Política de Segurança da Informação

Novembro 2024

V 3.1

Histórico do Documento

Versões

Versão	Data de Revisão	Sumário de Mudanças	Direcção
1.0	09-07-2018	1. Versão inicial.	DTI
1.1	10.04.2019	1. Inclusão do Grupo de Segurança da Informação no modelo de responsabilidades e pequenos ajustes	DTI/NSI
2.0	02.10.2020	1. Reorganização da Política; 2. Alinhamento a Lei n.º 22/11, Aviso n.º 02/2020 e Instrutivo n.º 10/2020 no BNA	DTI/NSI
3.0	13.12.2022	1. Alteração da Estrutura Organizacional NSI para GSI; 2. Descrição de documentos relevantes para o SGSI	GSI
3.1	-26-11-2024	1. Ajuste na metodologia de acordo com a norma vigente; 2. Adequação a Directiva n.º 05/DRO/DSB/2022; 3. Ajuste a composição da política.	GSI

Validação – Grupo de Trabalho de Validação de Políticas

Versão	Data de Validação
3.1	26-11-2024

Aprovação – Comissão Executiva

Versão	Data de Aprovação
3.1	26-11-2024

Aprovação – Conselho de Administração

Versão	Data de Aprovação
3.1	29-11-2024

Distribuição

Área
Conselho de Administração
Comissão Executiva
Todas as Direcções do Banco Económico

Compromisso do Banco Económico

O Conselho de Administração do Banco Económico, ciente das suas responsabilidades perante os seus clientes, accionistas, parceiros e colaboradores, aprova e compromete-se a executar a presente Política.

Pedro Filipe Pedrosa Pombo Cruchinho Presidente do Conselho de Administração	
Jorge Manuel Torres Pereira Ramos Presidente da Comissão Executiva	
Katila Perera Santos Rigal Administradora Executiva	
Elisa de Jesus Francês Baptista Administradora Executiva	
Victor Hariany Neves Faria Administrador Executivo	
Emanuel Maria Maravilhoso Buchartts Administrador não Executivo Independente	

ÍNDICE

1. Enquadramento

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, doravante designado por Banco, define e promove a estratégia de Segurança da Informação.

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

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.

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.

3. Enquadramento Regulamentar

A presente Política foi elaborada com base nos seguintes diplomas:

- ISO/IEC 27001:2022 - Cláusula 5.2 - Política de Segurança da Informação2
- 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;
- 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. Objectivo

Esta Política visa:

- 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.

5. Definições

Para efeitos da presente Política, entende-se por:

- **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.

6. Princípios Gerais

6.1. A Dimensão, Perfil de Risco e o Modelo de Negócios

O Banco Económico, é identificado como uma instituição financeira de grande dimensão, cujo modelo de negócio é orientado aos segmentos de Empresa, Particulares e Private; promovendo produtos que atendam as necessidades de cada segmento, assim como adopta um posicionamento conservador relativamente aos riscos, com a implementação de diferentes medidas que visam monitorizar os mesmos.

6.2. A Natureza da Operações, Complexidade dos Produtos, Serviços, Actividades e Processos

O Banco Económico possui um catálogo de produtos e operações diversificadas e de reduzida complexidade, onde são encontrados diferentes processos e procedimentos

operacionais, como os créditos, depósitos, transferências, protocolos, seguros, sendo todos eles disponibilizados com diferentes tipologias.

6.3. Sensibilidade dos Dados e das Informações Corporativas e de Negócios

Todos os dados e/ou informações são processadas pelo Banco Económico, com recurso a aplicação das melhores práticas de segurança da informação e protecção de dados, assim como adequação a regulamentação aplicável.

6.4. Definição da 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.

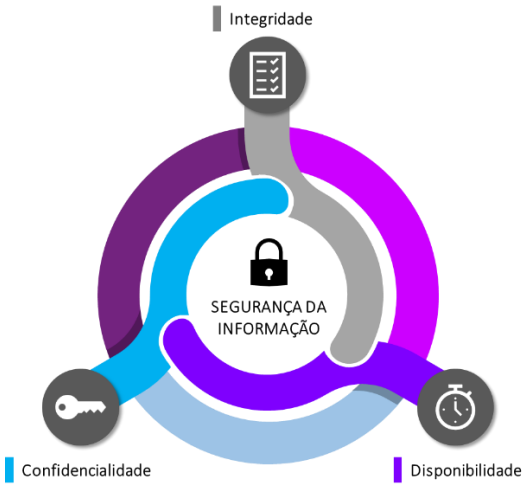

Figura 1 - Pilares da Segurança da Informação

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.

6.5. Consciencialização Para a Segurança da Informação

A Segurança da Informação diz respeito a todos os níveis de responsabilidade do Banco Económico, estando a respectiva eficácia dependente da interiorização e consciencialização por todo o seu universo (Colaboradores, Parceiros, Fornecedores e outras partes interessadas), dos seguintes princípios:

- **Sensibilização**: Ser conhecedora 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**: 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**: Agir de maneira célere e cooperativa para prevenir, detectar e responder a incidentes de Segurança da Informação;
- **Ética**: Respeitar os legítimos interesses dos demais;
- **Gestão de Risco**: Efectuar 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**: Incorporar a segurança 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**: Adoptar 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:** Adoptar 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**: Tratar de forma transparente toda a 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.

6.6. 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. Em uma declaração de compromisso, o Banco Económico, assegura o cumprimento dos seus objectivos estratégicos alinhados a Segurança da Informação.

6.7. Tratamento de Não Conformidade

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 Económico.

6.8. Tratamento de Excepções

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

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 Excepções do SGSI que determina, em traços gerais, a realização de uma avaliação do risco inerente à excepção.

7. Procedimentos Relacionados a Segurança de Informação

Esta política rege-se pelos princípios abaixo definidos.

7.1. Propriedade da Informação

a) Toda informação criada, armazenada, transportada ou descartada pelos colaboradores, 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 corporativo por terceiros é 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 mesma, se necessário, providenciará junto do concedente a documentação formal relativa aos direitos sobre a informação de terceiros antes da sua utilização.

7.2. Tratamento da Informação

a) Toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada é da responsabilidade do Banco Económico e são classificadas e protegidas adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade, disponibilidade e conforme as leis e regulamentos aplicáveis;

b) Toda informação institucional, se electrónica, estará armazenada nos servidores de ficheiros e bases de dados, estará salvaguardada por meio de cópia de segurança e sob gestão e administração da área competente e mantida em local que a proteja adequadamente e garanta sua recuperação em caso de perda da informação original, se não eletrónica, mantida em local que a salvaguarde adequadamente;

c) 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

d) 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) Estabelecer e gerir a infraestrutura necessária para fins de registo e resposta aos incidentes de segurança de informação;

b) Estabelecer uma equipa responsável pela gestão de incidentes relacionados com a segurança de informação; e
c) O utilizador de activos de informação é responsável por notificar, imediatamente, incidentes que afectam a segurança da informação ou o incumprimento das disposições desta política.

