



Política de Continuidade do Negócio

Resumo

A Política de Continuidade de Negócios do PAULISTA é o conjunto de diretrizes, de responsabilidades e de definição da estrutura de funcionamento operacional para a retomada de atividades e ativos críticos do PAULISTA em prazos e condições aceitáveis em situação de contingência, bem como a sua gestão.

Sumário

1. Objetivo.....	2
2. Público-alvo	2
3. Conceitos Básicos	2
3.1. Continuidade do Negócio.....	2
3.2. Plano de Continuidade do Negócio.....	2
3.2.1. Análise de Impacto nos Negócios (BIA)	2
3.2.2. Plano de Administração de Crise (PAC).....	2
3.2.3. Plano de Continuidade Operacional (PCO)	2
3.2.4. Plano de Recuperação de Desastres (PRD)	2
3.3. Gestão da Continuidade do Negócio	3
3.4. Estado de Contingência Operacional.....	3
3.5. Incidente.....	3
3.5.1. Análise da Gravidade do Incidente (Avaliação da Urgência X Estimativa do Tempo de Impacto)	3
3.6. Crise.....	3
3.7. Grupo Gestor de Crises.....	4
3.8. Ciclo do Gerenciamento da Contingência	4
4. Abrangência dos Processos para Continuidade do Negócio	6
5. Regras	6
5.1. Governança de Continuidade de Negócios.....	6
5.2. Gestão de Crises.....	6
5.3. Recursos Alternativos	6
5.4. Treinamento e Conscientização.....	7
5.5. Testes de Validação	7
5.6. Avaliação Independente	7
5.7. Revisão	7
6. Matriz de atribuição de responsabilidades (RACI)	7
7. Referência cruzada com outros Instrumentos Normativos Internos.....	8
8. Alinhamento com Órgãos Reguladores e Normas.....	8
9. Informações de Controle.....	8



Política de Continuidade do Negócio

1. Objetivo

Estabelecer a Política de Continuidade de Negócios do Grupo Paulista (PAULISTA), definida como o conjunto de diretrizes, de responsabilidades e de definição da estrutura de funcionamento operacional para a retomada de atividades e ativos críticos em prazos e condições aceitáveis em situação de contingência, bem como a sua gestão.

2. Público-alvo

Colaboradores, clientes, órgãos reguladores e diretoria do PAULISTA.

3. Conceitos Básicos

3.1. Continuidade do Negócio

A Continuidade de Negócios é um processo abrangente que identifica ameaças potenciais inerentes aos negócios do PAULISTA e os seus impactos nas operações. Contempla o gerenciamento da recuperação das atividades em caso de interrupção ou limitações técnicas não programadas.

Também deve contemplar o planejamento de uma estrutura para que se desenvolva um nível de resiliência organizacional que seja capaz de responder efetivamente e proteger os interesses das partes envolvidas, reputação, marca e atividades de valor agregado do PAULISTA.

3.2. Plano de Continuidade do Negócio

Conjunto de documentos que descrevem os procedimentos e responsabilidades que devem ser acionados em situações de Contingência.

É composto por:

- BIA – *Business Impact Analysis*
- PAC – Plano de Administração de Crise
- PCO – Plano de Continuidade Operacional
- PRD – Plano de Recuperação de Desastres
- PTV – Plano de Testes e Validação

3.2.1. Análise de Impacto nos Negócios (BIA)

A análise de impacto é um processo da Continuidade de Negócios que identifica e mensura a severidade de uma interrupção operacional nos negócios e possibilita a determinação das prioridades de recuperação, dos tempos de retomada e das necessidades mínimas de recursos e equipes, com base na avaliação de impactos quantitativos (perdas financeiras) e qualitativos (credibilidade, obrigações de prazo, grau de esforço para retomada, etc.).

O documento “Análise de Impacto nos Negócios” (BIA) está sob responsabilidade do *Compliance* Corporativo e fica à disposição da administração das áreas.

