processos disciplinares. Dependendo do tipo de infracção, as sanções disciplinares podem incluir ir de simples admoestação verbal até um despedimento disciplinar por justa causa.

Em todos os casos aplica-se o previsto na legislação em vigor, bem como nas políticas, normas, regulamentos e procedimentos internos do Banco.

5.5 Tratamento de Excepções

Os objectivos de Segurança da Informação são facilmente alcançados se os requisitos de Segurança da Informação e os respectivos processos e procedimentos forem idênticos para todas as Direcções, unidades orgânicas e serviços do Banco Económico.

Não obstante, há noção de que as normas, processos e procedimentos nem sempre são viáveis para uma área específica, projecto a decorrer, novo equipamento ou aplicação instalados.

É previsível que, no âmbito da normal actividade do Banco, surjam situações ou cenários que não podem ser tratados de forma eficaz dentro dos requisitos estabelecidos pela PSI ou pela restante documentação de Segurança da Informação.

Embora o desvio de processos e procedimentos estabelecidos centralmente seja altamente desencorajado, nalguns momentos os processos e procedimentos estabelecidos no Banco Económico, podem e devem ser alterados, desde que a alternativa apresentada seja suportada por uma justificação forte e provida de recursos suficientes para implementar adequadamente e manter os requisitos alternativos.

Para tratar atempadamente este tipo de situações e paralelamente continuar a assegurar a segurança da infraestrutura, sistemas e informação do Banco, deve ser seguido o Procedimento de Gestão de Exceções do SGSI que determina, em traços gerais, a realização de uma avaliação do risco inerente à excepção.

6. Estrutura Organizacional

6.1 Responsabilidades

As responsabilidades e autoridades específicas no âmbito da Segurança da Informação devem ser consultadas no documento de Estruturas Organizacionais de Segurança da Informação. No entanto, todos os utilizadores, incluindo o Conselho de Administração, a Comissão Executiva, bem como todos aqueles que fazem parte das Estruturas Organizacionais definidas para a Segurança da Informação, têm a responsabilidade de manter um comportamento responsável e consistente com os princípios e objectivos de Segurança da Informação, vertidos no Modelo Organizacional de Segurança da Informação.

Para tal, os utilizadores devem conhecer as instruções, regras e sanções relativas ao funcionamento dos recursos que utilizam, devendo ainda:

- Aceitar plenamente as regras e responsabilidades definidas neste documento e nas restantes normas e procedimentos internos do Banco Económico sobre a utilização dos recursos de tratamento da informação, incluindo, em especial os recursos de TI do Banco;
- Cumprir com o código de conduta e demais instrumentos de ética profissional estabelecidos pela legislação em vigor relacionadas com a actividade do sector financeiro, com especial atenção aos requisitos definidos pela autoridade de controlo e supervisão;
- Responder por actos que violem as regras de utilização dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na documentação referente a utilização destes recursos e, se aplicável, às penalidades impostas pela legislação em vigor;

- Comunicar imediatamente qualquer falha ou não conformidade identificada na Segurança da Informação, através do envio de uma mensagem para gsi@bancoeconomico.ao, de acordo com o procedimento de notificação de incidentes;
- Não se fazer passar por outra pessoa ou dissimular a sua identidade enquanto utilizar os recursos computacionais;
- Responsabilizar-se pela sua identidade electrónica, palavras-passe, credenciais de autenticação, autorização ou outro dispositivo de segurança, não partilhando com ninguém esta informação;
- Responder pela utilização indevida da sua conta e dos recursos computacionais em qualquer circunstância;
- Recolher, aceder, tratar e armazenar a dados pessoais apenas quando legitimado para tal, de acordo com a legislação em vigor relativa à privacidade e proteção de dados pessoais, bem como em conformidade com a documentação interna devidamente aprovada e actualizada; e
- Divulgar informação confidencial e interna apenas nas situações previstas pela documentação interna e nas situações previstas na lei, devendo, para tal efeito, recorrer a aconselhamento deontológico e jurídico.

