Política de Gestão de Continuidade de Negócios

Unidades Gestoras: Diretora Superintendente – **DISUP**
Gerência de Controladoria e Gestão de Riscos – **GECOR**
Gerência de Tecnologia da Informação - **GETIN**

Aprovada pelo Conselho Deliberativo do SERGUS em 29/12/2022

SUMÁRIO

1. INTRODUÇÃO 2
2. OBJETIVO 2
3. APLICAÇÃO 2
4. ATUALIZAÇÃO DA POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS (PGCN) 2
5. **GESTÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS** 2
6. DIRETRIZES DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS 3
7. AMPARO LEGAL 4
8. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN) 4
8.1. CONCEITO 4
8.2. PROCEDIMENTOS 4
8.3. CONTEÚDO MÍNIMO DE CADA PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN) 5
8.3.1. Análise de Risco 5
8.3.2. Análise de Impacto nos Negócios 6
8.4. TESTES 7
9. DISPOSIÇÕES FINAIS 9

1. INTRODUÇÃO

O Instituto Banese de Seguridade Social – SERGUS disponibiliza a Política de Gestão de Continuidade de Negócios (PGCN) contendo informações sobre a mitigação de riscos operacionais e de restauração eficaz dos serviços interrompidos ou degradados por eventos de qualquer natureza, formalizando as diretrizes, responsabilidades, atribuições e definições da estrutura de funcionamento de um Plano de Continuidade de Negócios (PCN).

2. OBJETIVO

Esta Política tem por objetivo definir estratégias para o Plano de Continuidade dos Negócios (PCN) da entidade, bem como os papéis e responsabilidade que irão garantir a sustentação dos planos e a minimizar os impactos financeiros, operacionais, legais e regulatórios decorrentes de indisponibilidades dos recursos – humanos, materiais e tecnológicos – essenciais para o funcionamento de suas operações.

3. APLICAÇÃO

Esta Política se aplica a todos os empregados, membros da Diretoria Executiva e demais colaboradores da Entidade.

4. ATUALIZAÇÃO DA POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS (PGCN)

A Política de Gestão de Continuidade de Negócios (PGCN) deverá ser atualizada anualmente, conforme normas estabelecidas no Plano de Continuidade de Negócios (PCN).

5. GESTÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

A Gestão do Plano de Continuidade de Negócios prevê a elaboração e administração de planos específicos, como os Planos de Contingência Operacional, de Recuperação de Desastres e de Gerenciamento de Crises:

a. *Planos de Contingência Operacional – PCO:* conjunto de cenários de inoperância previamente definidos e respectivos procedimentos alternativos planejados para manter a continuidade das atividades prioritárias.
b. *Planos de Recuperação de Desastres – PRD:* conjunto de cenários de desastre previamente definidos e de respectivos procedimentos de reação para garantir que as atividades prioritárias retomem nível de operação aceitável dentro de prazo tolerável.
c. *Planos 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 Planos de situações inesperadas ou incidentes (quer sejam operacionais, desastres ou crises) deverão estar descritos no Plano de Continuidade de Negócios (PCN), o qual deverá conter de forma sistematizada as ações de contingência que deverão ser executadas pelos colaboradores da Entidade, de acordo com as suas atribuições.

Os colaboradores designados pela Diretoria Executiva da Entidade para analisar os processos críticos identificados no Plano de Continuidade de Negócios (PCN) são responsáveis pela manutenção, atualização e validação do respectivo plano, de acordo com os critérios e procedimentos estabelecidos nesta Política.

A Diretoria Executiva participa da aprovação do Plano de Continuidade de Negócios (PCN) e na ocorrência de contingências significativas ou cenários em que seja necessária tomada de decisões estratégicas para a Entidade.

Os gestores da Entidade são responsáveis por efetuar contatos com os membros da Instituição, além de garantir a disseminação adequada da informação para as áreas internas, e supervisionar as atividades do grupo operacional, assegurando os recursos necessários para a operação do Plano de Continuidade de Negócios (PCN), além de gerir os cenários de contingência e apoio ao processo de decisão da Diretoria Executiva.

