NORMA
BRASILEIRA

ABNT NBR 15999-1

Primeira edição
22.10.2007

Válida a partir de
22.11.2007

Versão corrigida
01.02.2008

Gestão de continuidade de negócios
Parte 1: Código de prática

Business continuity management
Part 1: Code of practice

Palavras-chave: Gestão. Continuidade de negócios.
Descriptors: Management. Business continuity.

ICS 03.100.01

ISBN 978-85-07-00750-0

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR 15999-1:2007
40 páginas

Sede da ABNT
Av.Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 2220-1762
abnt@abnt.org.br
www.abnt.org.br

Impresso no Brasil

Sumário

Página

Prefácio

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais Temporárias (ABNT/CEET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras da Diretivas ABNT, Parte 2.

A Associação Brasileira de Normas Técnicas (ABNT) chama atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direito de patente. A ABNT não deve ser considerada responsável pela identificação de quaisquer direitos de patentes.

A ABNT NBR 15999-1 foi elaborada pela Comissão de Estudo Especial Temporária de Gestão de Riscos (ABNT/CEET-00:001.63). O Projeto circulou em Consulta Nacional conforme Edital nº 06, de 22.05.2007 a 21.06.2007, com o número de Projeto 00:001.63-002/01.

A ABNT NBR 15999-1, sob o título geral "*Gestão de continuidade de negócios – Parte 1: Código de prática*", tem previsão de conter as seguintes partes:

— Parte 1: Código de prática;

— Parte 2: Requisitos.

Esta Norma é baseada na BSI 25999:2006.

Esta versão corrigida da ABNT NBR 15999-1:2007 incorpora a Errata 1 de 01.02.2008.

0 Introdução

Esta Norma foi desenvolvida por especialistas da comunidade de continuidade de negócios, tendo como base suas experiências acadêmicas, técnicas e práticas da gestão da continuidade de negócios (GCN). Foi elaborada para fornecer um sistema baseado nas boas práticas de gestão da continuidade de negócios. Seu propósito é servir como um único ponto de referência para a maior parte das situações em que a gestão da continuidade de negócios é praticada e ser usada por organizações de grande, médio e pequeno portes, nos setores industriais, comerciais, públicos e de caráter voluntário.

0.1 Uso deste documento

Como um código de práticas, esta Norma tem a forma de um guia que possui recomendações. Não deve ser citada como uma especificação e convém que alegações de conformidade não sejam enganosas.

Qualquer usuário que afirme estar em conformidade com esta Norma deve ser capaz de justificar qualquer ação que se desvie de suas recomendações.

0.2 Convenções de apresentação

Esta Norma fornece recomendações expressas em frases em que a principal é a expressão **"convém que"**. A Seção 3 não contém quaisquer recomendações, mas fornece informações de suporte úteis sobre a gestão da continuidade de negócios (apesar de esta Norma não ter a intenção de ser um guia da gestão da continuidade de negócios para principiantes).

A palavra "pode" é utilizada no texto para exprimir permissão, ou seja, como uma alternativa à recomendação principal da seção. A palavra "pode" é usada também para expressar possibilidade, ou seja, a conseqüência de uma ação ou evento.

Comentários adicionais, explicações e material informativo em geral aparecem em fonte menor e em itálico, e não constituem elementos normativos.

0.3 Considerações legais e contratuais

Esta Norma não busca incluir todas as condições necessárias de um contrato. Os usuários são responsáveis por sua correta aplicação.

Gestão de continuidade de negócios
Parte 1: Código de prática

1 Escopo

Esta Norma estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN). O propósito desta Norma é fornecer uma base para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização além de obter confiança nos negócios da organização com clientes e outras organizações. Ela permite também que a organização avalie sua capacidade de GCN de uma maneira consistente e reconhecida.

Esta Norma fornece um sistema baseado nas boas práticas de GCN.

Esta Norma foi desenvolvida para ser usada por qualquer pessoa que seja responsável pelas operações de negócios e serviços, desde a alta direção, passando por todos os níveis da organização; por organizações com uma única sede e por empresas globais; por pequenas e médias empresas até organizações que empregam milhares de pessoas. Logo, é aplicável a qualquer pessoa responsável por alguma operação e, conseqüentemente, pela continuidade desta operação.

Esta Norma não cobre as atividades relacionadas ao planejamento de emergência, pois esse tópico está relacionado a emergências civis.

NOTA Independentemente dos esforços ou recursos investidos na gestão da continuidade de negócios, ainda é possível que uma organização tenha que se defrontar com um incidente ou uma combinação de incidentes que não foi prevista.

2 Termos e definições

Para os efeitos desta Norma, aplicam-se os seguintes termos e definições.

2.1
alta direção

pessoa ou grupo de pessoas que dirige e controla uma organização em seu nível mais alto

[ABNT NBR ISO 9000:2005]

NOTA A alta direção, especialmente em uma grande multinacional, pode não estar diretamente envolvida; porém, ela sempre possui responsabilidade por meio da cadeia de comando. Em uma organização pequena, a alta direção pode ser unicamente o dono ou proprietário.

2.2
análise de custo-benefício

técnica financeira que mede o custo de implementação de uma solução específica e o compara com o benefício que ela proporciona

NOTA O benefício pode ser definido em termos financeiros, de reputação, entrega de serviços, regulamentações ou outros termos que sejam apropriados à organização.

2.3
análise de impacto nos negócios (*BIA – business impact analysis*)
processo de analisar as funções de negócio e os efeitos que uma interrupção possa causar nelas

2.4
apetite a risco
quantidade total de risco que uma organização está preparada para aceitar, tolerar ou ser exposta a qualquer tempo

2.5
atividade
processo ou conjunto de processos executados por uma organização (ou em seu nome) que produzem ou suportem um ou mais produtos ou serviços

NOTA Exemplos desses processos incluem contas, "call centers", TI, manufatura, distribuição, entre outros.

2.6
atividades críticas
atividades que devem ser executadas de forma a entregar os produtos e serviços fundamentais da organização que a permitam atingir seus objetivos mais importantes e sensíveis ao tempo

2.7
avaliação de riscos
processo geral de identificação, análise e estimativa dos riscos

2.8
ciclo de vida da gestão da continuidade de negócios
série de atividades que, coletivamente, abordam todos os aspectos e fases do programa de gestão da continuidade de negócios

NOTA O ciclo de vida da gestão da continuidade de negócios está ilustrado na Figura 1.

2.9
conseqüência
resultado de um incidente que pode ter um impacto nos objetivos da organização

NOTA 1 Podem existir várias conseqüências a partir de um único incidente.

NOTA 2 Uma conseqüência pode ser certa ou incerta e pode causar impactos positivos ou negativos aos objetivos.

2.10
continuidade de negócios
capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções de negócios, para conseguir continuar suas operações em um nível aceitável previamente definido

2.11
declaração
ato de declarar que o plano de continuidade de negócios de uma organização precisa ser colocado em prática, de forma a continuar o fornecimento dos produtos ou serviços fundamentais.

2.12
emergência civil
evento ou situação que pode causar danos sérios ao bem-estar humano em um local, em um ambiente, ou à segurança do país ou de um local específico

2.13
estratégia de continuidade de negócios
abordagem de uma organização que garante a sua recuperação e continuidade, ao se defrontar com um desastre, outro incidente maior ou interrupção de negócios

2.14
ganho
conseqüência positiva

2.15
gestão da continuidade de negócios (GCN)
processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado

NOTA A gestão da continuidade de negócios envolve o gerenciamento da recuperação ou da continuidade das atividades no caso de uma interrupção de negócios e o gerenciamento do programa de continuidade por meio de treinamentos, testes e análises críticas, de forma a garantir que os planos de continuidade de negócios estejam sempre atualizados.

