POLÍTICA

GLOBAL DE SEGURANÇA DE INFORMAÇÃO

Ref: POL/DSI/2025/001/V01

Entrada em Vigor: 17/12/2025

Classificação de Segurança: **PÚBLICO**

CONTEÚDO

1 DISPOSIÇÕES GERAIS

1.1 OBJECTIVO E ÂMBITO

O presente documento fornece um conjunto de directrizes globais para a Segurança da Informação do Grupo Banco de Fomento Angola (adiante designado por BFA ou Banco), e endereça os pontos identificados na Tabela 1.

O estabelecido neste documento aplica-se a todos os Colaboradores, bem como a toda a informação que é propriedade do Banco e outra que não sendo da sua propriedade está, para efeitos legais, regulatórios, contratuais ou operacionais, sob a responsabilidade directa ou indirecta de qualquer uma das suas estruturas orgânicas, e a todos os seus processos, sistemas, soluções e infra-estruturas.

1.2 ENQUADRAMENTO LEGAL, REGULAMENTAR E NORMATIVO

O presente documento endereça a seguinte Legislação, Regulamentação e Normas:

Tabela 1— Referências, Legislação, Regulamentação e Normas endereçadas

NOME
Aviso n. º 1/2022 - Código do Governo Societário das Instituições Financeiras Bancárias: Alínea b) n. º3 do artigo 39, alínea z) ponto vii) artigo 3.
N. º1 do artigo 4, n. º1 do artigo 8, alínea a) do n.º do artigo 11º, n. º3 Art. º4,
ISO/IEC 27001:2022 Cláusula 4.4. Sistema de Gestão de Segurança da Informação Cláusula 5.1. Liderança e Comprometimento
ISO/IEC 27002:2022: Cláusula 5.1. Políticas para a Segurança da Informação Cláusula 5.2. Papéis e Responsabilidades de Segurança da Informação Cláusula 5.4. Responsabilidades da Gestão Cláusula 8.34. Controlos de Auditoria nos Sistemas de Informação

1.3 CONCEITOS E ABREVIATURAS

Detalha-se em seguida os principais termos utilizados na presente Política:

1.3.1 ABREVIATURAS

- CSI – Comité de Segurança da Informação
- DSI – Direcção de Sistemas de Informação
- GSI – Gabinete de Segurança da Informação
- SGSI – Sistema de Gestão para a Segurança da Informação

1.3.2 CONCEITOS

Não Aplicável.

1.4 REVOGAÇÃO DE NORMATIVO

A presente Política revoga os seguintes normativos:

- Política Global de Segurança de Informação - POL/DSI/2024/001/V01 (01.07.2024)

1.5 RESPONSABILIDADES

A presente Política traduz-se nas responsabilidades identificadas no ponto 2.6 - Modelo de Governo.

1.6 OMISSÕES

Os casos de omissão de regulamentação deverão ser endereçados ao BFA – Comité de Segurança de Informação (CSI) previamente à adopção de quaisquer medidas.

1.7 NÃO CUMPRIMENTO

Não Aplicável.

1.8 CONTACTOS

Questões relacionadas com este documento devem ser endereçadas ao BFA, através dos canais institucionais.

2 CONTEÚDOS REGULAMENTADOS

2.1 INTRODUÇÃO

O crescimento de canais digitais, o uso cada vez maior de dispositivos móveis e, consequentemente, a adopção massiva das tecnologias de informação, dentro e fora das organizações, provocou alterações profundas na forma de trabalhar (e.g. mobilidade e teletrabalho), nos comportamentos (e.g. exposição nas redes sociais), e nos hábitos de consumo (e.g. compras e pagamentos online). Por outro lado, criou ainda a oportunidade para o aparecimento, crescente, do cibercrime (e.g. ransomware, phishing) e inevitavelmente novos desafios ao nível da segurança das organizações.

Para enfrentar estes novos desafios as organizações adaptaram-se, nas suas várias vertentes do negócio, de modo a alinhar as expectativas entre os objectivos e metas estratégicas da organização com a disponibilização de novos produtos e funcionalidades aos utilizadores e parceiros (genericamente participantes), nomeadamente:

a) Melhoria da oferta ao nível dos serviços prestados em canais digitais (vantagem competitiva), de forma a tirar partido das novas capacidades introduzidas pela tecnologia;
b) Reforço das condições de segurança associadas ao acesso dos utilizadores aos serviços disponibilizados através de canais digitais, adequadas às necessidades das operações realizadas;
c) Foco na protecção da informação, considerando a importância vital desta no paradigma digital, e mitigação de potenciais consequências decorrentes de incidentes que violem a segurança da informação;
d) Recurso à tecnologia como facilitador na resposta eficiente aos crescentes requisitos de conformidade, regulação e supervisão.

Em resposta a este desafio, o Banco de Fomento de Angola pretende garantir que a Segurança da Informação constitui uma base para toda a estrutura organizacional e está contemplada em todos os processos de forma a assegurar a protecção contra as ameaças internas e externas, em permanência e de forma equilibrada, em todas as fases do seu ciclo de vida, garantindo a confidencialidade, integridade, disponibilidade e resiliência dos sistemas que os suportam.