6.2 Estrutura Documental

Para assegurar a gestão efectiva de Segurança da Informação deve ser criada e mantida uma estrutura documental responsável pela orientação, planeamento, implementação, manutenção e melhoria das práticas de Segurança da Informação. Esta estrutura deverá abranger vários níveis, considerando a necessidade de descentralizar as responsabilidades da gestão de Segurança da Informação pelas várias áreas do Banco Económico.

A estrutura documental de Segurança da Informação do Banco está definida no documento *Framework* de Documentação de Segurança da Informação.

Os seguintes documentos comprovativos são relevantes para esta política de segurança da informação e fornecem informações adicionais sobre a sua aplicação:

- Declaração de Aplicabilidade
- Plano de Resposta a Incidentes de Segurança
- Política de Criptografia
- Política de Controlo de Acessos
- Política de Privacidade e Protecção de Dados Pessoais
- Norma de Gestão da Segurança de Informação na Relação com Fornecedores

- Norma de Utilização Aceitável
- Norma de Computação em Nuvem
- Norma de Dispositivos Móveis
- Norma de BYOD
- Norma de Teletrabalho
- Norma de Anti-Malware
- Norma de Backup
- Norma de Registo e Monitorização
- Norma de Desenvolvimento Seguro de Software
- Norma de Gestão de Vulnerabilidades Técnicas
- Norma de Segurança de Rede
- Norma de Mensagens Eletrónicas
- Norma de Retenção e Protecção de Registos
- Norma de Ecrã e Mesa Limpa
- Norma de Segurança dos Recursos Humanos
- Norma de Gestão de Incidentes de Segurança da Informação
- Norma de Classificação da Informação
- Norma de Gestão de Segurança da Operações
- Norma de Gestão de Segurança da Informação na Continuidade de Negócios
- Norma de Palavra-Passe
- Procedimento de Due Diligence Para a Segurança da Informação
- Procedimento de Gestão de Acessos Lógicos
- Processo de Gestão de Acesso ao Utilizador

7. Princípios Gerais

Esta política aplica-se tanto no ambiente informatizado, quanto nos meios convencionais de processamento, comunicação e armazenamento da informação e rege-se pelos princípios abaixo definidos.

7.1 Propriedade da Informação

a) Toda informação criada, armazenada, transportada ou descartada pelos colaboradores do Banco Económico, no exercício das suas actividades, é da propriedade da instituição e é protegida segundo as diretrizes descritas nesta política e nas regulamentações em vigor;

b) O acesso aos activos de informação do Banco Económico por terceiros deve estar condicionado a uma solicitação e autorização formal providenciada pelo gestor da informação antes da sua disponibilização; e
c) Nos casos de obtenção de informação de terceiros, o gestor da área que solicitou a informação deverá, se necessário, providenciar junto do concedente a documentação formal relativa aos direitos sobre a informação de terceiros antes do seu uso.

7.2 Tratamento da Informação

a) Toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo Banco Económico é da responsabilidade do Banco Económico e são classificadas e protegidas adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita conforme as leis e regulamentos aplicáveis;
b) Toda informação institucional, se electrónica, estará armazenada nos servidores de ficheiros e bases de dados sob gestão e administração da área competente e, se não eletrónica, mantida em local que a salvaguarde adequadamente;
c) Toda informação institucional, sob a forma electrónica, estará salvaguardada por meio de cópia de segurança sob administração da área competente e mantida em local que a proteja adequadamente e garanta sua recuperação em caso de perda da informação original;
d) No descarte de informação institucional são observadas as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a tempo de retenção previsto na legislação; e
e) A informação classificada conforme a legislação vigente, produzida, armazenada e transportada em meios electrónicos, utilizará criptografia compatível com o grau de sigilo, em especial as informações de autenticação dos utilizadores das aplicações.

