TÍTULO I - **POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS - PGCN**

Capítulo I - **Objetivos**

1. Definir medidas a serem tomadas pelo BRDE no caso de paralisação de suas atividades, total ou parcialmente, para fazer com que seus processos de trabalho críticos voltem a funcionar plenamente, ou em um estado minimamente aceitável, dentro do tempo de espera previsto, evitando assim uma paralisação prolongada que possa gerar prejuízos.

2. Orientar a Gestão da Continuidade de Negócios (GCN) visando a contribuir para a resiliência e a sustentabilidade dos negócios do BRDE.

2.1. Continuidade de Negócios: é a capacidade de o BRDE antecipar-se a eventos que possam interromper os seus produtos e serviços, estando preparado para atuar e manter o andamento de suas atividades essenciais.

2.2. Meta: Evitar que a indisponibilidade de serviços cause impactos negativos, com potencial de disseminação rápida e em larga escala, capazes de expor a imagem e a reputação do BRDE, em diversos canais, inclusive redes sociais, sujeitando-a a reclamações de clientes e crises corporativas.

2.3. Política de Contingência e de Continuidade de Negócios: foi elaborada para proteger seus colaboradores, assegurar a continuidade dos processos essenciais em níveis aceitáveis de performance, salvaguardar as receitas e sustentar tanto a estabilidade dos mercados em que atua quanto a confiança de seus clientes, acionistas e parceiros estratégicos.

2.3.1. A GCN avaliará aspectos regulatórios, desenvolvendo metodologia, treinamentos e conscientização, respondendo aos órgãos reguladores e clientes institucionais e avalia novos produtos e projetos.

2.3.2. A GCN é contínua e está distribuída nas frentes a seguir:

I - Estabelecimento de Plano de Continuidade de Negócios: direciona os envolvidos na Gestão de Continuidade de Negócios do BRDE;

II - Conscientização e aculturamento: incorpora a continuidade de negócios na cultura do banco;

III - Análise da organização: identifica e avalia os impactos diante de uma eventual interrupção;

IV - Definição de estratégias: define estratégias viáveis para a continuidade das operações, considerando os aspectos técnicos e financeiros;

V - Implementação de soluções: responde de forma resiliente a um evento para que as funções de negócios essenciais possam continuar dentro de níveis e tempos previamente definidos e aceitáveis;

VI - Garantia de melhoria contínua: garante que as soluções de continuidade de negócios e a estrutura de resposta reflitam as necessidades do banco, e que os planos sejam efetivos e eficazes.

2.4. A presente política considera as melhores práticas de mercado e os requisitos regulatórios específicos.

Capítulo II - **Público Alvo**

3. Esta Política aplica-se aos agentes públicos vinculados ao BRDE, assim entendidos os membros do Conselho de Administração, do Comitê de Auditoria, da Diretoria e de todos os órgãos estatutários, os empregados, os estagiários, os jovens aprendizes e todos que, com ou sem remuneração, prestem serviços ao BRDE, inclusive de forma temporária, e, no que couber:

I - A todos os fornecedores, parceiros de negócios e prestadores de serviços do BRDE, bem como às entidades que direta ou indiretamente tenham relações formais ou vínculo com o BRDE, inclusive aquelas sem fins lucrativos, bem como as geridas por administradores ou empregados designados ou cedidos pelo BRDE;

II - Aos empregados em gozo de licença, bem como a todo agente que, por força de lei, contrato ou qualquer ato jurídico, preste serviços ao BRDE de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira.

Capítulo III - **Gestão da Continuidade de Negócios - GCN**

4. Exercida sob a responsabilidade do DIRAD, na forma prevista no Regimento Administrativo do BRDE e nesta Política, a GCN deverá dotar o BRDE de Plano de Contingência e de Continuidade de Negócios – PCN, contendo mecanismos de resposta para situações em que uma eventual interrupção nas atividades do BRDE, por determinado intervalo de tempo, possa ter impacto elevado nas entregas de um processo da cadeia de valor do BRDE.

4.1. A GCN deverá assegurar que as diversas unidades da estrutura organizacional do BRDE construam resiliência organizacional, identificando e planejando o que é necessário fazer para que o BRDE continue cumprindo suas obrigações no caso da ocorrência de um evento grave de interrupção nas suas operações.