É neste contexto que se estabelecem, no presente documento, os objectivos e orientações gerais para Segurança da Informação, que se traduzem em políticas específicas e regulamentação própria.

2.2 DEFINIÇÃO

A Segurança da Informação define-se genericamente como a salvaguarda das seguintes propriedades:

- **Confidencialidade**: garantia de que a informação é acedida apenas por quem detém autorização para tal e é restrita a utilizadores legítimos;
- **Integridade**: Salvaguarda da exactidão e completitude da informação e respectivos métodos de processamento, garantido a qualidade da informação em uso;
- **Disponibilidade**: garantia de que a informação e activos de informação correspondentes podem ser acedidos pelas entidades autorizadas sempre que necessário;
- **Não repúdio**: Garantia de que não é possível a contestação de acções realizadas pelos participantes.

2.3 OBJECTIVOS

Para este âmbito, a Gestão do Banco definiu os seguintes objectivos estratégicos:

a) Salvaguardar os interesses das partes interessadas;
b) Garantir a conformidade com os requisitos legais, regulamentares e contratuais aplicáveis;
c) Garantir que os riscos para a Segurança da Informação são acompanhados, compreendidos, e mitigados até um nível aceitável pelo Banco;
d) Controlar, prevenir e limitar o impacto de incidentes que possam pôr em causa a operação, imagem e reputação do Banco;
e) Capacitar o Banco para gerir eficaz e eficientemente a Segurança da Informação nos seus processos e actividades, de acordo com as melhores práticas, considerando os produtos e serviços disponibilizados e a natureza das operações e tendo presente as orientações estratégicas e modelo de negócio, a sua dimensão e perfil de risco;
f) Obter certificações relevantes no domínio da Segurança da Informação;
g) A gestão destes objectivos é suportada por um processo de melhoria contínua, cujo principal componente é o Sistema de Gestão de Segurança da Informação (SGSI), alinhado com a norma ISO/IEC 27001:2022.

2.4 ORIENTAÇÕES

Os objectivos definidos no ponto anterior, traduzem-se nas seguintes orientações:

a) Garantir que todos os Colaboradores do Banco agem em conformidade com a Política Global de Segurança da Informação e normativo associado, por forma a reduzir o risco de incidentes de Segurança da Informação e garantir um nível de segurança adequado, ao longo de todo o ciclo de vida dos activos de informação, em função da sensibilidade dos dados e da informação sob responsabilidade do Banco;
b) Gerir a segurança da informação de acordo com os princípios do menor privilégio (permissões necessárias e suficientes para a realização das actividades e desempenho das funções), necessidade de saber e segregação de funções;
c) Estabelecer, manter e melhorar de forma contínua, um Sistema Integrado de Gestão que enderece a Segurança da Informação;
d) Garantir a formação, consciencialização e comprometimento dos Colaboradores do Banco para o cumprimento adequado da Política Global de Segurança da Informação e normativo associado;
e) Garantir, desde a fase inicial, que as preocupações com a Segurança da Informação são adequadamente endereçadas em todos os projectos.

2.5 MODELO DOCUMENTAL

A Política Global de Segurança da Informação, fornece os objectivos e orientações para a gestão da Segurança da Informação no Banco. Esta política é suportada por um conjunto de documentos de vários níveis, de acordo com o estabelecido no normativo interno que formaliza a estrutura normativa do Banco e os processos de aprovação subjacentes.

2.6 MODELO DE GOVERNO

A segurança da informação, cada vez mais importante nas organizações modernas, é um dos activos mais relevantes para o negócio, em particular no contexto do BFA. A eficácia e a eficiência da segurança da informação poderão ser afectadas negativamente pela falta de atribuição de funções e responsabilidades neste âmbito. Com o intuito de robustecer e garantir a consistência do âmbito de actuação desta estrutura organizacional, foram consideradas as seguintes linhas de orientação:

- Promover o alinhamento entre os objectivos de negócio e segurança da informação;
- Dotar o BFA de uma estrutura de controlo e monitorização de segurança da informação;
- Qualificar e quantificar os benefícios da segurança da informação para o cumprimento dos objectivos estratégicos do BFA.

As funções posteriormente descritas são caracterizadas pelas suas responsabilidades no Sistema de Gestão da Segurança da Informação (SGSI) e nas funções dos processos aplicáveis, bem como na relação que a estrutura organizacional de Segurança da Informação poderá ter com outros processos que suportam as actividades de planeamento, operação, manutenção e melhoria contínua do SGSI.

O modelo de Governo foi estruturado em conformidade com o Modelo de Governação, tendo em consideração, designadamente, os seguintes princípios estruturantes: (i) o Conselho de Administração é globalmente responsável por manter e supervisionar uma governação adequada da Segurança da Informação; (ii) o Banco adopta uma estrutura organizacional consistente com o princípio do modelo das três-linhas de defesa; (iii) especificamente, o SGSI opera sob os limites estabelecidos no Quadro de Apetência pelo Risco (*Risk Appetite Framework*, RAF) e produz os indicadores para reporte em âmbito da Declaração de Apetência pelo Risco (*Risk Appetite Statement*, RAS).