7.3 Tratamento de Incidentes de Segurança

a) O Banco Económico deve estabelecer e gerir a infraestrutura necessária para fins de registo e resposta aos incidentes de segurança de informação;
b) O Banco Económico deve estabelecer uma equipa responsável pela gestão de incidentes relacionados com a segurança de informação; e
c) O utilizador de activos de informação do Banco Económico é responsável por notificar, imediatamente, incidentes que afectam a segurança da informação ou o incumprimento das disposições desta política.

7.4 Gestão de Riscos

a) O Banco Económico deve estabelecer e manter uma política de Gestão de Riscos com foco na segurança de informação e comunicação com vistas a minimizar possíveis impactos associados aos activos de informação e comunicações, baseando-se nas melhores práticas e normas complementares aplicáveis.

7.5 Gestão de Continuidade

a) O Banco Económico deve estabelecer e manter um Plano de Gestão de Continuidade de Negócio com foco na segurança da informação e comunicações, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de tecnologia de informação que suportam as operações do Banco Económico; e

b) Todos sistemas ou serviços críticos do Banco Económico deverão estar suportados pelo Plano de Gestão de Continuidade de Negócio.

7.6 Auditoria e Conformidade

a) A utilização dos recursos de tecnologias de informação e comunicação disponibilizados pelo Banco Económico é passível de monitorização e auditoria, e serão implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade dessa utilização; e

b) Serão mantidos procedimentos, tais como: registos de auditoria, rastreamento, acompanhamento, controlo e verificação de acessos para todos os sistemas corporativos e rede interna do Banco Económico.

7.7 Controlos de Acesso

a) O colaborador do Banco Económico que utilizar os recursos de tecnologias de informação e comunicação terá uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em norma específica;

b) O gestor da informação é responsável pela concessão e revogação dos privilégios de acesso às informações, considerando sempre o princípio do menor privilégio; e

c) A identificação do colaborador, qualquer que seja o meio e a forma, é pessoal e intransferível, e permite o reconhecimento de maneira inequívoca.

7.8 Utilização do Correio Electrónico

a) O correio electrónico do Banco Económico tem seu uso exclusivo para colaboradores no exercício de suas funções. As regras de acesso e utilização são

definidas por norma específica, em conformidade com esta política e demais legislação em vigor.

7.9 Acesso à Internet

a) O acesso à Internet no ambiente de trabalho do Banco Económico está condicionado às necessidades dos colaboradores no exercício de suas funções e será regido por norma específica, em conformidade com esta política e demais legislação em vigor.

7.10 Gestão de Alterações

a) Qualquer alteração nos ambientes, que tenha sido homologada e testada, necessita ser documentada e registada; e
b) O Banco Económico manterá uma política de gestão de alterações de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

7.11 Gestão de Activos de Informação

a) O Banco Económico manterá um processo de Inventário e Mapeamento dos Activos de Informação objectivando a segurança das infraestruturas críticas que garantem suas Informações; e
b) O processo de Inventário e Mapeamento de Activos de Informação subsidiará o conhecimento, valorização, protecção e a manutenção dos seus activos de informação, será dinâmico, periódico, e estruturado, para manter a Base de Dados de Activos de Informação actualizada.

7.12 Dispositivos Móveis

a) Todo dispositivo móvel utilizado para aceder a rede do Banco Económico estará submetido aos padrões estabelecidos por norma específica; e
b) O Banco Económico proverá uma rede segregada da rede corporativa para acesso à Internet pelos visitantes.

7.13 Computação na Nuvem

a) O ambiente de computação em nuvem, a infraestrutura e canal de comunicação devem estar aderentes às políticas e normas de Segurança da Informação e Comunicação, estabelecidas pelo Banco Económico, e legislação em vigor;

b) O contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gestão do prestador de serviço; e
c) O armazenamento de informação em nuvem deverá estar respaldado por um contrato entre o Banco Económico e o provedor de serviço em nuvem, de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem.