7.4. Gestão de Riscos

Estabelecer e manter uma política de gestão de riscos global, mas com a inserção da segurança de informação, 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 da Continuidade

a) Estabelecer e manter um plano de gestão de continuidade de negócio com a salvaguarda dos temas da segurança da informação, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de tecnologia de informação que suportam as operações da instituição; e
b) Todos sistemas ou serviços críticos do Banco Económico estarão 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, incluindo a rede interna do Banco Económico.

7.7. Gestão de Acesso

a) Todo o colaborador ao utilizar os recursos de tecnologias de informação e comunicação terá uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em Política, norma, procedimentos e processos específicos;
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. Correio Electrónico

O correio electrónico do Banco Económico é de utilização exclusiva 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. Serviço de Internet

O acesso ao serviço de 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) Um processo de Inventário e Mapeamento dos Activos de Informação será mantido, 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. Dispositivo Móvel

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 em Nuvem

a) O ambiente de computação em nuvem, a infraestrutura e canal de comunicação estarão aderentes às políticas e normas de Segurança da Informação e Comunicação e as políticas e normas de Protecção de Dados, estabelecidas pelo Banco Económico, alinhados a 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 terá o seu respaldo no 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 Comunicação será objecto 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 aspectos relevantes;
b) A norma interna de utilização segura das redes sociais estabelecerá 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 de TI 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, de cargo efectivo, 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 o 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 das Evidências

a) Os equipamentos 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

O Banco Económico estabelecerá e manterá uma norma 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. Estrutura Organizacional

8.1. 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, 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.

Todos os funcionários do Banco Económico são responsáveis por aderir a esta política e por contribuir para a segurança da informação dentro da organização, para tal, 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.suporte@bancoeconomico.ao (GSI Suporte), 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, palavra-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.

8.2. 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 Controlo de Acessos
- Política de Privacidade e Protecção de Dados Pessoais
- Norma de Criptografia

- 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

9. Incumprimento

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, ao Conselho de Administração resolver as dúvidas de interpretação que possam surgir.

11. Divulgação

A presente Política será objecto de divulgação, para consulta, no *site* de Intranet e Internet do Banco.

12. Alterações e Aprovação

A presente Política é revista com uma periodicidade mínima anual, podendo, no entanto, ao Gabinete de Segurança da Informação propor ao Conselho de Administração a revisão da mesma num prazo inferior, sempre que se considere oportuno.

A Política de Segurança da Informação foi aprovada pelo Conselho de Administração do Banco Económico.

13. Considerações Finais

A coordenação e execução da Política de Segurança da Informação é responsabilidade do Gabinete de Segurança da Informação, onde deve ser dirigida quaisquer questões relacionadas a mesma.

14. Revogação

A presente Política revoga a versão anterior publicada em 13 de dezembro de 2022.

15. 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

16. Anexo I–Modelo Organizacional da Segurança da Informação

Modelo Organizacional da Segurança da Informação

Versões

Versão	Data de Revisão	Sumário de Mudanças	Direcção
1.0	02-10-2020	1. Versão inicial.	DTI/NSI
1.1	21-04-2022	1. Adição da Estrutura Organizacional do GSI e respectivo E-mail.	GSI
1.2	-	1. Adequação a Nova Estrutura Orgânica e Nomenclatura.	GSI

1. Enquadramento

Nesse sentido, o presente documento define os vectores que constituem o âmbito de alto nível da Segurança da Informação, no Banco Económico. O mesmo, encontra-se alinhado com a Política de Segurança da Informação (PSI) que resume as orientações globais em matéria de Segurança da Informação, servindo de base para toda a estrutura documental que versa sobre o tema. Por conseguinte, figura como documento obrigatório para todas as áreas do Banco.

O documento, segue as boas práticas reconhecidas internacionalmente e tem como principal objectivo assegurar os níveis mínimos de Segurança da Informação em todos os processos executados ao nível das diferentes áreas, respeitando, ao mesmo tempo, possíveis condições locais que tenham a ver com factores jurídicos ou intrínsecos ao Banco.

Em suma, serve o presente documento para estruturar e definir os requisitos globais pelos quais deve ser regida a Segurança da Informação do Banco Económico e os quais são emanados pelo pacote documental constituído por políticas de Segurança da Informação que, posteriormente, são organizadas e estruturadas em níveis inferiores, constituindo assim o SGSI.

A existência de um SGSI, tem como principais vantagens:

- Aumento da confiança e credibilidade junto de todos os utilizadores, partes interessadas, clientes e entidades reguladoras;
- Cumprimento das leis e regulamentos aplicáveis;
- Aumento da confiança dos sistemas de informação, do conhecimento das suas fraquezas e da sua resistência a ataques;
- Aumento do conhecimento e consciencialização de todos os colaboradores do Banco Económico relativamente às questões da Segurança da Informação e às suas responsabilidades perante a temática;
- Redução do risco de eventos e incidentes de Segurança da Informação; e
- Redução do custo e impacto dos incidentes de Segurança da Informação, que são materializados.

2. Objectivos

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

- Definir os princípios de Segurança da Informação; e
- Definir os objectivos de Segurança da Informação, as métricas associadas, e o seu mecanismo de avaliação.

3. Princípios de Segurança da Informação

O Banco Económico, define e tem a preocupação de manter permanentemente actualizada uma estratégia clara ao nível de Segurança da Informação sendo possível a cada momento demonstrar inequivocamente o seu envolvimento e empenho na prossecução dos seus objectivos de Segurança da Informação, assim como, respeita e divulga de forma continuada, junto dos seus colaboradores, as disposições em matéria de segurança vigentes na instituição.

Os princípios de Segurança da Informação têm por base o suporte e protecção da actividade operacional do Banco Económico, assim como a promoção dos comportamentos aceitáveis e desejados, que todos os utilizadores devem adoptar, definindo assim uma cultura positiva de Segurança da Informação, transversal a todo a instituição.

3.1. Princípios de Segurança da Informação

Princípio A1 - Foco no negócio e nos serviços disponibilizados ao cliente:

- **Objectivo**: Garantir que a Segurança da Informação faz parte integrante de todas as actividades essenciais do Banco Económico.
- **Descrição**: A Segurança da Informação deve ser abordada de forma colaborativa entre as áreas de segurança e operacionais do Banco Económico, alinhando a alocação dos recursos e a realização de programas e projectos com os objectivos, processos e riscos do Banco. A colaboração deve envolver todos os níveis organizacionais para garantir a protecção dos activos e a gestão dos riscos actuais e futuros.