2.6.1 AS TRÊS LINHAS DE DEFESA ENQUANTO MODELO ORGANIZACIONAL

A organização do SGSI segue uma estrutura baseada no princípio da segregação de funções, assegurando uma separação entre as responsabilidades de identificação, controlo e monitorização dos riscos.

O princípio a que o número anterior se refere é operacionalizado de acordo com o modelo das três linhas de defesa (Figura 1). ~

A utilização deste modelo tem como objectivo clarificar a distribuição de responsabilidades entre áreas de negócio e suporte, áreas de supervisão e as de revisão independente.

Complementarmente a estas linhas de defesa, a organização está sujeita à fiscalização por auditores externos e autoridades de supervisão.

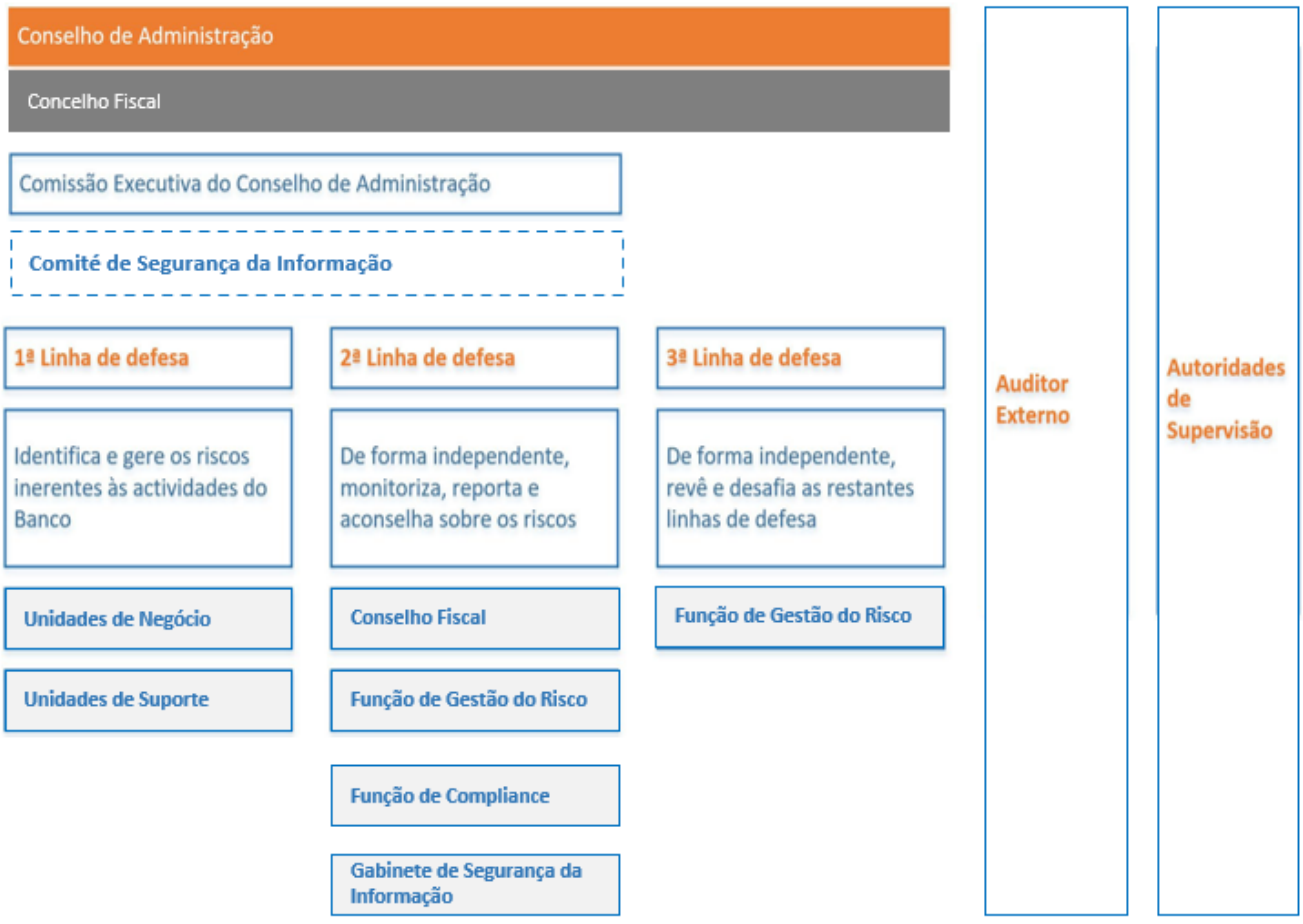

Figura 1 - Modelo organizacional do sistema de gestão da Segurança da Informação

2.6.1.1 PRIMEIRA LINHA DE DEFESA

Na primeira linha de defesa encontram-se as Direcções do Banco que são proprietárias dos activos de informação. Estas unidades são as primeiras responsáveis por identificar e gerir os riscos de Segurança da Informação que resultam das actividades do Banco e são inerentes à sua estratégia de negócio.