2.16
gestão de riscos
desenvolvimento estruturado e aplicação de uma cultura de gestão, políticas, procedimentos e práticas às tarefas de identificação, análise e controle dos riscos

2.17
impacto
conseqüência avaliada de um evento em particular

2.18
incidente
situação que pode representar ou levar a uma interrupção de negócios, perdas, emergências ou crises

2.19
interrupção
evento, seja previsto (por exemplo, uma greve ou furacão) ou não (por exemplo, um blecaute ou terremoto), que cause um desvio negativo imprevisto na entrega e execução de produtos ou serviços da organização, de acordo com seus objetivos

2.20
organização

grupo de pessoas e instalações com uma série de responsabilidades, autoridades e relacionamentos

EXEMPLO: Companhia, corporação, firma, empresa, instituição de caridade, profissional liberal ou associação, ou partes ou combinações destas.

NOTA 1 Esse grupo é geralmente bem ordenado.

NOTA 2 Uma organização pode ser pública ou privada. [NBR ISO 9000:2005].

2.21
partes interessadas
aqueles que possuem algum interesse nos resultados de uma organização

NOTA Este é um termo abrangente que inclui, entre outros, empregados internos e terceirizados, clientes, fornecedores, parceiros, empregados, distribuidores, investidores, seguradoras, acionistas, donos, o governo e os reguladores.

2.22
perda
conseqüência negativa

2.23
período máximo de interrupção tolerável
duração a partir da qual a viabilidade de uma organização será ameaçada de forma inevitável, caso a entrega de produtos e serviços não possa ser reiniciada

2.24
planejamento de emergência
desenvolvimento e manutenção de procedimentos acordados de forma a prevenir, reduzir, controlar, mitigar e escolher ações a serem tomadas no caso de uma emergência civil

2.25
plano de continuidade de negócios (PCN)
documentação de procedimentos e informações desenvolvida, consolidada e mantida de forma que esteja pronta para uso caso ocorra um incidente, de forma a permitir que a organização mantenha suas atividades críticas em um nível aceitável previamente definido

2.26
plano de gerenciamento de incidentes
plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes

2.27
probabilidade
possibilidade de algo acontecer que seja determinada, medida ou estimada, objetiva ou subjetivamente, em termos gerais (tais como raro, pouco provável, provável, quase certo etc.), freqüências ou probabilidades matemáticas

NOTA A probabilidade pode ser expressa qualitativa ou quantitativamente.

2.28
produtos e serviços
resultados benéficos que uma organização fornece a seus clientes e partes interessadas, como produtos manufaturados, seguros automobilísticos, conformidade com regulamentações e benefícios comunitários

2.29
programa de gestão da continuidade de negócios
processos contínuos de gestão e governança que são suportados pela alta direção e que recebem os recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por meio de treinamentos, testes, manutenção e análises críticas

2.30
resiliência
capacidade de uma organização de resistir aos efeitos de um incidente

2.31
risco
algo que pode ocorrer e seus efeitos nos objetivos da organização

NOTA 1 A palavra "risco" e suas ramificações são usadas coloquialmente de várias formas, como um substantivo ("um risco" ou, no plural, "riscos"), um verbo (arriscar [algo], ou colocar em risco), ou como um adjetivo ("arriscado"). O termo "um risco" pode se relacionar a um evento em potencial, suas causas, a chance de algo acontecer ou os efeitos desses eventos. Na gestão de riscos (ver 6.5), é importante ter uma distinção clara entre esses usos da palavra "risco".

NOTA 2 Risco é definido em relação a um objetivo em particular; assim sendo, a preocupação com vários objetivos implica a possibilidade de mais de uma medida de risco ter que ser usada para cada fonte de risco.

NOTA 3 O risco é geralmente quantificado como uma média de seus efeitos, por meio da soma do efeito de todas as conseqüências possíveis ponderada pela probabilidade associada a cada conseqüência, de forma a obter um "valor esperado". Porém, é preciso que existam distribuições probabilísticas de forma a quantificar o que se percebe quanto à variação de conseqüências possíveis. Alternativamente, estatísticas, tais como o desvio-padrão, podem ser usadas além do valor esperado.

2.32
tempo objetivado de recuperação (*RTO – recovery time objective*)
tempo alvo para:

— retomada da entrega de produtos ou serviços após um incidente; ou

— recuperação do desempenho de uma atividade após um incidente; ou

— recuperação de um sistema ou aplicação de TI após um incidente.

NOTA O tempo objetivado de recuperação deve ser menor que o período máximo de interrupção tolerável.

2.33
teste
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

NOTA 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.

3 Visão geral da gestão da continuidade de negócios (GCN)

3.1 O que é a GCN?

A gestão da continuidade de negócios (GCN) é um processo da organização que estabelece uma estrutura estratégica e operacional adequada para:

— melhorar proativamente a resiliência da organização contra possíveis interrupções de sua capacidade em atingir seus principais objetivos;

— prover uma prática para restabelecer a capacidade de uma organização fornecer seus principais produtos e serviços, em um nível previamente acordado, dentro de um tempo previamente determinado após uma interrupção; e

— obter reconhecida capacidade de gerenciar uma interrupção no negócio, de forma a proteger a marca e reputação da organização.

Ainda que os processos de continuidade de negócios sejam diferentes de acordo com o tamanho, a estrutura e as responsabilidades da organização, os princípios básicos não se alteram, sejam as organizações públicas, privadas ou instituições de caridade, independentemente de seu tamanho, escopo ou complexidade.

3.2 GCN e a estratégia organizacional

Todas as organizações, sejam elas grandes ou pequenas, possuem metas e objetivos, tais como crescer, fornecer serviços e adquirir outros negócios. Estas metas e objetivos geralmente são atingidos por meio de planos estratégicos que permitem atingi-los a curto, médio ou longo prazo. O entendimento da GCN no nível mais alto da organização ajuda a garantir que estas metas e objetivos não serão comprometidos por interrupções inesperadas.

As conseqüências de um incidente variam e podem ser abrangentes. Estas conseqüências podem envolver perda de vidas, ativos e renda, ou a incapacidade de entregar os produtos e serviços dos quais a estratégia, a reputação ou até mesmo a sobrevivência da organização dependem.

A GCN precisa reconhecer a importância estratégica das partes interessadas conhecidas. Além disso, de acordo com o desenrolar das conseqüências de uma interrupção, aparecem novas partes interessadas que podem ter um impacto na extensão total dos danos. Por exemplo, grupos específicos podem tentar pressionar a organização que enfrenta uma interrupção.

Todos esses assuntos são estrategicamente importantes para a organização.

3.3 GCN – relação com a gestão de riscos

A GCN é complementar a uma estrutura de gestão de riscos que busca entender os riscos às operações e negócios e suas conseqüências.

A gestão de riscos visa administrar o risco relacionado aos produtos e serviços fundamentais que uma organização fornece. A entrega desses produtos e serviços pode ser interrompida por uma grande variedade de incidentes, e muitos dos quais são de difícil previsão ou análise das causas.

Com foco no impacto da interrupção, a GCN identifica os produtos e serviços dos quais a organização depende para sobreviver e é capaz de identificar o que é necessário para que a organização continue cumprindo suas obrigações. Por meio da GCN, uma organização pode reconhecer o que precisa ser realizado antes da ocorrência de um incidente, de forma a proteger suas pessoas, instalações, tecnologia, informações, cadeia de fornecimento, partes interessadas e reputação. Reconhecendo isso, a organização pode então ter uma visão realista das respostas necessárias quando e se ocorrer uma interrupção, de modo que ela pode ter confiança de que conseguirá administrar eventuais conseqüências sem atrasos inaceitáveis na entrega de seus produtos e serviços.

Uma organização que tenha tomado as medidas apropriadas de GCN pode ser capaz de aproveitar oportunidades de alto risco.

3.4 Por que convém que uma organização adote a GCN?

A GCN é um elemento importante da boa gestão de negócios, fornecimento de serviços e prudência empresarial.

