Política de Segurança e de Sistema de Informação

Banco BAI Cabo Verde, S.A.
Edifício "BAICENTER" R/C •Chã D'Areia, Praia • Cabo Verde
Tel.: +238 2602300
Email: bai@bancobai.cv **• Portal:** www.bancobai.cv
C.R.P.C.A.P n.º 2728 • NIF 254746420
Capital Social: 2.092.385.000$00

Este documento foi elaborado em setembro de 2025 na sua versão inicial tendo posteriormente evoluído de acordo com as seguintes versões:

Versão	Motivo de alteração	Data	Responsável
V1	Revogação dos seguintes documentos: • Norma de Serviço nº 074/GSS/2024 - Política de Segurança da Informação; • Norma de Serviço nº 109/GSS/2024 - Política de Segurança Cibernética; • Norma de Serviço 075/GSS/2024 – Política de Segurança de Informação nas Relações com Fornecedores;	12/09/2025	CA

Índice

1. INTRODUÇÃO

A presente **Política de Segurança e de Sistema de Informação** do **Banco BAI Cabo Verde (BAICV)** constitui um documento que reflete os princípios e regras considerados fundamentais para garantir a segurança da informação e dos sistemas que a suportam, estabelecendo as diretrizes, os objetivos, as responsabilidades e os comportamentos necessários para gerir os ativos de informação num meio profissional seguro.

A presente Política estabelece como **principais objetivos**:

a) Reafirmar o comprometimento da Administração do BAICV com a melhoria contínua dos processos e recursos necessários para a segurança da informação, inovação e eficiência dos sistemas de informação;

b) Assegurar, por meio da definição de políticas, normas, procedimentos e controlos, a proteção dos ativos de informação nas vertentes da:

   I. **Confidencialidade** - Garantir que a informação seja de conhecimento exclusivo de pessoas especificamente autorizadas;

   II. **Integridade** - Garantir que a informação seja mantida, quer na forma como foi criada pelo seu autor quer no conteúdo, sem alterações indevidas - acidentais ou intencionais;

   III. **Disponibilidade** - Garantir que a informação esteja disponível a todas as pessoas autorizadas, em tempo útil.

c) Assegurar a conformidade do BAICV com os requisitos legais e regulamentares aplicáveis;

d) Assegurar adequada proteção dos sistemas e das informações do Banco, com uma abordagem orientada à gestão do risco;

e) Assegurar, através de procedimentos e de controlos, que toda a informação, independentemente da forma apresentada, seja protegida contra acessos indevidos, cópia, leitura, alteração, destruição e divulgação não autorizadas ou outros incidentes relevantes;

f) Assegurar, através de mecanismos de controlo de acesso, que os ativos de informação sejam acedidos e utilizados apenas por pessoas e para fins devidamente autorizados, estando sujeitos a monitorização, rastreabilidade e auditoria;

g) Assegurar a existência de processos para a continuidade de negócio e para a gestão de incidentes de segurança e de sistemas de informação, visando a proteção, deteção, resposta e recuperação face a ataques cibernéticos ou eventos disruptivos;

h) Promover programas de literacia digital, consciencialização e cultura de segurança da informação;

i) Promover o equilíbrio entre a segurança, a inovação e a produtividade.

2. ÂMBITO

Esta política aplica-se a:

a) Todos os utilizadores quer sejam colaboradores, clientes, prestadores de serviços, parceiros e qualquer entidade que tenha acesso aos sistemas de informação e ativos informacionais do Banco;

b) Toda a informação sob a responsabilidade ou uso do BAICV, independentemente do suporte de registo eletrónico, papel, audiovisual ou outro.

3. REFERÊNCIA

Na elaboração desta política, foram considerados legislação, regulamentação, códigos de conduta e outras boas práticas nacionais e internacionais reconhecidas ao nível dos sectores de atuação do BAICV.