Princípio A2 - Contributo para a criação de valor:

- **Objectivo**: Garantir que a Segurança da Informação contribui para a criação de valor e suporta os requisitos do Banco Económico.
- **Descrição**: As partes interessadas, internas e externas, devem ser envolvidas regularmente com as temáticas de Segurança da Informação para que possa existir uma resposta adequada às alterações dos seus requisitos de segurança. Por sua vez, a Segurança da Informação deverá contribuir para a criação de valor, designadamente para a satisfação das necessidades das partes interessadas, optimização de riscos e de recursos.

Princípio A3 - Conformidade com os requisitos legais e normativos relevantes:

- **Objectivo**: Garantir que as obrigações legais e normativas são cumpridas, que as expectativas das partes interessadas são geridas e endereçadas e que as coimas/multas aplicadas por entidades reguladoras são evitadas.
- **Descrição**: As obrigações legais e normativas devem ser identificadas, transpostas para requisitos específicos de Segurança da Informação e comunicadas a todas as

partes interessadas chave. As coimas associadas a não conformidades devem ser claramente geridas e entendidas. Os controlos devem ser monitorizados, analisados e actualizados de forma que sejam endereçadas futuras actualizações dos requisitos legais e normativos.

Princípio A4 - Entrega de informação actualizada e exacta sobre o desempenho da Segurança da Informação:

- **Objectivo**: Monitorizar continuamente o desempenho do SGSI, comunicando o mesmo para todas as partes interessadas, garantindo que essa informação suporta a tomada de decisão.
- **Descrição**: Os critérios relacionados com o desempenho da Segurança da Informação devem estar bem definidos, fundamentados em métricas rigorosas e relevantes (e.g., conformidade, incidentes, estado dos controlos e custos) e alinhados com os objectivos do Banco. A informação deve ser obtida de forma periódica, consistente e rigorosa para que permaneça correcta e para que os resultados possam suportar os objectivos das partes interessadas chave.

Princípio A5 - Avaliação das ameaças actuais e futuras:

- **Objectivo**: Analisar e avaliar as ameaças emergentes à Segurança da Informação, para que se possa actuar na mitigação dos riscos de forma informada e atempada.
- **Descrição**: As principais tendências e ameaças da Segurança da Informação devem ser classificadas e enquadradas numa *Framework* que abranja um conjunto alargado de tópicos tais como político, legal, económico, sociocultural e técnico. O conhecimento sobre ameaças emergentes deve ser partilhado para que se possa actuar sobre as causas e não apenas sobre sintomas.

Princípio A6 - Melhoria contínua da Segurança da Informação:

- **Objectivo**: Reduzir os custos, melhorar a eficácia e eficiência e promover uma cultura de melhoria contínua da Segurança da Informação.
- **Descrição**: A evolução constante dos modelos operacionais, associada às ameaças relacionadas, leva a que as técnicas de Segurança da Informação tenham de ser adaptadas e que o nível de eficácia seja melhorado de forma contínua. Deve ser mantido um conhecimento actualizado das técnicas de Segurança da Informação através das lições aprendidas dos incidentes, bem com da colaboração com organizações de investigação independentes.

3.2. Proteger a Actividade Operacional

Princípio B1 - Adopção de uma metodologia de avaliação e tratamento de risco:

- **Objectivo**: Garantir que os riscos são tratados de forma consistente e efectiva.

- **Descrição**: As opções de tratamento dos riscos relacionados com a Segurança da Informação devem ser analisadas para que as escolhas possam ser tomadas de forma informada e documentada, de acordo com a metodologia definida. A resposta aos riscos de Segurança da Informação resulta da escolha de uma ou mais opções, que normalmente consideram:
    - Mitigar os riscos aplicando os controlos de segurança adequados;
    - Aceitar os riscos através da aprovação do Conselho de Administração do Banco Económico, reconhecendo que a perda potencial não é suficiente para justificar o investimento necessário para mitigá-lo;
    - Transferir os riscos realizando *outsourcing* das atividades/processos e/ou contratando um seguro para os mesmos; ou
    - Evitar os riscos eliminando uma actividade ou um processo que é propenso ao risco.

Princípio B2 - Protecção da informação classificada:

- **Objectivo**: Evitar que a informação classificada seja divulgada a indivíduos não autorizados.
- **Descrição**: A informação deve ser identificada e classificada de acordo com o seu nível de confidencialidade, integridade e disponibilidade. A informação classificada deve ser protegida em todas as fases do seu ciclo de vida, desde a sua criação até à sua destruição, utilizado controlos adequados (e.g., encriptação, controlo de acessos, autorização).

Princípio B3 - Foco nas aplicações críticas para a actividade operacional e de suporte ao negócio:

- **Objectivo**: Orientar os recursos de Segurança da Informação para a protecção dos activos em que incidentes de segurança podem representar impactos relevantes para a actividade operacional do Banco.
- **Descrição**: O entendimento do impacto operacional causado por perdas de integridade (i.e. correção e exatidão da informação) ou de disponibilidade da informação nos sistemas de informação (e.g., processamento, armazenamento, transmissão) permite determinar o seu nível de criticidade, bem como fundamentar a necessidade de recursos de Segurança da Informação para suportar os objectivos do Banco Económico e as necessidades de todas as partes interessadas.

Princípio B4 - Aquisição, desenvolvimento e manutenção de sistemas, de forma segura:

- **Objectivo**: Adquirir, desenvolver e manter sistemas com qualidade em que os utilizadores possam confiar.

- **Descrição**: A Segurança da Informação deve fazer parte integrante do ciclo de vida do desenvolvimento, ou seja, desde a análise de requisitos, passando pelo desenho, desenvolvimento e testes, até à sua entrada nos ambientes de produção.

3.3. Promover Comportamentos Responsáveis de Segurança

Princípio C1 - Realização de acções de formação profissional e ética:

- **Objectivo**: Garantir que as actividades relacionadas com a Segurança da Informação são desenvolvidas de forma confiável, responsável e efetiva.
- **Descrição**: A Segurança da Informação depende da capacidade dos colaboradores desempenharem as suas funções com um claro entendimento sobre o impacto desta na protecção dos activos de informação do Banco. Periodicamente, e de forma regular, devem ser ministradas acções de formação e consciencialização para a temática, permitindo a todos os colaboradores demonstrar o seu compromisso com elevados padrões de qualidade nas suas tarefas, apresentar comportamentos éticos, coerentes, alinhados com as necessidades do Banco Económico e respeito por todos por todos os indivíduos.

Princípio C2 - Fomento de uma cultura positiva:

- **Objectivo**: Promover uma influência positiva da Segurança da Informação nos comportamentos dos utilizadores finais, reduzindo a probabilidade de ocorrência de incidentes de segurança e limitando o impacto na atividade operacional.
- **Descrição**: A Segurança da Informação deve fazer parte integrante do dia-a-dia, no Banco Económico, promovendo a consciencialização para a importância da mesma junto dos utilizadores e garantindo que estes têm as competências e conhecimento necessário para proteger os sistemas e a informação critica ou confidencial. Todos devem conhecer e entender os riscos relacionados com a informação e ser encorajados a garantir a sua protecção, bem como a identificar qualquer ponto fraco que possa constituir um risco de Segurança da Informação para o Banco.

