Política de Gestão da Continuidade de Negócio

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

Índice

1. INTRODUÇÃO

O Banco BAI Cabo Verde, doravante denominado por "BAICV", tendo em conta o mercado financeiro nacional e internacional em que se insere, os requisitos de regulamentação nacional a que se obriga e os compromissos de serviço que assume para com os seus clientes e investidores, define a garantia de continuidade das suas atividades críticas de suporte ao negócio como sendo fundamental para a sua credibilidade junto das partes interessadas identificadas.

Neste domínio, é de ressalvar que o Banco de Cabo Verde (BCV) determina, através do seu Aviso n.º 4/2017, que as instituições financeiras devem proceder à "definição, implementação e manutenção de planos de continuidade de negócio e ou de recuperação em caso de catástrofe".

O BAICV decidiu promover a implementação de um sistema de gestão para a continuidade de negócio, baseado em normas de referência internacionais e nas boas práticas que permitem a demonstração de eficácia para as medidas de tratamento do risco e dos controlos de segurança aprovados para este efeito.

2. ÂMBITO

Esta política aplica-se a:

a) Todos os utilizadores quer sejam colaboradores, clientes, prestadores de serviços, parceiros e qualquer entidade que no âmbito de continuidade de negócios, se relaciona com o Banco;

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.

Externo

- ISO 27001: A ISO (International Standards Organization) é uma entidade que estabelece a norma 27001 com vários padrões para a gestão de sistemas de segurança de informação;
- ISO 22301: A ISO (International Standards Organization) é uma entidade que estabelece a norma 22301 que define o padrão para a gestão de continuidade de negócio;

- **Aviso do Banco de Cabo Verde Nº 4/2017**, que determina a obrigatoriedade de as instituições financeiras procederem à "definição, implementação e manutenção de planos de continuidade de negócio e ou de recuperação em caso de catástrofe".

4. TERMOS E DEFINIÇÕES

Sistemas de SI: conjunto de aplicações, serviços, ativos de tecnologia da informação, ativos de TIC ou outros componentes do tratamento da informação, que inclui o ambiente de operação;

Serviços de SI: serviços fornecidos através de sistemas e prestadores de serviços de SI a um ou mais utilizadores internos ou externos;

Monitorizar: Processo que permite controlar, supervisionar, acompanhar e avaliar os registos que garantem a confidencialidade, a integridade e a disponibilidade dos ativos do BAICV;

Ativo de SI: um ativo de programas informáticos ou de equipamentos informáticos que se encontra no ambiente empresarial;

Ativo de informação: conjunto de informações, tangíveis ou intangíveis a proteger;

Ativo crítico: Ativo que suporta pelo menos um serviço essencial;

Proprietário do ativo: pessoa ou entidade com responsabilidade e autoridade sobre um ativo de informação e de SI;

Utilizador: todas as pessoas, singulares ou coletivas que interagem com a informação sob a responsabilidade do BAICV;

Utilizador interno: colaboradores, independentemente do seu vínculo contratual com o BAICV;

Utilizador externo: prestadores de serviços externos e outras pessoas, singulares ou coletivas, que necessitem de acesso a ativos de informação do BAICV;

Confidencialidade: característica que inibe a disponibilização ou a divulgação de informação a particulares, entidades, processos ou sistemas não autorizados;

Disponibilidade: característica de ser acessível e utilizável prontamente a pedido por uma entidade autorizada;

Integridade: característica de exatidão e integralidade;

Segurança da informação: preservação da confidencialidade, integridade e disponibilidade de informações ou dos sistemas de informação, podendo ainda envolver outras características, tais como autenticidade, responsabilidade, não rejeição e fiabilidade;

Cibersegurança: preservação da confidencialidade, integridade e disponibilidade de informações ou sistemas de informação através de meios cibernéticos;

Incidente: Um evento que constitui uma ameaça aos ativos do BAICV;

Incidente operacional ou de segurança: evento único ou uma série de eventos conexos e não previstos que têm, ou poderão vir a ter, um impacto negativo na integridade, disponibilidade e confidencialidade dos serviços e sistemas;

