Política de Segurança Cibernética

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

As informações contidas neste documento são de propriedade do **Banco BAI Cabo Verde, S.A.**, sendo permitida a sua leitura somente aos seus colaboradores ou a pessoas devidamente autorizadas para o efeito.

Este documento foi elaborado em janeiro de 2012 na sua versão inicial tendo posteriormente evoluído de acordo com as seguintes versões:

Versão	Motivo de alteração	Data	Responsável
V2	Criação de novas Unidades de Estrutura Capítulo 4.7 - Definição da periodicidade para realização dos testes de intrusão Inclusão dos seguintes novos capítulos: • Incumprimento • Revisão e aprovação	15/09/2023	CA

Índice

1. Introdução e Objetivo 4

2. Melhores Práticas 5

3. Atribuições e Responsabilidades 6

3.1. Comissão Executiva (CE) 6
3.2. Comissão de Supervisão de Gestão de Risco (CSGR) 6
3.3. Comissão de Supervisão de Controlo Interno (CSCI) 6
3.4. Unidades de Estrutura 7
3.5. Colaboradores 7
3.6. Donos da Informação 8
3.7. Direcção de Tecnologias de Informação (DTI) 8
3.8. Direção de Segurança de Informação (DSI) 8
3.9. Gabinete Jurídico e Contencioso (GJC) 9
3.10. Direcção de Capital Humano 9
3.11. Gabinete de Gestão de Risco (GGR) 10
3.12. Gabinete de Auditoria Interna (GAI) 10

4. Gestão da Segurança Cibernética 10

4.1. Gestão de Ativos da Informação 10
4.2. Classificação da Informação 10
4.3. Gestão de Acessos 11
4.4. Gestão de Riscos Cibernéticos 11
4.5. Gestão da Continuidade de Negócios 11
4.6. Gestão de Segurança das Aplicações e Adoção de Novas Tecnologias 12
4.7. Testes de Segurança Cibernética 13
4.8. Gestão de Incidentes de Segurança de Informação Tecnológica 13
4.9. Monitoramento de Segurança da Informação e Prevenção contra Ciberataques 14
4.10. Sensibilização sobre Segurança Cibernética 14

5. Adoção da Computação em Nuvem 15

6. Disposições Finais 15

7. Divulgação e Acesso 15

8. Incumprimento 16

9. Revisão e aprovação 16

1. INTRODUÇÃO E OBJETIVO

Sendo a informação uma das variáveis determinantes na composição da oferta de produtos e serviços destinados aos seus clientes e colaboradores, através da presente Política de Segurança Cibernética o Banco BAI Cabo Verde está engajado em garantir a integridade, confidencialidade e disponibilidade dos seus sistemas de informação, das informações que estes sistemas manuseiam, da privacidade dos seus clientes e colaboradores, bem como no cumprimento de requisitos legais vigentes enquanto fornece, de uma maneira eficiente e efetiva, a gestão desta informação e do negócio.

A presente Política tem como principais objetivos

a) Garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, empregados e fornecedores do Banco.

b) Proteger adequadamente os sistemas e as informações do Banco.

c) Garantir a continuidade do negócio do Banco, protegendo os processos críticos de interrupções.

d) Garantir que sejam respeitadas as finalidades aprovadas pelo Banco durante a prestação de serviços de terceiros aquando da contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

A presente Política abrange controlos para assegurar a confidencialidade, integridade e disponibilidade de informações, assim como medidas preventivas e corretivas, voltadas ao controlo do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de pontos de vulnerabilidades.

Entre os principais controlos adotados pelo Banco, estão:

- Autenticação;
- Criptografia;
- Prevenção e deteção de invasão;
- Realização periódica de testes e varreduras para deteção de vulnerabilidades;
- Proteção contra software malicioso;

- Estabelecimento de mecanismo de rastreabilidade da informação;
- Controlos de acesso e de segmentação da rede de computadores;
- Manutenção de cópias de segurança dos dados e das informações;
- Desenvolvimento seguro;
- Gestão de incidentes;
- Consciencialização de utilizadores, clientes e fornecedores;
    - Iniciativas de consciencialização para a cultura de segurança cibernética, incluindo a implementação de programas de treinamento e de avaliação periódica de todos os colaboradores;
    - Iniciativas de sensibilização sobre a segurança cibernética para clientes, empresas terceiras e prestadores de serviços relevantes.

