

# *Guia de Boas Práticas para Planos de Continuidade de Negócios*

COMISSÃO TÉCNICA REGIONAL  
SUDESTE DE GOVERNANÇA DA ABRAPP

Outubro de 2012



associação brasileira das  
entidades fechadas de  
previdência complementar

# COMISSÃO TÉCNICA REGIONAL SUDESTE DE GOVERNANÇA DA ABRAPP

## **Coordenador**

*Acyx Xavier Moreira*

*(PREVI e membro da Comissão Técnica Nacional de Governança)*

*Adriana Barreto Rodrigues (ELETROS)*

*Carlos Alexandre Pereira Dias (PRECE)*

*Denner Vieira Franklin (PETROS)*

*Isaac Ferreira da Silva (NUCLEOS)*

*Izana Sampaio (INFRAPREV)*

*Luiz Eduardo Guimarães Rodrigues (FUNDAÇÃO ATLÂNTICO)*

*Marcelo Côrtes da Cruz (REFER)*

*Maria Bernadete de Andrade Rosário (PREVI)*

*Ricardo da Silveira Ferreira (SÃO RAFAEL)*

*Sabrina Von Paumgarten Moss (VALIA)*

*Terezinha Maria Marques Ferreira (REAL GRANDEZA)*

## **Supervisão**

*Comissão Técnica Nacional de Governança*

## **Diretor Responsável**

*Milton Luis de Araújo Leobons (PRECE)*

# ÍNDICE

<b>SUMÁRIO</b>	<b>6</b>
<b>Capítulo 1 – POLÍTICA DE CONTINUIDADE DE NEGÓCIOS</b>	<b>8</b>
1.1. Definição de Plano de Continuidade de Negócios (PCN)	8
1.2. Objetivo	8
1.3. Amparo Legal	9
1.4. Benefícios da Adoção de um PCN	10
1.5. Diretrizes	10
1.6. Responsabilidades e Atribuições	11
1.7. Estrutura para o Funcionamento do PCN	12
<b>Capítulo 2 – PROJETO DO PLANO DE CONTINUIDADE DE NEGÓCIOS</b>	<b>14</b>
2.1. Fases do Projeto	14
2.2. Análise de Impacto do Negócio (Business Impact Analysis - BIA)	16
2.3. Priorização de Processos	20
2.4. Seleção das Estratégias de Tratamento: custos, riscos e benefícios	22
<b>Capítulo 3 – IMPLEMENTAÇÃO E GESTÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS</b>	<b>25</b>
3.1. Divulgação e Conscientização	28
3.2. Testes	30
3.3. Treinamento	34
3.4. Retorno à Normalidade	35
<b>Anexo – Check List para Avaliação do PCN</b>	<b>36</b>
<b>Referências Bibliográficas</b>	<b>38</b>





## INTRODUÇÃO

*O Guia de Boas Práticas para Planos de Continuidade de Negócios tem por objetivo fornecer diretrizes e orientações gerais a dirigentes, colaboradores e partes interessadas das Entidades Fechadas de Previdência Complementar (EFPC) quanto à Gestão da Continuidade de Negócios, visando contribuir para o fortalecimento do Sistema.*

*Busca promover a adoção de boas práticas de gestão, de forma que, realizadas de maneira prudente, ética e diligente, tenham como foco o gerenciamento e mitigação de riscos, bem como o pleno exercício do dever previdenciário.*

*Trata-se de interpretação de pontos relevantes, não sendo exaustivo e nem abrangente em toda a matéria, podendo ser adaptado em decorrência de possíveis mudanças nas entidades, na legislação corrente ou, mesmo, de evoluções em sua interpretação.*

*Nesse sentido, incentiva os seus usuários a buscar maior compreensão e aprofundamento técnico sobre as matérias tratadas tanto na legislação em vigor quanto na bibliografia nacional e internacional. O uso e a interpretação deste material são de inteira responsabilidade da entidade e de seus dirigentes.*

*O Guia está estruturado em capítulos que trazem orientações gerais para as EFPC, independentemente de seu porte, procurando abordar as melhores práticas relacionadas à Gestão de Planos de Continuidade de Negócios.*

# SUMÁRIO

A primeira parte do Guia apresenta os elementos necessários à elaboração de uma *Política de Gestão de Continuidade de Negócios (PGCN)* para Entidades Fechadas de Previdência Complementar, em situações de contingência.

A PGCN é o conjunto formado por diretrizes, responsabilidades, atribuições e definição da estrutura de funcionamento de um Plano de Continuidade de Negócios (PCN). Descreve a conduta considerada adequada para a manutenção da gestão quando identificadas ameaças em potencial e impactos nas operações de negócio caso essas ameaças se concretizem entre o impacto do evento até o retorno da normalidade (*Capítulo 1*).

Na sequência (*Capítulo 2*), são descritas as fases de um *Projeto do Plano de Continuidade de Negócios*: definição de responsabilidades, implementação e manutenção. Merecem destaque a *Análise de Impacto do Negócio*, a *Priorização de Processos* e a *Seleção de Estratégias de Tratamento*. Nessas ações são identificados riscos, tempos de recuperação, efeitos, custos e limites aceitáveis para a priorização de processos e ativação de medida de continuidade.

Considerando-se que um plano só se completa na ação, é necessário haver mecanismos de *gestão* que garantam a contínua interação entre o plano e a ação (*Capítulo 3*). Isso pode ser feito a partir da definição de planos mais específicos, com respectivos cenários e procedimentos (Planos de Contingência Operacional, de Recuperação de Desastres e de Gerenciamento de Crises).

Merecem destaque, na gestão do Plano de Continuidade de Negócios, os *Procedimentos de Resposta* e o de *Retorno à Normalidade*. O Plano só terá efetividade, ou seja, só estará apto a “responder” à demanda de continuidade se for devidamente testado, divulgado e treinado pelos colaboradores da EFPC. Quanto ao *Retorno à Normalidade*, o PCN deve estabelecer o término das ações do Plano e o reinício das atividades de negócios. Após o retorno, deverão ser produzidos relatórios com informações sobre o evento, os custos incorridos, recursos utilizados, tempos de recuperação, perdas estimadas e planos de ação, no caso de melhorias identificadas etc.

O *check list* para avaliação do PCN encontra-se no *Anexo 1* deste documento.



# Capítulo 1

## POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

A Política de Continuidade de Negócios deve formalizar o processo de definição do Plano de Continuidade de Negócios (PCN) adotado pela EFPC, incluindo os componentes apresentados a seguir.

### 1.1. Definição de Plano de Continuidade de Negócios (PCN)

Plano de Continuidade de Negócios (PCN) é o processo de gestão da capacidade de uma organização de conseguir manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de negócios críticos.