Situados igualmente na primeira linha encontram-se a Direcção de Sistemas de Informação (DSI) assim como o Responsável de Segurança Física, enquanto órgãos de suporte às Direcções na gestão do risco de Segurança da Informação e tendo em conta o caracter específico e especializado do tema.

2.6.1.2 SEGUNDA LINHA DE DEFESA

Na segunda linha de defesa encontra-se o Conselho Fiscal, o Gabinete de Segurança da Informação, por inerência o Responsável de Segurança da Informação, a Direcção de Gestão dos Riscos (DGR), os quais devem assegurar, de forma independente, a monitorização das actividades das unidades da primeira linha de defesa relativamente aos riscos de Segurança da Informação identificando qualquer desvio face à estratégia, políticas e limites estabelecidos e promovendo as medidas de reacção a esse desvio, designadamente através do reporte aos órgãos de administração dos desvios verificados e alerta aos responsáveis pelo risco.

Também é incluída na segunda linha de defesa do Banco está a Direcção de Compliance, a qual é responsável por aferir o cumprimento das obrigações legais e das políticas e directrizes internas.

2.6.1.3 TERCEIRA LINHA DE DEFESA

A terceira linha de defesa é assegurada pela Direcção de Auditoria e Inspecção (DAI), a qual avalia a eficácia e a efectividade do SGSI, identificando insuficiências e oportunidades de melhoria, apresentando recomendações e mantendo os órgãos de administração e fiscalização informados sobre essas matérias.

2.6.2 ÓRGÃOS DE GOVERNAÇÃO

O Banco estabeleceu um modelo de governação, liderado pelo seu Conselho de Administração, cujo desenho procura dar suporte à gestão global dos riscos, preservando os valores associados à organização das três linhas de defesa.

A estrutura dos órgãos de governação integra responsabilidades a dois níveis:

a) Gestão estratégica — definição das estratégias, objectivos, princípios e políticas que governam o sistema de gestão do risco, bem como o controlo global da sua implementação;
b) Gestão operacional — gestão, monitorização e o controlo do negócio e dos riscos associados (é neste conjunto de responsabilidades que se enquadram a primeira e a segunda linha de defesa do Banco).

2.6.2.1 CONSELHO DE ADMINISTRAÇÃO (CA)

O Conselho de Administração é o responsável máximo pelo Sistema de Gestão da Segurança da Informação do Banco, desenvolvendo as suas responsabilidades de acordo com os termos definidos no seu regulamento interno. Neste âmbito, compete ao Conselho de Administração:

a) Definir e aprovar a estratégia e políticas de segurança de informação;
b) Nomear e desvincular o Responsável de Segurança da Informação em conformidade com as políticas internas vigentes, sob parecer da Comissão de Governo, Nomeações, Avaliações e Remunerações;

c) Estabelecer a remuneração do Responsável de Segurança da Informação e dos Colaboradores encarregues do seu exercício, em conformidade com a política vigente no BFA;
d) Dotar o Responsável de Segurança da Informação de recursos materiais, humanos e financeiros adequados à execução da missão que lhe está confiada;
e) Promover a autoridade do Responsável de Segurança da Informação dentro do Banco e apoiar as iniciativas de segurança de informação;
f) Aprovar os documentos de suporte às actividades do Responsável de Segurança da Informação, entre estes o Orçamento e o Regulamento da Função;
g) Definir o apetite aos riscos de Segurança da Informação, no quadro da aprovação e revisão do RAS do BFA;
h) Analisar as informações sobre segurança de informação apresentadas pela CECA e promover actuação, de forma atempada, sobre as recomendações apresentadas, assegurando a melhoria continua do SGSI.

2.6.2.2 CONSELHO FISCAL

O Conselho Fiscal além de fazer parte da 2ª linha de defesa, é responsável por fiscalizar a eficácia do sistema de controlo interno do Banco. Deve elaborar pareceres anuais, dirigidos ao CA, sobre o relatório de governação corporativa e controlo interno, avaliando a adequação e a eficácia dos controlos estabelecidos. As suas responsabilidades e competências estão formalizadas em documento próprio, conforme a legislação aplicável e normativos emitidos pelas entidades de Supervisão e Reguladoras.

2.6.2.3 COMISSÃO EXECUTIVA DO CONSELHO DE ADMINISTRAÇÃO (CECA)

A Comissão Executiva do Conselho de Administração (CECA), nos termos do seu regulamento interno, é responsável pela gestão corrente do Banco e a primeira responsável pela implementação do sistema de gestão do risco do Banco, respectivas políticas e limites de risco, incluindo os riscos de Segurança da Informação.