3.2.2. Plano de Administração de Crise (PAC)

O Plano de Administração de Crise visa preparar o PAULISTA no gerenciamento de resposta, contingência e recuperação em situações adversas. O PAC relaciona o funcionamento das equipes (recursos humanos) antes, durante e depois da ocorrência da Crise. (GRC-12 A Anexo A – Plano de Administração de Crise).

3.2.3. Plano de Continuidade Operacional (PCO)

O PCO formaliza as ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada possam ser efetivas, evitando que os processos críticos de negócio do PAULISTA sejam afetados, o que pode acarretar em perdas financeiras. (GRC-12 A Anexo A – Plano de Administração de Crise, item 7).

3.2.4. Plano de Recuperação de Desastres (PRD)

Esse plano tem como objetivo formalizar os procedimentos e recursos definidos pelo Departamento de Tecnologia da Informação na recuperação operacional das atividades críticas dos negócios do PAULISTA em situações de crise. (GRC-12 D Anexo D – Plano de Recuperação de Desastres).

Política de Continuidade do Negócio

3.3. Gestão da Continuidade do Negócio

A Gestão da Continuidade de Negócios envolve treinamentos, testes, revisões e manutenções, a fim de garantir que o Plano de Continuidade de Negócios esteja atualizado e operacional.

3.4. Estado de Contingência Operacional

Situação em que os procedimentos operacionais dos negócios ocorrem de forma especial ou limitada.

3.5. Incidente

Qualquer evento que possa impactar negativamente a rotina operacional das atividades do PAULISTA. Dependendo da gravidade ou de sua extensão, pode ser classificada como Crise.

3.5.1. Análise da Gravidade do Incidente (Avaliação da Urgência X Estimativa do Tempo de Impacto)

A análise da Gravidade do Incidente leva em consideração uma avaliação qualitativa da urgência da necessidade de negócio em contrapartida da estimativa do tempo de impacto do evento.

Da composição da avaliação da urgência e da estimativa do tempo de impacto, classifica-se a gravidade do incidente.

AVALIAÇÃO DA URGÊNCIA	Estimativa do Tempo de Impacto	AVALIAÇÃO DA URGÊNCIA
“É possível aguardar o fim do impacto”		“NÃO É possível aguardar o fim do impacto”
TOLERÁVEL	até 1h	MUITO SÉRIO
RELEVANTE	entre 1h e 4h	GRAVE
MUITO RELEVANTE	entre 4h e 8h	MUITO GRAVE
SÉRIO	acima de 8h	DESASTRE

Dependendo da GRAVIDADE, o INCIDENTE deve ser classificado conforme a tabela a seguir:

GRAVIDADE	CLASSIFICAÇÃO DO INCIDENTE	ALÇADA DE ATUAÇÃO
TOLERÁVEL	Incidente	Gestor da área de negócios
RELEVANTE	Incidente	Gestor da área de negócios
MUITO RELEVANTE	Incidente	Gestor da área de negócios
SÉRIO	Incidente	Gestor da área de negócios
MUITO SÉRIO	Incidente	Gestor da área de negócios
GRAVE	Crise	Diretoria da área de negócios
MUITO GRAVE	Crise	Grupo Gestor de Crises
DESASTRE TOTAL	Crise	Grupo Gestor de Crises

3.6. Crise

É um incidente, ou uma série de incidentes, que pode exigir o deslocamento de pessoas para locais alternativos de trabalho.