O PCN deve ser desenvolvido preventivamente a partir de um conjunto de estratégias e planos táticos capazes de permitir o planejamento e a garantia dos serviços essenciais, devidamente identificados e preservados. Este processo orienta e define como e quais ações devem ser executadas para que se construa uma resiliência organizacional<sup>1</sup> capaz de responder efetivamente e salvaguardar os negócios.

### 1.2. Objetivo

O PCN tem como objetivo especificar as ameaças e riscos identificados na organização e analisar os impactos no negócio, caso

---

1. Capacidade estratégica e tática de uma organização para planejar, resistir e reagir aos efeitos de um incidente que provoque a interrupção das operações críticas, a tempo de reduzir ou eliminar os danos desta interrupção, com a finalidade de continuar as operações do negócio a um nível predefinido e aceitável.

essas ameaças se concretizem. Visa com isso tornar possível seu funcionamento em um nível aceitável nas situações de contingência<sup>2</sup>, resguardando os interesses dos intervenientes, a reputação, a imagem da organização e suas atividades fim de significativo valor agregado.

### 1.3. Amparo Legal

O Plano de Continuidade de Negócios (PCN) para uma EFPC constitui parte integrante de uma governança corporativa bem estruturada e apoiada em princípios de melhores práticas de gestão de controles internos. Para tanto, esses princípios devem ser continuamente observados e estar em conformidade com a Resolução MPAS/CGPC nº 13/04, que dispõe os princípios, regras e práticas de governança, gestão e controles internos a serem observados pelas EFPC:

*Art. 1º “As entidades fechadas de previdência complementar – EFPC devem adotar princípios, regras e práticas de governança, gestão e controles internos adequados ao porte, complexidade e riscos inerentes aos planos de benefícios por elas operados, de modo a assegurar o pleno cumprimento de seus objetivos”.*

*Art. 12. “Todos os riscos que possam comprometer a realização dos objetivos da EFPC devem ser continuamente identificados, avaliados, controlados e monitorados”.*

*Art. 18, § 1º “Deve haver previsão de procedimentos de contingência e segregação de funções entre usuários e administradores dos sistemas informatizados, de forma a garantir sua integridade e segurança, inclusive dos dados armazenados”.*

---

2. Situações de adoção de procedimentos com vistas a permitir que a entidade responda a um evento indesejado, que por ventura venha causar algum impacto negativo na organização.

### 1.4. Benefícios da Adoção de um PCN

A adoção de um Plano de Continuidade de Negócios é importante para a boa gestão e prudência na administração das EFPC e traduz-se em benefícios, tais como:

- identificação de processos críticos e do impacto de ruptura em toda a entidade;
- conhecimento do grau de exposição ao risco;
- resposta eficiente às interrupções, sobretudo em função de um planejamento das ações necessárias;
- treinamento do pessoal envolvido na resposta a ocorrências de impactos relevantes;
- preservação da reputação da entidade no que tange a uma administração profissional na gestão, em caso de ruptura;
- minimização de possíveis impactos às partes interessadas e ao patrimônio;
- significativo aumento da probabilidade de sobrevivência da entidade ou do negócio em caso de uma crise, quaisquer que sejam as suas causas;
- promoção de entendimento mais claro e amplo do *modus operandi* da entidade, permitindo a oportunidade de melhorias.

### 1.5. Diretrizes

A alta administração e os demais colaboradores da organização devem conhecer as fases do desenvolvimento do PCN e contribuir para a identificação das ameaças e dos riscos que podem afetar o negócio, mas que não constam do Plano.

O PCN deve ser elaborado inicialmente considerando as situações de risco com maior impacto e ampliar-se conforme a maturidade da organização frente à proteção dos seus ativos.

O treinamento e a conscientização de todos os colaboradores são de grande importância, permitindo que a organização gerencie os riscos, esteja preparada para os momentos de contingência e garanta a continuidade do negócio.

O PCN deve estar alinhado à missão, visão e metas estratégicas da entidade.

### 1.6. Responsabilidades e Atribuições

#### 1.6.1. Responsabilidades

A responsabilidade pela ativação do PCN, do ponto de vista das boas práticas de governança corporativa, deve estar situada no mais alto nível de decisão da entidade.

Deve haver a identificação de um responsável ou de uma equipe, dependendo do porte da entidade, para pôr em prática as medidas definidas no PCN.

No caso de uma equipe, cada membro deve ter responsabilidades e tarefas formalmente definidas e nominalmente atribuídas, com a previsão de um substituto.

O responsável ou a equipe responsável deve ter a possibilidade de decidir perante situações imprevistas ou inesperadas, devendo também estar prevista e formalmente definida a alçada dessa possibilidade de decisão.

Dentro deste contexto, todos os colaboradores de uma entidade devem observar as práticas de segurança que possam contribuir no processo de gestão eficaz de continuidade de negócios.

As áreas envolvidas nos processos críticos identificados no PCN são responsáveis pela manutenção, atualização e validação do respectivo plano, de acordo com os prazos e procedimentos estabelecidos.

#### Grupos Funcionais

O porte da estrutura organizacional irá influenciar o desdobramento das definições e formas de atuação.

#### a) Grupos Estratégicos

*Grupo Executivo:* Diretoria Executiva – participa da aprovação do PCN e na ocorrência de contingências significativas ou cenários em que seja necessária tomada de decisões estratégicas para a organização ou segmento de negócios.

*Grupo de Comunicação/Apoio ao Executivo* – é formado por colaboradores que subsidiam o processo de decisão associado aos negócios da empresa. É responsável por efetuar contatos com a imprensa, entidades externas e grupos de participantes e fornecedores, além de garantir a disseminação adequada da informação para as áreas internas. Este grupo deve ser composto, prioritariamente, por gerentes e assessores.

#### **b) Grupo Tático**

*Grupo de Administração de Crises* – colaboradores que tenham a atribuição de supervisionar as atividades do grupo operacional, assegurando os recursos necessários para operação do PCN, além de gerir os cenários de contingência e apoio ao processo de decisão do Grupo Executivo.

#### **c) Grupo Operacional**

Demais colaboradores com atribuições operacionais definidas no PCN, voltadas para apoio administrativo e à infraestrutura física e de tecnologia: alimentação, transporte, acesso às instalações, retorno do funcionamento do site etc.

### **1.6.2. Atribuições**

A partir da definição do(s) responsável(eis) pela implementação e gestão do PCN, a entidade deve mapear todas as atribuições necessárias para a sua elaboração, ativação, manutenção e monitoramento, registrando-as formalmente.