Os gestores com atribuições operacionais definidas no Plano de Continuidade de Negócios (PCN), voltadas para apoio administrativo e à infraestrutura física e de tecnologia deverão disponibilizar o acesso às instalações, retorno do funcionamento do site, etc. a todos os empregados, membros da Diretoria Executiva e colaboradores da Entidade.

6. DIRETRIZES DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A Gestão de Continuidade de Negócios da Entidade deverá seguir as fases do desenvolvimento do Plano de Continuidade de Negócios mencionada no item 8 desta política, identificando as ameaças e os riscos que podem afetar a execução das atividades, conforme diretrizes a seguir:

a. **Análise de Impacto nos Negócios - AIN**: identifica e avalia o impacto de uma interrupção nos serviços executados no SERGUS. Utilizada para determinar as prioridades de recuperação, os tempos de retomada e os requisitos mínimos para definição dos planos de continuidade de negócios.
b. **Avaliação de Vulnerabilidades e Ameaças**: identifica os riscos inerentes às instalações e localidades em que a Entidade mantém seus colaboradores, bem como recomenda planos de ação para os riscos identificados.
c. **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 a continuidade dos negócios de terceiros.
d. **Nível de Cobertura de Contingência**: indicador que mede o nível em que os serviços estão cobertos com soluções de contingência em situação de interrupção.
e. **Plano de Continuidade dos Negócios**: 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.
f. **Plano de Contingência de Local de Trabalho:** estratégias definidas para que os processos críticos e os serviços essenciais continuem em operação em local de trabalho alternativo caso a sede da Entidade fique inoperante ou inacessível.
g. **Plano de Contingência de Infraestruturas Tecnológicas:** estratégias definidas para que os serviços essenciais, inclusive os prestados por terceirizados, continuem em operação,

possibilitando a continuidade do funcionamento do SERGUS 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.

h. **Treinamentos**: todos os funcionários e membros da Diretoria Executiva devem ser treinados em Continuidade de Negócios.

7. AMPARO LEGAL

O Plano de Continuidade de Negócios constitui parte integrante de uma governança corporativa bem estruturada e apoiada em princípios de melhores práticas de gestão de controles internos. Esses princípios deverão ser continuamente observados e estar em conformidade com a Resolução CGPC nº 13, de 01 de outubro de 2004, que dispõe os princípios, regras e práticas de governança, gestão e controles internos a serem seguidos pela Entidade:

> 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".

8. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

8.1. CONCEITO

O Plano de Continuidade de Negócios (PCN) conterá o conjunto de estratégias e planos táticos capazes de permitir o planejamento e a garantia dos serviços essenciais, devidamente identificados e preservados a serem adotadas pelo SERGUS.

8.2. PROCEDIMENTOS

O Plano de Continuidade de Negócios (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.

Deverão ser respeitadas na elaboração de cada módulo, os seguintes objetivos do Plano de Continuidade de Negócios (PCN):

a. Identificar e analisar impactos nos negócios e perdas potenciais;
b. Garantir a continuidade dos negócios, operações e serviços;
c. Priorizar os processos críticos definidos corporativamente, incluindo todas as atividades desde a linha de frente até as áreas de suporte;

d. Estabelecer detalhadamente todas as atividades, procedimentos, responsabilidades e necessidades de recursos no momento de uma eventual interrupção no Plano de Continuidade de Negócios (PCN); e,
e. Assegurar que, em caso de incidentes graves, os serviços sejam reestabelecidos no menor prazo possível visando evitar impactos na prestação de serviços aos participantes dos planos de benefícios e prejuízos em decorrência da interrupção das atividades.

