POLÍTICA

CIBERSEGURANÇA

Ref: POL/GSI/2026/001/V01

Entrada em Vigor: 07/08/2026

Classificação de Segurança: **PÚBLICO**

CONTEÚDO

1 DISPOSIÇÕES GERAIS

1.1 OBJECTIVO E ÂMBITO

A presente Política de Cibersegurança fornece um conjunto de directrizes globais para a Cibersegurança do Banco Fomento Angola, S.A. Sociedade Aberta (adiante designado por BFA ou Banco) e estabelece os princípios, orientações e responsabilidades aplicáveis à protecção da informação e dos sistemas que a suportam, e endereça os pontos identificados, no presente documento, na Tabela 1 - Referências, Legislação, Regulamentação e Normas endereçadas.

O estabelecido neste documento aplica-se ao BFA e a todas as entidades legais relativamente às quais o Banco detenha, ou venha a deter, uma participação que lhe confira uma posição de controlo ou de domínio de gestão, a todos os Colaboradores, Fornecedores e Prestadores de Serviços, 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
Lei n.º 07/20217 - Lei de Protecção das Redes e Sistemas Informáticos
Aviso n.º 03/2026 - Regulamenta o Governo Societário e o Sistema de Controlo Interno e Define os Padrões Mínimos em que Deve Assentar a Cultura Organizacional das Instituições Financeiras
Aviso n.º 08/2020 - Política de Segurança Cibernética e Adopção de Computação em Nuvem
Instrutivo n. º10/2020 – Reporte de Incidentes de Segurança Cibernética
Directiva n.º 11/DSB/DRO/2021 – Guia de Implementação sobre a Gestão da Continuidade de Negócio das Instituições Financeiras
Circular 02-APD-24 - Incidentes e Acidentes Informáticos - APD
ISO/IEC 27001:2022 - Sistema de Gestão de Segurança de Informação
ISO/IEC 27002:2022 - Controlos de Segurança da Informação

Na tabela 2 - Normativos Internos relevantes são listados as Normas internas relevantes para o tema regulamentado no presente documento:

Tabela 2— Normativos Internos relevantes

NOME
Código de Conduta do BFA
Política Global de Segurança da Informação
Política Gestão Global dos Riscos
Política de Controlo Interno
Política Protecção de Dados Pessoais

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

Não aplicável.

1.5 RESPONSABILIDADES

O Comité de Segurança da Informação é responsável pela permanente actualização da presente Política.

A presente Política traduz-se nas responsabilidades dos intervenientes identificadas no presente documento no ponto 2.5 – Modelo de Governo.

1.6 OMISSÕES

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

1.7 NÃO CUMPRIMENTO

A violação do estabelecido no presente documento será objecto de análise por parte do Comité de Segurança de Informação (CSI) do BFA e, sempre que se justifique, da Direcção de Auditoria e Inspecção. Todas as violações identificadas deverão ser transmitidas ao Comité de Segurança de Informação (CSI) do BFA, de acordo com o estabelecido em Normativo Interno.

1.8 CONTACTOS

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

2 CONTEÚDOS REGULAMENTADOS

2.1 INTRODUÇÃO

A presente Política visa assegurar que a Cibersegurança seja integrada nos processos, actividades e decisões do Banco, contribuindo para a preservação da confidencialidade, integridade, disponibilidade e resiliência da informação, face a ameaças internas e externas.

2.2 DEFINIÇÃO

A Cibersegurança 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:

- Salvaguardar os interesses das partes interessadas;
- Garantir a conformidade com os requisitos legais, regulamentares e contratuais aplicáveis;
- Garantir que os riscos para a Cibersegurança são acompanhados, compreendidos, e mitigados até um nível aceitável pelo Banco;
- Controlar, prevenir e limitar o impacto de incidentes que possam pôr em causa a operação, imagem e reputação do Banco;
- Capacitar o Banco para gerir eficaz e eficientemente a Cibersegurança 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;
- Obter certificações relevantes no domínio da Segurança da Informação;
- 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:

- Garantir que todos os Colaboradores do Banco agem em conformidade com a Política de Cibersegurança e normativo interno 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;

- Gerir a Cibersegurança 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;
- Estabelecer, manter e melhorar de forma contínua, um Sistema Integrado de Gestão que enderece a Cibersegurança;
- Garantir a formação, consciencialização e comprometimento dos Colaboradores do Banco para o cumprimento adequado da Política de Cibersegurança e normativo interno associado;
- Garantir, desde a fase inicial, que as preocupações com a Cibersegurança são adequadamente endereçadas em todos os projectos.