Os gestores e proprietários têm a responsabilidade de manter a capacidade de funcionamento sem interrupção da organização. As organizações constantemente assumem compromissos ou têm o dever de entregar produtos e serviços, ou seja, assinam contratos e criam expectativas. Todas as organizações têm responsabilidades morais e sociais, particularmente em casos onde elas fornecem uma resposta de emergência ou um serviço público ou voluntário. Em alguns casos, as organizações têm obrigações legais ou regulamentares de efetuar uma GCN.

Toda atividade de negócios está sujeita a interrupções, tais como falhas tecnológicas, enchentes, interrupções nos serviços públicos e atos de terrorismo. A GCN fornece a capacidade de reagir adequadamente às interrupções operacionais enquanto protege o bem-estar e a segurança.

A GCN deve ser encarada não como um processo custoso de planejamento, mas como um processo que agrega valor à organização.

3.5 Benefícios de um programa eficaz de GCN

Os benefícios de um programa eficaz de GCN são que a organização:

— é capaz de identificar proativamente os impactos de uma interrupção operacional;

— tem uma resposta eficiente às interrupções, o que minimiza o impacto à organização;

— mantém uma capacidade de gerenciar os riscos que não podem ser segurados;

— promove o trabalho entre equipes;

— é capaz de demonstrar uma resposta possível por meio de um processo de testes;

— pode melhorar sua reputação; e

— pode ganhar uma vantagem competitiva por meio da capacidade demonstrada de manter a entrega de seus produtos e serviços.

3.6 Resultados de um programa eficaz de GCN

Os resultados de um programa eficaz de GCN são que:

— os principais produtos e serviços são identificados e protegidos, de forma a garantir sua continuidade;

— a organização desenvolve uma capacidade de gerenciamento de incidentes, de forma a fornecer uma resposta efetiva;

— a organização passa a entender a si mesma e a seus relacionamentos com outras organizações, agências reguladoras pertinentes ou departamentos governamentais, autoridades locais e serviços de emergência, desenvolvendo e documentando esse entendimento;

— a equipe é treinada de forma a responder de forma eficaz a um incidente ou interrupção por meio de testes apropriados;

— as necessidades das partes interessadas são entendidas e podem ser cumpridas;

— a equipe recebe o suporte e as comunicações necessárias em caso de interrupção;

— a cadeia de suprimentos da organização é assegurada;

— protege-se a reputação da organização; e

— a organização permanece em conformidade com suas obrigações legais e regulamentações aplicáveis.

3.7 Elementos do ciclo de vida da gestão da continuidade de negócios

O ciclo de vida de GCN é composto por seis elementos, que podem ser visualizados na Figura 1. Estes podem ser implementados em organizações de todos os tamanhos, em todos os setores: público, privado, sem fins lucrativos, educacional, manufatura etc. O escopo e a estrutura do programa de GCN podem variar e o esforço gasto será adaptado às necessidades de cada organização, mas esses elementos fundamentais serão sempre obrigatórios.

a) Gestão do programa de GCN (ver Seção 5)

A gestão do programa possibilita que a capacidade de continuidade de negócios seja estabelecida (se necessário) e mantida de forma apropriada ao tamanho e complexidade da organização;

b) Entendendo a organização (ver Seção 6)

As atividades associadas a esta seção fornecem informações que permitem a priorização dos produtos e serviços da organização e a urgência das atividades que são necessárias para fornecê-los. Isso estabelece os requisitos que irão definir a seleção das estratégias de GCN apropriadas;

Figura 1 — Ciclo de vida da gestão da continuidade de negócios

c) Determinando a estratégia de continuidade de negócios (ver Seção 7)

A definição da estratégia de continuidade de negócios permite que uma série de estratégias seja avaliada. Isso permite que uma resposta apropriada seja escolhida para cada produto ou serviço, de modo que a organização possa continuar fornecendo esses produtos e serviços:

— em um nível de operações aceitável, e

— em uma quantidade de tempo aceitável

durante e logo após uma interrupção. As escolhas feitas devem levar em conta a resiliência e as opções de contramedidas já presentes na organização;

d) Desenvolvendo eimplementando umaresposta deGCN (ver Seção 8)

O desenvolvimento e a implementação de uma resposta de GCN resultam na criação de uma estrutura de gestão e numa estrutura de gerenciamento de incidentes, continuidade de negócios e planos de recuperação de negócios que detalhem os passos a serem tomados durante e após um incidente, para manter ou restaurar as operações.

COMENTÁRIOS DE 3.7-d):

O termo "incidente" é usado nesta Norma de forma a refletir a escalabilidade 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, ele pode não resultar em uma crise. Porém, alguns eventos podem causar uma interrupção tão profunda aos objetivos da organização, a ponto de serem considerados 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 sigam o plano existente à risca, independentemente da situação, mas o adaptem às circunstâncias atuais. Um plano de continuidade de negócios nunca irá substituir a tomada de decisões competente e bem informada por parte da direção.

e) Testando, mantendoe analisando criticamente ospreparativos deGCN (ver Seção 9)

Testar, manter, analisar criticamente e auditar o GCN faz com que a organização seja capaz de:

— demonstrar aque pontosuas estratégias eplanos estãocompletos, atualizados eprecisos; e

— identificar oportunidades de melhoria.

f) Incluindo aGCN na cultura da organização (ver Seção 10)

A inclusão da GCN na cultura da organização permite que ela se torne parte dos valores da organização, dando confiança às partes interessadas quanto à capacidade da organização de sobreviver a interrupções.

4 A política de gestão da continuidade de negócios

4.1 Visão geral

4.1.1 A política de GCN define os seguintes processos:

— as atividades depreparação parase estabelecer umacapacidade decontinuidade de negócios;e

— o gerenciamento contínuo emanutenção destacapacidade decontinuidade denegócios.

4.1.2 As atividades de preparação incluem a especificação, planejamento completo, criação, implementação e testes iniciais da capacidade de continuidade de negócios.

4.1.3 As atividades de manutenção e gerenciamento permanentes são, por exemplo, a inclusão da continuidade de negócios na organização, o teste regular dos planos, sua atualização e comunicação, especialmente quando houver mudanças significativas nas instalações, pessoas, mercados, tecnologia ou estrutura organizacional.

COMENTÁRIOS DE 4.1

Os propósitos de se estabelecer uma política de continuidade de negócios são:

— *garantir que todas as atividades de GCN sejam conduzidas e implementadas de modo controlado e conforme o combinado;*

— *alcançar uma capacidade de continuidade de negócios que vá ao encontro das necessidades do negócio e que seja apropriada ao tamanho, complexidade e natureza da organização; e*

— *implementar uma estrutura claramente definida para a capacidade contínua de GCN.*

4.2 Contexto

Convém que a organização garanta que sua política de GCN é apropriada à natureza, escala, complexidade, geografia e criticidade de suas atividades de negócio e que ela reflete sua cultura, dependências e ambiente operacional. A política de GCN define os processos necessários para garantir que os preparativos de continuidade de negócios continuem a atender às necessidades da organização caso ocorra um incidente. Convém que essa política garanta que a capacidade de continuidade de negócios é promovida na cultura da organização. Convém que a capacidade de GCN seja integrada à atividade de gerenciamento de mudanças da organização de modo que seja incorporada ao crescimento e desenvolvimento dos produtos e serviços da organização.

4.3 Desenvolvimento da política de continuidade de negócios

Convém que a organização desenvolva sua política de continuidade de negócios que descreva os objetivos da GCN na organização. Inicialmente, isso pode ser uma declaração de alto nível, que é então refinada e melhorada de acordo com o desenvolvimento da capacidade da organização.

Convém que a política de continuidade de negócios forneça princípios documentados aos quais ela irá buscar e contra os quais a capacidade de continuidade de negócios da organização deverá ser medida. Convém que o responsável pela política de GCN possua um cargo de alto nível, como um diretor do conselho executivo ou um representante eleito.

A organização deve considerar o seguinte enquanto desenvolve sua política de GCN:

— definição do escopo do GCN dentro da organização;

— alocação de recursos para GCN;

— definição dos princípios, guias e políticas que precisam ser incluídos ou podem ser utilizados como referência;

— referência a normas pertinentes, regulamentos ou políticas que tenham que ser incluídos ou possam ser usados como referência.