4.2. As ações de GCN, além de terem como propósito específico o aumento da resiliência institucional, também servem como forma de disseminação da cultura de gestão de riscos.

Capítulo IV - **Diretrizes de Gestão de Continuidade de Negócios**

5. A GCN observará as seguintes diretrizes:

I - Análise de Impacto nos Negócios (BIA): identifica e avalia o impacto de uma interrupção nos processos do BRDE. Utilizada para determinar as prioridades de recuperação, os tempos de retomada e os requisitos mínimos para definição dos planos de continuidade de negócios;

II - Avaliação de Vulnerabilidades e Ameaças (AVA): identifica os riscos inerentes às instalações e localidades em que a Instituição mantém seus colaboradores, bem como recomenda planos de ação para os riscos identificados;

III - Avaliação de Terceiros: analisa se as contingências e os respectivos exercícios/testes dos serviços prestados por terceiros atendem às necessidades de tempo máximo de indisponibilidade acordado com o gestor do processo de negócio, além de avaliar os riscos relacionados à continuidade dos negócios em terceiros;

IV - Nível de Cobertura de Contingência (NCC): indicador que mede o nível em que os processos estão cobertos com soluções de contingência em situação de interrupção;

V - Plano de Continuidade dos Negócios (PCN):Documenta as estratégias de contingência, papéis e responsabilidades entre outras informações, desenvolvidas, consolidadas e mantidas de forma que esteja disponível para utilização em eventuais interrupções;

VI - Plano de Contingência de Local de Trabalho (PCLT): estratégias definidas para que os processos críticos e os serviços essenciais continuem em operação em local de trabalho alternativo caso o local principal fique inoperante ou inacessível;

VII - Treinamentos: todos os colaboradores devem ser treinados em Continuidade de Negócios.

Capítulo V - **Principais Papéis e Atribuições**

6. Compete ao Conselho de Administração, na forma do art. 35, incisos III, XVI, XVIII e XX, deliberar sobre a revisão desta Política de Gestão de Continuidade de Negócios – PGCN.

6.1. O Diretor Administrativo - DIRAD, na forma do art. 44, III, do Regimento Administrativo do BRDE, será o responsável pela Gestão da Continuidade de Negócios - GCN.

6.2. A Diretoria poderá promover, sem necessidade de submeter ao Conselho de Administração, mas ouvido o Comitê de Riscos, promover alterações no Plano de Contingência e de Continuidade de Negócios - PCCN sempre que houver determinação de autoridade competente.

6.3. Os demais papéis e atribuições específicas de atuação das áreas envolvidas nas atividades de continuidade de negócios estarão referidos no Plano de Continuidade de Negócios e nos documentos relativos aos Módulos que o compõem.

TÍTULO II - **PLANO DE CONTINGÊNCIA E DE CONTINUIDADE DE NEGÓCIOS - PCN**

7. Conceito: O PCN representando o instrumento formal no qual estarão descritos os procedimentos e as estratégias a serem adotados pelo BRDE

com o objetivo de recuperar e restaurar os processos críticos em um nível aceitável e no período de tempo adequado no caso de ocorrência de incidentes graves que causem a interrupção das atividades essenciais ou a inacessibilidade ao ambiente físico, de forma temporária ou contínua.

7.1. O PCN conterá o conjunto de estratégias e planos táticos capazes de permitir o planejamento e a garantia dos serviços essenciais, devidamente identificados e preservados.

7.2. O PCN contará com módulos, os quais deverão ser compatíveis com os riscos e os recursos envolvidos, bem como com o tipo de interrupção, permitindo que um ou mais módulos sejam acionados diante da situação emergencial.

7.2.1. Módulos: O PCN será composto, no mínimo, dos seguintes módulos principais:

I - Contingência Operacional - PCO: alternativas para execução de processos críticos, sejam elas sistêmicas, processuais ou resposta a emergências, visando a minimizar o tempo de parada, estabelecendo forma de funcionamento predefinida, abrangendo a gestão dos recursos humanos e a operacionalização das atividades afetadas por evento de emergência, tais como: visitas aos clientes; vistoria de bens para avaliação de garantias; gestão das atividades funcionais de empregados cuja função não gera troca de documentos (contínuo, servente, motorista, recepcionista); funcionamento das unidades organizacionais que dependem de acesso a dossiês, processos e entrevistas às pessoas das demais unidades.