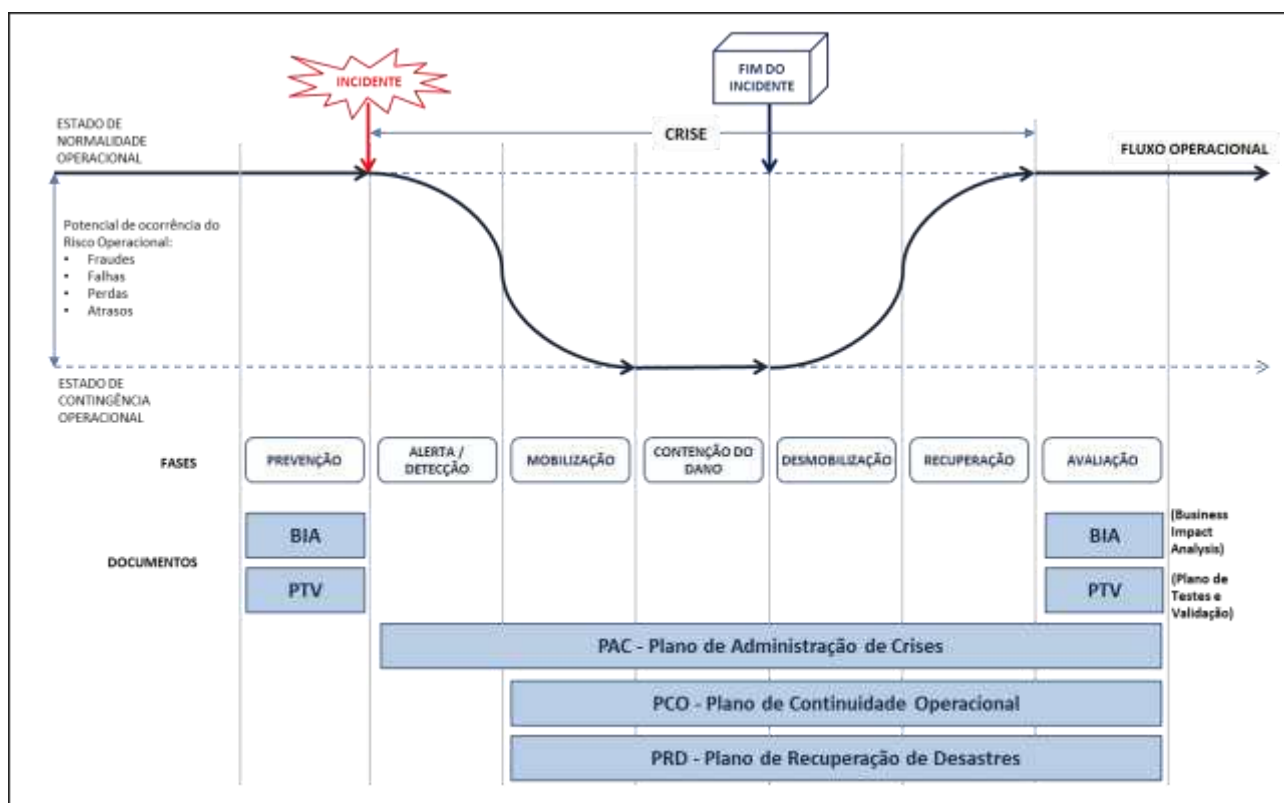
Política de Continuidade do Negócio

3.7. Grupo Gestor de Crises

O colegiado do PAULISTA tem a responsabilidade de decidir pela decretação do Estado de Contingência e o acionamento das pessoas envolvidas no Plano de Continuidade de Negócios. Inicialmente é composto pelos gestores das áreas relacionadas a seguir, podendo envolver outras pessoas (pessoas chaves), conforme a situação de contingência. (ver. **GRC-02 – Estruturas de Governança do Grupo Paulista**)

- Diretoria Geral Administrativa.
- Diretoria de Processamento e Liquidação.
- Departamento de Tecnologia da Informação.
- Compliance Corporativo.

3.8. Ciclo do Gerenciamento da Contingência



FASES:

PREVENÇÃO.

- Elaboração do *Business Impact Analysis* (BIA), dos Planos de Testes e Validação (PTV) e do Relatório do Teste e do Plano de Administração de Crise (PAC)
- Análise das ocorrências potenciais (ver. **SCI-03 - Procedimento de Gerenciamento do Risco Operacional**).
- Testes dos Planos de Continuidade Operacional (PCO).
- Testes do Plano de Recuperação de Desastres (PRD).
- Treinamento dos colaboradores (pessoas chaves) indicados pelas áreas.

ALERTA/DETECÇÃO.