Interno

- Política de Privacidade e Proteção de Dados;
- Código de Conduta;
- Política de Continuidade de Negócio;

Externo

- **Lei n.º 121/IX/2021 de 17 de março** que altera o regime jurídico geral de proteção de dados pessoais das pessoas singulares, aprovado pela Lei nº **41/VIII/2013**, de **17 de setembro;**
- **Decreto-lei nº 9/2021 de 29 de janeiro** que aprova o regime jurídico de cibersegurança;

- **Decreto-regulamentar nº 1/2021 de 29 de janeiro** que cria a Equipa de Resposta a Incidentes de Segurança Informática, define as suas funções e estrutura, bem como o seu enquadramento administrativo;
- Requisitos de Sistemas de Gestão de Segurança da Informação - **Norma ISO 27001:2022;**
- Requisitos de Sistema de Gestão de Continuidade de Negócio - **Norma ISO 22301:2022;**
- Requisitos de Segurança da Informação, Cibersegurança e Proteção da Privacidade: Critérios de Avaliação da Segurança Informática – **Norma ISO/IEC 15408-1:2022;**
- *Framework* **COBIT** (*Control Objectives for Information and Related Technologies*);
- *Framework* **ITIL** (*Information Technology Infrastructure Library*);
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de **27 de abril de 2016** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (**Regulamento Geral sobre a Proteção de Dados**).

4. TERMOS E DEFINIÇÕES

Ativos de informação*:* Aplica-se aos dados, às informações e aos sistemas de informação propriedade de ou usados pelo BAICV, bem como aos itens onde os dados são criados, processados, armazenados, transmitidos ou descartados, incluindo documentos em papel, telemóveis, computadores portáteis, estações de trabalho, servidores, equipamentos de rede e comunicação, dispositivos de armazenamento de dados, entre outros.

Sistema de Informação (SI): Qualquer recurso (sistemas, redes, serviços de rede, aplicações e informações) ou componente que armazena, transmite e processa dados de suporte aos processos e atividades do Banco.

Controlo de Acesso: Conjunto de procedimentos e meios utilizados com a finalidade de permitir ou bloquear um acesso após confirmação da autenticidade do utilizador.

Sistema de Gestão de Segurança da Informação (SGSI): Conjunto de medidas, políticas, processos, procedimentos, diretrizes e recursos associados, geridos coletivamente por uma organização, com o objetivo de proteger suas informações e garantir a confidencialidade, integridade e disponibilidade dessas informações.

Segurança da Informação: Preservação da confidencialidade, integridade e disponibilidade da informação.

Segurança Cibernética: Conjunto de medidas para proteger os sistemas digitais e redes contra-ataques cibernéticos.

5. PRINCÍPIOS ORIENTADORES

As políticas, normas, processos, procedimentos e todas as abordagens do BAICV relacionadas à segurança e sistemas de informação, quer na sua definição quer na sua concretização diária, orientam-se pelos seguintes princípios:

a) **Alinhamento estratégico:** O BAICV preza para garantir que os sistemas de informação estejam alinhados com os seus objetivos estratégicos e funcionem de forma eficiente e eficaz, devendo os sistemas apoiar diretamente os processos bancários, melhorar o atendimento ao cliente e promover a inovação;

b) **Garantia de proteção:** A informação é um recurso crítico para o eficaz desenvolvimento de todas as atividades do BAICV, sendo assim fundamental garantir a sua adequada proteção, nas vertentes de integridade, disponibilidade e confidencialidade;

c) **Conformidade:** Tanto a presente política como as tarefas executadas no seu âmbito estão sujeitas à legislação aplicável bem como às normas e regulamentos internos, especialmente as relativas ao tratamento de dados pessoais, informação privilegiada e salvaguarda do sigilo bancário;

d) **Necessidade de saber:** O acesso à informação deve restringir-se, exclusivamente, às pessoas que tenham necessidade de a conhecer para cumprimento das suas funções e tarefas;