Convém que a organização mantenha e regularmente realize análise crítica da sua política de GCN, suas estratégias, planos e soluções de acordo com suas necessidades.

Convém que o escopo da política de GCN defina claramente quaisquer limitações ou exclusões que possam ser aplicáveis, como, por exemplo, exclusões geográficas ou de produto.

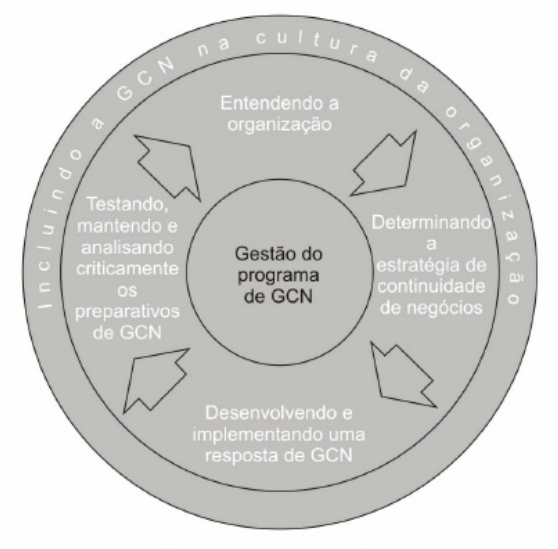
4.4 Escopo do programa de GCN

A alta direção deve definir o escopo do programa de GCN por meio da identificação dos produtos e serviços fundamentais que suportam os objetivos, obrigações e deveres estatutários da organização. Convém que a definição do que é fundamental seja consistente com a análise de impacto nos negócios descrita em 6.2, mas com considerações de um nível mais alto.

4.5 Atividades terceirizadas

Se um produto, serviço ou atividade for terceirizado, o risco deste continua vinculado à organização. Conseqüentemente, convém que a organização garanta que seus principais fornecedores ou parceiros de terceirização possuem planos de GCN eficazes. Um método de fazer isso é obter evidência auditada que demonstre a viabilidade dos planos de continuidade dos fornecedores e de seus programas de teste e manutenção.

5 Gestão do programa de GCN



A gestão do programa está no cerne do processo de GCN. Uma gestão do programa eficiente estabelece a abordagem da organização à continuidade de negócios.

A participação da alta direção é fundamental para garantir que o processo de GCN seja corretamente introduzido, suportado e estabelecido como parte da cultura da organização.

5.1 Visão geral

Convém que um programa de GCN seja colocado em prática para alcançar os objetivos definidos na política de continuidade de negócios (ver 4.3). A gestão do programa de GCN envolve três passos:

— atribuição de responsabilidades (ver 5.2);

— implementação da continuidade de negócios na organização (ver 5.3); e

— a gestão contínua da continuidade de negócios (ver 5.4).

5.2 Designando responsabilidades (governança)

5.2.1 Convém que a direção da organização:

— aponte ou nomeie uma pessoa com a senioridade e autoridade apropriadas para ser responsável pela política de GCN e sua implementação;

— aponte ou nomeie um ou mais indivíduos para implementar ou manter o programa de GCN.

COMENTÁRIOS DE 5.2.1

As pessoas que recebem a tarefa de implementar e manter o programa de continuidade de negócios podem ser de várias áreas de uma organização, dependendo de seu tamanho, escala e complexidade. É essencial, porém, que uma pessoa com a devida autoridade (por exemplo, proprietário, diretor do conselho executivo ou representante eleito) tenha a responsabilidade geral sobre o GCN e seja diretamente responsável por garantir a continuidade do sucesso desta capacidade.

5.2.2 Se a estrutura da organização assim indicar, a alta direção pode nomear representantes de outros níveis do negócio por função ou localização para ajudar na implementação do programa de GCN.

Convém que os papéis, responsabilidades e autoridades sejam integrados nas descrições de trabalho e grupos de habilidades.

Convém que o processo de auditoria da organização analise criticamente estas responsabilidades. Estas responsabilidades podem ser reforçadas por meio de sua inclusão na política de avaliação, recompensa e reconhecimento da organização.

COMENTÁRIOS DE 5.2.2

Em organizações de grande porte, é possível que haja a necessidade de uma equipe formada por representantes de continuidade de negócios, cada um com seu papel e responsabilidade. Em organizações menores, a responsabilidade pela continuidade de negócios pode pertencer a um ou mais indivíduos.

5.3 Implementando a continuidade de negócios na organização

5.3.1 Convém que as atividades de implementação do programa de continuidade de negócios incluam o planejamento, desenvolvimento e implementação do programa.

Convém que a organização:

— comunique o programa às partes interessadas;

— organize ou forneça treinamento apropriado para a equipe; e

— teste sua capacidade de continuidade de negócios (ver Seção 9).

5.3.2 A organização pode adotar um método reconhecido de gerenciamento de projetos para garantir que a implementação seja efetivamente gerenciada.

5.4 Gestão contínua

5.4.1 Visão geral

Convém que as atividades da gestão contínua assegurem que a continuidade de negócios esteja incorporada na organização. Convém que cada componente da capacidade de continuidade de negócios da organização seja analisado criticamente, exercitado e atualizado regularmente. Além disso, convém que os planos e soluções de continuidade de negócios sejam analisados criticamente e atualizados sempre que haja uma mudança significativa no ambiente operacional da organização ou em suas pessoas, processos ou tecnologias, assim como quando um teste ou incidente revelar deficiências.

5.4.2 Manutenção contínua

Independentemente de como sejam alocados os recursos de GCN, existem atividades que devem ser executadas tanto inicialmente quanto durante a sua execução. Estes podem incluir:

— 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 negócio atual por meio das boas práticas;

— promover a continuidade de negócio 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 (ver 5.5);

— 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.

5.5 Documentação de GCN

Convém que os indivíduos responsáveis por manter a continuidade de negócios devam criar e manter a documentação de continuidade de negócios. Isso pode incluir os seguintes documentos:

a) política de GCN:

   — declaração do escopo de GCN;

   — termos de referência de GCN;

b) análise de impacto nos negócios (BIA);

c) avaliação de riscos e ameaças;

d) estratégias de GCN;

e) programa de conscientização;

f) programa de treinamento;

g) planos de gerenciamento de incidentes;

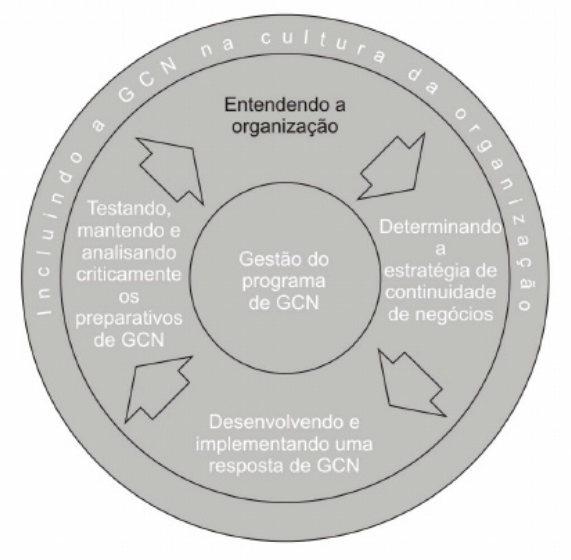
h) planos de continuidade de negócio;

i) planos de recuperação de negócios;

j) agenda de testes e relatórios;

k) contratos e acordos de níveis de serviço.

6 Entendendo a organização



O objetivo desse elemento do ciclo de vida de GCN é ajudar na compreensão da organização por meio da identificação de seus produtos e serviços fundamentais e das atividades críticas e dos recursos que a suportam. Esse elemento garante que o programa de GCN esteja alinhado aos objetivos, obrigações e responsabilidades legais da organização.