Com efeito, a presente Política rege-se pela regulamentação e melhores práticas sobre a matéria bem como pelos normativos vigentes.

Esta política aplica-se a todos os colaboradores e demais intervenientes nos sistemas de informação do Banco.

2. MELHORES PRÁTICAS

O modelo de Gestão da Segurança Cibernética está assente em *frameworks*, princípios e diretrizes internacionalmente aceitos, que visam assegurar a confidencialidade, integridade e disponibilidade das redes, dos dados e dos sistemas de informação utilizados, sendo eles:

- ISO/IEC 27001 - Sistemas de Gestão da Segurança da Informação
- ISO/IEC 27035 - Gestão de Incidentes de Segurança de Informação
- ISO/IEC 27032 - Guidelines for Cybersecurity
- NIST Cybersecurity Framework V1.1
- CIS Controls V8

3. ATRIBUIÇÕES E RESPONSABILIDADES

Para estabelecer o processo de Gestão da Segurança Cibernética é necessário determinar as atribuições e responsabilidades dos responsáveis e co-responsáveis pelos controlos internos de tecnologia e segurança da informação.

Cabe ao Conselho de Administração (CA) aprovar a Política de Segurança Cibernética e suas revisões, anualmente, ou sempre que seja considerado necessário, e delegar à Comissão Executiva (CE) a supervisão e aprovação dos documentos para aplicação da política.

3.1. Comissão Executiva (CE)

- Aprovar as autorizações de acesso para toda informação sob sua responsabilidade, na matriz que relaciona cargos e funções com as autorizações de acesso concedidas (Matriz de Acessos);
- Analisar os relatórios de controlo de acesso com objetivo de identificar desvios em relação à Política e Procedimentos de Segurança da Informação aprovados, devendo adotar as ações corretivas necessárias;
- Decidir sobre a aplicação de medidas disciplinares referentes aos casos de incumprimento da Política e dos Procedimentos de Segurança da Informação.

3.2.Comissão de Supervisão de Gestão de Risco (CSGR)

- Aconselhar o Conselho de Administração (CA) no que respeita à estratégia do risco de segurança da informação;
- Supervisionar a implementação da estratégia do risco de segurança da informação.

3.3.Comissão de Supervisão de Controlo Interno (CSCI)

- Propor alterações nas versões da Política de Segurança de Informação, incluindo a revisão ou adoção de normas complementares;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Supervisionar as medidas aplicáveis nos casos de incumprimento das Políticas e/ou das Normas de Segurança da Informação complementares.

3.4.Unidades de Estrutura

- Cumprir e fazer cumprir a Política e os Procedimentos de Segurança Cibernética bem como as disposições legais e regulamentares vigentes sobre a matéria;
- Assegurar que as suas equipas tenham acesso e conhecimento da Política e dos Procedimentos de Segurança Cibernética;
- Garantir que todos os colaboradores tenham acesso à Política e dos Procedimentos de Segurança Cibernética;
- Comunicar imediatamente ao DSI (Direção de Segurança de Informação) eventuais casos de violação de segurança, pelos canais definidos no Normativo relativo à Gestão de Incidentes de Segurança da Informação.

3.5.Colaboradores

- Cumprir fielmente a Política a Política e os Procedimentos de Segurança de Informação, incluindo o Regulamento Interno do Colaborador, o código de conduta e outros normativos aplicáveis;
- Buscar orientação do superior hierárquico direto em caso de dúvidas relacionadas com a segurança da informação;
- Assinar o Termo de Responsabilidade, concordando com a Política e Procedimentos de Segurança da Informação em vigor, bem como assumir responsabilidade pelo seu cumprimento;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo Banco;
- Assegurar que os recursos informáticos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Banco;
- Cumprir as leis e as normas que regulamentam os aspetos de carácter intelectual;
- Comunicar de imediato o superior hierárquico sobre qualquer incumprimento ou violação desta Política e dos Procedimentos definidos.