4. Objectivos da Segurança da Informação

A identificação de objectivos é essencial para a monitorização do desempenho do SGSI. Os objectivos de Segurança da Informação estão directamente ligados com os objectivos gerais do Banco Económico. A estes objectivos estão associadas métricas de avaliação que são atualizadas periodicamente com o intuito de servirem o Banco de forma adequada e precisa.

4.1. Objectivos e Métricas

Tendo em consideração os objectivos gerais do Banco Económico e as normas e boas práticas internacionais, foram definidos os seguintes objectivos de Segurança da Informação e respetivas métricas:

Objectivo OBJSI.01 - Conformidade com Leis e Normativos.

Métricas			
ID	*Descrição*	*Periodicidade*	*Escala*
OBJSI.01.01	**Custo** de não-conformidades relacionadas com a Segurança da Informação, incluindo multas e impacto na credibilidade do Banco.	Anual	Kwanzas
OBJSI.01.02	**Número** de incidentes relacionados com a Segurança da Informação reportados ao Conselho de Administração, passíveis de gerar comentários ou constrangimentos públicos.	Anual	Número
OBJSI.01.03	**Número** de incidentes e/ou não-conformidades relacionados com acordos contratuais com os prestadores de serviços externos.	Mensal	Número

Tabela 2 – Métricas associadas à Conformidade com Leis e Normativos

Objectivo OBJSI.02 - Gestão dos Riscos de Segurança da Informação.

Métricas			
ID	*Descrição*	*Periodicidade*	*Escala*
OBJSI.02.01	**Frequência** de actualização do perfil de risco.	Anual	Frequência
OBJSI.02.02	**Percentagem** de avaliações de risco do Banco que incluem riscos relacionados com a Segurança da Informação.	Anual	Percentagem
OBJSI.02.03	**Número** de incidentes significativos de Segurança da Informação que não foram identificados nas avaliações de risco.	Anual	Número

Tabela 3 - Métricas associadas à Gestão dos Riscos de Segurança da Informação

Objectivo OBJSI.03 – Gestão de Incidentes de Segurança da Informação.

Métricas			
ID	*Descrição*	*Periodicidade*	*Escala*
OBJSI.03.01	**Número** de incidentes de confidencialidade que causaram perda financeira, interrupção de serviço ou impacto na credibilidade e robustez.	Mensal	Número
OBJSI.03.02	**Número** de incidentes de disponibilidade que causaram perda financeira, interrupção de serviço ou impacto na credibilidade e robustez.	Mensal	Número
OBJSI.03.03	**Número** de incidentes de integridade que causaram perda financeira, interrupção de serviço ou impacto na credibilidade e robustez.	Mensal	Número

Tabela 4 - Métricas associadas à Gestão de Incidentes de Segurança da Informação

Objectivo OBJSI.04 - Conformidade com as Políticas Internas.

Métricas			
ID	*Descrição*	*Periodicidade*	*Escala*
OBJSI.04.01	**Número** de incidentes relacionados com não-conformidades com políticas internas.	Mensal	Número
OBJSI.04.02	**Número** de exceções às políticas internas, identificadas e documentadas.	Mensal	Número
OBJSI.04.03	**Percentagem** de documentação do SGSI revista e atualizada dentro dos prazos definidos.	Anual	Frequência

Tabela 5 - Métricas associadas à Conformidade com as Políticas Internas

Para o cumprimento dos objectivos, estão associadas métricas que servirão como mecanismo de avaliação do sucesso das iniciativas relacionadas com a Segurança da Informação permitido medir os benefícios da sua implementação e criar valor para o Banco Económico e para as suas partes interessadas. A definição e utilização sistémica das métricas garante a transparência na avaliação dos resultados da implementação da Segurança da Informação e uma melhor comunicação com as restantes áreas, com a Comissão Executiva e com o Conselho de Administração do Banco.

As métricas de Segurança da Informação encontram-se definidas de modo a permitir o detalhe dos objectivos de Segurança da Informação tornando-os específicos e mensuráveis.

4.2. Metas

As metas de Segurança da Informação devem ser estabelecidas anualmente pelo Gabinete de Segurança da Informação, de acordo com o processo de planeamento dos objectivos anuais e/ou estratégicos do Banco Económico**.**

Para assegurar que os objectivos de Segurança da Informação serão realistas e exequíveis é crucial considerar no processo de definição de metas o desempenho actual da Segurança da Informação e a disponibilidade dos recursos necessários para atingir os objectivos pretendidos.

As metas estabelecidas para cada período devem ser documentadas, formalizadas e comunicadas internamente às partes afetadas.

5. Alterações e Aprovação

O presente Modelo Organizacional da Segurança da Informação é revisto com uma periodicidade mínima anual, podendo, no entanto, cabe ao Gabinete de Segurança da Informação propor ao Conselho de Administração a revisão da mesma num prazo inferior, sempre que se considere oportuno.

O Modelo Organizacional da Segurança da Informação foi aprovado pelo Conselho de Administração do Banco Económico.

6. Considerações Finais

A coordenação e execução do Modelo Organizacional da Segurança da Informação é de responsabilidade do Gabinete de Segurança da Informação, onde deve ser dirigida quaisquer questões relacionadas a mesma.

7. Revogação

O presente Modelo Organizacional da Segurança da Informação revoga a versão anterior publicada em 13 de dezembro de 2022.

17. Anexo II–Estruturas Organizacionais da Segurança da Informação

Estruturas Organizacionais da Segurança da Informação

Versões

Versão	Data de Revisão	Sumário de Mudanças	Direcção
1.0	02-10-2020	1. Versão inicial.	DTI/NSI
1.1	21-04-2022	1. Adição da Estrutura Organizacional do GSI e respectivo E-mail.	GSI
1.2	-	1. Adequação a Nova Estrutura Orgânica e Nomenclatura.	GSI

1. Enquadramento

O presente documento vem trazer directrizes sobre as Estruturas Organizacionais da Segurança da Informação, no Banco Económico.

2. Objectivos

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

- Formalizar a estrutura responsável pelo governo e gestão da Segurança da Informação; e
- Definir os intervenientes, os seus papéis, as autoridades e as responsabilidades de alto nível.

3. Responsabilidades de Segurança da Informação

3.1. Estruturas Organizacionais da Segurança da Informação

Para assegurar a gestão efectiva da Segurança da Informação, está definida uma estrutura que se estende pelo nível estratégico, tático e operacional, sendo esta responsável pela orientação, planeamento, implementação, manutenção e melhoria contínua da Segurança da Informação. Nesse sentido, se descentralizaram as responsabilidades pela gestão da Segurança da Informação, por diferentes áreas do Banco Económico, desde o Conselho de Administração até às Equipas Operacionais.