6.1 Introdução

6.1.1 Em um contexto de continuidade de negócios, o entendimento da organização deriva de:

— identificar os objetivos da organização, obrigaçõesdas partes interessadas, deveres legais eo ambiente no qual a organização opera;

— identificar as atividades, ativos erecursos, incluindo osexternos, que dãosuporte àentrega desses produtos e serviços;

— avaliar oimpacto e as conseqüências sobreo tempo de falha destas atividades, ativos erecursos (ver 6.2);

— identificar e avaliar as ameaças que possam interromper os produtos e serviços fundamentais e osativos, atividades e recursos que os suportam.

6.1.2 É importante que a organização compreenda:

a) a interdependência de suas atividades; e

b) qualquer dependência com organizações externase quaisquer terceirosque dependam dela.

6.2 Análise de impacto no negócio (BIA)

6.2.1 Convém que a organização defina e documente o impacto de uma interrupção nas atividades que suportam seus produtos e serviços fundamentais. Esse processo é comumente conhecido como análise de impacto nos negócios (BIA).

6.2.2 Para cada atividade que suporta a entrega de produtos e serviços fundamentais para a organização, dentro do escopo do programa de GCN, convém que a organização:

a) verifique, conforme o passar do tempo, o impacto que aconteceria caso a atividade fosse interrompida;

b) estabeleça o período máximo de interrupção tolerável de cada atividade, identificando:

— o tempo máximo decorrido após o início de uma interrupção para que uma atividade precise ser reiniciada;

— o nível mínimo no qual a atividade tem que ser desempenhada após seu reinício;

— o tempo máximo até a retomada dos níveis normais de operação;

COMENTÁRIOS DE 6.2.2-b)

Durante uma interrupção, o impacto geralmente aumenta com o passar do tempo e afeta diferentemente cada atividade. O impacto também pode variar de acordo com o dia, mês ou ponto do ciclo de vida do negócio.

c) identificar quaisquer atividades interdependentes, ativos, infra-estrutura de suporte ou recursos que também precisem ser mantidos continuamente ou recuperados ao longo do tempo.

6.2.3 Ao avaliar os impactos, convém que a organização considere aqueles que se relacionam a seus objetivos de negócio e às partes interessadas. Estes podem incluir:

a) impacto ao bem-estar das pessoas;

b) dano ou perda de instalações, tecnologias ou informação;

c) não cumprimento de deveres ou regulamentações;

d) danos à reputação;

e) danos à viabilidade financeira;

f) deterioração da qualidade de produtos ou serviços;

g) danos ambientais.

Convém que a organização documente a sua abordagem de avaliação do impacto de uma interrupção e suas descobertas e conclusões.

6.3 Identificação de atividades críticas

A organização deve categorizar suas atividades de acordo com suas prioridades de recuperação. Aquelas atividades cuja perda, de acordo com os resultados da BIA, teriam o maior impacto no menor tempo e que necessitem ser recuperadas mais rapidamente devem ser chamadas de “atividades críticas”. Cada atividade crítica suporta um ou mais produtos ou serviços principais.

A organização pode querer focar suas atividades de planejamento em atividades críticas, mas convém que reconheça que as outras atividades também necessitarão ser recuperadas dentro de seu período máximo de interrupção tolerável e podem também precisar que os devidos preparativos sejam realizados.

COMENTÁRIOS DE 6.3

O período de tempo máximo para a restauração das atividades pode variar entre segundos e meses, dependendo da natureza da atividade. As atividades que são sensíveis a tempo podem necessitar de especificações de tempo com alto grau de precisão, por exemplo, em minutos ou em horas. Atividades menos sensíveis a tempo podem necessitar de menos precisão.

O período máximo de interrupção tolerável influenciará o tempo objetivado de recuperação (RTO) de cada atividade durante a definição de estratégias de GCN (ver Seção 7).

6.4 Determinando requisitos de continuidade

Convém que a organização estime os recursos que cada atividade necessitará durante sua recuperação. Estes podem incluir:

a) recursos de pessoal, incluindoquantidade, habilidadese conhecimento (depessoas);

b) localização dos trabalhos e instalações necessárias (dependências);

c) tecnologia, equipamentose plantas que suportam o negócio (tecnologia);

d) informação (eletrônica ou em papel) sobre trabalhos anteriores ou trabalhos atualmente em progresso, suficientemente atualizada e precisa, de forma a permitir que as atividades continuem no nível acordado (informação); e

e) serviços e fornecedores externos (suprimentos).

Convém que a organização leve em conta as necessidades das partes interessadas ao determinar os níveis de recursos.

COMENTÁRIOS DE 6.4

Tecnologia implica uso de equipamento no sentido mais abrangente e relevante para a organização. Isso pode incluir, mas não está limitado a, software e hardware de TI, equipamento de telecomunicações, tornos, máquinas de preparo de alimentos, máquinas de selagem a vácuo ou qualquer outro recurso essencial à capacidade de produção e manufatura.

Se registros ou informações sobre trabalhos em andamento não estão disponíveis, são imprecisos ou não suficientemente atualizados, é possível que a restauração das atividades seja impedida ou criticamente atrasada. Os requisitos de se fornecer tais informações são usados para formular estratégias apropriadas de gerenciamento de backup e registros durante a definição das estratégias de GCN (Ver Seção 7).

6.5 Avaliando ameaças a atividades críticas (realizando uma avaliação de riscos)

6.5.1 Em um contexto de GCN, convém que o nível de risco seja entendido especificamente no que diz respeito às atividades críticas da organização e aos riscos de uma interrupção destas. As atividades críticas têm como base recursos como pessoas, instalações, tecnologia, informações, suprimentos e partes interessadas. Convém que a organização entenda as ameaças a esses recursos, as vulnerabilidades de cada recurso e o impacto que haveria se uma ameaça se tornasse um incidente e causasse uma interrupção no negócio.

6.5.2 A decisão do método de avaliação de riscos é da organização, mas é importante que esse método seja apropriado a todos os requisitos da organização.

6.5.3 A ABNT NBR ISO/IEC 27001 define uma estrutura de avaliação de riscos a ser escolhida através da definição dos elementos obrigatórios que o processo deve conter. Alguns elementos típicos são:

a) definição dos critérios de aceitação dos riscos. Esses critérios descrevem as circunstâncias em que a organização pode aceitar riscos;

b) identificação dos níveis aceitáveis derisco. Independentemente daestratégia de avaliação deriscos escolhida, a organização precisa identificar o nível de risco que ela considera aceitável;

c) análise dos riscos. É necessário que a estratégia de avaliação dos riscos enderece todos os conceitos discutidos em 6.5.4, 6.5.5 e 6.5.6.

6.5.4 Ameaças específicas podem ser descritas como eventos ou ações que possam, em algum ponto, causar um impacto aos recursos, como, por exemplo, incêndio, enchente, queda de energia, perda de equipe, equipe ausente, vírus de computador e falha de *hardware*.

6.5.5 As vulnerabilidades podem existir como fraquezas nos recursos e podem, em algum ponto, ser exploradas pelas ameaças, como, por exemplo, pontos únicos de falha e inadequações na proteção contra incêndio, em instalações elétricas, na quantidade de pessoas na equipe, na segurança e facilidade de recuperação dos recursos de TI.

6.5.6 Os impactos (ver 6.2.3) podem resultar da exploração de vulnerabilidades pelas ameaças.

COMENTÁRIOS DE 6.5

Pode ser útil consultar registros de riscos que já tenham sido estabelecidos em outra parte da organização ou por terceiros.

6.6 Determinando escolhas

6.6.1 Visão geral

Como resultado da BIA e da avaliação de riscos, convém que a organização identifique medidas que reduzam o período de interrupção e que:

a) reduzam a chance de uma interrupção;

b) diminuam o período de interrupção; e

c) limitem o impacto de uma interrupção dos produtos e serviços fundamentais da organização.

Estas medidas são conhecidas como mitigação de perdas e tratamento de riscos.