2.5 MODELO DE GOVERNO

A Cibersegurança enquadra o Sistema de Gestão de Segurança de Informação (SGSI) do Banco enquanto subárea da Segurança da Informação, que orienta a protecção dos sistemas, redes, aplicações e dados contra as ameaças do meio digital (vulgo ciberespaço).

O modelo de Governo estabelecido observa designadamente os seguintes princípios estruturantes: (i) o Conselho de Administração é globalmente responsável por manter e supervisionar uma governação adequada; (ii) o Banco adopta uma estrutura organizacional consistente com o princípio do modelo das três-linhas de defesa; (iii) no cumprimento das orientações do Regulador, o Banco adopta o principio da proporcionalidade; (iv) os riscos de Cibersegurança são geridos sob os limites estabelecidos no Quadro de Apetência pelo Risco (Risk Appetite Framework (RAF), enquanto subárea da Segurança de Informação do Banco.

2.5.1 AS TRÊS LINHAS DE DEFESA ENQUANTO MODELO ORGANIZACIONAL

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

Este princípio é operacionalizado de acordo com o modelo das três linhas de defesa com o 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 actuação do Conselho Fiscal, dos auditores externos e autoridades de supervisão.

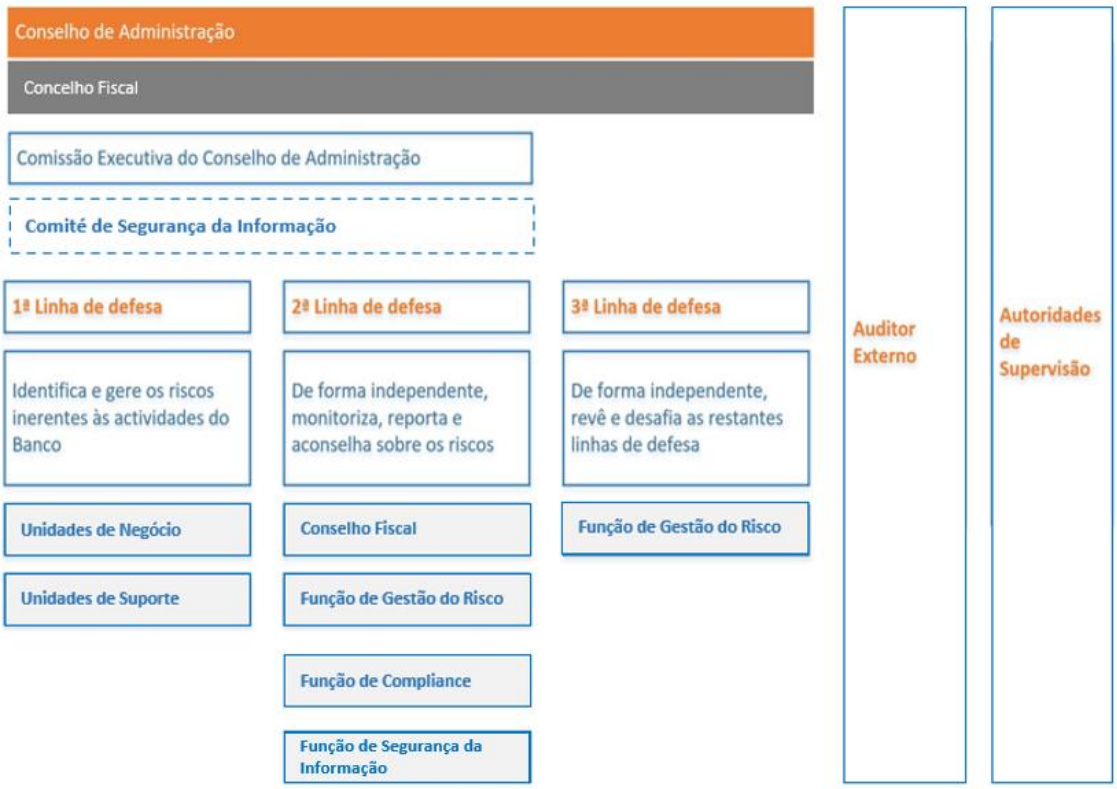

Figura 1 - Modelo organizacional do Sistema de Gestão da Segurança da Informação

2.5.2 ÓRGÃOS DE GOVERNAÇÃO

O Banco estabeleceu um modelo de governação para a Segurança de Informação definido na Política Global de Segurança de Informação, 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. Destacam-se os seguintes órgãos de governação no âmbito da subárea de Segurança de Informação - Cibersegurança.

2.5.2.1 CONSELHO DE ADMINISTRAÇÃO (CA)

As responsabilidades do Conselho de Administração são estabelecidas em regulamento próprio e adicionalmente na Política Global de Segurança de Informação. Em particular, compete-lhe:

- Aprovar a estratégia de Cibersegurança do Banco;
- Aprovar a presente Política e supervisionar a sua eficácia e cumprimento.

2.5.2.2 COMISSÃO EXECUTIVA DO CONSELHO DE ADMINISTRAÇÃO (CECA)

As responsabilidades da CECA são estabelecidas em regulamento próprio e adicionalmente na Política Global de Segurança de Informação. Em particular, compete-lhe:

- Assegurar a implementação da presente Política e aprovar os normativos internos necessários à sua aplicação.