II - Contingência de Local de Trabalho - PCLT: estratégias definidas para que os processos críticos e os serviços essenciais, inclusive os prestados por terceirizados, continuem em operação em local de trabalho alternativo caso o local principal fique inoperante ou inacessível;

III - Contingência de Infraestruturas Tecnológicas – PCIT: estratégias definidas para que os processos críticos e os serviços essenciais, inclusive os prestados por terceirizados, continuem em operação, possibilitando a continuidade do funcionamento do BRDE diante a quaisquer eventualidades (materiais ou pessoais), além de estabelecer escopos estratégicos e ações para nortear a prevenção de incidentes e recuperação em caso de desastres.

7.2.2. Grupo Tático: Cada módulo conterá a identificação dos colaboradores que terão atribuições na administração de crise e na supervisão das atividades, responsáveis por assegurar os recursos necessários para operação do PCN, além de gerir os cenários de contingência e apoio ao processo de decisão.

8. Objetivo do PCN: São os seguintes os objetivos do PCN, devendo ser respeitados na elaboração de cada módulo:

I - Identificar e analisar impactos nos negócios e perdas potenciais;

II - Garantir a continuidade dos negócios, operações e serviços;

III - Priorizar os processos críticos definidos corporativamente, incluindo todas as atividades desde a linha de frente até as áreas de suporte;

IV - Estabelecer detalhadamente todas as atividades, procedimentos, responsabilidades e necessidades de recursos no momento de uma eventual interrupção no PCN;

V - Assegurar que, em caso de incidentes graves, os processos de negócios críticos sejam reestabelecidos no menor prazo possível visando evitar impactos na prestação de serviços aos clientes e prejuízos em decorrência da interrupção das atividades.

9. Abrangência: Todos os processos, dependências e unidades organizacionais devem ser avaliados quanto à criticidade que representam para o BRDE e consequentemente sua necessidade de recuperação imediata, observando, especificamente, as seguintes necessidades de contingência:

9.1. Infraestruturas Tecnológicas: compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecomunicações, rede e segurança.

9.2. Infraestruturas Físicas: assim compreendidas:

I - As situações de emergência ou de calamidade pública decorrentes de catástrofes, naturais ou não, que impeçam o acesso e/ou utilização das instalações do BRDE;

II - A ocorrência de danos físicos relevantes a instalações e/ou equipamentos necessários ao normal funcionamento do BRDE, intencionais ou não, e ainda falhas no fornecimento de serviços essenciais, incluindo energia elétrica, telecomunicações e processamento de dados.

9.3. Recursos Humanos: aquelas onde o pessoal a serviço do BRDE não possa comparecer ao trabalho por motivos de greve, bloqueio, doença, licença etc.

9.4. Serviços Terceirizados: compreende as situações de não prestação de serviço contratado considerado crítico ou essencial aos processos do BRDE, cujo módulo deverá respeitar o seguinte:

10. Conteúdo mínimo de cada Módulo do PCN: Cada módulo deve conter, no mínimo:

10.1. Análise de Risco: a probabilidade de ocorrência de um evento indesejado e ou imprevisível causando graves rupturas operacionais. A avaliação dos riscos aos quais o BRDE deve ser considerar:

I - A PROBABILIDADE de que o evento produza rupturas graves;

II - A GRAVIDADE do evento;

III - A SEVERIDADE do risco;

IV - O ÍNDICE de exposição ao risco.

10.1.1. Probabilidade: A probabilidade de consequências prejudiciais aumenta com a maior exposição.

PROBABILIDADE		
Frequência	**Significado**	**Pontuação**
Frequente	Ocorrência provável	5
Ocacional	Provável que ocorra ocasionalmente	4
Remoto	Improvável, mas possível de ocorrer	3
Improvável	Muito improvável que ocorra	2
Estremamente Improvável	Quase inconcebível que ocorra	1

10.1.2. Gravidade do Evento:

GRAVIDADE DO EVENTO		
Escala	**Significado**	**Pontuação**
Gravíssimo	Destruição de equipamento ou instalações. Morte	A
Grave	Destruição de equipamento. Instalações inacessíveis. Lesão grave	B
Médio	Equipamentos parcialmente comprometidos. Acesso limitado.	C
Baixo	Instalações e equipamentos operacionais. Uso alternativo de redes	D
Insignificante	Consequências leves	E

