POLÍTICA DE CONTINUIDADE DE TI

cbj.com.br

	Tipo: Política Corporativa	**Código:** P-POL-GTI- 002	
	Área: Gestão Adm. Financeira	**Data de Publicação:** 02/01/2021	
	Responsável: Renato Araújo	**Data de Vencimento:** 02/01/2023	
		Vigência: 2 anos	**V.:** 01
Título: POLÍTICA DE CONTINUIDADE DE TI			

Sumário

	Tipo: Política Corporativa	**Código:** P-POL-GTI- 002	
	Área: Gestão Adm. Financeira	**Data de Publicação:** 02/01/2021	
	Responsável: Renato Araújo	**Data de Vencimento:** 02/01/2023	
		Vigência: 2 anos	**V.:** 01
Título: POLÍTICA DE CONTINUIDADE DE TI			

APROVAÇÕES	
Gestor da Área: 30/11/2020	**Gestão Executiva:** 17/12/2020

CONTROLE DE REVISÕES				
Versão	**Descrição sucinta das alterações**	**Revisão**	**Aprovação**	**Data**
01	Emissão Inicial	Adm. Financeiro	Executivo	30/11/2020

1- Objetivos do plano

- Definir as regras aplicáveis com base na estrutura da CBJ
- Assegurar que todos conheçam o Plano de Continuidade de Negócio (PCN).

1.1- Processos Vitais embasados na ABNT NBR 1599:

- Gerenciamento de riscos, limites e concentração;
- Compliance e
- Comunicação.

1.2- Premissas e Objetivos do Projeto

O Plano de Continuidade de Negócios (PCN) assegurará ao **CBJ** a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos. *O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos*.

Os processos críticos a continuidade foram mapeados por meio de levantamento de informações com os Gestores das principais áreas de negócio.

Para tanto, o PCN é definido como (PCN = PAC + PCO + PRD), a saber:

- **PAC** = Programa de Administração da Crise – É acionado após decretada a Crise, e é voltado paratodo o processo. Tem seu término quando se volta à normalidade;

- **PCO** = Plano de Continuidade Operacional – São acionados os primeiros procedimentos do PAC,e é voltado aos processos de negócio;

- **PRD** = Plano de Recuperação de desastres – É acionado junto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PCN.

O desenvolvimento do Plano de Continuidade de Negócios (PCN) é baseado na avaliação dos processos críticosestabelecidos pelo Responsavel Tecnio do TI, compreendendo às suas principais etapas:

- Análise de riscos de TI;
- Análise de Impacto nos Negócios;
- Estratégia de recuperação.

Desta forma será necessário simular situações de emergências, definir responsabilidades e escopo de atuação para cada colaborador na execução do PCN.
A manutenção do PCN atualizado e o treinamento dos colaboradores são fatores crítico de sucesso.

Site Principal e Site de Redundância

A **CBJ** conta com duas unidades de recuperação de dados e sistema: a principal (Backup em nuvem e a de redundância Backup Fisico e Servidor Instantaneo disponiveis na rede).

A unidade principal (Servidor Principal) situa-se à em sala reservada com acesso restrito, aos colaboradores preparados e nomeados para tal atribuição, onde o gerenciamento de rede é executada em condições normais.

A unidade de redundância (Servidor/Nobreak) contém exatamente todos os mesmos recursos tecnológicos da Unidade Principal, podendo cada estação de trabalho utilizar tanto a Unidade Principal e ou secundária como o de Redundância. Portanto, em situações de contingência, os funcionários designados devemse dirigir para esse local (TI), conforme preceitua o provimento 74/2018 de forma que haja o mínimo impacto possível dentro das atividades da **SEDE ADMINISTRATIVA** .

SEDE Administrativa da CBJ

Localização	Rua Capitão Salomão, 40 – Humaitá – Rio de Janeiro - RJ
Contato	Leonardo Responsável pelo TI
Telefone	Tel.: 55 (27) 99244-7700
E-mail	

Em função do modo/ modelo de redundância atender os processos críticos em caso de contingência, segue abaixo adesignação dos colaboradores aptos para área de TI :

Área	Local de Contigência
Gestão	Servidor TI
Risco e Compliance	Servidor Externo
Distribuição	Home Office
Administrativo	Home Office
TI	Depende da situação

2- Plano de Monitoração

2.1- Definição de Desastre

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado no item CLASSE 1 – PRÉ-REQUISITOS – 30 MIN – Provimento 74/2018.

2.2- Monitoração de Comunicação de Eventos

Qualquer colaborador, ao constatar alguma anormalidade que paralise quaisquer processos apontados no item supra deste Plano deverá comunicar o fato ao seu responsavel técnico pelo TI, este por sua vez comunicará o fato ao Oficial Titular,e tentarão em conjunto solicionar o problema em tempo habil a saber:

Staff	Nome	Telefone	E-mail
Resposável pelo TI	Leonardo Rosário	55 (27) 99244-7700	

Este é o meio de comunicação a ser utilizado pelos colaboradores da **SEDE ADMINISTRATIVA** como ponto central de contato para solicitar ajuda ou relatar alguma situação que demande o acionamento do PCN.