## **1.7. Estrutura para o Funcionamento do PCN**

A entidade deve observar a existência de uma estrutura mínima de PCN para o efetivo funcionamento em caso de ocorrências que acarretem interrupções. Em outras palavras, a EFPC deve ter cumprido as seguintes etapas do PCN:

- a) Política de Gestão de Continuidade de Negócios – deve estar prevista em documento que discipline regras para o seu correto funcionamento.

- b) Conhecimento da Organização, por meio de:

- mapeamento de processos críticos;
- Análise de Impacto no Negócio – BIA;<sup>3</sup>
- definição da estrutura da Gestão de Continuidade de Negócios (GCN), contendo os objetivos, os grupos funcionais, os planos de contingência associados e os resultados esperados.

- c) Planos de Continuidade – Elaboração e Implementação.

- d) Treinamentos.

- e) Revisão, aprimoramento e monitoramento dos planos.

- f) Realização periódica de testes.

---

3. A análise de impactos no negócio tem por finalidade apresentar os prováveis impactos de forma qualitativa e quantitativa dos principais processos de negócios mapeados e entendidos na organização, no caso de interrupção dos mesmos (o tema será tratado no item 2.2, deste Guia).

## Capítulo 2

# PROJETO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

O desenvolvimento de um Plano de Continuidade de Negócio deve responder as seguintes questões:

- Quais são os processos críticos<sup>4</sup> – que não podem deixar de ser executados?
- O que pode impedir que esses processos críticos sejam performatados? (Análise de risco)
- De que forma a interrupção desses processos poderá afetar o negócio? (Análise do impacto no negócio)
- Neste caso, o que é necessário fazer para retornar as operações?

As respostas ajudarão não só a encontrar as medidas necessárias para mitigar o risco, mas também a desenvolver estratégias de continuidade do negócio que devem ser documentadas, dando assim forma ao PCN.

### 2.1. Fases do Projeto

As principais referências são as normas BS 25999 e ABNT NBR 15999.

A norma britânica BS 25999 estabelece processos, princípios e terminologias da Gestão de Continuidade de Negócios (GCN). De forma genérica, seu conteúdo pode ser aplicado em toda a organização ou em parte dela, independente do tipo, tamanho, natureza ou setor do negócio (privado ou público).

---

4. Podem também ser denominados prioritários, essenciais, vitais ou chave. São processos que devem ser executados para viabilizar os serviços fundamentais da entidade.

Originária da BS 25999, a norma brasileira ABNT NBR 15999 foi elaborada para fornecer um sistema baseado nas boas práticas de gestão da continuidade de negócios. Assim, a exemplo da norma britânica, seu objetivo é garantir informações dos processos fundamentais para que a empresa possa passar por um incidente<sup>5</sup> gerador de uma ruptura do negócio e retornar a sua condição normal, conseguindo desta forma minimizar os prejuízos.

Internamente, o conhecimento prévio da entidade – sua missão, visão, metas estratégicas e processos – é necessário para a adoção de um PCN.

Em linha com esse entendimento da entidade, definem-se três eixos principais:

- a) responsabilidades;
- b) implementação;
- c) manutenção.

#### a) Responsabilidades

A entidade deve nomear um colaborador responsável pelo PCN. Dependendo do porte, a entidade pode necessitar de uma equipe de pessoas dedicadas.

Em termos de governança, este colaborador deve se reportar diretamente à alta administração.

---

5. Incidente (crise, interrupção, desastre) - O termo incidente é usado neste Guia de forma a refletir a gradação dos eventos, de pequeno, médio ou grande porte, que podem afetar a organização. Um único incidente ou uma série de incidentes pode resultar em sérias interrupções na capacidade da organização de cumprir suas obrigações. Se um incidente for bem gerenciado, pode não resultar em uma crise – período prolongado dos impactos do incidente e de busca de solução. Porém, alguns eventos podem causar uma interrupção tão profunda aos objetivos da organização, a ponto de serem considerados como crise imediatamente.

Um incidente pode exceder o nível de preparação da organização, mesmo que ela tenha cuidadosamente avaliado medidas de respostas para um determinado nível de dano esperado. É, então, imperativo que a direção e as estruturas que a suportam não se limitem a seguir o plano existente à risca, independentemente da situação, mas o adaptem às circunstâncias atuais. (ABNT 15.999).



Não obstante a definição dos responsáveis, é importante ressaltar que a alta administração e os demais colaboradores da entidade devem conhecer as fases do desenvolvimento do PCN, tendo conhecimento das ameaças e riscos que podem afetar seu negócio.

### **b) Implementação**

Conforme previsto na Política de Gestão de Continuidade de Negócios, o PCN pode ser elaborado inicialmente considerando as situações de risco com maior impacto e, posteriormente, alcançar os demais processos, na medida em que se obtém maior domínio a partir do resultado das análises contínuas.

O mapeamento de processos deve anteceder a definição do modelo estrutural a ser adotado pela entidade.

No âmbito do PCN, o mapeamento tem como objetivo estabelecer os conceitos e critérios da rotina de forma direcionada, com descrição dos processos críticos, suas inter-relações com outros processos, visando à elaboração de procedimentos que limitem o risco a um patamar definido pela entidade.

### **c) Manutenção**

A Gestão de Continuidade de Negócios (GCN) é contínua e deve ser permanentemente realimentada e sistematicamente atualizada, até a normatização das atividades. Devem acontecer revisões anuais ou quando a entidade sofrer alteração significativa de seus processos e/ou estrutura organizacional.

Tais revisões, bem como o monitoramento dos planos deverão ser conduzidos pelo(s) responsável(eis) pelo PCN a partir dos registros gerados nas atividades da GCN e nas alterações dos processos da entidade.

## **2.2. Análise de Impacto do Negócio (Business Impact Analysis – BIA)**

Business Impact Analysis (BIA) é um componente essencial de um plano de continuidade de negócios. A análise tem por objetivo revelar vulnerabilidades e subsidiar o desenvolvimento de estratégias para minimizar os riscos. O resultado é um relatório

de análise de impacto, que descreve os riscos potenciais específicos para a entidade no caso de uma interrupção do negócio. Um dos pressupostos básicos do BIA é que existe dependência entre os processos da organização e que alguns são mais cruciais que outros. Por isso, a manutenção desses processos será prioritária durante uma situação de contingência. Ou seja, um relatório BIA quantifica a importância dos processos do negócio e sugere alocação de recursos adequados para protegê-los.