Gestão do risco: Atividades coordenadas para dirigir e controlar os riscos que constituem uma ameaça à segurança da informação do BAICV;

Risco: Uma circunstância ou um evento razoavelmente identificável, com um efeito adverso potencial na segurança das redes e dos sistemas de informação;

Tolerância ao risco: Disposição do BAICV para assumir o risco após o seu tratamento, por forma a poder alcançar os seus objetivos;

Ameaça: Potencial causa de um incidente que pode provocar danos aos ativos da BAICV;

Impacto: efeito de uma atividade ou circunstância que possa colocar em causa a integridade, disponibilidade ou confidencialidade da informação do BAICV;

Ciberataque: qualquer tipo de pirataria informática que conduza a uma tentativa prejudicial ou maliciosa de destruir, expor, alterar, incapacitar, roubar ou obter acesso não autorizado ou fazer uma utilização não autorizada de um ativo de informação que tenha como alvo os sistemas;

Prestador de serviços: entidade terceira que desempenha, no todo ou em parte, um processo, um serviço ou uma atividade ao abrigo de um acordo de subcontratação;

Evento ou Ameaça: evento ou fenômeno que provoca o desastre;

Vulnerabilidade: falhas ao nível do recurso (e.g. Erros de programação, erros de configuração, desenho inadequado de processos, materiais inadequados para as instalações) que podem causar falha de funcionamento do recurso;

Crise: momento em que ocorre qualquer incidente que comprometa a operação da empresa;

Contingência: é o momento em que há a mobilização de recursos para responder ao evento e garantir a continuidade das atividades críticas durante este evento;

RTO (Recovery Time Objective): tempo após desastre para disponibilizar recursos críticos. É interpretado como tempo máximo que um processo pode estar indisponível sem se ativar recursos alternativos para a continuidade de negócio;

RPO (Recovery Point Objective): tempo máximo de dados salvaguardados antes do desastre. É interpretado como a quantidade de dados salvaguardados a uma determinada data antes do desastre que permita a sua recuperação em caso de desastre dentro de um período aceite pela organização para perda de dados entre essa data de salvaguarda e data de desastre.

5. PRINCÍPIOS ORIENTADORES

5.1. Princípios

As normas de continuidade de negócio do BAI Cabo Verde, quer na sua definição, quer na sua concretização diária, orientam-se pelos seguintes princípios:

a) Alinhamento com gestão de risco por processo: a classificação de ativos para efeito de determinação de recuperação de desastre tem por base os riscos por processos analisados numa perspetiva de impacto para o negócio em caso de ocorrência de incidente;

b) Visão integrada de continuidade de negócio:

1. Continuidade operacional para incidentes em ativos de infraestrutura física patrimonial onde ocorrem operações de negócio que implica uma deslocação de local de trabalho;

2. Continuidade tecnológica para incidentes em ativos de sistemas e tecnologias de informação de suporte aos processos de negócio que implica a execução de processos de forma alternativa.

c) Ao nível de política de continuidade geral deve-se considerar o seguinte:

1. Deve existir uma análise de eventos que possam originar situações de desastre ao nível de recursos físicos ou tecnológicos com avaliação de probabilidade de ocorrência;

2. Deve existir uma equipa de gestão de crise com colaboradores afetos em duplicado para cada função;

3. Todos os colaboradores devem, preferencialmente, ter um contacto alternativo pessoal para casos de desastre;

4. A entrada em situação de desastre deve ser determinada pela equipa de gestão de crise após análise do evento ocorrido e impacto associado;

5. O plano de continuidade de negócio deve ser testado no mínimo 1 vez por ano para simulação de desastres e verificação de eficiência e eficácia dos procedimentos e meios afetos ao funcionamento em contingência e recuperação da normalidade;

6. O resultado dos testes deve ser formalizado em relatório com menção explicita sobre melhorias a introduzir ao plano de continuidade de negócio e respetivas normas.

d) Ao nível de política de continuidade operacional deve-se considerar o seguinte:

1. Devem ser identificados os recursos físicos ao nível de edifícios onde existe atividade de colaboradores com modelo de funcionamento em contingência em caso de impedimento;

2. Devem ser definidos colaboradores críticos para modelo de funcionamento em contingência para garantir a continuidade de negócio, considerando no mínimo 2 recursos por unidade orgânica. Estes recursos devem ter acesso a Laptop para funcionamento em contingência;

3. Devem ser identificados os parceiros críticos para estabelecer um modelo de continuidade de interação com os mesmos em caso de contingência devido a desastres no BAICV, ou no próprio parceiro.

e) Ao nível de política de continuidade tecnológica deve-se considerar o seguinte:

1. Deve existir um Data Center alternativo, onde devem ficar alojados os recursos tecnológicos e backup de dados definidos como sendo críticos para a continuidade de negócio;

2. A definição de recursos tecnológicos a serem considerados para o Data Center alternativo deve basear-se numa análise de dependência face a processos de negócio com estabelecimento de RTO e RPO associado;

3. De acordo com o RTO e RPO definido, devem os sistemas em DR ser atualizado de forma adequada em termos de infraestrutura, software e dados para garantir os níveis de recuperação definidos.

5.2.Normas

1. As normas de continuidade de negócio são alteradas sempre que necessário para garantir a atualização face a mudanças ocorridas nas atividades do BAI Cabo Verde.

2. A não aplicação das normas de continuidade de negócio por razões técnicas, operacionais ou legais, só poderá ocorrer após:

a) Identificação, documentação, justificação e descrição da proposta de medidas que possam mitigar os riscos em causa;

b) Comunicação da informação descrita na alínea a), por escrito, ao Responsável de Continuidade de Negócio, que dá parecer;

c) Aprovação pela Comissão Executiva. Desta aprovação é dado conhecimento ao Responsável de Segurança da Informação.

3. Para manter a continuidade de negócio, são adotadas as seguintes normas de continuidade de negócio:

a) Definição e teste do plano de continuidade de negócio: estabelece os princípios de elaboração, atualização e teste do plano de continuidade de negócio.

b) Ativação do plano de continuidade de negócio: determina os princípios para a ativação, gestão em crise, recuperação de ativos e retorno à normalidade.

c) Comunicação do plano de continuidade de negócio: descreve os princípios de comunicação e formação do plano de continuidade de negócio para colaboradores, parceiros e reguladores.

d) Retorno à normalidade: descreve as ações necessárias para que se possa voltar a operar normalmente após um incidente ou desastre que tenha afetado as atividades.

6. RESPONSABILIDADES E ATRIBUIÇÕES

A gestão da continuidade de negócios é suporta e 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:

b) **Conselho de Administração (CA)**: Órgão social composto por administradores executivos e não-executivos do Banco responsável, no âmbito das suas funções, pela aprovação da presente política.

c) **Comissão Executiva (CE)**: Órgão de gestão corrente do Banco responsável, no âmbito das suas atribuições, pela aprovação dos normativos que regulam a atividade do Banco e pela promoção da implementação do Sistema de Gestão da Continuidade de Negócio (SGCN) e seu contínuo aprimoramento suportado por recursos apropriados para alcançar os objetivos estabelecidos.

d) **Comissão de Supervisão de Gestão de Risco (CSGR):** Órgão de supervisão e controlo, encarregue de auxiliar e aconselhar o Conselho de Administração (CA) no que respeita à estratégia de gestão dos riscos do Banco.

e) **Comissão de Supervisão de Controlo Interno (CSCI):** Órgão de supervisão e controlo, encarregue de auxiliar o Conselho da Administração (CA) na supervisão geral e fiscalização do controlo interno, auditoria e conformidade com as políticas, normas e requisitos do negócio.

f) **Direção de Segurança de Informação (DSI):** Unidade de estrutura responsável, no âmbito das suas atribuições, pela implementação das Políticas de Segurança de Informação e pela coordenação

operacional do Sistema de Gestão da Continuidade de Negócio (SGCN) e do Plano de Continuidade de Negócio (PCN).