Estratégias de mitigação de perdas podem ser usadas em conjunto com outras opções, visto que nem todos os riscos podem ser prevenidos ou reduzidos a um nível aceitável. A organização pode incluir uma, várias ou até mesmo todas as estratégias de 6.6.2 a 6.6.5 para cada atividade crítica.

6.6.2 Continuidade de negócios

Se a continuidade de negócios for a estratégia escolhida para um produto ou serviço fundamental, convém que um tempo objetivado de recuperação (RTO) seja estabelecido e as estratégias de continuidade da Seção 7 sejam avaliadas contra esse objetivo.

As estratégias de continuidade buscam melhorar a resiliência da organização a interrupções, garantindo que as atividades críticas continuem ou sejam recuperadas em um nível mínimo aceitável e no tempo estipulado pela BIA.

6.6.3 Aceitação

Um risco pode ser aceitável sem que nenhuma outra ação seja realizada. Mesmo se ele não for aceitável, a capacidade de se executar qualquer ação frente a alguns riscos pode ser limitada, ou o custo de tomar esta ação pode ser desproporcional ao benefício em potencial. Nesses casos, a resposta pode ser tolerar o nível existente de risco, se a alta direção definir que o risco seja aceitável e dentro do apetite a riscos da organização. Em algumas circunstâncias, o impacto de um risco pode estar fora do apetite a riscos usual da organização, mas, devido a uma baixa probabilidade de ocorrência do risco e/ou ao custo de controle fora das possibilidades econômicas da organização, a alta direção pode aceitar o risco.

A aceitação pode ser suplementada por um plano de tratamento dos possíveis impactos, caso o risco se concretize.

6.6.4 Transferência

Para alguns riscos, a melhor resposta pode ser transferi-los. Isso pode ser realizado por meio de um seguro convencional ou de acordos contratuais, ou pagando-se um terceiro para assumir o risco de outra forma. Esta opção é particularmente boa na mitigação de riscos financeiros ou riscos a ativos. Os riscos podem ser

transferidos de forma a reduzir a exposição a riscos da organização ou porque outra organização pode ter uma melhor capacidade de gerenciar esses riscos. É importante notar que alguns riscos não são (totalmente) transferíveis; em particular, geralmente não é possível transferir riscos à reputação, mesmo se a entrega de um serviço for terceirizada.

As apólices de seguro podem ser parte de uma estratégia de tratamento de risco e fornecem alguma recompensa financeira por determinadas perdas. Porém, nem todas as perdas são totalmente seguráveis (por exemplo, incidentes não cobertos, danos à marca ou reputação, perda de valor para as partes interessadas, redução da participação no mercado e conseqüências humanas). É improvável que apenas um acordo financeiro proteja totalmente a organização de forma a satisfazer as expectativas das partes interessadas. Os seguros são geralmente usados em conjunto com outras estratégias.

6.6.5 Mudar, suspender ou terminar

Em algumas circunstâncias, pode ser apropriado mudar, suspender ou terminar o serviço, produto, atividade, função ou processo. Esta opção só deve ser considerada quando não houver conflito com os objetivos da organização, sua conformidade com as regras e as expectativas das partes interessadas. Esta abordagem é geralmente considerada nos casos em que um serviço, produto, atividade, função ou processo tem um tempo de vida limitado.

NOTA Estas estratégias são conhecidas às vezes como o modelo "4 T": "Tratar" (continuidade de negócios), "Tolerar" (aceitar o risco), "Transferir" e "Terminar".

6.7 Aprovação

Convém que a alta direção aprove a lista que documenta os principais produtos e serviços, a análise de impacto nos negócios e a avaliação de riscos, de forma a garantir que o trabalho foi realizado de forma apropriada e reflete verdadeiramente a realidade da organização.

7 Determinando a estratégia de continuidade de negócios

Este elemento do ciclo de vida da GCN segue logicamente o elemento "Entendendo a organização". Como resultado da análise anterior, uma organização estará numa posição apropriada para efetuar a escolha das estratégias de continuidade apropriadas ao alcance de seus objetivos.

7.1 Introdução

Convém que a abordagem da organização para determinar suas estratégias de GCN:

a) implemente as medidas apropriadas, de forma a reduzir a probabilidade de ocorrência de incidentes e/ou reduzir os potenciais efeitos desses incidentes;

b) mantenha um registro das medidas de resiliência e mitigação;

c) forneça continuidade para as atividades críticas durante e após um incidente; e

d) mantenha um registro das atividades que não foram identificadas como críticas.

COMENTÁRIOS DE 7.1

A Seção 7, assim como as seguintes, são relacionadas aos produtos e serviços fundamentais que são alvo da continuidade de negócios. Em todos os outros casos (por exemplo, suspensão, término ou aceitação do risco), o produto ou serviço não é coberto pela GCN e não pode ser considerado em conformidade com esta Norma.

7.2 Opções de estratégia

7.2.1 Convém que a organização considere opções estratégicas para suas atividades críticas e para os recursos que cada atividade consumirá durante sua restauração. A(s) estratégia(s) mais apropriada(s) depende(m) de uma série de fatores, como:

a) o período máximo de interrupção tolerável da atividade crítica;

b) os custos de implementação de uma ou mais estratégias; e

c) as conseqüências de não se agir.

7.2.2 Estratégias podem ser necessárias para os seguintes recursos da organização:

a) pessoas (ver 7.3);

b) instalações (ver 7.4);

c) tecnologia (ver 7.5);

d) informação (ver 7.6);

e) suprimentos (ver 7.7);

f) partes interessadas (ver 7.8).

Em cada caso, convém que a organização minimize a probabilidade de implementar uma solução de continuidade de negócios que possa ser afetada pelo mesmo incidente que causou a interrupção no negócio.

7.3 Pessoas

Convém que a organização identifique as estratégias apropriadas para manter as habilidades e conhecimentos fundamentais. Convém que essa análise se estenda além dos empregados, até prestadores de serviço e outras partes interessadas que possuam habilidades e conhecimento especializados. Estratégias que protejam ou forneçam estas habilidades podem incluir:

a) documentação do método de execução das atividades críticas;

b) treinamento multidisciplinar dos funcionários e prestadores de serviço;

c) 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);

d) uso de terceiros;

e) planejamento de sucessão; e

f) retenção e gestão do conhecimento.

7.4 Instalações

Convém que a organização desenvolva uma estratégia que reduza o impacto da indisponibilidade de suas instalações normais de trabalho. Isso pode incluir um ou mais dos seguintes:

a) instalações (ambientes) alternativas dentro da organização, incluindo a realocação de outras atividades;

b) ambientes alternativos fornecidos por outras organizações (por meio ou não de acordos recíprocos);

c) ambientes alternativos fornecidos por terceiros especializados;

d) trabalho a partir de casa ou de locais remotos;

e) outros locais que sejam acordados como apropriados; e

f) uso de força de trabalho alternativa em um local estabelecido.

NOTA 1 Caso a equipe seja movida para instalações alternativas, estas serão próximas o suficiente para que a equipe possa se deslocar para lá, levando em consideração quaisquer possíveis dificuldades causadas pelo incidente. Porém, estas instalações alternativas serão suficientemente distantes a ponto de não serem afetadas pelo mesmo incidente.

NOTA 2 O uso de instalações alternativas para fins de continuidade deve ser apoiado por uma declaração sobre se essas instalações são para uso exclusivo da organização. Se as instalações alternativas forem compartilhadas com outras organizações, um plano, de forma a mitigar a indisponibilidade destas instalações, é desenvolvido e documentado.

NOTA 3 Pode ser apropriado relocar a carga de trabalho em vez da equipe, quando for possível, como, por exemplo, no caso de uma linha de produção ou um "call center".