A partir do mapeamento de processos, a entidade deve relacionar:

- critérios para aferir a relevância / criticidade dos processos;
- atividades críticas realizadas em cada processo;
- entregas de demandas regulatórias;
- dependências de sistemas e pessoas;
- impactos financeiros (perdas) que poderiam ocorrer se estes processos fossem suspensos; e
- impactos operacionais (segurança, por exemplo), legais e de imagem (como “satisfação do cliente”), finalizando com a verificação da existência de contingência (se há *backup* – cópia de segurança de informações contidas em sistemas ou quaisquer mídias digitais – de sistema, de pessoas etc.).

Na Análise de Impacto de Negócios (BIA) deve ser contemplado o tempo real de recuperação para cada atividade crítica dentro da organização. Para tal, os aspectos a seguir devem ser considerados:

- identificação de riscos e definição de cenários possíveis de falha para cada processo crítico, levando em conta a probabilidade de ocorrência de cada falha;
- duração dos efeitos e consequências resultantes;
- custos inerentes e os limites máximos aceitáveis de permanência da falha sem a ativação da respectiva medida de contingência.

O documento do BIA deve contemplar:

- breve resumo dos processos críticos e descrição das principais atividades;

- perfil e quantidade dos profissionais envolvidos;
- dependências entre os processos da entidade;
- tecnologias que suportam as atividades;
- impactos de localidade (onde é realizada a atividade);
- impactos financeiros, legais, operacionais e de imagem ocasionados por uma ruptura;
- critérios para priorização dos processos em face do tipo de impacto (financeiro, legal, operacional ou imagem);
- priorização por impacto;
- definição do nível de criticidade, ou seja, da gravidade das consequências do impacto, para cada atributo (impacto no setor e impacto corporativo, por exemplo);
- definição do RTO (*Recovery Time Objective*) e RPO (*Recovery Point Objective*);
- determinação dos acordos com fornecedores e parceiros externos de produtos e serviços dos quais as atividades críticas dependam.

Na avaliação do resultado do BIA devem ser observados os seguintes aspectos:

- aumento de custo operacional;
- perda de oportunidade de negócio;
- impacto ao bem-estar das pessoas;
- dano ou perda de instalações, tecnologia ou informação;
- não cumprimento de deveres ou regulamentação;
- danos à reputação;
- danos à viabilidade financeira;
- deterioração da qualidade de produtos ou serviços; e
- danos ambientais.

A partir do BIA, a entidade deve identificar as medidas que reduzam o período de interrupção (mitigação de perdas e tratamento de riscos) e seus custos.

### 2.2.1. Fases da implantação do BIA

#### a) Definição do projeto

A entidade deve definir o responsável pela sua implantação e sua autoridade, escopo, objetivos e prazos.

#### b) Elaboração do questionário

A elaboração de um questionário para coleta das informações subsidia a análise do BIA na identificação dos impactos resultantes de interrupções ao longo do tempo, dos recursos necessários para recuperação e da existência ou não de rotinas para situações de contingência (*backup* de sistema, por exemplo). É uma boa prática conjugar no questionário questões qualitativas e quantitativas.

Não existe uma receita de questionário pronta, aplicável a qualquer organização, no entanto os seguintes itens podem constar do questionário: número de colaboradores envolvidos, custo da operação por período, prejuízo por tempo parado, aspectos legais de uma interrupção de serviço, aspectos de imagem e demais prejuízos intangíveis, dependência de hardware, software, aplicações, rede, comunicação etc.

Elaboradas as questões, os critérios devem ser definidos: se o entrevistado responder perguntas pela atribuição de valores, por exemplo, de 1 a 5, é imprescindível explicar a distinção destas cinco notas. Não é raro que o mesmo evento seja avaliado de uma forma pelos colaboradores de nível funcional mais operacional e de outra pela alta administração.

#### c) Entrevista

Elaborado o questionário, parte-se para a entrevista. Os melhores resultados, com esclarecimento de questões e respostas coerentes, são obtidos quando a entrevista é realizada diretamente com o responsável por uma atividade crítica.

#### d) Determinação dos “tempos reais de recuperação” (RTO - *Recovery Time Objectives*) somente depois de identificadas todas as interdependências processuais.

O *Recovery Time Objective* – RTO ou tempo real de recuperação é o período dentro do qual um processo deve ser restabelecido

após um incidente, a fim de evitar consequências inaceitáveis relacionadas com uma quebra na continuidade dos negócios. Pode incluir o tempo para tentar corrigir o problema sem uma recuperação, a recuperação em si, testes e comunicação para os usuários.

A título de exemplo, com o resultado do questionário é possível concluir que para a atividade crítica “A” o tempo máximo aceitável de interrupção é de dois dias, porém, o tempo máximo aceitável de interrupção para a atividade crítica “B” é de um dia. Além disso, esta atividade não pode ser recuperada sem a ajuda da atividade crítica “A”. Isso significa que o tempo real de recuperação para “A” será um dia e não dois.

#### **e) Estabelecimento do “ponto real de recuperação” (RPO – Recovery Point Objective)**

*Recovery Point Objective* – RPO ou ponto real de recuperação é definido pelo período máximo de tolerância em que informações podem ser perdidas ou ficarem indisponíveis devido a um incidente. Deve ser definido em função das necessidades e requisitos do negócio. Por exemplo, o RPO pode traduzir-se em minutos, horas ou dias desde o último *backup*.

### **2.3. Priorização de Processos**

O produto da avaliação do BIA deve ser a identificação de todos os processos críticos de negócio da entidade – cujas falhas podem representar risco à sua continuidade – objetivando a priorização dos mesmos.

Tal priorização deve ser efetuada a partir da verificação do nível de criticidade do processo obtido a partir da análise dos impactos financeiros, operacionais, legais e de imagem, cada um podendo ter um peso diferenciado.

A seguir, estão relacionados os principais impactos:

**a) Impacto financeiro** – Uma análise financeira considera cenários de perda, estimando o impacto na rentabilidade e custos adicionais para mitigar a perda potencial de recursos.

**b) Impacto Operacional** – Falhas operacionais estão relacionadas a pessoas, processos e tecnologia. Deve ser estimado o grau de impacto da interrupção do processo de negócio no funcionamento da entidade.

**c) Impacto Legal** – Devem ser identificados possíveis descumprimentos de legislação que possam resultar da interrupção do processo de negócio.

**d) Impacto de Imagem** – Danos de imagem que possam resultar da interrupção do processo de negócio.

Deve haver um processo definido, documentado e adequado para avaliação de riscos que possibilitará à organização entender as ameaças e vulnerabilidades nas suas atividades críticas e recursos de suporte, incluindo aqueles fornecidos por parceiros externos e fornecedores.

Este processo deve levar em conta os seguintes aspectos:

- redução da probabilidade de interrupção;
- diminuição do período da interrupção e;
- limitação do impacto de uma interrupção nos produtos e serviços críticos da entidade.