10.1.3. Severidade do Risco:

SEVERIDADE DO RISCO					
PROBABILIDADE	**Gravíssimo A**	**Grave B**	**Médio C**	**Baixo D**	**Insignificante E**
Frequente - 5	**5A**	**5B**	**5C**	**5D**	**5E**
Ocasional - 4	**4A**	**4B**	**4C**	**4D**	**4E**
Remoto - 3	**3A**	**3B**	**3C**	**3D**	**3E**
Improvável - 2	**2A**	**2B**	**2C**	**2D**	**2E**
Extremamente Improvável - 1	**1A**	**1B**	**1C**	**1D**	**1E**

10.1.4. Tolerância ao Risco: Com base nas avaliações de riscos podemos ordená-los por prioridade orientada pelos critérios de aceitabilidade dos riscos.

I - **Aceitável –** quando não é necessário adotar medidas mitigatórias, a menos que se possa reduzir mais o risco com pouco custo ou esforço;

II - **Tolerável –** o BRDE está preparado para suportar o risco. Medidas mitigatórias são recomendadas;

III - **Intolerável –** condições que impliquem em cessar as operações até que o risco se reduza ao nível tolerável.

Gestão de Risco	Severidade de Risco	Tolerância
Intolerável	**5A; 5B; 5C; 4A; 4B; 3A**	**Inaceitável sob as circunstânicas existentes**
Tolerável	**5D; 5E; 4C; 4D; 4E; 3B; 3C; 3D; 2A; 2B; 2C**	**Aceitável com mitigação de risco**
Aceitável	**3E; 2D; 2E; 1A; 1B; 1C; 1D; 1E**	**Aceitável**

10.2. Análise de Impacto nos Negócios (BIA):

I - Identificação dos processos operacionais críticos, com o levantamento das respectivas interdependências, principalmente daqueles nos quais participam fornecedores, empresas subcontratadas e parceiras no desenvolvimento de negócios, entre outros;

II - Classificação e documentação dos processos críticos de negócio;

III - Avaliação dos potenciais efeitos da interrupção dos processos mencionados no inciso I, com elaboração de cenários.

10.2.1. Serviços públicos essenciais: avaliar o impacto decorrente da interrupção no fornecimento de serviços públicos essenciais, tais como: energia elétrica, comunicações, transportes, segurança e nos serviços financeiros de infraestrutura (transferências financeiras relacionadas a recebimentos e pagamentos).

10.2.2. Estratégia de continuidade de negócios: define as atividades críticas, as interdependências, os objetivos do tempo de recuperação, a estratégia de gerenciamento e as táticas que garantam a continuidade de negócios, a recuperação de recursos e a estratégia para atividades críticas individuais, compreendendo, no mínimo:

I - 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;

II - 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;

III - 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 empregados; cadastro de fornecedores; e documentos legais (contratos de empréstimo, termos de adesão etc.). Cópias também devem ser guardadas em instalações alternativas, previamente estabelecidas;

IV - Instalações – realização de trabalho em casa ou em locais remotos, uso de força de trabalho alternativa em local estabelecido e outras.

10.2.3. Recuperação de Desastre (PRD): define os principais componentes envolvidos no negócio, o pessoal da equipe de recuperação de desastres com detalhes de contato, objetivo de tempo de recuperação e métodos de comunicação no momento do desastre, instalação alternativa e lista principal de todos os inventários, locais de armazenamento, cliente/fornecedor, formulários e políticas. Inclui a lista de procedimentos de recuperação e de verificação, explicando como as pessoas devem lidar frente a um desastre e se recuperar de seus efeitos posteriores.

10.2.3.1. Objetivo do tempo de recuperação (RTO): refere-se ao tempo máximo permitido para restaurar o funcionamento do BRDE ou o site ao seu modo totalmente funcional após um desastre, de modo que o tempo de inatividade permaneça 'tolerável' baixo. Quanto menor a tolerância do processo para o tempo de inatividade, menor deverá ser a duração permitida do RTO para o Módulo.

10.2.3.2. Objetivo do ponto de recuperação (RPO): medida de quão recentes e atualizadas os arquivos devem ser, os quais, quando recuperados, garantem operações normais. O RPO é expresso em tempo passado, com referência ao momento em que o desastre / tempo de inatividade ocorre. A unidade de medida é horas ou minutos. Um número baixo nessa métrica indica um PCN.