Neste âmbito compete à Comissão Executiva do Conselho de Administração:

a) Demonstrar o seu comprometimento com as temáticas da Segurança da Informação através do estabelecimento de objectivos e estratégias adequadas, que reflictam as inerentes necessidades operacionais, garantido a devida integração no planeamento e desenvolvimento organizacional;
b) Validar e submeter para aprovação do CA, as políticas, o plano estratégico e orçamento no âmbito da Segurança da Informação propostas pelo Responsável de Segurança da Informação;
c) Aprovar os critérios e métricas internas adequadas para a avaliação do desempenho dos controlos associados ao SGSI, propostos pelo Responsável de Segurança da Informação;
d) Implementar as estratégias e as políticas relacionadas com a Segurança da Informação, ou delegar essa função no Responsável de Segurança da Informação e outros órgãos de estrutura com o perfil adequado;
e) Analisar as informações sobre segurança da informação apresentadas pelo Responsável de Segurança da Informação e assegurar a monitorização do cumprimento das políticas e do plano estratégico no âmbito da Segurança da Informação, promovendo a melhoria contínua e aferindo que são atingidos os resultados pretendidos;
f) Promover activamente junto dos órgãos de estrutura do Banco a importância de uma gestão eficaz da Segurança da Informação e em conformidade com as políticas definidas neste âmbito, e que garanta que os princípios e requisitos subjacentes integram em permanência os processos da organização;
g) Garantir a disponibilização de recursos e atribuição das autoridades necessárias para atingir os objectivos estabelecidos no âmbito da Segurança da Informação;

h) Proporcionar as condições necessárias para a criação, aprovação e divulgação eficaz de normativos complementares em matéria de segurança da informação;
i) Decidir acerca da activação da Gestão de Crise no âmbito de incidentes de Segurança da Informação;
j) Validar e submeter a aprovação do Conselho de Administração a Política de Segurança da Informação e os objectivos de segurança da informação;
k) Assegurar postura de segurança da informação do Banco alinhada com o apetite de risco do Banco.

2.6.2.4 COMITÉ DE SEGURANÇA DA INFORMAÇÃO (CSI)

Ao Comité de Segurança da Informação (CSI) compete acompanhar a implementação, e posterior operação, do SGSI nos termos do previsto no seu Regulamento próprio. Compete, em especial, ao Comité:

a) Recomendar à CECA as linhas estratégicas relativamente à Segurança da Informação;
b) Propor à CECA políticas específicas, com respeito à operação do SGSI;
c) Acompanhar a evolução do Contexto Interno e Externo, promovendo a revisão periódica da documentação associada ao SGSI, e respectiva aprovação;
d) Criar e submeter à consideração da CECA, sempre que se justifique, os critérios e métricas internas adequadas para a avaliação do desempenho dos controlos associados ao SGSI, e supervisionar e avaliar, de forma crítica, o seu desempenho;
e) Reportar periodicamente à CECA a evolução da postura de segurança do Banco;
f) Apoiar as Direcções do Banco na adopção de boas práticas alinhadas com os requisitos de Segurança da Informação;
g) Propor à CECA, sempre que se justifique, a atribuição de responsabilidade sobre os riscos de Segurança da Informação;
h) Apoiar as restantes direcções, proprietários dos activos e proprietários dos riscos na criação dos planos de tratamento de risco no âmbito de Segurança da Informação, validar os planos elaborados e submetê-los à consideração da CECA, sempre que se justifique;
i) Monitorizar a implementação das medidas correctivas definidas no plano de tratamento de riscos;
j) Analisar os incidentes reportados e incorporá-los no processo de gestão de riscos para a Segurança da Informação.

2.6.2.5 RESPONSÁVEL DE SEGURANÇA DA INFORMAÇÃO

Ao Responsável de Segurança da Informação compete-lhe planear, implementar, coordenar e manter o SGSI e demais questões relacionadas com a segurança da informação do Banco. Compete em especial ao Responsável de Segurança da Informação:

a) Garantir o cumprimento das atribuições gerais da estrutura;
b) Definir o Plano de Actividades do Gabinete, alinhado com a estratégia definida, assegurando o acompanhamento da sua execução e monitorizando os resultados, de forma a identificar necessidades de ajustamento atempadamente;
c) Coordenar o Comité de Segurança da Informação, nos moldes previstos em Regulamento próprio deste órgão;
d) Nomear uma Equipa responsável pela implementação, monitorização e melhoria contínua do SGSI;
e) Garantir que este tem os meios e recursos adequados ao desenvolvimento das suas responsabilidades, considerando para o efeito os constantes avanços tecnológicos e a evolução do panorama de ameaças;
f) Constituir o ponto de contacto principal para a implementação ou tratamento de questões operacionais relacionadas com a Segurança da Informação;
g) Estabelecer, em articulação com o CSI, a estratégia de segurança da informação a ser adoptada pelo Banco;
h) Suportar a sua equipa na definição de metodologias, processos, procedimentos, controlos e directrizes adequadas para endereçar a implementação das Políticas de Segurança da Informação;

