Instituto de Previdência dos Servidores do Distrito Federal

Plano de Continuidade de Negócio

Dezembro de 2018

1. Introdução

As atividades relacionadas aos negócios de uma instituição estão sujeitas a interrupções frequentes pelos mais diversos motivos, e se faz necessária à preparação para uma reação adequada frente a estas questões. Esta é parte integrante da governança coorporativa de TIC a qual se estrutura nos princípios e melhores práticas de gestão de serviços internos e externos.

O plano de continuidade de negócio é constituído por um conjunto de planos de ação visando fornecer uma base para a obtenção da confiança nos negócios da organização de forma consistente e reconhecida de acordo com sua capacidade de gestão de continuidade de negócio.

2. Objetivo e Benefícios

Seu objetivo é a formalização de estratégias capazes de realizar a recuperação, a continuidade e a retomada em momentos de crise, evitando que os processos críticos da instituição sejam afetados gerando impactos, resultando na resiliência organizacional.

Podem ser citados como benefícios de um plano de continuidade de negócio eficaz:

- Capacidade de identificar proativamente os impactos de uma interrupção operacional;
- Resposta eficiente às interrupções, resultando na minimização do impacto à organização;
- Manutenção da capacidade de gerenciar os riscos que não podem ser segurados;
- Incentivo do trabalho entre equipes;
- Capacidade de apresentar uma resposta possível por meio de um processo de testes; e
- Melhoria da reputação da instituição.

3. Metodologia

A metodologia utilizada para a construção do Plano de Continuidade se utilizou de materiais baseados na ABNT NBR 15999-1, a qual objetiva fornecer recomendações sobre as boas práticas de gestão da continuidade de negócios.

A base das recomendações é o ciclo de vida da continuidade de negócio, apresentado na figura 1:

Figura 1: Ciclo de vida da gestão da continuidade de negócios (ABNT 15999-1)

O ciclo de vida apresentado é dividido em 6 etapas.

3.1. Gestão do programa de GCN

A gestão do programa possibilita o estabelecimento e manutenção da capacidade de continuidade do negócio de forma apropriada, portanto a ativa participação da alta gestão é fundamental para que o programa de GCN seja devidamente introduzido, estabelecido e suportado como cultura da organização.

Sua gestão é separado em três etapas.

- Atribuição de Responsabilidades

O qual consiste em selecionar responsáveis pelo programa de GCN em cada unidade e sua respectiva responsabilidade no processo.

- Implementação da continuidade de negócio

Nessa etapa é realizada a divulgação do programa às partes interessadas, realização de treinamentos para a equipe e a realização de testes de continuidade.

A implantação de fato deverá se utilizar de método de gerenciamento de projetos já adotado pela organização.

- Gestão contínua

As seguintes atividades constituem essa etapa:

  - definir o escopo, papéis e responsabilidades de GCN;
  - nomear uma pessoa ou equipe apropriada para gerenciar a capacidade contínua de GCN;

- manter o programa de continuidade de negócios atual por meio das boas práticas;
- promover a continuidade de negócios por toda a organização de forma ampla, onde for apropriado;
- administrar o programa de testes;
- coordenar a análise crítica e atualização regular da capacidade de continuidade de negócios, incluindo analisar criticamente ou refazer avaliações de risco e análises de impacto no negócio (BIA);
- manter uma documentação apropriada ao tamanho e complexidade da organização;
- monitorar o desempenho da capacidade de continuidade de negócios;
- gerenciar os custos associados à capacidade de continuidade de negócios; e
- estabelecer e monitorar o gerenciamento de mudanças e o regime de sucessão da gestão.

3.2. Entendendo a organização

A compreensão da organização, identificando seus produtos e serviços fundamentais e atividades críticas e os respectivos recursos e que às suportam. Com isso é garantida a conformidade do Plano de Continuidade com os objetivos, obrigações e responsabilidades legais da organização.