3.6.Donos da Informação

- Autorizar o acesso à informação devendo observar o definido na Matriz de Acessos e na Política e Procedimentos de Segurança da Informação;
- Cumprir com o estipulado na Política de Classificação da Informação do Banco.

3.7.Direcção de Tecnologias de Informação (DTI)

- Manter o registo e controlo atualizado de todos os acessos concedidos, determinando, sempre que necessário, a pronta suspensão, alteração ou cancelamento de acessos que não sejam necessários;
- Reavaliar, sempre que necessário, as autorizações de acesso concedidos, cancelando aquelas que não forem necessárias;
- Observar o cumprimento de normas de proteção e processamento de dados, bem como as normas inerentes a destruição de documentos;
- Participar da investigação de incidentes de segurança relacionados com a informação sob sua responsabilidade;
- Realizar testes na implementação de novas tecnologias e sistemas de informação antes de serem implementados na infraestrutura informática;

3.8.Direção de Segurança de Informação (DSI)

- Identificar, proteger, detetar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações;
- Rever, atualizar e divulgar a Matriz de Acessos;
- Verificar, regularmente, os acessos implementados nos sistemas de informação para garantir a conformidade com as políticas (perfis de acessos) definidas na Matriz de Acessos;
- Avaliar as notificações de incidentes de segurança da informação remetidos pelas unidades de estrutura e colaboradores;

- Acompanhar a investigação de incidentes de segurança relacionados com a informação sob sua responsabilidade;
- Identificar e avaliar sistematicamente os riscos relacionados à segurança da informação;
- Solicitar e/ou realizar testes e análise de risco na infraestrutura dos sistemas de informação a fim de certificar que as vulnerabilidades e riscos dos sistemas de informação são adequadamente resolvidos;
- Efetuar, periodicamente, controlos às Políticas de Segurança da Informação aprovadas para assegurar a sua confidencialidade.

3.9. Gabinete Jurídico e Contencioso (GJC)

- 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;
- Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do Banco;
- Avaliar, quando solicitada, os Procedimentos de Segurança da Informação em vigor.

3.10. Direcção de Capital Humano

- Dar a conhecer aos novos colaboradores a presente política e a Política de Segurança da Informação e obter a assinatura do Termo de Confidencialidade da Informação;
- Informar prontamente a DTI a admissão ou demissão de colaboradores para que possam ser cadastrados ou excluídos do quadro funcional do Banco;
- Disponibilizar mensalmente a lista de colaboradores suspensos, admitidos e demitidos, incluindo estagiários e transferências de áreas, para que a DTI possa estar informada e proceder à devida atualização no sistema de acesso;
- Adotar medidas disciplinares necessárias em caso de incumprimento do estabelecido na presente política e normativos relacionados aplicáveis.

3.11. Gabinete de Gestão de Risco (GGR)

- Participar na revisão do Plano de Continuidade de Negócio (PCN), com base nos riscos de sistemas de informação e de incidentes disruptivos;
- Apoiar a DSI, sempre que necessário, na definição de metodologia para avaliação do risco de cibersegurança.
- Apoiar a DSI, sempre que necessário, no tratamento de incidentes de segurança da informação, com foco no apuramento do risco dos mesmos para o Banco.

3.12. Gabinete de Auditoria Interna (GAI)

- 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 mecanismos de segurança cibernética implementados com os princípios e regras definidos nas políticas para a segurança da informação;
- Emitir recomendações baseadas nos resultados das avaliações realizadas e verificar a sua observância;
- Elaborar e apresentar aos vários órgãos a quem reporta relatórios periódicos com síntese das principais deficiências detetadas nas ações de controlo.

4. GESTÃO DA SEGURANÇA CIBERNÉTICA

O Banco possui políticas, regulamentos e procedimentos para assegurar que as informações estejam adequadamente protegidas, baseadas nos requisitos e nas melhores práticas reconhecidas pelo mercado.

4.1. Gestão de Ativos da Informação

Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, de eventuais adulterações de dados e ter documentação e planos de manutenção atualizados.

4.2. Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, abrangendo inclusive a criptografia de dados e de acordo com a classificação dos níveis de relevância:

- Confidencial;

- Restrita;
- Uso Interno; e
- Pública.