i) Supervisionar a implementação das políticas de segurança da informação;
j) Propor à CECA critérios e níveis de aceitação do risco da segurança da informação, validando-os previamente em CSI;
k) Apoiar as restantes Direcções, proprietários dos activos e proprietários dos riscos na criação dos Planos de Tratamento de Risco no âmbito de Segurança da Informação, para posterior validação em CSI;
l) Em articulação com a DGR, promover a avaliação regular dos riscos de segurança da informação e assegurar a implementação de medidas correctivas apropriadas definidas no Plano de Tratamento dos Riscos;
m) Garantir a actualização permanente da lista dos riscos pertinentes para o SGSI e, com uma cadência no mínimo trimestral, submetê-la para apreciação do CSI;
n) Estabelecer e submeter para validação do CSI métricas e indicadores definidos para monitorizar o desempenho do SGSI;
o) Submeter à consideração da CECA, sempre que se justifique, os critérios e métricas internas adoptados para a avaliação do desempenho dos controlos associados ao SGSI;
p) Realizar reportes regulares aos membros do CSI sobre o desempenho do SGSI, com base nas métricas definidas.
q) Monitorizar o cumprimento dos KPIs de segurança da informação através de revisões periódicas e análise de indicadores;
r) Garantir que, no âmbito da Segurança da Informação, estão a ser geradas as evidências necessárias para efeitos de auditoria;
s) Colaborar com as equipas de auditoria, fornecendo informação e evidências quando solicitado;
t) Garantir o suporte contínuo da Gestão de Topo para todas as iniciativas da segurança da informação assegurando inclusive, a cada momento, a definição clara de funções e responsabilidades;
u) Elaborar pareceres em matéria de segurança da informação sobre todas as iniciativas ou projectos corporativos que tenham um impacto ou possam impactar a segurança da informação do Banco;
v) Monitorizar a implementação de todas as actividades que visem melhorar continuamente o SGSI do Banco, promovendo a sua revisão, sempre necessário;
w) Garantir a operação, evolução e aumento da maturidade da organização em matérias de Segurança da Informação;
x) Promover a activação da Gestão de Crise junto do Responsável de Continuidade de Negócio e da CECA, sempre que se justifique.

2.6.3 INTERVENIENTES E RESPONSABILIDADES

Seguidamente são identificados os restantes intervenientes nos processos relacionados com a Segurança da Informação.

2.6.3.1 GABINETE DE SEGURANÇA DA INFORMAÇÃO (GSI)

Ao Gabinete de Segurança da Informação compete-lhe realizar a avaliação de riscos associados à segurança da informação, assegurar a monitorização e controlo de segurança, assim como responder adequadamente aos incidentes de segurança da informação e as medidas de controlo de segurança da informação na prática operacional do Banco, nos termos do definido no respectivo MEO. Compete em especial ao Gabinete de Segurança da Informação:

a) Garantir a definição da estratégia do Gabinete, alinhando-a com a estratégia do BFA, de forma a contribuir para a consecução dos objectivos do Banco;
b) Produzir, no âmbito da sua actividade, recomendações de natureza construtiva e implementável, com valor acrescentado para o Banco;
c) Identificar e propor iniciativas de optimização do Gabinete, em alinhamento com as tendências do sector, através da divulgação e/ou adopção das melhores práticas;
d) Definir o Plano de Acção do Gabinete, alinhado com a estratégia definida, assegurando o acompanhamento da sua execução e monitorizando os resultados, de forma a identificar necessidades de ajustamento atempadamente;

e) Garantir o reporte periódico ao Administrador do Pelouro das actividades desenvolvidas e do grau de concretização dos indicadores do Gabinete;
f) Elaborar, implementar e rever as políticas operacionais de segurança da informação, metodologias, processos, procedimentos, os controlos e as directrizes adequadas para endereçar a implementação das Políticas de Segurança da Informação;
g) Identificar, avaliar e gerir proactivamente os riscos de segurança da informação;
h) Desenvolver estratégias de mitigação e planos de tratamento para os riscos de segurança da informação identificados, assegurando que os mesmos sejam geridos dentro dos níveis de apetite ao risco definidos;
i) Garantir o cumprimento com os requisitos e controlos de Segurança da Informação estabelecidos na norma ISO/IEC 27001:2022 e com requisitos legais aplicáveis ao Banco e relevantes em matéria de segurança da informação, de forma a acompanhar activamente a operacionalização e o cumprimento de políticas, processos e procedimentos de segurança da informação;
j) Auxiliar a Academia BFA no elaborar do Programa de Formação e Awareness no âmbito de Segurança da Informação;
k) Apoiar o Responsável de Segurança da Informação na elaboração de pareceres e recomendações adequadas;
l) Promover a análise e gestão de vulnerabilidades de forma sistemática e contínua, trabalhando em conjunto com outras áreas para resolver vulnerabilidades e mitigar riscos;
m) Apoiar o Responsável de Segurança da Informação na elaboração de relatórios de status para a CECA, relativamente às iniciativas de Segurança da Informação em curso.
n) Realizar a monitorização contínua dos sistemas e redes para detectar actividades suspeitas ou anómalas;
o) Avaliar e priorizar os alertas de segurança para determinar quais requerem investigação imediata.
p) Identificar e documentar indicadores de comprometimento (IoCs) que possam ser utilizados para detectar actividades maliciosas;
q) Gerir e coordenar a resposta a incidentes de segurança de informação e cibernéticos;
r) Planear e executar simulações, simulacros e testes de segurança.