É necessária a compreensão total da interdependência entre as atividades que a organização exerce, bem como relações externas com outras organizações. Mas para que isso seja feito deve-se:

- identificar os objetivos da organização, obrigações das partes interessadas, deveres legais e o ambiente no qual a organização opera;
- identificar as atividades, ativos e recursos, incluindo os externos, que dão suporte à entrega desses produtos e serviços;
- avaliar o impacto e as consequências sobre o tempo de falha destas atividades, ativos e recursos;
- categorizar suas atividades de acordo com suas prioridades de recuperação;
- identificar e avaliar as ameaças que possam interromper os produtos e serviços fundamentais e os ativos, atividades e recursos que os suportam.

Finalizada a compreensão interna da instituição, convém realizar a avaliação dos impactos quanto ao:

- bem-estar das pessoas;
- dano ou perda de instalações, tecnologias ou informação;
- não cumprimento de deveres ou regulamentações;
- danos à reputação;

- danos à viabilidade financeira;
- deterioração da qualidade de produtos ou serviços;
- danos ambientais.

Convêm que a organização estime os recursos necessários durante a recuperação de cada atividade, sendo ele de pessoas, dependências, tecnologia, informação e suprimento (serviços e fornecedores externos).

Nem todos os riscos podem ser identificados e mitigados, ou mesmo que sejam, a capacidade de se executar uma ação a frente dele pode ser limitada ou seu custo pode ser desproporcional ao beneficio em potencial.

Em sua análise deve ser cogitada a hipótese de aceitação desse risco, transferência do risco (contratação de seguro) ou até a mudança, suspensão ou término do serviço, produto, atividade, função ou processo relacionado.

3.3. Determinando a estratégia de continuidade de negócios

Essa etapa dá continuidade ao elemento “Entendendo a organização”, pois se utilizando do resultado da análise feita anteriormente é possível avaliar um conjunto de estratégias para que seja escolhida a resposta mais apropriada para cada produto ou serviço.

As estratégias escolhidas devem focar na resiliência e contramedidas já existentes na organização. Visando sua continuidade considerando um nível de operação aceitável e seu respectivo tempo.

Para cada recurso da organização deve ser traçado: período máximo de interrupção tolerável da atividade crítica; Custos de implementação das estratégias selecionadas; e Consequências de não se agir.

Os recursos da organização devem ter estratégias identificadas e apropriadas, conforme consolidado na tabela a seguir:

Recurso	As estratégias dos respectivos recursos podem incluir
Pessoas	• documentação do método de execução das atividades críticas; • treinamento multidisciplinar dos funcionários e prestadores de serviço; • separação das habilidades fundamentais, de modo a reduzir a concentração do risco (isso pode causar uma separação física dos funcionários com habilidades fundamentais ou garantir que mais de uma pessoa possua estas); • uso de terceiros; • planejamento de sucessão; e • retenção e gestão do conhecimento

Instalações	• instalações (ambientes) alternativas dentro da organização, incluindo a realocação de outras atividades; • ambientes alternativos fornecidos por outras organizações (por meio ou não de acordos recíprocos); • ambientes alternativos fornecidos por terceiros especializados; • trabalho a partir de casa ou de locais remotos; • outros locais que sejam acordados como apropriados; e • uso de força de trabalho alternativa em um local estabelecido.
Tecnologia	As estratégias de tecnologia dependem da natureza tecnológica utilizada. Podem incluir: • distribuição geográfica da tecnologia, ou seja, manter a tecnologia em locais diferentes que não serão afetados pela mesma interrupção de negócios; • armazenar o equipamento mais antigo como substituto em caso de emergências; e • mitigação de risco adicional para equipamento único ou para um prazo de entrega longo. Especificamente estratégias referentes aos serviços de TI: • tempo objetivado de recuperação (RTO) de sistemas e aplicativos que suportam as atividades fundamentais identificadas na BIA; • local e distância entre instalações tecnológicas; • quantidade de instalações tecnológicas; • acesso remoto; • uso de instalações vazias (sem equipe) em vez de instalações ocupadas; • conectividade de telecomunicações e roteamento redundante; • natureza do “fail over ” (se é necessária intervenção manual para ativar os recursos alternativos de TI ou se isso deve ocorrer automaticamente); e • conectividade com terceiros e links externos.
Informação	Toda e qualquer informação de forma física (impresso) ou virtual (eletrônica) que está diretamente ligada à realização de atividades críticas na organização deve possuir um nível adequado de: • confidencialidade; • integridade; • disponibilidade; e • atualização.
Suprimentos	• aumento do número de fornecedores; • recomendação ou exigência de que os fornecedores