8.3. CONTEÚDO MÍNIMO DE CADA PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

8.3.1. Análise de Risco

A análise de risco deverá considerar: a probabilidade de que o evento produza rupturas graves, a gravidade do evento, a severidade do risco e o índice de exposição ao risco conforme gráfico descrito a seguir:

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

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

b. Gravidade do Evento:

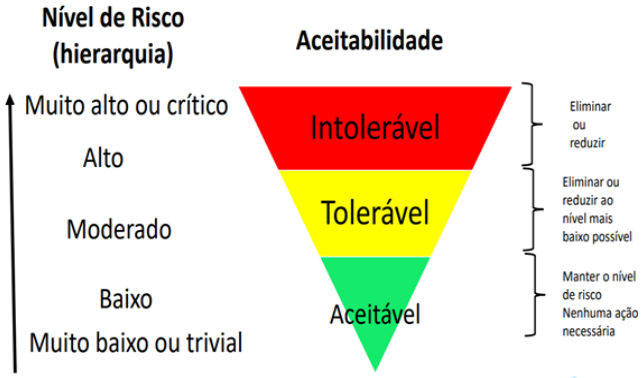
GRAVIDADE		
Escala	Significado	Pontuação
Gravíssimo	Destruição de equipamento ou instalações. Morte.	A
Grave	Destruição de equipamento. Instalação inacessíveis. Lesão grave.	B
Médio	Equipamentos parcialmente comprometidos. Acesso limitado.	C
Baixo	Instalações e equipamentos operacionais. Uso alternativo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

c. Severidade do Risco:

SEVERIDADE DO RISCO					
PROBABILIDADE DO RISCO	**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

d. **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 SERGUS 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.



8.3.2. Análise de Impacto nos Negócios

A análise de impacto no negócio (Business Impact Analysis — BIA, do inglês) permite aos gerentes determinar e avaliar os potenciais efeitos qualitativos e quantitativos que uma interrupção poderá causar às atividades críticas da Entidade, decorrente de fatores mínimos ou extremos (como desastres naturais ou acidentes fatais).

O processo de BIA é conduzido pela gerente da área de Controladoria e Gestão de Riscos - GECOR, que tem como missão avaliar, precisa e coerentemente, a potencialidade do impacto que determinado tipo de evento pode causar em cada departamento. Deverá seguir duas alternativas: entrevistar os gerentes das áreas e tomar como base as informações coletadas ou fazer com que eles se encarreguem de preencher os questionários.

Os questionários deverão ser elaborados prezando sempre pela objetividade, onde as perguntas contidas no item colocarão os gerentes frente as possíveis causas de indisponibilidade; caberá a eles preencher os campos de resposta de acordo com o nível do impacto que o problema causaria. Poderá, por exemplo, estabelecer quatro níveis de impacto:

1. Marginal (baixo dano);
2. Tolerável (prejuízo administrável);
3. Alto (coloca o negócio em risco);
4. Catastrófico (riscos de falência).

Na prática, os gerentes de área analisarão os níveis de impacto (de 1 a 4) sobre cada evento hipotético. Contudo, não só o impacto deverá ser avaliado na BIA: questões relativas ao limite

aceitável de informações perdidas, aos recursos necessários para a recuperação do negócio e à dependência de fornecedores, também precisam compor o processo, cabendo aos gerentes atentar às cláusulas do contrato assinado pelas partes.

8.4. TESTES

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.

Os testes têm por objetivo assegurar a eficiência e a efetividade do Plano de Continuidade de Negócios - PCN e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação e aprovação pela Diretoria Executiva da Entidade.

Para garantir que os planos estejam aptos a cumprir seus objetivos, deverá ser elaborado um programa de testes periódicos ou extraordinários e de avaliação dos resultados respectivos, levando em conta a legislação e as regulamentações vigentes, para situações de emergência que facilitem as ações em casos reais e que as falhas identificadas sejam registradas.

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

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da Gerência de Controladoria e Gestão de Riscos – GECOR, cabendo a área afim a sua execução.

Os testes deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela Diretoria Executiva da Entidade, sendo arquivado pela Gerência de Controladoria e Gestão de Riscos – GECOR.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nas dependências da Entidade e deverão ser conduzidos em total conformidade com o aprovado. As simulações deverão ser realizadas sobre ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.

Os resultados dos testes, as críticas recebidas e os relatórios periódicos deverão ser integrados e consolidados, de modo a instruir o processo de aperfeiçoamento do Plano de Continuidade de Negócios - PCN.