A entidade deve entender o impacto que pode surgir caso uma ameaça identificada se torne um incidente e cause uma interrupção do negócio.

Após a identificação e avaliação dos impactos cabe à alta administração da entidade definir os riscos que representam ameaça à continuidade do seu negócio.

#### **Elaboração de Quadro Resumo**

Concluído o projeto e aprovado pela alta administração, os processos críticos selecionados para serem geridos no PCN podem ser esquematizados em um quadro que permita fácil visualização para subsidiar a tomada de decisão, conforme (Quadro 1), a seguir:



**Quadro 1 – Processos Críticos do PCN**

Processo	Criticidade	RPO	RTO	Impacto*			
				Financeiro	Legal	Imagem	Operacional
A	1	... dias(s)	... hora(s)				
B	2	... dias(s)	... hora(s)				
C	3	... dias(s)	... hora(s)				
D	4	... dias(s)	... hora(s)				

\* Podem ser adotadas métricas como: “baixo, médio ou alto”, “irrelevante, médio, significativo” etc.

## 2.4. Seleção das Estratégias de Tratamento: Custos, Riscos e Benefícios

A identificação de cenários de ruptura (Figura 1) é necessária para determinação do ponto de recuperação (item 2.2.1.e) e da seleção das estratégias de continuidade.

**Figura 1 – Cenários de Ruptura**



A partir das análises de impactos financeiros, operacionais, legais e de imagem, deve ser efetuada a comparação entre estes para embasar a definição da estratégia de continuidade.

Após a definição da estratégia, devem ser estabelecidas ações que podem variar desde a realização de *backup* de dados até a criação de um site de contingência. Todo o processo deve considerar a avaliação de custo, risco, benefício das alternativas disponíveis para escolha e implantação de tratamento de riscos apropriado para cada atividade crítica e de acordo com seu nível de risco aceitável.

Esses custos devem ser comparados ao custo que a entidade incorreria na contingência.

Consultadas as estratégias sugeridas pela Norma ABNT 15.999-1 e considerando-se que os recursos necessários para a continuação e recuperação dos negócios devem ser identificados em diferentes pontos do tempo, as soluções de continuidade podem incluir:

- Pessoas** – logística de transporte, planejamento de sucessão, uso de recursos humanos terceirizados, documentação do método de execução das atividades críticas de forma a propiciar que outras pessoas executem as rotinas etc.
- Tecnologia** – acesso remoto, distribuição geográfica da tecnologia, ou seja, manter a tecnologia em locais diferentes que não deverão ser afetados pela mesma interrupção de negócios etc.
- Informações** – as estratégias de informações devem incluir formatos físicos (impressos) e eletrônicos, sobretudo para aquelas consideradas essenciais como informações financeiras, folha de pagamento, cadastro de participantes, cadastro de fornecedores e documentos legais (contratos de empréstimo, termos de adesão etc.). Cópias também devem ser guardadas em instalações alternativas, previamente estabelecidas.
- Instalações** – realização de trabalho em casa ou em locais remotos, uso de força de trabalho alternativa em local estabelecido etc.

e) *Gestão das partes interessadas* – identificação de responsáveis pela comunicação com as partes interessadas, autoridade e mídia.

A entidade deve permanentemente buscar evitar que as ameaças se concretizem, quer seja por meio da descontinuidade de atividades, produtos ou serviços que gerem os riscos.

No entanto, se após a identificação e avaliação das ameaças não for possível evitá-las, três estratégias de tratamento podem ser escolhidas.

A primeira delas é a própria **continuidade de negócios** (objeto deste guia), ou seja, buscar melhorar a capacidade de restaurar o funcionamento das atividades a níveis previamente estabelecidos.

Caso a paralisação das atividades não tenha qualquer estratégia de continuidade que possibilite sua recuperação, mesmo que parcial, ou o custo de tomar esta ação seja desproporcional ao benefício em potencial, a entidade deve **aceitá-la**.

Por fim, para alguns riscos, a melhor resposta pode ser **transferi-los**. Isso pode ser realizado por meio de um seguro ou pagando-se um terceiro para assumir o risco de outra forma. Essa opção é particularmente boa na mitigação de riscos financeiros ou riscos ao patrimônio.

## Capítulo 3

# IMPLEMENTAÇÃO E GESTÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

Definidos Política de Gestão de Continuidade de Negócios (Capítulo 1) e Projeto do PCN (Capítulo 2), parte-se para a gestão efetiva da continuidade de negócios.

A metodologia a ser empregada na gestão do PCN pode prever a elaboração e administração de planos específicos, como os Planos de Contingência Operacional, de Recuperação de Desastres e de Gerenciamento de Crises (inspirados nas Normas ABNT NBR 15999-1 e 15999-2):

- **Plano de Contingência Operacional – PCO:** conjunto de cenários de inoperância previamente definidos e respectivos procedimentos alternativos planejados para manter a continuidade das atividades prioritárias.
- **Plano de Recuperação de Desastres – PRD:** conjunto de cenários de desastre (incidente maior com interrupção de negócios) previamente definidos e de respectivos procedimentos de reação para garantir que as atividades prioritárias retomem nível de operação aceitável dentro de prazo tolerável.
- **Plano de Gerenciamento de Crises – PGC:** conjunto de cenários de crises previamente definidos e de respectivos procedimentos de gestão para administrar, neutralizar ou eliminar impactos até a superação da crise.

Os referidos cenários de situações inesperadas ou incidentes (quer sejam operacionais, desastres ou crises) deverão estar descritos no PCN, o qual deverá conter de forma sistematizada as ações de contingência que deverão ser executadas pelas equipes envolvidas, de acordo com as suas atribuições.

Os grupos funcionais, descritos no tópico 1.6. deste Guia, deverão ter suas responsabilidades definidas para até quatro momentos: “antes do incidente”, “durante o incidente”, “durante a contingência” e “depois da contingência”.

Assim, pode ser definido, por exemplo, que o **Grupo Executivo**:

- *Antes do incidente* – determine o que deve ser atendido prioritariamente durante a contingência.
- *Durante o incidente* – autorize ou proíba o acionamento da contingência.
- *Durante a contingência* – mantenha-se informado e supervisione as ações de contingência.
- *Depois da contingência* – declare o encerramento da situação de contingência e o retorno operacional.