	tenham uma capacidade de continuidade de negócios • validada; • obrigações contratuais e/ou acordos de nível de serviços com os principais fornecedores; ou • a identificação de fornecedores alternativos que sejam capazes de atender à demanda.

3.4. Desenvolvendo e implementando uma resposta de GCN

Esta etapa é relacionada diretamente com o desenvolvimento e implantação dos preparativos realizados anteriormente para que na existência de qualquer incidente se tenha uma estrutura mínima que permita a organização:

- confirme a natureza e extensão do incidente,
- tome controle da situação,
- controle o incidente, e
- comunique-se com as partes interessadas.

Passando assim por todas as fases temporais após a ocorrência de um incidente, conforme apresentado na figura a seguir:

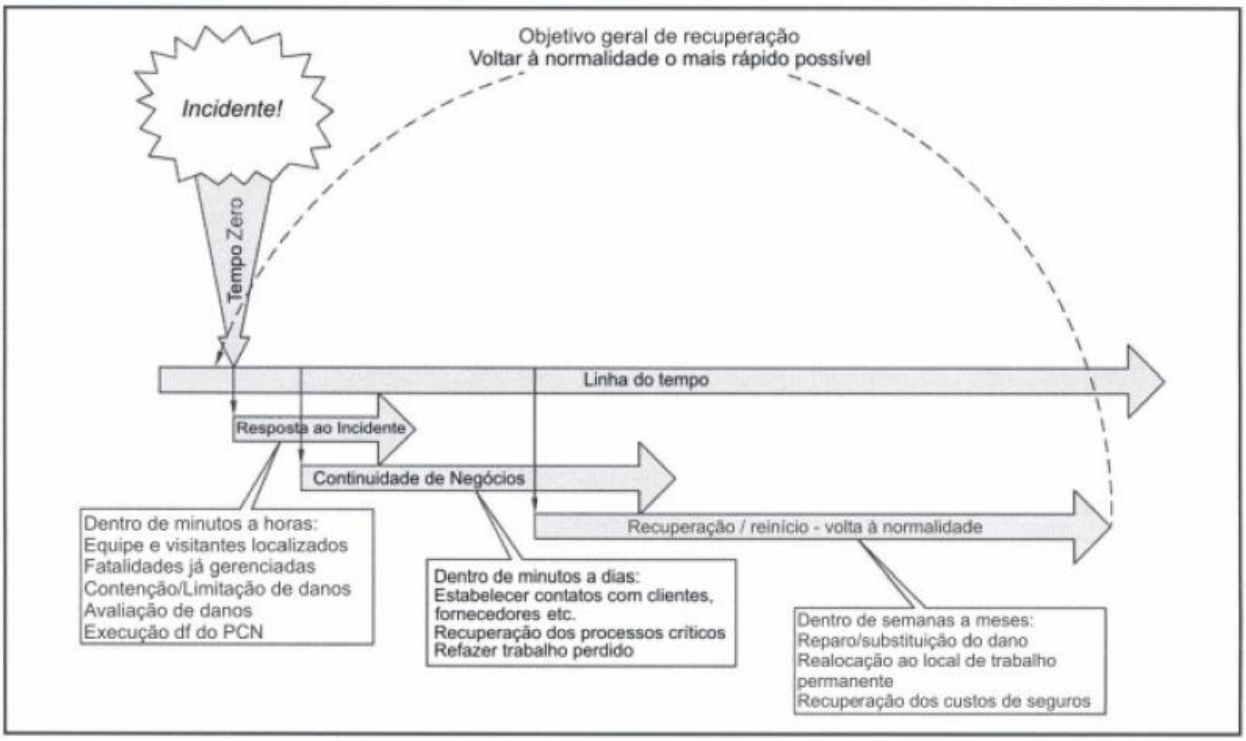

Figura 2: Principais fases de tempo de um incidente e a relação entre o gerenciamento do incidente (ABNT 15999-1)

Tendo em vista a dificuldade de definição clara do que seria a normalidade após um incidente, a estratégia aplicada deve garantir uma operabilidade estendida, de forma a assegurar a recuperação do serviço, produto ou processo.

O processo de ativação do plano de continuidade, o conjunto de critérios que os indivíduos colocam em prática e suas respectivas circunstâncias devem estar claramente documentadas.

Parte das orientações devem estar disponíveis no Plano de Gerenciamento de incidentes (PGI), documento que deve ser flexível, viável e relevante, de fácil compreensão além de fornecer a base para se administrar todos os possíveis problemas, incluindo aqueles com partes interessadas e externos, que podem ser enfrentados pela organização durante um incidente.

Nessa etapa também é elaborado ou revisado e implementado o Plano de Continuidade de Negócio, o qual já foi descrito anteriormente. No que se refere ao mantimento dos documentos, é necessário a seleção de responsável, aplicação de um sistema de controle de versões e ampla disponibilização da versão mais atualizada.