4.3. Gestão de Acessos

As concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso. Os acessos devem ser rastreáveis, a fim de garantir a identificação de acesso e transação.

Os níveis de controlos aplicados na gestão de controle de acessos do Banco variam de acordo com a classificação do ativo, incluindo, dentre outros, os seguintes mecanismos de controle:

- Controlos de autenticação;
- Criptografia;
- Controlos de autorização;
- Segregação de funções; e
- Revisão periódica de acessos.

4.4. Gestão de Riscos Cibernéticos

Os riscos cibernéticos devem ser mapeados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação do Banco, a fim de que sejam endereçadas as proteções adequadas.

4.5. Gestão da Continuidade de Negócios

Os controlos adotados pelo Banco, na gestão de infraestrutura tecnológica, possuem como objetivo primário garantir que o Banco se mantenha operacional frente a ameaças cibernéticas, de modo a assegurar a confidencialidade, integridade e disponibilidade da informação.

O gerenciamento de riscos cibernéticos deve garantir a manutenção da continuidade dos negócios, abrangendo serviços relevantes e a capacidade de continuar a entrega de produtos ou serviços em um nível mínimo aceitável e previamente definido, quando da ocorrência de um evento que interrompa as operações do Banco.

Os seguintes controlos devem ser adotados:

- Backup (cópias de segurança) dos dados e das informações;
- Elaboração de cenários de incidentes considerados nos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos; e
- Os resultados dos testes de continuidade de negócios devem ser informados para a confeção do relatório sobre o plano de ação e de resposta a incidentes.

4.6. Gestão de Segurança das Aplicações e Adoção de Novas Tecnologias

As principais premissas aplicáveis à gestão de segurança das aplicações e adoção de novas tecnologias pelo Banco devem incluir:

- O desenvolvimento de novas aplicações de serviços relevantes deve estar alinhado com as melhores práticas de segurança cibernética recomendadas por padrões internacionais e pelas políticas do Banco, específicas para desenvolvimento seguro;
- Na adoção de novas tecnologias também deve ser submetido a controlos de segurança cibernética proporcionais à classificação de criticidade do ativo, sendo que estas passam por processos de classificação, avaliação de riscos e implementação de correções ou adequações antes de serem disponibilizadas no ambiente produtivo;
- Controlos e mecanismos de rastreabilidade das informações;
- Testes de segurança, como teste de penetração e teste de código seguro, também devem ser executados para os serviços relevantes antes da implementação no ambiente de produção;
- Testes de segurança da informação gerais (como, por exemplo, análise de código seguro);
- Controlos para assegurar a segregação entre os ambientes de desenvolvimento, homologação/teste e produção, com o objetivo de reduzir os riscos de acessos não autorizados ou alterações indevidas no ambiente operacional, banco de dados e/ou aplicações.

4.7. Testes de Segurança Cibernética

A gestão de testes de segurança cibernética do Banco inclui os seguintes mecanismos de controle:

- Testes de segurança cibernética para novas aplicações;
- Testes de segurança cibernética para aplicações existentes;
- Testes de segurança cibernética para a infraestrutura de rede;
- Testes de intrusão, realizados por uma entidade externa, com periodicidade mínima trienal;
- Acompanhamento de correções segurança de falhas identificadas durantes os testes; e
- Execução de novos testes de segurança cibernética para confirmação de que as falhas foram corrigidas.

4.8. Gestão de Incidentes de Segurança de Informação Tecnológica

A gestão e plano de respostas a incidentes cibernéticos para serviços relevantes do Banco, inclusive os ocorridos em sistemas operados ou instalados em empresas contratadas que prestam serviços relevantes, deve ser executado considerando as análises de causa, impacto e efeito dos incidentes, bem como deve incluir, dentre outros, os seguintes controlos:

- Plano de Ações de Resposta a Incidentes;
- Medidas preventivas e mitigantes de incidentes relacionados com o ambiente cibernético;
- Processos e ferramentas utilizados na prevenção e resposta a incidentes;
- Designação de área responsável pelo registo e controle dos efeitos de incidentes relevantes;
- Registo de incidentes, com informações sobre papéis e responsabilidades;
- Classificação do incidente cibernético;
- Análise de causa e impacto;
- Recebimento de informações de fornecedores, relacionadas com incidentes com impacto na prestação de serviços relevantes;

- Definição de mecanismos para prevenir, detetar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
- Elaboração do relatório anual sobre o plano de ação e de resposta para incidentes;
- Iniciativas para compartilhamento de informações sobre os incidentes cibernéticos relevantes com outras instituições financeiras do Grupo BAI ocorridos no Banco e/ou comunicados pelos prestadores de serviços relevantes do Banco; e
- Comunicação tempestiva às entidades reguladoras e supervisoras das ocorrências de incidentes cibernéticos relevantes e das interrupções de serviços relevantes.