3- Declaração de Contingência

3.1- Ações e procedimentos

Qualquer colaborador deverá estar apto a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao responsavel tecnico do Plano de Continuidade de Negócios e TI.

3.2- Impossibilidade de Acesso ao prédio

Dentre as ameaças que impossibilitam o acesso ao prédio destacamos:

- Princípio de Incêndio;
- Ameaça de Bomba;
- Bloqueios;

- Manifestações.

Ações de 05 a 10 minutos após a evidência

- Bombeiros: 193 (Incêndio e Ameaça de Bomba);
- Defesa Civil: 199 (Ameaça de Bomba, Greves, Bloqueios e Inundações);
- Polícia Civil: 147 (Ameaça de Bomba, Roubo e Furto de Informações e ativos).

Ações em até 20 minutos após a conclusão da etapa anterior

- Entrar em contato com o responsável pelo TI, conforme indicação supra, para avisá-lo sobre a ocupação dos integrantes das áreas contingenciadas e disponibilizar local, notebook e impressora, assim como acesso à Internet, bem como avisar os colaboradres que atuarão em regime Home Office.

3.3- Falha na Infraestrutura e Tecnologia

- Servidores
- Telecom
- Energia Elétrica

Na falta de energia elétrica, além das baterias próprias dos Notebooks, são ativados automaticamenteos nobreaks localizados no SERVIDOR principal no TI e nas respectivas estações com autonomia de 30 min.

As áreas abastecidas pelos Nobreaks são as mesmas mapeadas com processos críticos.

- Distribuição de redes
- Tecnologia da Informação
- BackOffice
- Administrativo/Financeiro
- Gestão de Riscos e Compliance

3.4- Acionamento da Contingência Externa

Manter contato com o gestor da empresa contratada para prestação de serviços de redundância / backup e contingência e avisar do início do processo de contingência.

As equipes irão dar continuidade aos Serviços em HomeOffice.

Manter contato com a empresa ***LBM INFO***. - Tel. (27) 99244-7700 e solicitar o encaminhamento de todas as ligações para os ramais dos Contribuintes em Teleatendimento "Home Office", se for o caso.

4- Procedimento de retorno à normalidade

Cabe ao Líder da Contingência encerrar o PCN e comunicar ao Juizo Diretor e aos Gestores envolvidos no processo.

Quando o acesso ao prédio estiver liberado e em condições de normalidade, comunicar a todos os colaboradores do Ofício por meio de seus gestores para que retornem aos seus postos de trabalho no dia seguinte.

Solicitar à área de TI que retire o comunicado publicado no site da Serventi sobre a situação de contingência.

5- Administração do plano

A continuidade de negócios de uma organização, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias.

O processo de Continuidade de Negócios é de responsabilidade e gestão da área Compliance, que determina o ciclo e as etapas que deverão ser executadas para que tanto os cenários de risco e impacto sobre os negócios como as estruturas e estratégias que embasam o PCN possam ser atualizadas refletindo o ambiente de negócios da SEDE ADMINISTRATIVA .

Para que a área de TI possa verificar o grau de atualização do PCN e decidir quanto ao momento em queo processo de continuidade de negócios será atualizado, os processos de planejamento de negócios e tecnológico, gerenciamento de mudanças, gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação desta área nas decisões relevantes destes processos.

6- Divulgação e treinamento

Um dos fatores primordiais para o funcionamento deste plano são o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a equipe da SEDE ADMINISTRATIVA definiu que serão realizadas anualmente sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios.
Estas sessões serão organizadas pela área de TI em conjunto com a área de Administrativa/Financeira com o objetivo de manter os colaboradores atualizados sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres e continuidade de negócios.

Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para funções críticas especificas, principalmente aqueles que pertencem à equipe de contingência, deverão ser instruídos das suas respectivas responsabilidades no plano.

O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias do PCN, incluindo as alterações recentes.

7- Realização de Testes

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenáriosa serem contemplados é da área de Tecnologia da Informação.

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela Ofical Titular, que dever ser arquivado por um período mínimo de 5 (cinco) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios da SEDE ADMINISTRATIVA e deverão ser conduzidos pela equipe de contingência em total conformidade com o definido. As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.

CBJ
BRASIL

cbj.com.br

PREPARADOS PARA VENCER

PATROCINADOR MASTER | PATROCINADOR OFICIAL | FORNECEDOR OFICIAL | APOIO | PARCEIROS DE MÍDIA

bradesco | cielo | MIZUNO | LEI DE INCENTIVO AO ESPORTE | PÁTRIA AMADA BRASIL | GLOBO | SPORTV