COMENTÁRIOS DE 7.4

As estratégias de locais de trabalho podem variar significativamente e uma série de opções pode estar disponível. Diferentes tipos de incidentes ou ameaças podem precisar da implementação de diferentes ou múltiplas opções. As estratégias mais corretas vão, em parte, ser definidas pelo tamanho da organização, setor e distribuição de atividades, partes interessadas e base geográfica. Por exemplo, autoridades públicas necessitarão manter um serviço de atendimento junto às suas comunidades.

7.5 Tecnologia

7.5.1 As estratégias de tecnologia dependem da natureza da tecnologia empregada e da sua relação com as atividades críticas, mas basicamente serão uma ou mais combinações das condições a seguir:

a) provisão interna à organização;

b) serviços entregues à organização; e

c) serviços realizados externamente por terceiros

COMENTÁRIOS DE 7.5.1

As estratégias de tecnologia variam significativamente entre as organizações de acordo com o tamanho, natureza e complexidade do negócio. Estratégias específicas devem ser desenvolvidas de forma a proteger, substituir ou restaurar as tecnologias desenvolvidas sob medida que demorariam muito para ser desenvolvidas novamente.

Pode ser necessário que a organização seja capaz de funcionar com base em operações manuais antes que todos os serviços de tecnologia sejam recuperados.

7.5.2 As estratégias de tecnologia podem incluir:

a) distribuição geográfica da tecnologia, ou seja, manter a tecnologia em locais diferentes que não serão afetados pela mesma interrupção de negócios;

b) armazenar o equipamento mais antigo como substituto em caso de emergências; e

c) mitigação de risco adicional para equipamento único ou para um prazo de entrega longo.

7.5.3 Os serviços de tecnologia da informação (TI) freqüentemente necessitam de estratégias de continuidade complexas. Nos casos em que estas estratégias sejam necessárias, convém que seja levado em consideração o seguinte:

a) tempo objetivado de recuperação (RTO) de sistemas e aplicativos que suportam as atividades fundamentais identificadas na BIA;

b) local e distância entre instalações tecnológicas;

c) quantidade de instalações tecnológicas;

d) acesso remoto;

e) uso de instalações vazias (sem equipe) em vez de instalações ocupadas;

f) conectividade de telecomunicações e roteamento redundante;

g) natureza do "*fail over*" (se é necessária intervenção manual para ativar os recursos alternativos de TI ou se isso deve ocorrer automaticamente); e

h) conectividade com terceiros e links externos.

NOTA 1 Se for utilizada uma estratégia de "fail over" de um local para outro, a distância de rede entre os dois locais deve ser cuidadosamente considerada, pois poderia ter impacto negativo na operação dos sistemas de TI.

NOTA 2 Em casos em que mais de um local hospede a TI da organização, pode haver uma estratégia de recuperação de TI mútua, de forma que os sistemas, redes e armazenamento em cada local estejam dimensionados para suportar o tráfego e trabalho adicional, além da sua própria carga.

NOTA 3 Uma alternativa a esta realocação de pessoal é fornecer acesso aos serviços de TI de forma discada ou por meio da Internet, utilizando redes privadas virtuais (VPN) ou tecnologias similares.

NOTA 4 Mais informações sobre continuidade de TI e de hardware de telecomunicações podem ser encontradas em documentos como PAS 77, ABNT NBR ISO/IEC 27001 e ISO/IEC 20000 (ambas as partes).

7.6 Informação

Convém que as estratégias de informação garantam que a informação vital para a operação da organização esteja protegida e seja recuperável de acordo com os limites de tempo descritos na BIA.

NOTA 1 Mais orientações estão disponíveis na ABNT NBR ISO/IEC 27001. O armazenamento e a recuperação destas informações devem estar em conformidade com a legislação pertinente.

Convém que qualquer informação que seja necessária para permitir a realização das atividades críticas da organização possua, em nível apropriado:

a) confidencialidade;

b) integridade;

c) disponibilidade; e

d) atualização.

Convém que as estratégias de informação sejam documentadas para que seja possível recuperar informações que ainda não tenham sido copiadas ou caso não tenha sido realizado *backup* em um local seguro.

Convém que as estratégias de informação sejam estendidas de forma a incluir:

a) formatos físicos (impressos); e

b) formatos virtuais (eletrônicos) etc.

NOTA 2 Em todos os casos, a informação precisa ser recuperada em um intervalo de tempo conhecido e acordado com a alta direção. Podem ser utilizados vários métodos de cópia, tais como backups eletrônicos ou em fita, microfilme, fotocópias, criação de duas cópias durante a produção, entre outros. Esse ponto de recuperação é geralmente conhecido como "ponto objetivado de recuperação" (RPO).

7.7 Suprimentos

7.7.1 Convém que a organização identifique e mantenha um inventário dos suprimentos fundamentais que suportem suas atividades críticas. As estratégias para fornecer esses suprimentos podem incluir:

a) armazenamento de suprimentos adicionais em outro local;

b) acordos com terceiros para entregas emergenciais;

c) remanejamento de entregas programadas para outros locais;

d) armazenamento de materiais em armazéns ou bases de envio;

e) transferência de atividades de montagem de unidades para um local alternativo que possua esses suprimentos; e

f) identificação de suprimentos alternativos/substitutos.

7.7.2 Em situações em que as atividades críticas dependam de suprimentos especiais, convém que a organização identifique os principais fornecedores e as fontes únicas de suprimentos. As estratégias para gerenciar a continuidade dos suprimentos podem incluir:

a) aumento do número de fornecedores;

b) recomendação ou exigência de que os fornecedores tenham uma capacidade de continuidade de negócios validada;

c) obrigações contratuais e/ou acordos de nível de serviços com os principais fornecedores; ou

d) a identificação de fornecedores alternativos que sejam capazes de atender à demanda.

COMENTÁRIOS DE 7.7

Em ambientes de escritório, os suprimentos podem ser cheques etc. Em indústrias, pode significar o estoque de vendas, os suprimentos necessários para seu funcionamento ou combustíveis.

7.8 Partes interessadas

7.8.1 Ao determinar as estratégias de GCN, convém que a organização considere e proteja os interesses de suas principais partes interessadas. Convém que essas estratégias levem em consideração os aspectos socioculturais pertinentes.

7.8.2 Convém que a organização identifique as estratégias apropriadas para gerenciar suas relações com as principais partes interessadas, fornecedores e parceiros de negócios ou serviços. Cada um desses grupos pode precisar de considerações específicas. As estratégias para proteger os interesses das principais partes podem incluir preparativos especiais, de forma a garantir o bem-estar das partes interessadas com necessidades especiais, como deficiências físicas, doenças ou gravidez.

7.8.3 Convém que a organização identifique pessoa(s) para garantir o bem-estar de todos após o incidente.

7.9 Emergências civis

7.9.1 Convém que as organizações que buscam definir, implementar ou validar suas estratégias de gerenciamento de incidentes e gestão da continuidade de negócios conheçam as autoridades responsáveis por responder a emergências. Estas autoridades têm como tarefas as atividades de antecipação, avaliação, prevenção, preparação, resposta e recuperação em casos de emergências civis que ocorram dentro de suas áreas de atuação.

7.9.2 Estas autoridades serão fundamentais para a declaração oficial de que ocorreu uma emergência civil, além de fornecer:

a) ajuda pré ou pós-incidente (por exemplo, avaliações de risco);

b) procedimentos de aviso e informação; e

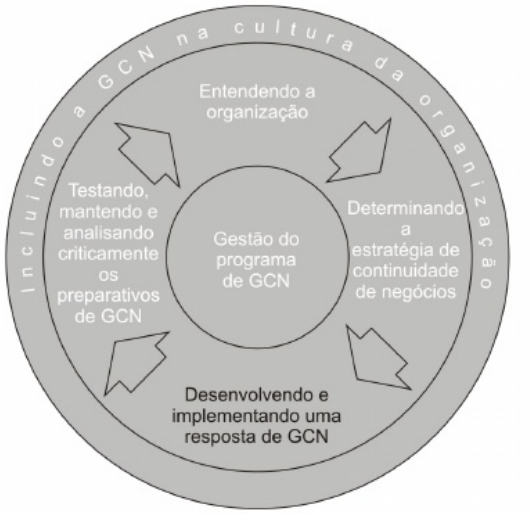
c) acordos de recuperação comunitária após uma emergência civil.