e) **Privilégio Mínimo:** Ao utilizador devem ser atribuídos direitos/privilégios de acesso à informação e aos sistemas de informação estritamente necessários ao correto desempenho das suas funções;

f) **Segregação de funções**: Sempre que aplicável, a organização interna dos sistemas e segurança de informação deve considerar a segregação de funções entre operação e controlo, bem como a capacidade de gestão por perfis por forma que nenhum utilizador possa ter total autoridade para a realização completa de uma transação, operação ou atividade crítica;

g) **Transparência:** A transparência é assegurada, conjugando o dever de informar com a fixação, de forma clara, das regras e procedimentos a adotar para a segurança da informação sob a responsabilidade do BAICV;

h) **Proporcionalidade:** As atividades impostas pela segurança da informação devem ser proporcionais aos riscos a mitigar e limitadas ao necessário, minimizando a entropia no regular funcionamento do Banco;

i) **Responsabilidades:** As responsabilidades e o papel das entidades intervenientes na segurança da informação são definidos de forma clara e são alvo de monitorização e de auditorias periódicas;

j) **Avaliação do risco:** A avaliação do risco de segurança e sistemas de informação identifica os diversos tipos de ameaças a que a informação se encontra sujeita, contribuindo para a sua eliminação e os recursos utilizados na proteção da informação são diretamente proporcionais à relevância da informação a proteger e aos riscos de concretização das ameaças acima referidas;

k) **Controlo:** Todos os incidentes de segurança e de sistemas de informação, bem como as fragilidades detetadas na segurança da informação, são objeto de comunicação imediata e registo de forma a proporcionar uma resposta tempestiva. O processo de registo deve prever a identificação de um ponto único de contacto para onde devem ser canalizadas todas as comunicações atrás referidas;

l) **Comunicação:** Todas as políticas e normas relativas à segurança e sistemas de informação são publicitadas e comunicadas a todos os utilizadores que deles necessitem para o desempenho das suas funções e tarefas;

m) **Formação:** É planeado, aprovado e executado um plano de formação e de divulgação que incida sobre o domínio da segurança da informação e sobre as políticas e normas adotadas neste âmbito.

5.1. Organização e Planeamento

Os princípios orientadores para organização e planeamento têm por base as referenciais de boas práticas COBIT 2019, CIS Controls e ISO 27001, que permitam a gestão de fornecedores, arquitetura SI/TI, alinhamento com plano estratégico de negócio, gestão de colaboradores e gestão de risco envolvidos no registo, tratamento e disponibilização de informação.

Neste contexto, o BAICV assume os seguintes compromissos:

1. Garantir a definição formal de uma arquitetura de sistemas e tecnologias de informação composta por níveis de arquitetura aplicacional, tecnológica, gestão de SI/TI e governação de SI/TI, integrada com segurança de informação;
2. Garantir o alinhamento do plano estratégico de sistemas e segurança de informação com o plano estratégico de negócio;

3. Existência de um plano de atividades operacionais alinhado com os processos de sistemas e segurança de informação;
4. Garantir uma gestão de fornecedores adequada com risco de terceiras partes e garantir cláusulas contratuais adequadas, de níveis de serviço, conformidade de entidade contratada e racionalização de custos-benefícios;
5. Assegurar uma gestão eficiente de motivação, desenvolvimento, capacitação e desempenho de colaboradores em matéria de sistemas e segurança de informação;
6. Existência de programas de literacia em sistemas e segurança de informação para todos os utilizadores e colaboradores;
7. Assegurar uma gestão de *metadados* e classificação de informação digital e física como parte da classificação da informação enquanto orientação para criptografia e regulamentos de proteção de dados;
8. Assegurar uma gestão de ativos de SI/TI alinhados com imobilizado financeiro;
9. Existência de um sistema de gestão de risco e conformidade de sistemas e segurança de informação.