O **Grupo de Comunicação**, por sua vez – considerada a importância de um processo de comunicação (Orduña, 2002) – pode:

- *Antes do incidente* – determinar o formato da comunicação (notas de imprensa, carta, reuniões com representantes ou conferência de imprensa etc.), elaborar lista de contatos para comunicação em situação de emergência, estabelecer mecanismo de monitoração imediata em todos os meios para comprovar o alcance da crise, determinar a sequência e a coerência da comunicação (ou seja, quem liga para quem, e quem retorna informando que todos os colaboradores estão cientes da situação e dos próximos passos numa situação de contingência).
- *Durante o incidente e durante a contingência* – informar, com o prévio conhecimento e aprovação da alta direção, evitar que sejam dadas declarações públicas sem preparo prévio das intervenções, registrar o contato de todos os membros dos Grupos de Comunicação/Apoio e de Administração de Crise (nome completo, cargo na companhia, endereço eletrônico – da entidade e outro que possa acessar desde uma conexão remota –, números de telefones da em-

presa, da residência e dos celulares), manter banco de dados de contatos com todos os interessados/afetados pela crise (bombeiros, polícia, políticos, sindicatos, fornecedores, participantes, meios de comunicação, associações civis etc.).

Com relação ao sistema de telecomunicação, a entidade deve monitorar diariamente o tráfego telefônico e performance da rede, realizar análises e oferecer alternativas para solução de contingência como, por exemplo, redirecionar as ligações para um número alternativo.

- *Depois da contingência* – propor o plano de ação para a revisão ou reforço, se necessário, da imagem corporativa que contemple a todos os públicos, bem como identificar o que não aconteceu conforme planejado.

O **Grupo de Administração de Crises (GAC)**, por sua vez, poderá ser convocado pelo Grupo Executivo, quando este for informado pelo gestor de um processo sobre situação de emergência e considerar iminente a sua evolução para um cenário de crise.

O GAC avaliará a situação apresentada e caso considere que todas as medidas de recuperação já foram tomadas e que houve a evolução para um cenário de crise, contemplado ou não no PCN, proporá a declaração da situação de crise ao Grupo Executivo.

Os colaboradores do Grupo Operacional, conforme previsto na Política de Continuidade de Negócios, têm atribuições voltadas para o apoio administrativo e à infraestrutura física e de tecnologia.

No que diz respeito ao tratamento da tecnologia de informação durante a contingência, por exemplo, tão importante quanto conhecer os riscos a que o site está exposto, está a velocidade em que ele pode ser ativado. Sites próximos à sede geralmente tem um tempo de ativação relativamente rápido, quando bem estruturados, no entanto podem estar expostos aos mesmos riscos do site principal.

A complexidade e o detalhamento da estratégia de *backup* dependem do porte e das necessidades de cada entidade: de *backup* de dados uma vez por semana a *backup* que exija plataforma contínua da proteção dos dados (Moraes, 2007).



Antes de se fazer o *backup* dos sistemas da entidade e/ou das máquinas das estações de trabalho, é necessário fazer a classificação da informação, com atributos como permissões de acesso, data, tempo de retenção, local de armazenamento etc.

Um plano de *backup* deve prever, de acordo com o referido autor, dentre outros, os seguintes procedimentos:

- Classificação da informação – análise de riscos das informações, considerando, no mínimo, criticidade da informação para os negócios, prioridade de recuperação e período de retenção.
- Armazenamento – pode ser apenas dos dados necessários e armazenamento apenas pelo período necessário.
- Documentação de todos os processos de *backup* e recuperação de dados.
- Escolha de hardware, software e mídias.
- Definição do local dos dados a serem armazenados – com garantia de segurança física e lógica.
- Contratação de site remoto considerando, no mínimo, segurança física e lógica, que deve ser igual ou melhor que a do *backup* local, distância geográfica, e a probabilidade de acontecer um desastre que atinja o *backup* local e remoto, acessibilidade, ou tempo necessário para se recuperar o *backup* e conformidade da empresa contratada com padrões de segurança.
- Definição de responsabilidades – com equipe, ou pelo menos um responsável para todas as etapas acima, com treinamento constante para esse(s) responsável(eis).

### 3.1. Divulgação e Conscientização

O desenvolvimento da cultura de Gestão de Continuidade de Negócios (GCN) na entidade deve prever sua aderência aos valores básicos e à gestão efetiva da entidade.

A criação e inclusão de uma cultura de GCN pode ser um processo longo e de difícil execução e ainda encontrar um nível de resistência acima do esperado. Por isso, para uma entidade disseminar a cultura de GCN é importante ter como suporte:

- liderança do PCN pela alta administração da entidade;
- atribuição de responsabilidades;
- conscientização;
- desenvolvimento de habilidades;
- plano de testes.

A entidade deve ter mecanismos para conscientizar e avaliar a eficiência da implantação da GCN, como a educação e a divulgação permanente de informações, tais como:

- processo de consulta a toda a equipe sobre a implantação do programa de GCN;
- discussão da GCN nos informativos, apresentações, programas ou reportes diários da entidade;
- inclusão da GCN nas páginas pertinentes da web ou intranet, de fácil acesso, inclusive remoto (o plano de continuidade, por conter informações estratégicas, é documento confidencial e deve ser de uso interno e restrito, por isso é importante que o site seja seguro e com acessos limitados por login e senhas);
- GCN como um dos temas nas reuniões de equipe;
- comunicação a todos os colaboradores sobre a importância de atingir os objetivos da gestão de continuidade de negócios e conformidade com a política de continuidade de negócios;
- garantia de que todas as pessoas chave estejam cientes da relevância e importância de suas atividades de continuidade de negócios e de que forma contribuem para atingir os objetivos do GCN.

### 3.2. Testes

Para garantir que os planos estejam aptos a cumprir seus objetivos, deve ser elaborado programa de testes periódicos ou extraordinários e de avaliação dos resultados respectivos, levando em conta a legislação e as regulamentações vigentes.

Segundo a Norma ABNT NBR 15999-1, teste é definido como atividade na qual os planos de continuidade de negócios são exercitados parcial ou integralmente, de forma a garantir que os planos contenham as informações apropriadas e produzam o resultado desejado quando colocados em prática.

A norma esclarece ainda que um teste pode envolver a execução de procedimentos de continuidade de negócios, mas é mais provável que envolva apenas uma simulação de um incidente de continuidade de negócios, previamente anunciada ou não, na qual os participantes interpretam papéis de forma a avaliar quais os problemas que podem ocorrer antes de uma execução real.

Este programa de testes deve ser elaborado de forma que, ao longo do tempo, garanta o alcance do objetivo, ou seja, que o PCN funcionará como previsto, quando necessário e no tempo presumido.

Os resultados dos testes, as críticas recebidas e os relatórios periódicos devem ser integrados e consolidados, de modo a instruir processo de aperfeiçoamento do PCN.