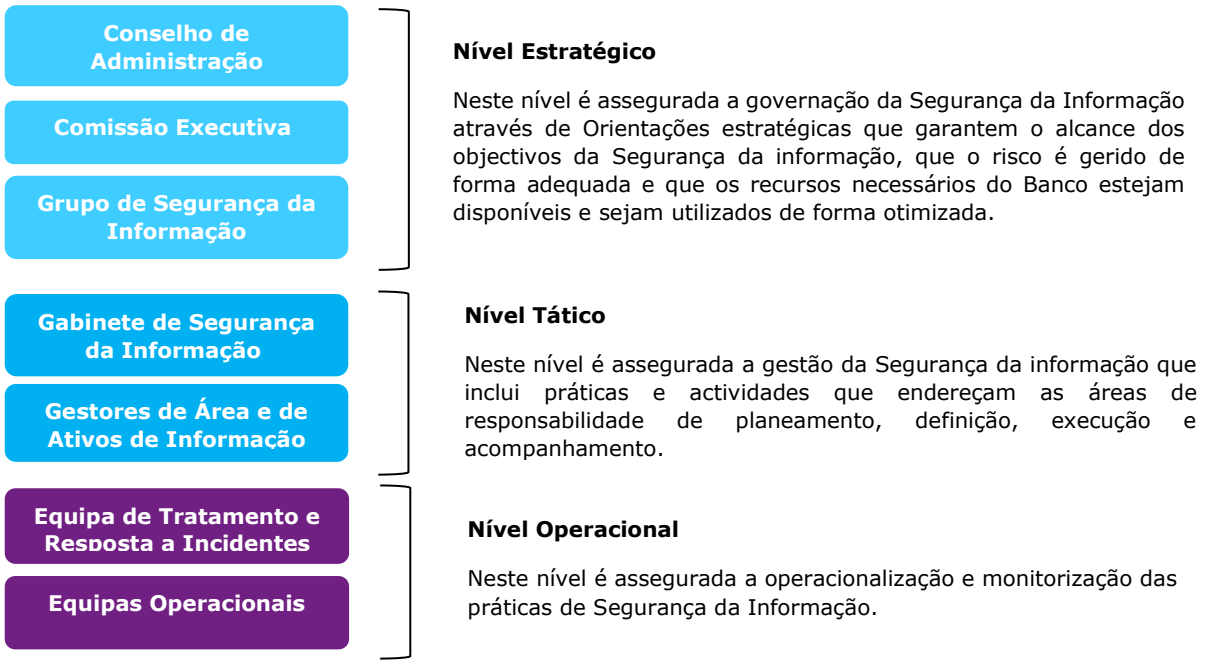

Figura 2 – Estruturas Organizacionais

3.1.1. Nível Estratégico

3.1.1.1. Conselho de Administração

O Conselho de Administração define e acompanha os objectivos estratégicos do Banco, assumindo a liderança e o compromisso para com a Segurança da Informação. Nesse sentido, tem como responsabilidade promover a criação de um ambiente de Segurança da Informação, em linha com as exigências da lei, reguladores, melhores práticas internacionais e necessidades do Banco, para defesa dos seus activos de informação.

Toda a documentação respeitante ao nível Estratégico, de acordo com a *Framework* de Documentação de Segurança da Informação, é aprovada pelo Conselho de Administração.

No que diz respeito à gestão de risco de Segurança da Informação, o Conselho de Administração tem as seguintes responsabilidades:

- Definir e aprovar o nível de risco que o Banco Económico está disposto a aceitar, enquanto prossegue com a sua estratégia e atividades operacionais, ou seja, o apetite ao risco;
- Aprovar a aceitação dos riscos categorizados como **ALTOS** e **MUITO ALTOS**, bem como da respetiva definição de responsabilidades pela decisão e tratamento dos mesmos;
- Aprovar a aceitação excepcional dos riscos cujo risco residual se situe acima do apetite ao risco previamente definido e aprovado; e
- Rever a aprovar qualquer desvio ou excepção a políticas, normas, regulamentos, processos e procedimentos.

3.1.1.2. Comissão Executiva

A Comissão Executiva é um órgão afecto ao Conselho de Administração, encarregue pela gestão corrente do Banco. Compete à Comissão Executiva a prática de todos os actos de gestão corrente do Banco, nos termos da deliberação de delegação de competências do Conselho de Administração, e nos demais consagrados na lei, com inequívoca exclusão dos poderes que a lei, os Estatutos e o Regulamento do Conselho de Administração considerem competência absoluta deste.

Toda a documentação respeitante ao nível Tático, de acordo com a *Framework* de Documentação de Segurança da Informação, é aprovada pela Comissão Executiva.

Relativamente à Segurança da Informação, a Comissão Executiva tem como principais responsabilidades:

- Assegurar a aprovação e implementação de toda a documentação de Segurança da Informação (e.g., políticas, normas, procedimentos) e a efectiva Gestão de Segurança Informação no Banco Económico;
- Implementar um ambiente de Segurança da Informação, em linha com as exigências da lei, reguladores, melhores práticas internacionais e necessidades do Banco, para defesa dos seus activos de informação; e
- Estabelecer o Grupo de Segurança da Informação (ou equivalente) e nomear um Director ou Gestor de Segurança da Informação.

3.1.1.3. Grupo de Segurança da Informação

O Grupo de Segurança da Informação assume a responsabilidade pela Governance e gestão de Segurança da Informação, tendo a responsabilidade de garantir a revisão das políticas, normas e procedimentos de Segurança da Informação, assegurando a sua adequada publicação e divulgação para todo o universo Banco Económico.

Nesse sentido, o Grupo de Segurança Informação tem como principais responsabilidades:

- Acompanhar o desenvolvimento, implementação e melhoria contínua do SGSI, validando as suas iniciativas para aprovação da Comissão Executiva e do Conselho de Administração do Banco;
- Acompanhar o desenvolvimento e manutenção de uma Framework de governação e gestão de Segurança da Informação com base nas normas e boas práticas internacionais (e.g., ISO 27001, COBIT, NIST), que promova a colaboração contínua com as áreas de negócio;
- Garantir que o Banco Económico identifica as acções necessárias para implementar o seu SGSI, e mantém os recursos adequados;
- Comunicar sobre o SGSI para as áreas de negócio;
- Rever a efectividade da implementação do SGSI, assegurando que as iniciativas são desenvolvidas dentro dos prazos e orçamento acordado;
- Rever e aprovar Planos de Tratamento de Risco que visam mitigar os riscos cuja análise e avaliação tenham determinado uma classificação que se situa acima do apetite ao risco formalmente aprovado pelo Banco;
- Garantir que a arquitectura de Segurança da Informação, dos sistemas e plataformas de segurança propostas são consistentes com a arquitectura e plano estratégico do Banco Económico;
- Assegurar que o Banco Económico adota uma metodologia de gestão de Segurança da Informação estruturada, que deve ser utilizada transversalmente em todas as suas iniciativas e processos;
- Validar os incidentes de Segurança da Informação críticos para a actividade operacional do Banco;

- Monitorizar e reportar regularmente sobre a implementação e operação do SGSI, de acordo com o programa aprovado e com ênfase na gestão de segurança, gestão de risco, gestão da concretização dos benefícios e de uma efectiva gestão de mudança; e
- Reconhecer de forma proactiva a necessidade de mudança nos serviços, guiando o Banco Económico na adopção de novas tecnologias de segurança.