g) **Gabinete de Gestão de Risco (GGR):** Unidade de estrutura responsável, no âmbito das suas atribuições, em participar na revisão do Plano de Continuidade de Negócio (PCN) com base nos riscos operacionais e de continuidade das atividades críticas do Banco.

h) **Gabinete de Marketing e Comunicação (GMC):** Unidade de estrutura responsável, no âmbito das suas atribuições, pela definição e execução dos procedimentos de comunicação com as partes interessadas identificadas em função da análise de cada situação do PCN.

i) **Gabinete de Auditoria Interna e Inspeção (GAI):** Unidade de estrutura responsável, no âmbito das suas atribuições, pela realização de ações de auditoria, de forma a assegurar o controlo e cumprimento das orientações, processos e procedimentos de Gestão da Continuidade de Negócio estabelecidos nesta política e demais normativos aplicáveis.

j) **Direção de Capital Humano (DCH):** Unidade de estrutura responsável, no âmbito das suas atribuições, pela componente humana da continuidade de negócio e pela promoção de ações de formação e capacitação nesta matéria.

k) **Gabinete do Secretário da Sociedade (GSS):** Unidade de estrutura responsável, no âmbito das suas atribuições, pelo levantamento e atualização do catálogo de processos, bem como pela colaboração na definição da criticidade dos mesmos.

l) **Direção de Tecnologias de Informação (DTI):** Unidade de estrutura responsável, no âmbito das suas atribuições, pela componente tecnológica da continuidade de negócio.

m) **Direção de Banca Digital (DBD**) – Unidade de estrutura responsável, no âmbito das suas atribuições, sendo responsável pela conceção, desenvolvimento, gestão e evolução contínua de todos os canais digitais do Banco em conformidade com a Política de Gestão da Continuidade de Negócio.

n) **Direção de Património e da Sociedade (DPL):** Unidade de estrutura responsável, no âmbito das suas atribuições, pela componente logística e de edificado relacionados com a continuidade de negócio.

o) **Gabinete Jurídico e Contencioso (GJC):** Unidade de estrutura responsável, no âmbito das suas atribuições, por assessorar a elaboração e verificação da legalidade dos regulamentos, termos, políticas e controlos utilizados para proteger os ativos de informação, garantir que os contratos celebrados com terceiros, sempre que necessário, contenham cláusula de confidencialidade e que preservem a segurança dos ativos de informação e garantir que a existência das diretrizes estabelecidas com base nesta Política e a necessidade do cumprimento de suas premissas sejam referenciadas nos contratos e acordos com terceiros, bem como nos contratos firmados com os colaboradores, de forma que cada um saiba suas obrigações, direitos e deveres no âmbito desta Política.

p) **Unidades de Estrutura (UE):** Responsáveis, no âmbito das suas atribuições, pela colaboração na implementação e operacionalização da presente política e do PCN.

q) **Gestores:** Responsáveis por unidades de estrutura que, no âmbito das suas funções, devem assegurar a gestão do cumprimento desta Política, por parte de seus colaboradores e prestadores de serviço, identificar os desvios praticados e adotar as medidas corretivas apropriadas, reportando a situação à área de Risco e Compliance e por permitir o acesso a ativos de informação e infraestrutura física patrimonial somente por parte de colaboradores ativos.

r) **Utilizadores:** Colaboradores com contrato a termo certo ou temporários, bem como utilizadores de parceiros de negócio, clientes e fornecedores com acessos ao sistema de informação do BAICV responsáveis, no âmbito das suas atribuições, por cumprir e a fazer cumprir a presente política e as respetivas normas, proceder à comunicação de qualquer evento que provoque, ou possa provocar, uma quebra de funcionamento de ativos e serviços, utilizar os Sistemas de Informações e ativos físicos somente para os fins previstos nas suas atribuições, responder por todo e qualquer acesso aos ativos e serviços; e comunicar ao seu superior imediato e aos responsáveis de Compliance o conhecimento de qualquer irregularidade ou desvio verificado no âmbito da presente Política, com a garantia que sua comunicação será tratada de modo sigiloso e sem identificação pública de que foi feita.

7. INCUMPEIMTNO

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.