O Programa de Testes deve abranger os seguintes tópicos:

#### a) Execução de testes:

- dos aspectos técnicos, logísticos, administrativos, de procedimento e outros sistemas em operação do PCN; e
- dos preparativos e da infraestrutura da GCN, incluindo papéis, responsabilidades e quaisquer locais de gerenciamento de incidentes e áreas de trabalho, entre outros;

b) Validação da recuperação da tecnologia e das telecomunicações, incluindo a disponibilidade e remanejamento de pessoal.

Os benefícios de um Programa de Testes são:

- demonstração das possíveis respostas ao plano de continência;
- treino da equipe de forma a responder de maneira eficaz a um incidente ou interrupção;
- adiantamento de resultado previsto, ou seja, que tenha sido antecipadamente planejado e incluído no escopo;
- possibilitar à entidade desenvolver ações inovadoras;
- verificação de que todas as atividades críticas da organização, suas dependências e prioridades estejam contempladas pelo PCN;
- geração de confiança nos colaboradores envolvidos no teste;
- aumento da consciência do processo de continuidade de negócios pela organização por meio da publicação do teste;
- demonstração da competência das equipes titulares de resposta a incidentes e de seus substitutos.

Quando da estruturação dos testes, é recomendável especial atenção para as seguintes abordagens:

- definição da escala e complexidade dos testes de forma apropriada aos objetivos de recuperação da organização;
- planejamento de acordo com as partes interessadas (principais fornecedores, parceiros terceirizados e outros), que seria esperado participarem das atividades de recuperação;
- busca de não interrupção dos processos de negócios, resultado direto de acidente do teste (exemplo: não coincidir com datas de fechamento contábil, de auditorias ou de outro período crítico para o negócio);

- elaboração do relatório e de análises após o teste com evidências quanto ao alcance dos objetivos e recomendações de melhorias;
- avaliação das recomendações contidas no relatório e estabelecimento de previsão de implantação destas;
- aptidão para refazer testes que demonstrem deficiências sérias ou imprecisões no PCN, depois de as ações corretivas terem sido completadas.

Os testes e as simulações podem ser realizados pelos gestores e suas equipes com o uso de diferentes instrumentos:

- **Testes de mesa** – consistem na avaliação, com base em listas de verificação, das ações descritas no procedimento, com o objetivo de atualizar e/ou validar o conteúdo do plano.
- **“Walk-through”** – consiste na conferência de todos os passos descritos no PCN.
- **Teste de atividades críticas** – consiste na realização de operações críticas, descritas nos PCN, em ambiente controlado, por tempo determinado.
- **Simulação** – consiste nos testes dos principais pontos de um procedimento, com a finalidade de validar parcialmente o plano.
- **Teste completo** – consiste nos testes de todos os pontos de um procedimento, com a finalidade de validar integralmente o plano.

### 3.2.1. Elementos de um modelo básico de Plano de Contingência Operacional (PCO)

<b>Plano de Contingência Operacional</b>	
<b>Área</b> (Diretoria, Gerência)	
<b>Responsável pelo PCO</b> (nomes, cargos, e-mail e telefones)	
<b>Contatos de emergência na EFPC</b> (nomes, cargos, e-mail e telefones)	
<b>Objetivo do PCO</b> (Assegurar condições para continuidade do referido processo durante a contingência, reduzindo perdas)	
<b>Tempo real de recuperação</b> (Recovery Time Objective – RTO)	
<b>Teste do PCO</b> (tipo de teste e data de realização)	
<b>Data da aprovação do PCO pelo Grupo Executivo</b>	
<b>Data de Revisão do PCO</b>	



<i>Procedimentos</i>	
<i>Antes do Incidente</i>	
<i>Durante o Incidente</i>	
<i>Durante a Contingência</i>	
<i>Após a Contingência / Retorno à Normalidade</i>	

<i>Contingência – Local, Sistemas e Tecnologia</i>	
<i>Espaço Físico (Identificação do local)</i>	
<i>Sistemas Críticos</i>	
<i>Tecnologia (hardware, software, equipamento de telecomunicações)</i>	

### 3.3. Treinamento

Os programas de treinamento deverão ajustar seu conteúdo em função do público-alvo a ser atingido, que deverá incluir desde a alta direção até os colaboradores com missão essencialmente operacional e os fornecedores mais diretamente vinculados ao tema.

A base estrutural desta etapa requer que a entidade treine:

a) a equipe de GCN para tarefas como:

- desenvolvimento e implantação de PCN;
- avaliação de riscos e ameaças;

- execução de análise de impacto nos negócios;
- execução de programa de testes de PCN;
- comunicação com a mídia.

b) os colaboradores não relacionados diretamente à GCN que necessitem de habilidades específicas para desempenhar seu papel, em respostas a incidentes ou recuperação de negócios.

É conveniente que habilidades e competências de resposta na organização sejam desenvolvidas por meio de treinamentos práticos, incluindo participação ativa em testes.

### 3.4. Retorno à Normalidade

O processo de retorno à normalidade começa durante a execução do próprio PCN, quando tiverem sido adotadas as estratégias de resposta a incidentes e a EFPC já estiver funcionando de forma contingencial.

Após o retorno, deverão ser produzidos relatórios com informações sobre o evento, os custos incorridos, recursos utilizados, tempos de recuperação etc.

Ainda que o objetivo geral de recuperação seja o retorno à normalidade o mais rápido possível, em alguns casos ou incidentes os planos de recuperação desenvolvidos pelas empresas não podem ser utilizados imediatamente. Assim, convém que cada PCN seja capaz de operar por um período estendido, se necessário, permitindo que os planos de recuperação possam ser executados assim que possível, buscando o retorno à normalidade.

## Anexo

### CHECK LIST PARA AVALIAÇÃO DO PCN

	Item	Institucionalizado (sim/não)	Avaliação (legenda)	Observação
1	Estabelecimento da estrutura gerencial para iniciar, coordenar, implantar e manter todo o processo de PCN.			
2	Avaliação contínua e consequentes ajustes do PCN.			
3	Definição dos responsáveis, e substitutos, com funções e alçadas claramente definidas.			
4	Documentação detalhada sobre as definições de critérios para identificação de processos críticos e as atividades afetadas.			
5	Identificação dos ativos envolvidos nos processos identificados como críticos (mapeamento dos processos).			
6	Identificação da relação entre processos/atividades, ponderando as dependências de sistemas, de pessoas, finanças entre outros.			
7	Identificação dos eventos que podem gerar interrupção.			
8	Identificação das possibilidades de ocorrência dos eventos de ruptura e seus impactos (eventos/cenários).			
9	Análise dos impactos financeiro, operacional, imagem e legal.			