3.5. Testando, mantendo e analisando criticamente os preparativos de GCN

Nessa etapa são realizados os testes e as análises críticas dos planos anteriormente implantados. A realização de testes é de suma importância para o desenvolvimento do trabalho em equipe, da competência, da confiança e do conhecimento, fatores vitais na ocorrência de um incidente.

Convém que os testes possam adiantar um resultado previsto que tenha sido antecipadamente planejado e incluído no escopo além de permitir a utilização da inovação na organização.

O objetivo principal da realização de testes é a busca pela melhor garantia de que o Plano de Continuidade de Negócio funcione conforme o previsto quando necessário, portanto devem:

- Testar os aspectos técnicos, logísticos, administrativos, de procedimento e outros sistemas em operação do PCN;
- Testar os preparativos e a infraestrutura de GCN, incluindo papéis, responsabilidades e quaisquer locais de gerenciamento de incidentes e áreas de trabalho, entre outros; e
- Validar a recuperação da tecnologia e das telecomunicações, incluindo a disponibilidade e remanejamento de pessoal.

Entre as vantagens das melhorias da capacidade de Gerencia de Continuidade de Negocio pode-se elencar:

- Exercitar a capacidade da organização de se recuperar de um incidente;

- Verificar se todas as atividades críticas da organização, suas dependências e prioridades estão contempladas pelo PCN;
- Realçar premissas que devam ser questionadas;
- Gerar confiança nos participantes envolvidos no teste;
- Aumentar a consciência do processo de continuidade de negócios pela organização por meio da publicação do teste;
- Validar a funcionalidade e tempestividade do processo de restauração das atividades críticas; e
- Demonstrar a competência das equipes titulares de resposta a incidentes e de seus substitutos.