10.2.4. Plano de treinamento e conscientização: visão geral detalhada sobre como os funcionários serão conscientizados para realizar as tarefas planejadas e como eles são treinados sobre a importância da continuidade de negócios.

10.2.5. Plano de exercícios e testes de continuidade de negócios: descreve como os planos serão exercitados e testados com o objetivo de identificar as ações corretivas necessárias e aprimorar o plano.

10.2.6. Plano de revisão e manutenção do PCN: visão geral detalhada sobre como os planos e outros documentos do PCN devem ser mantidos para garantir seu funcionamento em caso de interrupção nos negócios.

10.2.7. Testes e revisões: especificar quais testes, com periodicidade adequada aos riscos envolvidos e estipular os pontos de revisão do respectivo Módulo.

10.2.8. Comunicações necessárias. respeitadas as competências e atribuições previstas na Política de Porta Vozes.

10.2.9. Revisão pós-incidentes: roteiro a ser utilizado para analisar a eficácia dos planos após um incidente.

10.3. Atribuições e competências: especificar quem são os responsáveis pela execução das providências previstas em cada Módulo, as quais serão cumpridas além das já previstas na regulamentação da Estrutura Organizacional e neste instrumento, observando, ainda:

10.3.1. **SUPIN**:

I - Elaborar, administrar e executar o Módulo PCLT, observando o seguinte no tocante aos serviços terceirizados relevantes:

a) Premissas: São considerados serviços terceirizados relevantes, tendo em vista a definição constante na Política de Gerenciamento do Risco Operacional:

1. Serviços cuja interrupção afetaria a efetividade das atividades essenciais do BRDE;
2. Serviços cuja alteração de fornecedor afetaria a efetividade das atividades essenciais do BRDE, ainda que apenas no curto prazo;
3. Serviços contratados com a finalidade principal de mitigar riscos operacionais classificados como altos na Matriz de Riscos do BRDE.

b) Classificação: O PCLT deverá conter a identificação de todos os serviços terceirizados contratados pelo BRDE, classificados conforme a relevância e essencialidade para o funcionamento do Banco, observadas as premissas referidas na alínea “a” anterior;

c) Monitoramento:

1. SUPIN: Cabe à SUPIN informar à SURIS, trimestralmente:
   - A regularidade da prestação dos serviços terceirizados;
   - A adequação dos serviços ao respectivo PCLT.
2. SURIS: Cabe à SURIS incluir no Relatório Trimestral de Riscos Operacionais a avaliação quanto à relevância de cada serviço, a situação de cada contrato e, para aqueles identificados como serviços terceirizados relevantes na forma da alínea “a” do tem 10.2.1, I:
   - A existência de risco operacional relevante decorrente da opção pela terceirização da atividade;
   - A existência de eventuais inadequações e/ou inconformidades em contratos;

- A necessidade de estabelecimento de controles e elaboração de plano de ação de contingência.

II - Participar da elaboração e das revisões do Plano de Contingência Operacional - PCO;

III - Assegurar que o BRDE mantenha equipes treinadas nas suas respectivas responsabilidades para agilizarem o processo de recuperação e continuidade de qualquer negócio;

IV - Analisar periodicamente a documentação existente para suportar a restauração do ambiente em situação de contingência;

V - Manter uma lista de contatos atualizada, inclusive de principais fornecedores e clientes, disponibilizando-a em meios que possam ser consultados, no caso de emergência, por qualquer colaborador do BRDE, bem como terceiros relacionados a providências e ações previstas em cada Módulo;

VI - Programar e coordenar simulação de situações emergenciais, bem como garantir que sejam realizados testes periódicos das ações para restauração do ambiente;

VII - Coordenar as ações necessárias à recuperação do funcionamento regular do BRDE em termos de PCLT, dando suporte a todas as necessidades para execução das ações de recuperação relativas ao PCIT;

VIII - Caso seja necessário o deslocamento de funcionários para a implementação do PCN de forma emergencial, o SUPIN poderá autorizar a realização das despesas necessárias para o transporte diretamente pelo funcionário, efetuando o posterior ressarcimento mediante apresentação da documentação comprobatória, observadas, no que couber, as disposições do Regulamento de Viagens, Transportes, Uso, Locação, Aquisição e Alienação de Veículos.