2.5.2.3 FUNÇÃO DE SEGURANÇA DA INFORMAÇÃO

As responsabilidades da Função de Segurança da Informação constam de um regulamento próprio. No âmbito do presente documento, compete em particular à Função de Segurança da Informação:

- Identificar e controlar proactivamente os riscos de Cibersegurança e desenvolver estratégias de mitigação, apoiar e acompanhar os planos de tratamento, assegurando que os riscos são geridos dentro dos níveis de apetite ao risco definidos;
- Propor, em articulação com o CSI, a estratégia de Cibersegurança a adoptar pelo Banco e coordenar iniciativas neste âmbito;
- Propor e implementar metodologias, processos, procedimentos, controlos e directrizes adequadas para endereçar a implementação do estabelecido na presente Política e demais normativo interno, directa ou indirectamente relacionado;
- Garantir o cumprimento dos requisitos e controlos de Ciberseguranca estabelecidos pelo Banco bem como dos requisitos legais e regulamentares aplicáveis e relevantes;
- Estabelecer e acompanhar métricas e indicadores para monitorizar o desempenho do Banco no âmbito da Cibersegurança e supervisionar o cumprimento dos KPIs de Cibersegurança;
- Acompanhar o risco de terceiros, em especial fornecedores de serviços *on cloud*, desde a avaliação inicial de segurança até à monitorização contínua do cumprimento dos requisitos contratuais por fornecedores e parceiros;
- Promover a análise e gestão de vulnerabilidades de forma sistemática e contínua bem como, analisar relatórios operacionais e identificar situações de não conformidade;
- Promover e acompanhar a análise, resposta e resolução de incidentes de Cibersegurança ao longo do seu ciclo de vida, garantindo a comunicação às partes interessadas relevantes;
- Realizar reportes regulares aos órgãos relevantes sobre o desempenho e evolução da postura do Banco no âmbito da Cibersegurança;
- Propor e acompanhar acções de formação e de sensibilização dos Colaboradores do Banco em Cibersegurança.

2.5.2.4 RESPONSABILIDADES TRANSVERSAIS À ORGANIZAÇÃO

A responsabilidade pela Cibersegurança no Banco é partilhada por toda a organização, sendo assegurada de forma proporcional às funções, competências e níveis de intervenção de cada órgão ou direcção, em conformidade com o estabelecido nos seus regulamentos próprios, na Política Global de Segurança de Informação e demais normativo interno aplicável.