3.1.2. Nível Tático

3.1.2.1. Gabinete de Segurança da Informação

O Gabinete de Segurança da Informação é a entidade que está no nível mais sénior de gestão de todos os assuntos relacionados com Segurança da Informação. É, por isso, responsável máximo por toda a Segurança da Informação, independentemente da forma em que ela se apresente, sendo sua função canalizar e orientar os princípios e objectivos de Segurança da Informação definidos.

Nesse sentido, deve garantir:

- Formalização dos objectivos estratégicos relativos à Segurança da Informação;
- Definição, implementação, manutenção e melhoria contínua da Segurança da Informação;
- Comunicação da importância de uma gestão de Segurança da Informação eficaz e integração dos requisitos de Segurança da Informação, nos processos do Banco Económico;
- Desenvolver e manter a Política de Segurança da Informação (PSI), dentro do contexto da estrutura de gestão do negócio;
- Revisão anual da Política de Segurança da Informação;
- Disponibilização de recursos suficientes para desenvolver, implementar, operar e manter a Segurança da Informação, em parceria com as restantes estruturas organizacionais a considerar;
- Efectuar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
- Manter-se informado de forma permanente em relação as leis, regulamentos e outros assuntos relativos à segurança da informação e comunicações;
- Promover a formação, sensibilização e desenvolvimento das competências necessárias;

- Articular as questões relacionadas com a Segurança da Informação com os Gestores de Área, assegurando o planeamento e coordenação de todas as atividades necessárias para operacionalização, monitorização e revisão regular das práticas de Segurança da Informação, no Banco; e
- Participar em fóruns, redes nacionais e internacionais relativas à Segurança da Informação.

3.1.2.2. Gestores de Área e de Activos de Informação

Compete aos Gestores de Área, e aos Gestores de Activos de Informação, garantir que a estratégia em cada uma das suas áreas engloba os objectivos de Segurança da Informação do Banco Económico. Nesse sentido, tem como principais responsabilidades:

- Garantir a segurança dos activos de informação sob sua responsabilidade;
- Definir e gerir os requisitos de segurança para os activos de informação sob sua responsabilidade, em conformidade com esta política;
- Efectuar solicitações para a Concessão e revogação de acessos aos activos de informação;
- Comunicar à Equipa de Tratamento e Resposta a Incidentes qualquer caso em que se verifique a quebra de um controlo de segurança, bem como a ocorrência de incidentes de Segurança da Informação;
- Proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta política;
- Co-responsabilizar-se pelas acções realizadas por aqueles que estão sob sua responsabilidade;
- Consciencializar os utilizadores sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;
- Incorporar aos processos de trabalho de sua área, práticas inerentes à Segurança da Informação;
- Tomar as medidas administrativas necessárias para que sejam aplicadas acções correctivas nos casos de comprometimento desta política por parte dos utilizadores sob sua supervisão;
- Realizar o tratamento e a classificação da informação;
- Autorizar, de acordo com a legislação vigente e com a política de classificação da informação, a divulgação das informações produzidas na sua área de negócio; e
- Manter um inventário actualizado dos activos de informação sob sua responsabilidade com seus respectivos gestores.

3.1.3. Nível Operacional

3.1.3.1. Equipa de Resposta e Tratamento de Incidente

A Equipa de Segurança da Informação responde directamente ao Gabinete de Segurança da Informação, e tem como função coordenar a vertente operacional de Segurança da Informação, nomeadamente na resposta a eventos e incidentes de Segurança da Informação.

Nesse sentido, tem como principais responsabilidades:

- Facilitar e coordenar as actividades de tratamento e resposta a incidentes de Segurança da Informação;
- Promover a recuperação atempada dos sistemas;
- Agir proactivamente com o objectivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de Segurança da Informação, avaliando as condições de segurança de todo o Ecossistema da instituição por meio de verificações de conformidade;
- Realizar acções reactivas que incluem alertas e notificações de incidentes, orientação de equipas na reparação de danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
- Analisar ataques e intrusões a Infraestrutura do Banco Económico;
- Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes; e
- Comunicar e cooperar com outras equipas de Tratamento e Resposta a Incidentes, incluindo equipas pertencentes a Autoridades Nacionais de Supervisão e Controlo.

3.1.3.2. Equipas Operacionais

Compete às restantes Equipas Operacionais, incluindo colaboradores e outros utilizadores, garantirem que os objectivos da Segurança da Informação são acomodados nas suas unidades, seja por solicitação do Gabinete de Segurança da Informação ou por indicação do Gestor da Área respectiva. Nesse sentido, têm como principais responsabilidades:

- Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta política, bem como as demais políticas, normas e procedimentos que constituem o SGSI;
- Obedecer aos requisitos de controlo especificados pelo Gestor de Área, Gestores da Informação e Gestores de Activos de Informação; e

- Comunicar atempadamente os eventos e incidentes que possam impactar a segurança dos activos de informação e comunicações à Equipa de Tratamento e Resposta a Incidentes.

Estas competências têm por objectivo a mitigação dos riscos associados à implementação dos controlos de Segurança da Informação, no contexto transversal ao Banco Económico.

4. Gestão de Projectos

A Segurança da Informação deve ser integrada na gestão de todos os projectos do Banco Económico independentemente do tipo de projecto, de forma a garantir que os riscos de Segurança da Informação são identificados e endereçados como parte integrante de todos os projectos.

A gestão de projecto deve assegurar:

- A inclusão dos objectivos de Segurança da Informação nos objectivos do projecto;
- A inclusão de requisitos de Segurança da Informação nos requisitos do projecto;
- A realização de uma avaliação de riscos de Segurança da Informação, na fase inicial do projecto, de forma a identificar os controlos necessários; e
- O endereçamento da Segurança da Informação em todas as fases da gestão de projecto.

Adicionalmente, as responsabilidades da Segurança da Informação devem ser definidas e alocadas a funções definidas na gestão de projecto.

5. Alterações e Aprovação

A presente Estrutura Organizacional da Segurança da Informação é revista com uma periodicidade mínima anual, podendo, no entanto, cabe ao Gabinete de Segurança da Informação propor ao Conselho de Administração a revisão da mesma num prazo inferior, sempre que se considere oportuno.

A Estrutura Organizacional da Segurança da Informação foi aprovada pelo Conselho de Administração do Banco Económico.