5.2. Aquisição e Implementação de Sistemas

Os princípios orientadores para aquisição e implementação têm por base as referenciais de boas práticas COBIT 2019, CIS Controls e ISO 27001, que permitam a gestão de ciclo vida de desenvolvimento seguro de ativos de SI/TI.

Neste contexto, o BAICV assume os seguintes compromissos:

1. Garantir a existência de requisitos técnicos, funcionais, de segurança e serviços para qualquer necessidade de aquisição ou desenvolvimento de ativos de SI/TI, quer seja por fornecedores quer seja por desenvolvimento interno;
2. Garantir a existência de metodologia de gestão de projetos que assegure o planeamento, execução, monitorização e encerramento de qualquer projeto;
3. Garantir a existência de metodologia específica para pequenas melhorias e correções de sistemas que assegurem a análise de impacto, planeamento, execução, monitorização e encerramento de alteração;

4. Assegurar o controlo de versões, configurações e gestão de passagem entre ambientes;

5. Assegurar segregação de funções entre quem desenvolve e quem coloca em produção qualquer sistema;

6. Assegurar a segregação entre quem solicita, quem implementa, quem testa e quem aprova qualquer implementação ou alteração de ativos de SI/TI;

7. Existência de ambientes tecnológicos de teste/qualidade, produção e recuperação de desastre para as aplicações críticas face à análise de impacto de negócio, bem como eventual ambiente de desenvolvimento;

8. Adotar metodologias de ciclo de desenvolvimento seguro para qualquer ativo de SI/TI, quer seja aplicacional, tecnológico ou de gestão de SI/TI que envolva software e/ou hardware;

9. Assegurar controlos de segurança aplicacional alinhados com padrões internacionais e devidamente testados antes de entrada em produção;

10. Assegurar controlos específicos de qualidade de informação em qualquer sistema aplicacional como parte dos testes técnicos e funcionais;

11. Assegurar a existência de documentação técnica e funcional de qualquer sistema antes da entrada em produção.

5.3. Operação de Sistemas

Os princípios orientadores para operação de sistemas têm por base as referenciais de boas práticas COBIT 2019, CIS Controls e ISO 27001, que permitam a gestão da operação de sistemas implementados.

Neste contexto, o BAICV assume os seguintes compromissos:

1. Assegurar a monitorização de sistemas aplicacionais ao nível de integridade, desempenho e disponibilidade via controlos preventivos e reativos face a comportamento de hardware e software;

2. Assegurar a monitorização de desempenho e disponibilidade de sistemas de gestão de base de dados;

3. Assegurar a monitorização de ativos específicos de redes e comunicações de dados para garantir o seu desempenho e disponibilidade;

4. Assegurar a salvaguarda de dados de sistemas e bases de dados para recuperação operacional e replicação para ambiente de recuperação de desastre tecnológico;

5. Assegurar as atualizações de hardware necessárias para prever eventuais anomalias;

6. Assegurar as atualizações de software necessárias para prever eventuais anomalias;

7. Existência de sistemas anti-malware de acordo com o tipo de dispositivos de hardware;

8. Registar os incidentes e problemas reportados por utilizadores, ou detetados de forma automática como parte dos processos de monitorização, por forma a manter o registo do ciclo de vida de identificação, análise, tratamento e encerramento de qualquer anomalia;

9. Assegurar a gestão física do Data Center primário caso On Premise ao nível de funcionamento de alarmística ambiental e acessos físico. No caso de Data Center externo, deve ser assegurada a análise de relatórios de cumprimento de melhores práticas e requisitos contratuais de serviço de Data Center.

5.4. Melhoria Contínua

O BAICV compromete-se em manter um **Sistema de Gestão de Segurança da Informação (SGSI)** fundamentado em padrões internacionais e orientado à gestão de risco de segurança e sistemas de informação.