7.14 Redes Sociais

a) A utilização institucional das redes sociais nos aspetos relacionados à Segurança da Informação e Comunicações deverá ser objeto de norma interna específica que, além da segurança de informação e comunicação, abordará a estratégia de comunicação social, o processo de gestão de conteúdo e outros aspetos relevantes;
b) A normatização interna de utilização segura das redes sociais deverá estabelecer directrizes, critérios, limitações e responsabilidades na gestão da utilização segura das redes sociais por utilizadores que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social a partir da infraestrutura das redes de computadores do Banco Económico;
c) Os perfis institucionais mantidos nas redes sociais devem ser administrados e geridos por um colaborador, ou estar sob a coordenação e responsabilidade deste; e
d) O Banco Económico nomeará um colaborador, ocupante de cargo efetivo, para a função de Responsável pela gestão e utilização segura de cada perfil institucional nas redes sociais.

7.15 Aquisição, Desenvolvimento e Manutenção de Sistemas

a) O Banco Económico estabelecerá critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e das actividades de manutenção; e
b) O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

7.16 Preservação de Evidências

a) Os equipamentos servidores de rede, bem como todo e qualquer outro activo de informação que assim o permita, devem ser configurados para armazenar registos

históricos de eventos (*Logs*) em formato que permita a completa identificação dos fluxos de dados e das operações de seus administradores;

b) Os registos devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos; e

c) Os activos de informação devem ser configurados de forma a armazenar seus registos de auditoria não apenas localmente, como também remotamente, por meio de tecnologia aplicável.

7.17 Criptografia

a) O Banco Económico deve estabelecer e manter uma política de Gestão de Controlos Criptográficos, garantindo a utilização adequada e eficaz da criptografia para proteger a confidencialidade, autenticidade e integridade dos activos de informação.

8. Responsabilidade da Política

Na sua actuação, cabe a Comissão Executiva, enquanto órgão com competência para deliberar, definir, formalizar, acompanhar a implementação, divulgação e periodicamente a revisão da Política de Segurança da Informação.

9. Incumprimentos

O incumprimento das regras descritas nesta Política pode ser considerado violação grave dos deveres de conduta e, em consequência, pode dar lugar à aplicação de medidas disciplinares, sanções contratuais ou a eventual responsabilidade criminal.

10. Interpretação

A presente política deve ser interpretada em conformidade com as normas legais e estatutárias que sejam aplicáveis cabendo, a Comissão Executiva resolver as dúvidas de interpretação que possam surgir.

11. Divulgação

A presente política será objecto de divulgação interna através da publicação na Intranet do Banco Económico.

A Direção de Capital Humano divulgará, igualmente, a mesma através de acções de formação (i.e. e-learning) para todos os colaboradores do Banco e Sociedades Participadas.

Para esclarecimento de qualquer dúvida relacionada com este documento ou com qualquer outro assunto relativo à temática de Segurança da Informação, os colaboradores deverão enviar um e-mail para gsi@bancoeconomico.ao (Gabinete de Segurança da Informação).

12. Alterações e Aprovações

A presente Política é revista com uma periodicidade mínima anual. O Gabinete de Segurança da Informação pode, no entanto, propor a Comissão Executiva a revisão da Política num prazo inferior, sempre que considere oportuno.

A presente Política foi aprovada pela Comissão Executiva do Banco, podendo apenas ser alterada por deliberação deste órgão.

13. Documentos Relacionados

ID Documento	*Documento*
BE-DOR004	Modelo Organizacional de Segurança da Informação
BE-DOR005	Estruturas Organizacionais de Segurança da Informação
BE-DOR006	*Framework* de Documentação de Segurança da Informação

Tabela 1 - Documentos Relacionados com a Política de Segurança da Informação