- Identificação do Incidente.
- Avaliação da Gravidade do Incidente.
- Decisão da decretação do Estado de Contingência Operacional.
- Acionamento do Departamento de Marketing e Produtos para enviar comunicado aos colaboradores, fornecedores, clientes, parceiros, mercado, órgãos reguladores e imprensa, dependendo da avaliação da Gravidade do Incidente.



Política de Continuidade do Negócio

MOBILIZAÇÃO.

- Acionamento das pessoas chave.
- Acionamento dos processos alternativos.
- Acionamento dos recursos alternativos.

CONTENÇÃO DO DANO.

- Atendimento das necessidades de negócios em Estado de Contingência Operacional.
- Dependendo da Gravidade do Incidente, iniciar os procedimentos de tratamento da Crise.
- Para as situações não previstas, busca de soluções para contornar o evento e superar os problemas dele oriundos.

DESMOBILIZAÇÃO.

- Avaliação se a Crise foi contornada.
- Comunicação da implementação da correção dos problemas provocados pelo incidente.
- Decisão do início da recuperação do Estado de Normalidade Operacional.
- Registro da ocorrência no sistema de Gerenciamento de Risco Operacional (v. **SCI-03 Procedimento de Gerenciamento do Risco Operacional**).

RECUPERAÇÃO.

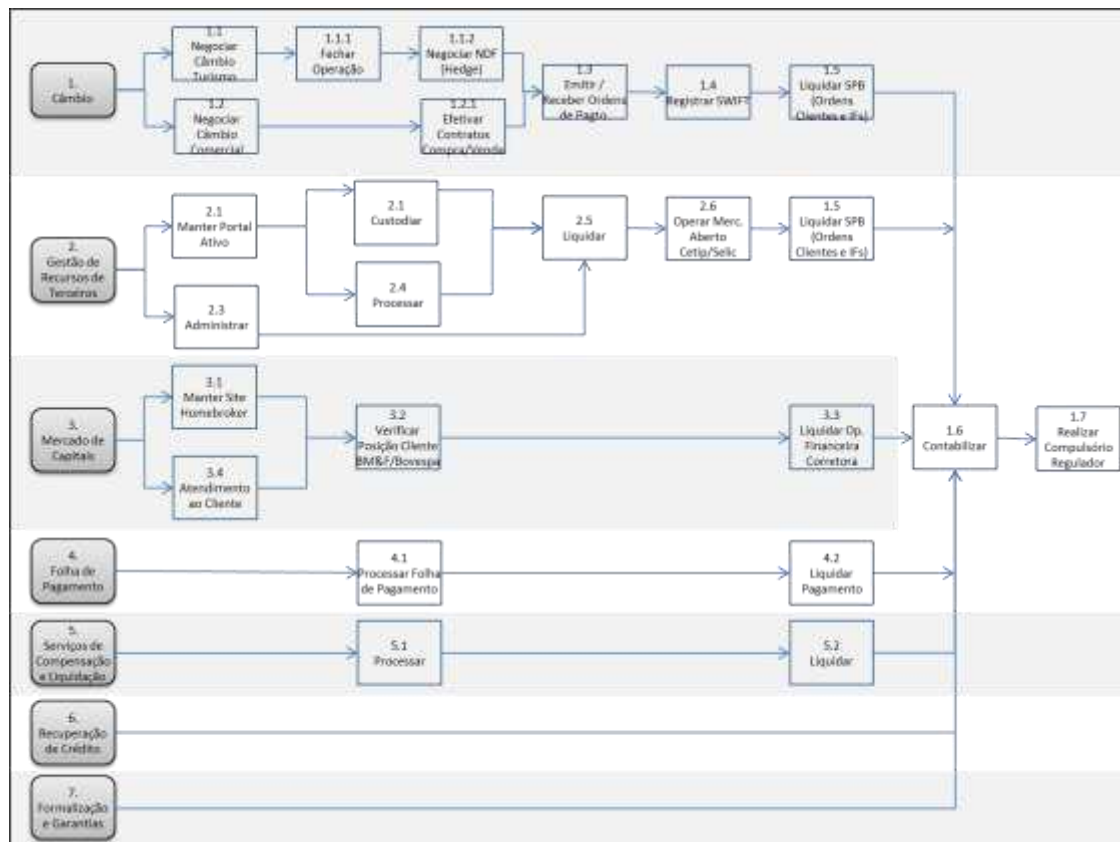
- Procedimentos para retomada do Estado de Normalidade Operacional.
- Verificação da integridade das operações cursadas durante o Estado de Contingência Operacional.
- Acionamento do Departamento de Marketing e Produtos para enviar comunicado aos colaboradores, fornecedores, clientes e imprensa.