4.9. Monitoramento de Segurança da Informação e Prevenção contra Ciberataques

O processo de monitoramento de segurança da informação e prevenção contra ciberataques do Banco consistem em um conjunto de controlos e corretivos, com o objetivo de evitar a concretização de ameaças cibernéticas, dentre os quais destacam-se:

- Aplicação de atualizações e correções de segurança;
- Monitoramento de ataques cibernéticos e prevenção contra invasões;
- Verificação de conformidade de requisitos de segurança cibernética;
- Realização periódica de testes e varredura de vulnerabilidades;
- Monitoramento de status das ferramentas de anti-vírus e de alertas gerados;
- Proteção contra softwares maliciosos;
- Prevenção de fuga de dados.

4.10. Sensibilização sobre Segurança Cibernética

O Banco deve garantir a disseminação dos princípios e diretrizes de Segurança Cibernética por meio de programas de sensibilização e capacitação, fortalecendo a cultura de segurança cibernética e de informação, em todos os níveis operacionais.

5. ADOÇÃO DA COMPUTAÇÃO EM NUVEM

O Banco, quando da utilização de serviços em nuvem, atenderá aos critérios internacionalmente recomendados, considerando a criticidade e a sensibilidade dos dados e das informações suportadas pelo referido serviço, de acordo com a sua classificação, bem como o risco associado em caso de acesso indevido.

Na gestão de seus fornecedores de serviços em nuvem, o Banco busca principalmente garantir a execução de controlos para prevenção de incidentes a serem adotados por fornecedores que tratam dados sensíveis ou que sejam relevantes para as atividades do Banco. Os referidos controlos devem ser compatíveis com os processos e mecanismos de segurança cibernética adotados pelo próprio Banco.

6. DISPOSIÇÕES FINAIS

A presente Política é parte integrante dos regulamentos internos do BAI Cabo Verde. O seu incumprimento será considerado como uma violação das normas internas do BAI Cabo Verde. Assim, a inobservância e incumprimento dos princípios e regras constantes desta Política constituirá sempre uma infração disciplinar, sem prejuízo da responsabilidade civil ou criminal que ocorra no caso, ficando o colaborador em causa sujeito aos procedimentos legais e disciplinares que se mostrem adequados e aplicáveis às circunstâncias apuradas.

No que respeita a prestadores de serviços externos, a violação das políticas de segurança da informação pode resultar no imediato cancelamento das respetivas autorizações de utilização dos SI e/ou na suspensão ou termo da respetiva relação contratual, sem prejuízo de indemnizações a acionar.

Qualquer incumprimento ou violação das políticas de segurança da informação deve ser imediatamente reportado à DSI, sendo da competência deste assegurar o seu tratamento.

7. DIVULGAÇÃO E ACESSO

A presente Política de Segurança Cibernética deve ser divulgada a todos os colaboradores e deve estar acessível a qualquer colaborador para que possa ser consultada sempre que necessário. As alterações ou revisões devem ser prontamente comunicadas e divulgadas a todos os colaboradores do Banco e entidades externas relevantes.

Este documento poderá ser divulgado a partes interessadas externas como são o caso de entidades reguladoras e supervisoras.

A sua publicação será sempre feita em modo seguro, em formato digital PDF, através do uso de controlos de segurança adequados a este objetivo.

8. INCUMPRIMENTO

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

9. REVISÃO E APROVAÇÃO

A presente Política deve ser revista anualmente ou sempre que seja considerada desadequada em cumprimento da legislação e regulamentação em vigor.

Qualquer alteração ou revisão desta política deverá ser submetida ao Conselho de Administração para aprovação.