10.3.2. **GERAD**:

I - Implementar as ações previstas no PCLT relativas à respectiva Dependência, incluindo os escritórios regionais, cabendo à AGPOA/GERAD as ações necessárias à DIGER e ao ESCRJ;

II - Em caso de impossibilidade de acesso às dependências ou de indisponibilidade total de recursos, os funcionários não designados como responsáveis por ações no âmbito do PCN deverão ser orientados a permanecer em suas residências até que recebam instruções sobre a retomada das atividades;

III - A comunicação aos terceirizados, exceto aqueles relacionados ao PCIT, cuja responsabilidade é da SUTEC;

IV - Informar aos novos funcionários e fornecedores, sobre a política existente na instituição e, incentivar a participação no treinamento do plano de contingência e de continuidade de negócios.

10.3.3. **GADIR**: implementar as ações previstas no PCN relativas às comunicações à comunidade, aos órgãos externos, fiscalizadores ou não, e mídia, respeitadas as competências e atribuições previstas na Política de Porta Vozes.

10.3.4. **SUTEC**:

I - Elaborar, administrar e executar o Módulo PCIT, de forma compatível com o Programa de Segurança Cibernética (SegCiber) e o Plano de Ação e de Resposta a Incidentes, instituído no âmbito da Política de Segurança da Informação, Cibernética e de Comunicações – PoSIC, abordando, no mínimo:

a) Política e procedimentos para *backup*;

b) *Status* do *backup*;

c) Verificação e teste de restauração;

d) Ciclos de *backup*;

e) Armazenamento de *backup*;

f) Efetiva contingência;

g) Estrutura de Suporte;

h) Lista de Informações;

i) Procedimentos de contingência.

II - Viabilizar o trabalho dos funcionários-chave de forma remota, disponibilizando acesso VPN e os recursos necessários ao desenvolvimento das atividades laborais;

III - O Comitê de Riscos poderá autorizar a locação de recursos físicos, inclusive *hardware*, ou lógicos, de forma emergencial, visando a atender as necessidades decorrentes do evento de descontinuidade de negócios.

10.3.5. **AUDIN**:

I - Avaliar o PCN, inclusive cada um de seus Módulos, enfocando a aplicação em cada Unidade Organizacional;

II - Acompanhar a auditoria externa e os órgãos reguladores por ocasião de avaliações do PCN.

10.3.6. **SURIS**:

I - Elaborar o PCN a partir dos módulos desenvolvidos pelas unidades responsáveis, conforme estipulado nesta Política, coordenando a elaboração do Plano de Contingência Operacional – PCO;

II - Garantir que as informações sobre o PCN estejam sempre atualizadas e acessíveis (física e eletronicamente);

III - Assegurar que a natureza, o escopo e a frequência dos testes previstos em cada Módulo do PCN devem ser determinados de acordo com a criticidade dos processos envolvidos e com as definições dos órgãos reguladores;

IV - A revisão e atualização periódica do PCN, com frequência máxima anual, compreendendo cada Módulo, submetendo as eventuais modificações à apreciação do Comitê de Riscos;

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

VI - Produzir e encaminhar à apreciação do CORIS e da Diretoria relatórios gerenciais que contenham, também, os resultados dos testes e das revisões.

10.3.7. **SUCEC, SUFIN, SUPLA, SUARC, SUPOA, SUFLO e SUCUR:** Participar do grupo de elaboração, revisão e atualização do Plano de Contingência Operacional – PCO, o qual será coordenado pela SURIS.

10.3.8. **CORIS:** Exercer as competências previstas no Regimento Administrativo do BRDE, responsabilizando-se pela existência e efetividade da PGCN, do PCN e de seus módulos, acompanhando os relatórios sobre os testes e as ações em situações de crise, bem como as demais competências previstas na PGCN ou no PCN.

10.3.9. **Conselho de Administração**: Exercer as competências previstas no Regimento Administrativo do BRDE, responsabilizando-se pela existência e efetividade da PGCN.

11. Vigência:

I - A PGCN será revisada a cada dois anos;

II - O PCN será revisado anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo;

III - Os documentos poderão ser alterados, ainda, a qualquer tempo em razão de circunstâncias que demandem tal providência.