10	Definição do tempo de recuperação para cada atividade identificada como crítica (RTO).			
11	Definição do período máximo de perda ou indisponibilidade de dados (RPO).			
12	Mapeamento dos custos da contingência.			
13	Identificação de medidas que reduzam ou evitem a probabilidade de interrupção.			
14	Identificação de medidas que reduzam o período de interrupção.			
15	Identificação de medidas que limitem o impacto de uma interrupção nos produtos/serviços críticos.			
16	Identificação de medidas que reduzam o risco e o custo durante o período de interrupção.			
17	Definição do nível das ações de contingência, a partir dos processos/atividades críticas e eventos/cenários de ruptura. Exemplo: <i>backup</i> , site de contingência.			
18	Definição dos recursos necessários (exemplo: pessoas, instalações, TI) para cada nível de ação de contingência.			
19	Definição da estratégia de recuperação (critérios e procedimentos de implementação).			

#### LEGENDA:

0 – não possui

1 – incipiente / em elaboração / em desenvolvimento

2 – atende parcialmente

3 – em fase de conclusão

4 – atende totalmente

## REFERÊNCIAS BIBLIOGRÁFICAS

O Guia de Boas Práticas para Planos de Continuidade de Negócios foi elaborado a partir das experiências acadêmicas e profissionais dos membros da Comissão Técnica Regional Sudeste de Governança e da consulta às seguintes fontes listadas abaixo.

Associação Brasileira de Normas Técnicas – ABNT 15999-1 NBR – *Gestão de continuidade de negócios*. 2007. 40p.

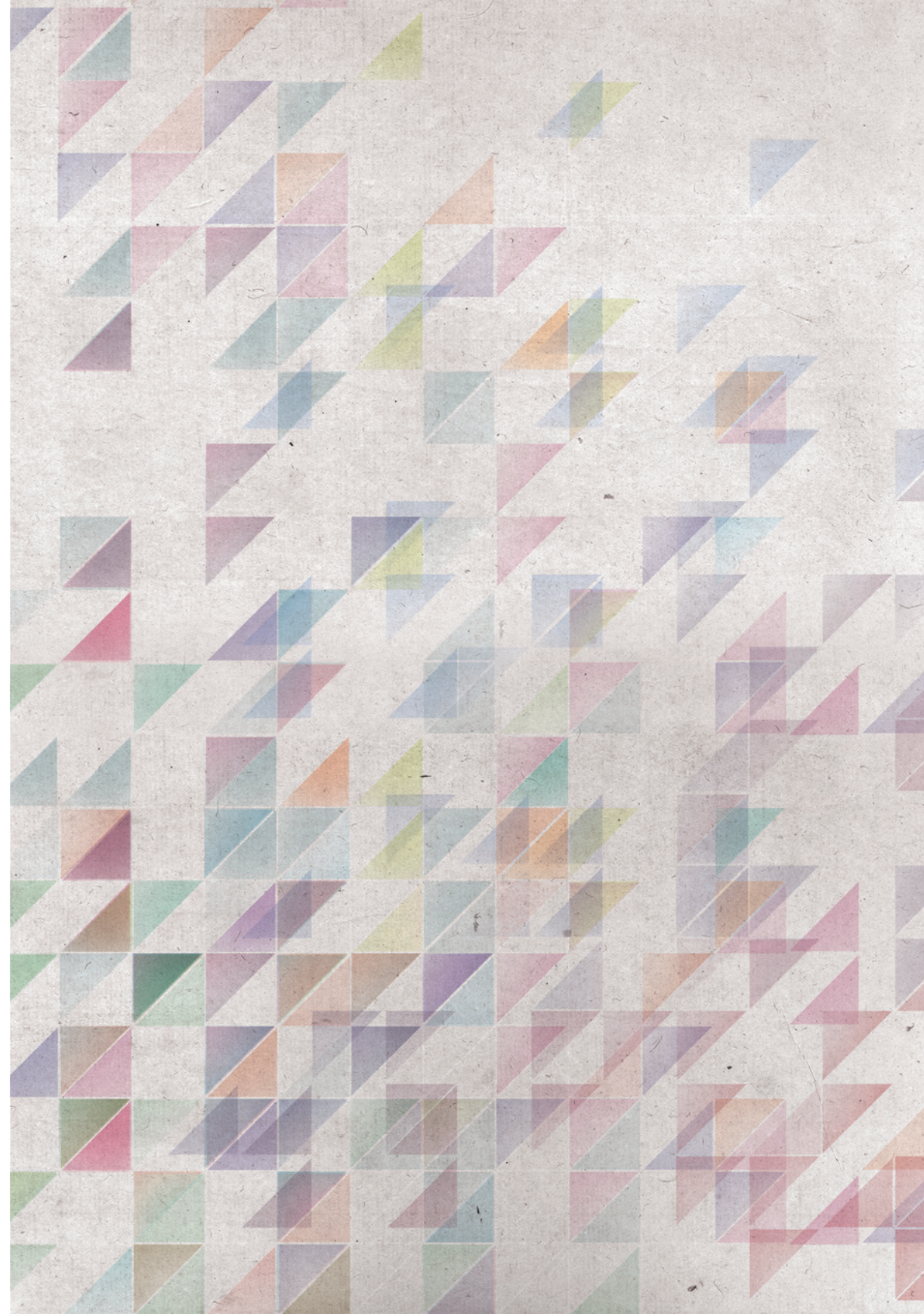
Coral, E. *Avaliação e gerenciamento dos custos da não qualidade*. Universidade Federal de Santa Catarina. Tese de mestrado. 1996.

Moraes, E.M. *Planejamento de back up de dados*. Tese de mestrado. 2007. 124p.

Norma BS 25999-1:2006 (Gestão de continuidade de negócios – Parte 1: Código de práticas).

Orduña, O.I.R. *A comunicação em momentos de crises*. Paper 7p. s.d.

Oliveira *et alii*. *Plano de continuidade de negócios*. Apresentação. [http://www.lyfreitas.com.br/artigos\\_mba/artpcn.pdf](http://www.lyfreitas.com.br/artigos_mba/artpcn.pdf). Acessado em Maio/2012.







ABRAPP

Associação Brasileira das Entidades Fechadas de Previdência Complementar


[www.portaldosfundosdepensao.org.br](http://www.portaldosfundosdepensao.org.br)


Tel.: (11) 3043.8777

Fax: (11) 3043.8778/3043.8780

Av. das Nações Unidas, 12551 – 20º andar – Brooklin Novo

04578-903 – São Paulo – SP

 @abrapp

 [www.facebook.com/abrapp](http://www.facebook.com/abrapp)