2.6 MODELO DOCUMENTAL

A presente 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 BFA e os processos de aprovação e de revisão subjacentes.

2.7 PRINCÍPIOS DE CIBERSEGURANÇA

O Banco adopta princípios de Cibersegurança orientados à protecção dos seus sistemas, redes, aplicações, dados, infra-estruturas tecnológicas e demais activos digitais, assegurando que estes são geridos de forma adequada ao seu nível de criticidade, sensibilidade e exposição ao risco.

2.7.1 GESTÃO DE ACTIVOS

Os activos do Banco devem ser identificados, inventariados, classificados e protegidos ao longo de todo o seu ciclo de vida, desde a sua criação ou aquisição até à sua descontinuação ou eliminação. A gestão destes activos deve permitir conhecer a sua finalidade, criticidade, proprietário, localização, dependências tecnológicas e requisitos de protecção, bem como suportar a definição dos controlos de Cibersegurança aplicáveis em função do risco associado.

2.7.2 CLASSIFICAÇÃO E PROTECÇÃO DA INFORMAÇÃO

A informação em formato digital deve ser classificada de acordo com o seu nível de sensibilidade, criticidade e impacto potencial para o Banco, clientes, colaboradores, parceiros e demais partes interessadas. A classificação da informação deve orientar a aplicação de medidas adequadas de protecção, incluindo restrições de acesso, mecanismos de encriptação, retenção, transmissão segura, cópias de segurança e eliminação controlada.

2.7.3 GESTÃO DE ACESSOS

O acesso aos sistemas, aplicações, redes, dados e demais recursos tecnológicos do Banco deve ser concedido com base nos princípios da necessidade de saber, menor privilégio, segregação de funções e rastreabilidade. A criação, alteração, revisão e revogação de acessos deve obedecer a processos formais, aplicáveis a utilizadores internos, externos e terceiros autorizados.

Os acessos devem ser periodicamente revistos, monitorizados e ajustados, sempre que ocorram alterações funcionais, organizacionais ou contratuais.

2.7.4 GESTÃO DE RISCOS DE CIBERSEGURANÇA

Os riscos cibernéticos devem ser identificados, avaliados, tratados e monitorizados de forma contínua, considerando ameaças, vulnerabilidades, impactos potenciais e a criticidade dos activos digitais afectados. O Banco deve adoptar medidas preventivas, detectivas, correctivas e de recuperação adequadas ao seu perfil de risco. As decisões de tratamento dos riscos devem ser devidamente documentadas, acompanhadas e revistas pelos órgãos e direcções competentes.

2.7.5 CONTINUIDADE E RESILIÊNCIA DE CIBERSEGURANÇA

A Cibersegurança deve contribuir para a continuidade e resiliência dos serviços digitais e processos críticos do Banco. Para esse efeito, devem ser implementados controlos que permitam prevenir, resistir, responder e recuperar de eventos cibernéticos capazes de afectar a disponibilidade, integridade ou confidencialidade dos sistemas e dados. Os planos de continuidade, recuperação tecnológica e resposta a incidentes devem contemplar cenários de ameaça cibernética, incluindo indisponibilidade de sistemas, perda de dados, comprometimento de infra-estruturas e falhas em serviços tecnológicos relevantes.

2.7.6 SEGURANÇA DE APLICAÇÕES E NOVAS TECNOLOGIAS

A adopção, desenvolvimento, alteração ou integração de aplicações e novas tecnologias deve incorporar requisitos de Cibersegurança desde as fases iniciais do ciclo de vida. O Banco deve assegurar que os projectos tecnológicos são avaliados quanto aos riscos de Cibersegurança, que os controlos necessários são implementados antes da entrada em produção e que existe segregação adequada entre ambientes de desenvolvimento, teste, homologação e produção. Sempre que aplicável, devem ser realizados testes de segurança, análise de vulnerabilidades e validações técnicas antes da disponibilização de novos serviços ou funcionalidades.