AVALIAÇÃO.

- Avaliação das causas do Incidente.
- Registrar ocorrência no Sistema de Gestão de Risco Operacional para mitigação de novas ocorrências.
- Avaliação da efetividade do Plano de Continuidade de Negócios.
- Se necessário, atualização do Plano de Continuidade de Negócios.

Política de Continuidade do Negócio

4. Abrangência dos Processos para Continuidade do Negócio



OBSERVAÇÃO: Em situações de Crise, os gestores das áreas que estão fora da abrangência dos Processos para Continuidade do Negócio devem aguardar instruções do Grupo Gestor de Crise e participar da Árvore de Comunicação descrita no **Anexo A – Plano de Administração de Crise**.

5. Regras

5.1. Governança de Continuidade de Negócios

Supervisionar as políticas, estratégias e processos corporativos de continuidade de negócios e gestão de crises. O Departamento de *Compliance* Corporativo – Segurança da Informação zela pela qualidade e efetividade dos planos estabelecidos.

5.2. Gestão de Crises

- Identificar e avaliar eventuais ameaças e situações de crise.
- Coordenar a comunicação interna/externa e centraliza a forma de agir, por meio de procedimentos e métodos de identificação e classificação de eventos com impactos negativos para cada um dos serviços e negócios críticos.
- A partir dessa classificação, definir grupos de ação, planos de resposta e resolução a serem tomadas.
- Coordenar a comunicação interna e externa de todas as etapas do ciclo de gerenciamento da contingência a partir do momento incidente.

5.3. Recursos Alternativos

O PAULISTA disponibilizará um site backup ou site de contingência, no mínimo a um quilômetro de distância onde haja infraestrutura mínima para que as pessoas chaves dos planos de continuidade operacional possam executar os principais processos de negócio, enquanto o departamento de TI e demais responsáveis restauram a operação normal da organização.

Também será disponibilizado um local (“sala de crise”) onde a Diretoria e o Grupo Gestor de Crises irão se reunir durante a crise.

Política de Continuidade do Negócio

5.4. Treinamento e Conscientização

Assegurar que os colaboradores estejam cientes de seus papéis e responsabilidades e preparados para atuar em eventuais interrupções.

5.5. Testes de Validação

Realizar, periodicamente, testes para avaliar a efetividade e a funcionalidade de seus Planos de Continuidade Operacional e Planos de Recuperação de Desastres. A natureza, o escopo e a frequência dos testes são determinados de acordo com a criticidade dos negócios envolvidos e com as definições dos órgãos reguladores locais.

Os resultados dos testes são documentados, criados relatórios gerenciais a cada teste executado, técnicos e periodicamente são avaliados, permitindo o aprimoramento contínuo dos procedimentos e gerenciamento de riscos e recuperação.

5.6. Avaliação Independente

Avaliar, de acordo com os testes, a efetividade desta política.

5.7. Revisão

A revisão da documentação de Continuidade de Negócios deve ocorrer após qualquer alteração significativa nos processos de negócios.

Essas alterações podem decorrer de atualizações, migrações, implantação de novos produtos, novas demandas, entre outras modificações informadas pelas unidades de negócios para que o impacto apurado para cada processo esteja condizente com a realidade dos negócios.

6. Matriz de atribuição de responsabilidades (RACI)

A **matriz RACI** apresenta a relação entre papéis desempenhados e atividades e/ou artefatos a serem entregues. RACI é o acrônimo (em inglês) para:

Responsible (responsável): É efetivamente quem trabalha na atividade.