Vale a pena ressaltar que todos os testes devem ser realistas, cuidadosamente planejados, alinhados com as partes interessadas. Seus objetivos, escalas e complexidades devem estar claramente definidos, gerando relatórios e análises pós-teste. Conforme apresentado na tabela a seguir:

Tabela 1: Tipos e métodos de teste de estratégias de GCN (adaptação da ABNT 15999-1)

Complexidade	Teste	Processo	Variações	Frequência recomendada
Simples	Teste de mesa	Análise crítica/correção	Atualização/Auditoria /Verificação	Anualmente
	Repassar os passos do plano	Questionar conteúdo do PCN	Incluir interação e validar papeis	Anualmente
Médio	Simulação	Utilizar situação hipotética para validar se o plano possui todas as informações necessárias	Incorporação de planos associados	De 1 à 2 vezes ao ano
	Testar atividades críticas	Execução em ambiente controlado	Execução de operações selecionadas a partir de um local alternativo	Minimamente anualmente
Complexo	Testar todo o PCN e o PGI	Teste envolvendo toda zona	-	Anualmente

A manutenção da GCN se consiste na análise crítica questionando quaisquer premissas adotadas para qualquer componente do gerenciamento. Bem como sua ampla divulgação atualizada, corrigida ou alterada.

A análise pode ser realiza por auditorias internas ou externas, ou até mesmo através de autoavaliação, com o foco na verificação dos pontos listados a seguir:

- Todos os produtos e serviços fundamentais e as atividades e recursos críticos que o suportam foram identificados e incluídos na estratégia de GCN da organização;
- A política de GCN da organização, suas estratégias, estrutura e planos refletem precisamente suas prioridades e requisitos (os objetivos da organização);

- A competência de GCN da organização e sua capacidade são eficazes e adequados e vão permitir o gerenciamento, comando, controle e coordenação de um incidente;
- As soluções de GCN da organização são efetivas, atualizadas e adequadas, além de apropriadas ao nível de risco enfrentado pela organização;
- Os programas de manutenção e testes de GCN da organização foram efetivamente implementados;
- As estratégias e planos de GCN incorporam as melhorias identificadas durante os incidentes e testes e no programa de manutenção;
- A organização tem um programa contínuo de treinamento e conscientização de GCN;
- Os procedimentos de GCN foram efetivamente comunicados à equipe relevante e se esta equipe entende seus papéis e responsabilidades;
- Os processos de controle de alterações estão implementados e funcionam de forma eficaz.

Um processo de autoavaliação de GCN tem um papel importante para garantir que a organização tem competência e capacidade sólidas, eficazes e adequadas. Esse processo verifica qualitativamente a capacidade da organização de se recuperar de um incidente. Convém que seja realizada uma autoavaliação que verifique os objetivos da organização e também leve em conta as normas pertinentes e as boas práticas.

3.6. Incluindo a GCN na cultura da organização

Todo o processo de Gestão da Continuidade de Negócio só se tornará efetiva caso se torne parte efetiva da gestão da organização de forma transversal, atingindo sua totalidade independente do tamanho e setor.

Podem ser apontados como características de instituições que tem uma cultura positiva de GCN:

- Capacidade de desenvolver um programa de GCN com mais eficiência;
- Passar confiança às partes interessadas (especialmente funcionários e clientes) quanto à sua habilidade de gerenciar interrupções de negócios;

Aumentar sua resiliência ao longo do tempo ao garantir que as implicações da GCN são consideradas em todos os níveis de decisão; e

- Minimizar a probabilidade e o impacto das interrupções.

O desenvolvimento de uma cultura de GCN é suportado por:

- Liderança dos níveis superiores da organização;
- Atribuição de responsabilidades;
- Conscientização;
- Desenvolvimento de habilidades; e
- Planos de testes.

A contínua educação e consciência coletiva devem permanecer na instituição mesmo depois da finalização de implantação e testes. Mantendo consultas periódicas junto a toda a equipe, discussão sobre o assunto e o aprendizado e compartilhamento de experiências de incidentes.

Cabe a equipe de GCN as tarefas de gestão do programa, execução de análise de impacto nos negócios, desenvolvimento, implementação, teste e avaliação de riscos e ameaças dos planos de continuidade, além de uma constante comunicação com a mídia.