2.7.7 TESTES DE CIBERSEGURANÇA

O Banco deve realizar testes de Cibersegurança de forma periódica e sempre que alterações relevantes sejam introduzidas nos sistemas, aplicações, redes ou infra-estruturas tecnológicas. Estes testes devem permitir identificar vulnerabilidades, validar a eficácia dos controlos implementados e confirmar a correcção de falhas detectadas. Os resultados devem ser documentados, priorizados em função do risco e acompanhados até à implementação das medidas correctivas necessárias.

2.7.8 GESTÃO DE INCIDENTES DE CIBERSEGURANÇA

Os incidentes de Cibersegurança devem ser geridos através de processos formais de identificação, registo, classificação, análise, contenção, erradicação, recuperação e comunicação. O Banco deve assegurar que existem responsabilidades definidas, canais de reporte adequados e mecanismos de resposta proporcionais à gravidade e impacto dos incidentes. A gestão de incidentes deve incluir a análise de causa, a avaliação dos impactos, a definição de medidas correctivas e a incorporação das lições aprendidas na melhoria contínua dos controlos de Cibersegurança.

2.7.9 MONITORIZAÇÃO E PREVENÇÃO DE CIBERATAQUES

O Banco deve manter mecanismos de monitorização contínua dos seus ambientes tecnológicos, com o objectivo de detectar actividades suspeitas, comportamentos anómalos, tentativas de intrusão, software malicioso, vulnerabilidades exploráveis e outras ameaças de cibersegurança. A prevenção de ciberataques deve incluir a aplicação atempada de correcções de segurança, a protecção contra código malicioso, a gestão de vulnerabilidades, a monitorização de alertas, a prevenção de fuga de dados e a verificação do cumprimento dos requisitos de Cibersegurança definidos.

2.7.10 SENSIBILIZAÇÃO E CULTURA DE CIBERSEGURANÇA

O Banco deve promover uma cultura de Cibersegurança assente na sensibilização, formação e responsabilização dos Colaboradores, prestadores de serviços e demais terceiros abrangidos pela presente Política. As iniciativas de capacitação devem reforçar comportamentos seguros, boas práticas de utilização dos recursos tecnológicos, prevenção de *phishing* e engenharia social, protecção de credenciais, reporte de incidentes e cumprimento dos normativos internos aplicáveis.

2.7.11 ADOPÇÃO DE SERVIÇOS *CLOUD*

A utilização de serviços *cloud* deve observar os requisitos legais, regulamentares, contratuais e internos aplicáveis, considerando a criticidade dos serviços suportados, a sensibilidade dos dados tratados e os riscos associados ao acesso, armazenamento, processamento e transmissão da informação.

O Banco deve assegurar que os fornecedores de serviços *cloud* adoptam controlos de Cibersegurança compatíveis com os requisitos definidos pelo Banco.

2.8 DIVULGAÇÃO, REVISÃO E ACTUALIZAÇÃO

A presente Política de Cibersegurança deve estar disponível através dos canais internos definidos pelo Banco e no site BFA.

A Política deve ser revista periodicamente, na cadencia definida em normativo interno, ou sempre que ocorram alterações legais, regulamentares, tecnológicas, organizacionais ou de risco que justifiquem a sua actualização.

2.9 EXCEPÇÕES

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

CONTROLO DOCUMENTAL

PROPRIEDADES DO DOCUMENTO

Tabela 3— Propriedades do Documento

PROPRIEDADES DO DOCUMENTO					
Nome	Política de Cibersegurança				
Tipo	Política	**Classificação**	PÚBLICO		
ID	2198				
Versão	1 | 2026	**Referência**	POL/GSI/2026/001/V01	**Referência SG**	2026-1404-BFA CECA GSI
Autor	GSI	**Aprovador**	Conselho de Administração (CA)		
Data de Aprovação	30/07/2026	**Data de entrada em vigor**	07/08/2026		
Data de Publicação	07/08/2026	**Data de Revisão**	07/08/2027		
Proprietário do Documento	Comité de Segurança da Informação				
Audiência	Todos os Colaboradores e Público em geral				
Disponibilização	Este documento encontra-se actualizado na intranet do Banco e na Internet através do Site Publico BFA.				