2.6.3.2 RESPONSÁVEL DE SEGURANÇA FÍSICA

Ao Responsável de Segurança Física compete-lhe planear, implementar, coordenar e manter os sistemas de segurança física relacionadas com o SGSI do Banco. Compete em especial ao Responsável de Segurança Física:

a) Implementar os controlos adequados para endereçar o estabelecido nas Políticas de Segurança da Informação, no âmbito da Segurança Física;
b) Implementar as medidas correctivas definidas no plano de tratamento de riscos, no âmbito da Segurança Física;
c) Constituir o ponto de contacto principal para a implementação ou tratamento de questões operacionais relacionadas com a Segurança Física;
d) Elaborar e manter actualizado Plano de Emergência, para posterior submissão para aprovação;
e) Reportar periodicamente aos membros do CSI o desempenho dos controlos de segurança física implementados, de acordo com as métricas definidas;
f) Analisar os relatórios gerados no âmbito das operações de Segurança Física e identificar situações de não-conformidade;
g) Acompanhar as actividades desenvolvidas no âmbito da gestão de incidentes relacionados com Segurança Física;
h) Elaborar, e submeter para análise do CSI, relatórios de incidentes relacionados com Segurança Física;
i) Garantir que, no âmbito da Segurança da Física, estão a ser geradas as evidências necessárias para efeitos de auditoria;
j) Colaborar com as equipas de auditoria, fornecendo informação e evidências quando solicitado.

2.6.3.3 RESPONSÁVEL DE CONTINUIDADE DE NEGÓCIO

a) Garantir que são endereçados os requisitos de continuidade da Segurança da Informação;

b) Garantir o alinhamento entre as iniciativas relativas à Continuidade de Negócio com a estratégia da Segurança da Informação.

2.6.3.4 DIRECÇÃO DE GESTÃO DE RISCO (DGR)

À DGR compete a monitorização dos riscos da Segurança da Informação de acordo com o definido no RAS e nos termos da respectiva MEO.

2.6.3.5 DIRECÇÃO DE AUDITORIA E INSPECÇÃO (DAI)

A DAI é responsável por avaliar o desempenho do SGSI em conformidade com a legislação e regulamentação em vigor, normativos internacionais (ISO/IEC 27001:2022 ou outros pertinentes), política de segurança da informação e as melhores práticas, nos termos do definido no respectivo MEO.

2.6.3.6 DIRECÇÃO DE SISTEMAS DE INFORMAÇÃO (DSI)

A DSI é responsável por garantir, em todo o ciclo de vida, que as soluções informáticas estão de acordo com os requisitos estabelecidos nas Políticas de Segurança da Informação, nos termos do definido no respectivo MEO. Compete-lhe nomeadamente submeter ao CSI a informação pertinente para a Segurança da Informação, relativa a novos projectos sob a sua competência.

2.6.3.7 DIRECÇÃO INSTALAÇÕES E PATRIMÓNIO (DIP)

À DIP compete elaborar e manter os Planos de Manutenção para os activos físicos sob a sua responsabilidade, nos termos do definido no respectivo MEO.

2.6.3.8 DIRECÇÃO DE EFICIÊNCIA QUALIDADE E INOVAÇÃO (DEQI)

A DEQI é responsável por assegurar que foram integrados os requisitos do SGSI nos processos da organização, em fase de formalização, nos termos do definido no respectivo MEO.

Compete-lhe adicionalmente submeter ao CSI a informação pertinente para a Segurança da Informação, relativa a novos projectos sob a sua competência.

2.6.3.9 DIRECÇÃO DE CAPITAL HUMANO (DCH)

A DCH é responsável por garantir a Segurança da Informação em todo o ciclo de vida da relação com os Colaboradores, nos termos do definido no respectivo MEO.

2.6.3.10 ACADEMIA BFA

A Academia é responsável por sensibilizar e formar os Colaboradores com respeito às boas práticas da Segurança da Informação, nos termos do definido no respectivo MEO.

2.6.3.11 DIRECÇÃO DE COMPLIANCE (DC)

A DC é responsável por zelar pelo cumprimento do estabelecido na legislação e regulamentação em vigor, no âmbito da Segurança da Informação, nos termos do definido no respectivo MEO. Compete em especial à Direcção de Compliance:

a) Estabelecer e manter um registo permanente e actualizado da legislação e dos normativos internos e externos a que o Banco está sujeito, no âmbito da Segurança da Informação;

b) Estabelecer e manter um registo permanente e actualizado com a identificação dos responsáveis pelo cumprimento do definido em normativos e pelos respectivos incumprimentos detectados.