A gestão da segurança da informação do BAICV assenta numa abordagem de acordo com o modelo **PDCA** (*Plan, Do, Check, Act*) previsto na norma **ISO/IEC 27001:2022** e compreende quatro fases:

1. **Planeamento** - tem por objetivo identificar periodicamente o risco de SI e planear as medidas de mitigação, de acordo com as orientações da **Norma de Gestão de Risco de Segurança e Sistemas de Informação**;

2. **Implementação** - tem por objetivo adequar e aplicar as Políticas e Normas da Segurança aos processos do Banco, bem como implementar as medidas de mitigação do risco e tratar os incidentes de Segurança da Informação;

3. Controlo - tem por objetivo assegurar que a política de segurança e que os processos e controlos definidos são aplicados;
4. Acompanhamento - tem por objetivo acompanhar de forma sistemática a adequação e a eficácia das Políticas para a Segurança da Informação.

6. RESPONSABILIDADES E ATRIBUIÇÕES

A segurança da informação e dos sistemas que a suporta é garantida pelos vários órgãos e unidades de estrutura do Banco, assenta em um modelo de governo e operação que envolve os seguintes papéis e responsabilidades:

a) Concelho de Administração (CA):

I. Aprovar a presente Política, bem como supervisionar a sua eficácia.

II. Delegar à Comissão Executiva (CE) a supervisão e a aprovação dos documentos para aplicação da política.

b) Comissão Executiva (CE):

I. Promover a implementação do SGSI e seu contínuo aprimoramento suportado por recursos apropriados para alcançar todos os objetivos definidos nas Políticas relacionadas à segurança e sistemas de informação;

II. Analisar o SGSI a fim de aferir a sua adequabilidade, eficácia e necessidade de ajustamento ou melhoria;

III. Decidir sobre a aprovação e revisão das políticas e normativos relativos à segurança e sistemas de informação.

c) Comissão de Supervisão de Gestão de Risco (CSGR):

I. Aconselhar o Conselho de Administração (CA) no que respeita à estratégia do risco de segurança e de sistema da informação;

II. Supervisionar a implementação da estratégia do risco de segurança e de sistema da informação.

d) Comissão de Supervisão de Controlo Interno (CSCI):

I. Propor alterações nas versões da Política de Segurança e de Sistemas de Informação, incluindo a revisão ou adoção de normas complementares;

II. Supervisionar as medidas aplicáveis nos casos de incumprimento das Políticas e/ou das Normas de Segurança e de Sistema de Informação complementares.

e) Direção de Segurança de Informação (DSI):

I. Implementar o Sistema de Gestão da Segurança da Informação (SGSI) de acordo com as políticas para a segurança e sistemas de informação instituídas, bem como reportar o seu desempenho;

II. Definir as políticas, normas, procedimentos e controlos de segurança da informação, assegurando a monitorização da sua aplicação e efetividade;

III. Coordenar as atividades operacionais de segurança dos sistemas de informação;

IV. Identificar e avaliar sistematicamente os riscos relacionados à segurança e sistemas de informação;

V. Participar na especificação dos requisitos de segurança na fase de gestão de projetos, independentemente do tipo de projeto.

f) Direção de Tecnologia de Informação (DTI):

I. Garantir que os sistemas de informação estejam alinhados com os objetivos do Banco e funcionem de forma eficiente e eficaz;

II. Garantir a integração da segurança da informação no planeamento, desenho, implementação, operação e exploração dos sistemas de informação;

III. Assegurar a implementação dos controlos tecnológicos de proteção aos ativos de informação;

IV. Manter atualizado um repositório centralizado com informação detalhada dos componentes de SI/TI, incluindo hardware, software, serviços e demais itens de configuração.

g) **Gabinete do Secretário da Sociedade (GSS)**:

I. Elaborar e manter atualizado o catálogo de processos do Banco;

II. Garantir a integração dos requisitos de segurança nos processos de negócio.

h) **Gabinete de Gestão de Risco (GGR)**:

I. Participar na revisão do Plano de Continuidade de Negócio (PCN), com base nos riscos de segurança e sistemas da informação e análise de impacto no negócio;

II. Apoiar a DSI, sempre que necessário, no tratamento de incidentes de segurança e de Sistema da informação, com foco no apuramento do risco dos mesmos para o Banco.

i) **Gabinete de Auditoria Interna (GAI)**:

I. Elaborar e manter atualizado um plano de auditoria para examinar e avaliar a adequação e a eficácia do sistema de controlo interno ao nível de conformidade dos sistemas de informação implementados com os princípios e regras definidos nas políticas para a segurança e sistemas da informação;

II. Emitir recomendações baseadas nos resultados das avaliações realizadas e verificar a sua observância;

III. Elaborar e apresentar aos vários órgãos a quem reporta relatórios periódicos com síntese das principais deficiências detetadas nas ações de controlo.

j) **Gabinete de Compliance (GCO)**:

I. Assessorar a elaboração e verificação da legalidade das normas, procedimentos, políticas e controlos utilizados para proteger os ativos de informação;

k) **Gabinete Jurídico e Contencioso (GJC)**:

I. Manter as unidades de estrutura informadas sobre eventuais alterações legais e/ou jurídicas que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;

II. Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, nomeadamente confidencialidade, privacidade e proteção de dados.

l) **Direção de Capital Humano (DCH)**:

I. Colaborar na promoção dos programas de consciencialização em matéria de literacia digital e cultura de segurança;

II. Disponibilizar informação sobre a movimentação de colaboradores (contratação, desvinculação, transferência, alteração de funções) de modo a permitir a gestão de identidade e controlo de acessos com base em perfil funcional.

m) **Unidades de Estrutura (UE)**:

I. Cumprir e fazer cumprir as Políticas e os Procedimentos de segurança e de Sistema da informação bem como as disposições legais e regulamentares vigentes sobre a segurança e de sistema da informação;

II. Assegurar que as suas equipas tenham acesso e conhecimento das Políticas e dos Procedimentos de Segurança e de Sistema da informação;

III. Comunicar ao DSI qualquer anormalidade, fragilidade ou violação, observada ou suspeita, que possa estar relacionada com um incidente de segurança da informação.

n) **Colaboradores**:

I. Conhecer, assumir e cumprir as políticas, normas e procedimentos de segurança vigentes, devendo comunicar, com carácter de urgência e segundo os procedimentos estabelecidos, as possíveis incidências ou problemas de segurança que detetem.

As responsabilidades pela gestão integrada da segurança da informação, da cibersegurança e da continuidade de negócio devem ser asseguradas pela **Direção de Segurança de Informação (DSI)**, enquanto a **Direção de Tecnologia de Informação (DTI)** é responsável pela gestão e exploração dos sistemas e tecnologias de informação.

7. INCUMPRIMENTO

O incumprimento dos princípios orientadores descritos na presente política pelos Colaboradores do BAICV, será considerado como uma violação das normas internas do Banco.

Como tal, a inobservância do conteúdo desta política, constituirá sempre uma infração disciplinar para colaboradores internos ou contratual para entidades externos, sem prejuízo da responsabilidade civil ou criminal que ocorra no caso, ficando o colaborador, ou entidade contratada em causa sujeita aos procedimentos legais e disciplinares que se mostrem adequados e aplicáveis às circunstâncias apuradas.

8. REVISÃO E ATUALIZAÇÃO

A presente política deve ser revista sempre que se considera desadequado em cumprimento da legislação ou regulamentação interna ou externa, e respeitando o tempo previsto para atualização definido no BAICV. Qualquer alteração ou revisão desta política deverá ser submetida ao Conselho de Administração para aprovação.

9. DIVULGAÇÃO E ACESSO

A presente política é objeto de divulgação através da intranet e disponibilizada igualmente em outros canais definidos para comunicação do Banco.