6. Considerações Finais

A coordenação e execução da Estrutura Organizacional da Segurança da Informação é de responsabilidade do Gabinete de Segurança da Informação, onde deve ser dirigida quaisquer questões relacionadas a mesma.

7. Revogação

A presente Estrutura Organizacional da Segurança da Informação revoga a versão anterior publicada em 13 de dezembro de 2022.

18. Anexo III–Framework de Documentação da Segurança da Informação

Framework de Documentação da Segurança da Informação

Versões

Versão	Data de Revisão	Sumário de Mudanças	Direcção
1.0	02-10-2020	1. Versão inicial.	DTI/NSI
1.1	21-04-2022	1. Adição da Estrutura Organizacional do GSI e respectivo E-mail.	GSI
1.2	-	1. Adequação a Nova Estrutura Orgânica e Nomenclatura.	GSI

1. Enquadramento

O presente documento possui orientações sobre a organização documental da Segurança da Informação, no Banco Económico.

2. Objectivos

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

- Instituir o modelo de estrutura documental de Segurança da Informação; e
- Definir as responsabilidades sobre a estrutura documental.

3. Framework de Documentação

3.1. Estrutura da Documentação

A gestão da Segurança da Informação do Banco Económico deve ser documentada de modo a garantir não só a fácil comunicação e acesso por parte dos seus Colaboradores e partes interessadas que tenham de seguir tais orientações, mas também a viabilidade de revisões independentes à própria gestão e respectivas melhorias.

Para dar resposta a este ponto, a documentação no âmbito da Segurança da Informação está organizada de acordo com os seguintes três níveis hierárquicos:

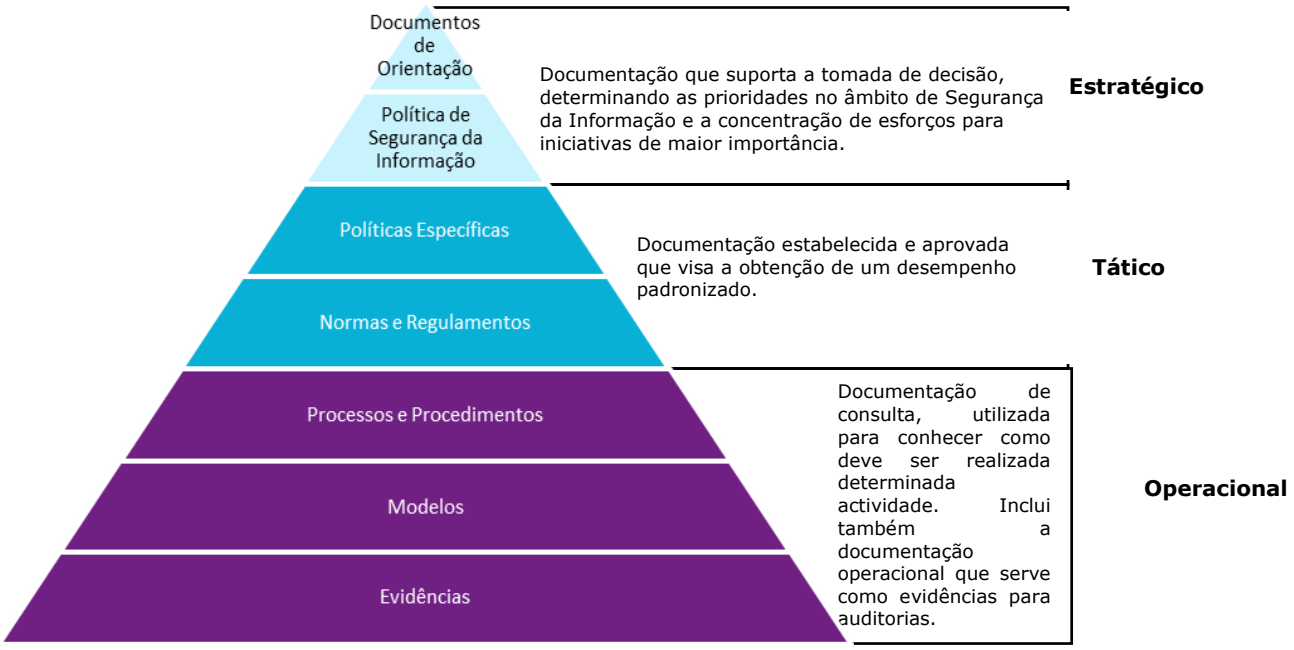

Figura 3 - Estrutura Documental de Segurança da Informação

3.1.1. Nível Estratégico

Este nível é constituído por documentação de base orientada aos fundamentos do estabelecimento das responsabilidades de Segurança da Informação. A documentação constante do nível estratégico deve ser revista, pelo menos, anualmente ou sempre que ocorram alterações significativas que impactem a mesma.

3.1.1.1. Documentos de Orientação

3.1.1.1.1. Framework da Segurança da Informação

A Framework de Segurança da Informação apresenta a visão estratégica do Banco Económico para a definição e operacionalização do seu SGSI de forma a proteger a confidencialidade, integridade e disponibilidade dos seus activos de informação, respeitando os requisitos e expectativas de todas as partes interessadas, internas e externas. A implementação da Framework é realizada com recurso a um ciclo PDCA (i.e. Plan-Do-Check-Act), de acordo com os requisitos emanados pela normas e boas práticas internacionais, estabelecendo um conjunto de políticas, normas e procedimentos que definem toda a gestão, monitorização e melhoria contínua da Segurança da Informação.

3.1.1.1.2. Modelo Organizacional da Segurança da Informação

O Modelo Organizacional de Segurança da Informação pressupõe o alinhamento com a estratégia interna do Banco, nomeadamente no que concerne aos princípios, objectivos e políticas de Segurança da Informação necessários a um nível de segurança coerente e robusto com as necessidades expectáveis.

3.1.1.1.3. Modelo Organizacional da Segurança da Informação

As Estruturas Organizacionais de Segurança da Informação têm como finalidade formalizar a estrutura responsável pela governação e gestão da Segurança da Informação, bem como definir os intervenientes, os seus papéis, as autoridades e as responsabilidades de alto nível em relação à Segurança da Informação do Banco Económico.

3.1.1.2. Política de Segurança da Informação

A Política de Segurança da Informação (PSI) tem carácter permanente e define a Segurança da Informação do Banco Económico, orientando o desenvolvimento de todos os documentos dos níveis Tático e Operacional, bem como todas as actividades operacionais relacionadas com a Segurança da Informação. Todos os normativos de Segurança da Informação dos níveis inferiores (e.g., políticas específicas, normas internas, procedimentos) devem ser baseados ou refletir as preocupações e considerações estabelecidas por este documento.

3.1.2. Nível Tático

Este nível é constituído por documentação de duas tipologias distintas, Políticas Específicas e Normas e Regulamentos. Esta documentação visa determinar e guiar as actividades materializadas no Nível Operacional, estabelecendo a base mínima de conformidade que tem de ser garantida.