2.6.3.12 RESTANTES DIRECÇÕES E OUTROS CARGOS COM FUNÇÃO DE LIDERANÇA

Os responsáveis de cada Direcção, assim como outros cargos relevantes com funções de liderança, desempenham um papel crucial na promoção e disseminação das práticas de segurança da informação, assegurando que estas sejam integralmente adotadas e respeitadas em todos os níveis da organização.

A Liderança de cada Direcção, juntamente com os detentores de outros cargos de importância estratégica na hierarquia organizacional que exercem funções de liderança, ocupam uma posição decisiva na promoção da segurança da informação. São assim, os principais responsáveis por conhecer, comunicar activamente, incentivar e assegurar a adesão e cumprimento das políticas de Segurança da Informação e às demais normas de segurança da informação em vigor, fortalecendo assim a cultura de segurança em toda a organização.

2.6.3.13 RESPONSÁVEIS POR PROCESSOS, PROPRIETÁRIOS DE ACTIVOS E PROPRIETÁRIOS DOS RISCOS

Compete aos responsáveis por processos, proprietários de activos e proprietários de riscos integrar os requisitos do SGSI nos processos sob sua responsabilidade, nos termos do previsto nos respectivos Regulamentos próprios (MEO). Compete-lhes nomeadamente:

a) Realizar a classificação de informação e definir os perfis de acesso a aplicar aos activos de informação sob sua responsabilidade;
b) Colaborar na realização e revisão periódica da apreciação de risco de Segurança da Informação dos processos e activos de informação sob a sua responsabilidade;
c) Identificar alterações ao contexto com impacto nos cenários de risco e nos controlos implementados;
d) Identificar requisitos de Segurança da Informação para a elaboração e planos de tratamento de risco de Segurança da Informação;
e) Elaborar e submeter para validação os planos para o tratamento dos riscos no âmbito da Segurança da Informação relacionados com os activos sob a sua responsabilidade e garantir que estes são geridos de forma apropriada.

2.6.3.14 COLABORADORES

Compete a todos os colaboradores a responsabilidade pela informação que transmitem e pelos activos que lhes são confiados. Neste sentido, é imperativo que assegurem a protecção efectiva dos activos e a confidencialidade das informações, abstendo-se de partilhar quaisquer dados ou detalhes aos quais não estejam explicitamente autorizados a divulgar.

Os colaboradores do BFA, independentemente das suas funções e responsabilidades, devem zelar pela Segurança da Informação do Banco. Assim sendo, é sua responsabilidade:

a) Conhecer e cumprir as Políticas de Segurança da Informação e demais normas sobre segurança da informação;
b) Informar os fornecedores e prestadores de serviços, bem como outras terceiras partes com quem contactem no desempenho das suas funções, sobre as responsabilidades e obrigações que lhes concernem, em matéria de segurança da informação;
c) Comunicar atempadamente os eventos e incidentes de segurança da informação com que se deparem, utilizando os mecanismos disponibilizados para o efeito;
d) Manter a informação de autenticação em segredo, assegurando que a mesma não é revelada a terceiros, propositada ou inadvertidamente;
e) Não divulgar informação sensível ou confidencial a terceiros sem autorização expressa, sob qualquer forma de comunicação.

2.7 MODELO DE GESTÃO

O modelo de gestão implementado visa sistematizar a implementação e melhoria contínua da Segurança da Informação, mantendo em permanência o alinhamento com os objectivos estratégicos.

As fases deste modelo incluem as seguintes actividades:

2.7.1 PREPARAÇÃO

- Análise do Contexto Interno e Externo;
- Identificação dos objectivos e orientações;
- Identificação dos requisitos legais e regulamentares.

2.7.2 GESTÃO DO RISCO

- Identificação dos activos de informação;
- Apreciação dos riscos;
- Avaliação e selecção de controlos de segurança;
- Definição do plano de tratamento do risco;
- Implementação de controlos.

2.7.3 MONITORIZAÇÃO E AUDITORIA

- Monitorização do desempenho e eficácia do SGSI;
- Realização de auditorias ao SGSI.

2.7.4 MELHORIA

- Tratamento de não conformidades identificadas;
- Implementação de acções correctivas.

2.8 EXCEPÇÕES

Todas as excepções ao presente documento deverão ser devidamente documentadas, incluindo o parecer do Comité de Segurança de Informação (CSI), e aprovadas formalmente pelo Conselho de Administração (CA).

CONTROLO DOCUMENTAL

PROPRIEDADES DO DOCUMENTO

Tabela 2— Propriedades do Documento

PROPRIEDADES DO DOCUMENTO					
Nome	Política Global de Segurança de Informação				
Tipo	Política	**Classificação**	PÚBLICO		
ID	489				
Versão	1/2025	**Referência**	POL/DSI/2025/001/V01	**Referência SG**	2025-2420-BFA CECA DOQ
Autor	DEQI	**Aprovador**	Conselho de Administração		
Data de Publicação	17/12/2025	**Data de Revisão**	17/12/2028		
Audiência	Colaboradores do Banco e Público em Geral.				
Disponibilização	Este documento encontra-se actualizado na intranet do Banco e no Site Público do BFA.				