Accountable (aprovador): É o papel do responsável pelo aceite formal da tarefa ou produto entregue. Este pode delegar a função para outros profissionais, entretanto ele é quem se responsabiliza pelo recebimento do trabalho.

Consulted (consultado): é o responsável por fornecer informações ou pareceres sobre a tarefa ou produto a ser entregue.

Informed (informado): é quem necessita ser mantido informado sobre o andamento da atividade.

MATRIZ RACI (legenda)		Comitê GRC	Grupo Gestor de Crises	Compliance Corporativo	Gestores de Negócios	Departamento de TI	Colaboradores	Auditoria Interna
Ref.	Procedimento							
5.1	Governança de Continuidade de Negócios	A	C	R	C	R	I	
5.2	Gestão de Crises	I	R	C	C	C	I	
5.3	Recursos Alternativos	A	I	R	I	R	I	
5.4	Treinamento e Conscientização	A	I	R	I	I	I	
5.5	Testes de Validação	I	C	R	R	C	C	
5.6	Avaliação Independente	I	C	C	C	C		R
5.7	Revisão	A	C	R	C	R		



Política de Continuidade do Negócio

7. Referência cruzada com outros Instrumentos Normativos Internos

- GRC-02 – Estruturas de Governança do Grupo Paulista
- GRC-11 – Política de Segurança da Informação
- GRC-12.A – Anexo A - Plano de Administração de Crise
- GRC-12.B – Anexo B - Plano de Testes e Validações
- GRC-12.D – Anexo D – Plano de Recuperação de Desastres
- SCI-03 - Procedimento de Gerenciamento do Risco Operacional

8. Alinhamento com Órgãos Reguladores e Normas

Resolução 3.380/06 CMN - Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional.

Instrução CVM nº 313 - Dispõe sobre os procedimentos a serem adotados para a adequação dos sistemas eletrônicos.

Instrução CVM nº 380 - Estabelece normas e procedimentos a serem observados nas operações realizadas em bolsas e mercados de balcão organizado por meio da rede mundial de computadores e dá outras providências.

Código ANBIMA de Regulação e Melhores Práticas de Fundos de Investimento

Código ANBIMA de Regulação e Melhores Práticas para Serviços Qualificados ao Mercado de Capitais

Código ANBIMA de Regulação e Melhores Práticas de Negociação de Instrumentos Financeiros

Norma ABNT NBR ISO/IEC 15999-1:2007 - Gestão da Conformidade do Negócio

9. Informações de Controle

Vigência: até 24.fev.2018

Registro das alterações (últimos dois anos):

Versão	Item alterado	Descrição resumida da alteração	Motivo	Dt. Publicação
02	Todo o documento	Utilização da nomenclatura PAULISTA em referência às empresas componentes do Grupo Paulista Padronização da nomenclatura da estrutura organizacional	Atualização	02.abr.2015
03	Todo o documento		Atualização	09.set.2016
04	Todo o documento	Reorganização dos tópicos e introdução do conceito de Evento de Alerta. Revisão do conceito de Incidente e de Crise	Aperfeiçoamento	24.fev.2017

Responsáveis pelo Instrumento Normativo:

Etapas	Responsável	Contato	Unidade Organizacional
Elaboração	Rodrigo Duarte	rodrigo.duarte@bancopaulista.com.br	Compliance Corporativo
Revisão	Eduardo Kuniyoshi	eduardo.kuniyoshi@bancopaulista.com.br	Compliance Corporativo
	Marcos Palmieri	marcos.palmieri@bancopaulista.com.br	Tecnologia da Informação
	Nelson Heleno	nelson.heleno@bancopaulista.com.br	Compliance Corporativo
	Denilson Santos	denilson.santos@bancopaulista.com.br	Compliance Corporativo
Aprovação	Gerson Brito	gerson.brito@bancopaulista.com.br	Diretoria Geral Administrativa

Comitê GRC