A documentação constante do Nível Tático deve ser revista, pelo menos, anualmente ou sempre que ocorram alterações significativas que impactem a mesma.

3.1.2.1. Políticas Específicas

As Políticas Específicas de Segurança da Informação são os documentos que estabelecem regras, orientações e responsabilidades de alto nível dentro das respetivas dimensões de Segurança da Informação. As Políticas Específicas devem ser baseadas ou refletir as preocupações e considerações estabelecidas pela PSI e respeitar os Princípios de Segurança da Informação.

3.1.2.2. Normas e Regulamentos

As Normas e Regulamentos de Segurança da Informação são os documentos mais detalhados que fazem menção especial às tecnologias, métodos, procedimentos de implementação e outros detalhes, sendo o tempo da sua aplicabilidade inferior ao das políticas, tendo em conta a sua natureza mais técnica. As Normas e Regulamentos devem ser baseadas ou refletir as preocupações e considerações estabelecidas pelas Políticas Específicas, dentro do respetivo domínio de Segurança da Informação.

3.1.3. Nível Operacional

Os Processos e Procedimentos, Modelos e Evidências de Segurança da Informação são documentos que materializam as tarefas relacionadas com a Segurança da Informação, bem como definem do ponto de vista operacional o que deve ser assegurado pelas Equipas responsáveis. Os Processos e Procedimentos, Modelos e Evidências devem ser baseados ou refletir as preocupações e considerações estabelecidas pelas Políticas Específicas e pelas Normas e Regulamentos, dentro do respetivo domínio de Segurança da Informação.

A documentação constante do Nível Operacional deve ser revista sempre que ocorram alterações significativas que impactem a mesma, nomeadamente, alterações em qualquer da documentação dos Níveis Estratégico ou Tático.

3.1.3.1. Processos e Procedimentos

Os Processos e Procedimentos são documentos que regulam a operação das atividades de Segurança da Informação passo-a-passo, detalhando a forma como devem ser realizadas e como devem ser utilizadas as tecnologias, métodos e outras ferramentas para alcançar os objectivos respeitantes às mesmas. A aplicabilidade dos Processos e Procedimentos

deve ser analisada e rectificada sempre que existir alguma alteração operacional aos mesmos. Os Processos e Procedimentos devem reflectir e operacionalizar as considerações estabelecidas nas Normas e Regras dentro do respectivo domínio de Segurança da Informação.

3.1.3.2. Modelos

Os Modelos são ferramentas que suportam as actividades definidas nos Processos e Procedimentos por forma a garantirem a correcta realização dos mesmos. Estes modelos podem ser desenhados pelos Colaboradores que realizam as actividades, mas terão de ser sempre analisados e validados pelo Gabinete de Segurança da Informação por forma a garantir que estão de acordo com os objectivos de Segurança da Informação do Banco.

3.1.3.3. Evidências

As Evidências são produtos da instanciação das actividades emanadas pelos Processos e Procedimentos que evidenciam e comprovam as acções realizadas nas auditorias periódicas.

4. Nomenclatura e Codificação

Devem ser seguidos critérios e regras de nomenclatura para todos os documentos relacionados com a Segurança da Informação de modo a optimizar a gestão documental. Nesse sentido, deve ser evitada a ambiguidade de identificação dos documentos, através da referência e identificação unívoca e devem também ser evitadas as inconsistências decorrentes da caducidade ou alteração da documentação.

Nesse sentido, deve ser seguida uma nomenclatura consistente que permita a flexibilidade na criação de documentos de Segurança da Informação.

A nomenclatura a utilizar deverá ser a seguinte:

BE-[Tipo de Documento][Número] [Nome do Documento] – AAAA.MM.DD – vN.n

Onde os campos são representados da seguinte forma:

- **BE**: Banco Económico;
- **[Tipo de Documento]**: Referência ao tipo do documento composta por três caracteres:
  - **DOR**: Documentos de Orientação;
  - **PSI**: Política de Segurança da Informação;
  - **PES**: Políticas Específicas;
  - **NRM**: Normas e Regulamentos;
  - **PRC**: Processos e Procedimentos;
  - **MOD**: Modelos; e

- **EVI**: Evidências.

- **[Número]**: Número de três caracteres que são incrementados à medida que são criados documentos com o mesmo tipo. Os números atribuídos deixam de estar disponíveis mesmo que o documento seja descontinuado. Deve ser mantida uma listagem de gestão documental nesse sentido;
- **[Nome do Documento]**: Nome pelo qual o documento possa ser identificado de forma célere (e.g. título do documento);
- **AAAA.MM.DD**: Data de modificação do documento em causa, composta pela concatenação do ano, mês e dia, separados por pontos; e
- **vN.n**: Número que identifica a versão do documento.

Como exemplo, o presente documento toma a seguinte nomenclatura:

BE-DOR006 Framework de Documentação – 2020.05.04 – v1.0

5. Responsabilidades Sobre os Documentos

Dada a divisão nos três níveis hierárquicos, é necessário assegurar as responsabilidades associadas a cada um:

Nível	*Tipos de Documento*	*Responsável*	*Revisor*	*Aprovador*
Estratégico	▪ Documentos de Orientação ▪ Política de Segurança da Informação	Gabinete de Segurança da Informação	Grupo de Segurança da Informação	Conselho de Administração
Tático	▪ Políticas Específicas ▪ Normas e Regulamentos	Gabinete de Segurança da Informação	Grupo de Segurança da Informação	Comissão Executiva
Operacional	▪ Processos e Procedimentos ▪ Modelos ▪ Evidências	Equipas Operacionais	Gestor de Área	Gabinete de Segurança da Informação

Tabela 6 - Fluxo de Aprovação da Documentação de Segurança da Informação

Caso surja alguma excepção ao fluxo de aprovação da documentação de Segurança da Informação, cabe ao Gabinete de Segurança da Informação gerir a excepção por forma a garantir o seu fluxo de aprovação formal. Em último caso, as excepções podem seguir para aprovação da Conselho de Administração.

6. Alterações e Aprovação

A presente Framework de Documentação da Segurança da Informação é revista com uma periodicidade mínima anual, podendo, no entanto, cabe ao Gabinete de Segurança da

Informação propor ao Conselho de Administração a revisão da mesma num prazo inferior, sempre que se considere oportuno.

A presente Framework de Documentação da Segurança da Informação foi aprovada pelo Conselho de Administração do Banco Económico.

7. Considerações Finais

A coordenação e execução da Framework de Documentação da Segurança da Informação é de responsabilidade do Gabinete de Segurança da Informação, onde deve ser dirigida quaisquer questões relacionadas a mesma.

8. Revogação

A presente Framework de Documentação da Segurança da Informação revoga a versão anterior publicada em 13 de dezembro de 2022.