O programa de Testes deverá abranger os seguintes tópicos:

a) Os aspectos técnicos, logísticos, administrativos, de procedimento e outros sistemas em operação do PCN; e,

b) Os preparativos e da infraestrutura da Gestão de Continuidade de Negócios, incluindo papéis, responsabilidades e quaisquer locais de gerenciamento de incidentes e áreas de trabalho, entre outros.
c) Validação da recuperação da tecnologia e das telecomunicações, incluindo a disponibilidade e remanejamento de pessoal.

A estrutura dos testes deverá conter as seguintes abordagens:

a. Definição da escala e complexidade dos testes de forma apropriada aos objetivos de recuperação da organização;
b. Planejamento de acordo com as partes interessadas (principais fornecedores, parceiros terceirizados, etc.);
c. 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 outros períodos críticos para a Entidade);
d. Elaboração do relatório e de análises após o teste com evidências quanto ao alcance dos objetivos e recomendações de melhorias;
e. Avaliação das recomendações contidas no relatório e estabelecimento de previsão de implantação destas;
f. Aptidão para refazer testes que demonstrem deficiências sérias ou imprecisões na PCN, depois de as ações corretivas terem sido completadas.

A realização de testes deverá seguir o seguinte critério de execução:

EVENTO	PERIODICIDADE	RESPONSÁVEL
Simulação de evacuação do escritório em caso de desastre (incêndio, alagamento, suspeita de atentado terrorista, etc.).	Semestral	Gerência de Controladoria e Gestão de Riscos – **GECOR**.
Rodízio de colaboradores, para execução de atividades (exemplo: alocar, por um dia, um colaborador de "Empréstimos" na área de "Seguridade").	Eventual (fora de períodos críticos)	Gerente da área (GEAFC, GETIN, GECOR, GESEG, GEINV).
Home Office: liberar, por um dia, colaboradores cuja atividade principal possa ser executada de casa, estabelecendo controles de atuação remota.	Eventual	Gerente da área (GEAFC, GETIN, GECOR, GESEG, GEINV).
Simulação de situações para validar se os planos possuem informações suficientes para a atuação em caso de contingência.	Semestralmente (selecionar plano e executá-lo)	Gerente da área (GEAFC, GETIN, GECOR, GESEG, GEINV).
Testar recursos alternativos de TI.	Anualmente	Gerente de Tecnologia da Informação – GETIN.

Todos os testes do Plano de Continuidade de Negócios (PCN) deverão ser formalmente planejados e acordados entre as áreas envolvidas. Simulações de evacuação do SERGUS deverão ser aprovadas pela Diretoria Executiva do SERGUS. Os testes com recursos de Tecnologia da

Informação - TI e utilização de Home Office deverão ter a aprovação de, pelo menos, um Diretor da Entidade. A execução dos demais testes serão decididos pelos próprios gestores das áreas (GEAFC, GETIN, GECOR, GESEG, GEINV).

9. DISPOSIÇÕES FINAIS

Este documento tem efeito de Política e entra em vigor a partir da sua aprovação pelo Conselho Deliberativo da Entidade.

A Política de Gestão de Continuidade de Negócios do Instituto Banese de Seguridade Social – SERGUS deverá ser disponibilizada a todos os empregados, membros da Diretoria Executiva e colaboradores da Entidade.

As situações não contempladas neste documento seguem o disposto na Legislação vigente, nas recomendações do Comitê de Ética e Conduta e nas deliberações da Diretoria Executiva do SERGUS.

Compete as Gerências de Controladoria e Gestão de Risco e Tecnologia da Informação, propor a revisão ou alteração do texto desta Política, anualmente, devendo submeter à aprovação da Diretoria Executiva do SERGUS, cabendo a esta encaminhar ao Conselho Deliberativo do SERGUS para deliberação e aprovação.

A gestão de risco é responsabilidade dos Conselheiros, Diretores e Empregados, por isso é importante: desenvolver cultura interna que enfatize e demonstre a importância da continuidade de negócios a todos os empregados, membros da Diretoria Executiva e colaboradores da Entidade.