NOTA As emergências civis podem resultar em morte e dano físico, além de poder ter um impacto profundo e duradouro no bem-estar psicológico, social e econômico dos indivíduos envolvidos e de suas comunidades. As emergências podem causar interrupções significativas nos serviços de transporte público, redes de telecomunicação, infra-estruturas críticas e no fluxo de bens, serviços e suprimentos. Tendo em vista esse potencial, é importante que as organizações se familiarizem com o funcionamento das autoridades locais responsáveis.

7.10 Aprovação

Convém que a alta direção aprove as estratégias que foram documentadas, de forma a confirmar que a determinação das estratégias de continuidade foi efetuada de forma correta e abrange as mais prováveis causas e efeitos de incidentes, e que as estratégias escolhidas são apropriadas para alcançar os objetivos da organização, dentro do seu apetite a riscos.

8 Desenvolvendo e implementando uma resposta de GCN



Este elemento do ciclo de vida de GCN é relacionado ao desenvolvimento e implementação dos planos apropriados e dos preparativos realizados, de forma a garantir a continuidade das atividades críticas e o gerenciamento dos incidentes.

8.1 Introdução

As Seções 6 e 7 definem como convém que a organização:

a) identifique suas atividades críticas;

b) avalie as ameaças a estas atividades críticas;

c) escolha estratégias apropriadas que diminuam a probabilidade e os impactos dos incidentes; e

d) escolha estratégias apropriadas que permitam a continuidade ou recuperação de suas atividades críticas.

Convém que a gama de ameaças para a qual existirão planos seja definida pelo apetite a riscos da organização.

8.2 Estrutura de resposta a incidentes

8.2.1 Convém que a organização defina uma estratégia de resposta a incidentes que permita uma resposta efetiva e uma recuperação pós-incidente.

8.2.2 Em qualquer incidente, convém que exista uma estrutura simples e rapidamente formada que permita à organização:

a) confirmar a natureza e extensão do incidente,

b) tomar controle da situação,

c) controlar o incidente, e

d) comunicar-se com as partes interessadas.

Convém que a mesma estrutura emita uma resposta de continuidade de negócios adequada. Esta estrutura pode ser chamada de equipe de gerenciamento de incidentes ou equipe de gerenciamento de crise.

8.2.3 Convém que as equipes possuam planos, processos e procedimentos de gerenciamento de incidentes e que estes sejam suportados por ferramentas de continuidade de negócios, de forma a permitir a continuidade e a recuperação de atividades críticas.

8.2.4 Convém que a equipe possua planos para a ativação, operação, coordenação e comunicação da resposta ao incidente.

A Figura 2 ilustra as três principais fases de tempo de um incidente e a relação entre o gerenciamento do incidente e a continuidade de negócios.

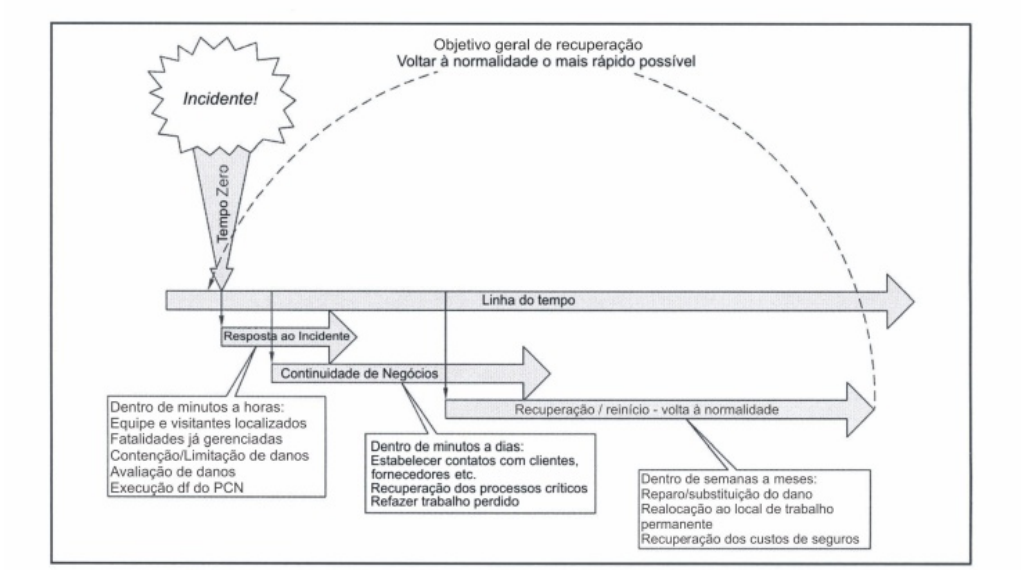


Figura 2 — Linha do tempo do incidente

NOTA Em alguns casos, a ativação dos planos de gerenciamento de incidentes, continuidade de negócios e recuperação de negócios pode ocorrer em rápida sucessão ou simultaneamente.

8.2.5 As organizações podem desenvolver planos específicos para recuperar ou retomar suas operações num estado "normal" (planos de recuperação). Mas em alguns incidentes pode não ser possível definir o que é "normal" até um período após o incidente, de forma que pode não ser possível executar os planos de recuperação imediatamente. Desta forma, as organizações devem garantir que os planos de continuidade de negócio sejam capazes de operar por um período estendido, de forma a assegurar que haja tempo para o desenvolvimento e execução de planos de recuperação (“volta à normalidade”).

COMENTÁRIOS DE 8.2

Em organizações pequenas, a responsabilidade pelo gerenciamento de incidentes e de continuidade de negócios pode ser de um único indivíduo. Organizações maiores podem usar uma estrutura em níveis e podem estabelecer diferentes equipes, de forma a focalizar os problemas de gerenciamento de incidentes, continuidade de negócios e recuperação do negócio. Em alguns casos, estas equipes podem ter o suporte de outras equipes que sejam responsáveis por atividades como comunicação com a mídia e questões de pessoal.

8.3 Conteúdo dos planos

8.3.1 Introdução

Convém que todos os planos, sejam eles de gerenciamento de incidentes, continuidade de negócios ou recuperação de negócios, sejam concisos e acessíveis àqueles que possuam responsabilidades definidas nesses planos. Convém queos planos contenhamos elementos descritos em 8.3.2 a 8.3.6.

COMENTÁRIOS DE 8.3.1

Uma organização pequena pode ter um único plano que tenha como abrangência todos os requisitos do negócio e que cubra todas as suas operações. Uma organização muito grande pode ter vários planos, com cada um especificando em detalhes a recuperação de:

a) uma parte específica de seu negócio;

b) instalações específicas; ou

c) um cenário específico,

d) e pode haver documentação separada para os estágios de incidente, continuidade e recuperação.

8.3.2 Objetivo e escopo

Convém que o objetivo e o escopo de cada plano específico sejam definidos, acordados com a alta direção e entendidos pelas pessoas que irão realizar o plano. Convém que qualquer relação com outros planos ou documentos pertinentes que existam na organização seja claramente especificada e o método de obtenção desses documentos seja descrito.

Convém que cada plano de gerenciamento de incidentes, continuidade de negócios e recuperação de negócios defina objetivos priorizados em termos de:

a) atividades críticas que necessitem de recuperação;

b) escala de tempo em que esta recuperação deveocorrer;

c) níveis de recuperação necessários paracada atividade crítica; e

d) situação em que cada plano pode ser utilizado.

COMENTÁRIOS DE 8.3.2

Cada plano deve conter claramente o que ele não busca alcançar e por que.

8.3.3 Papéis e responsabilidades

Convém que os papéis e responsabilidades das pessoas e equipes que possuam autoridade (tanto no que se refere à tomada de decisões quanto aos gastos), durante e após um incidente, sejam claramente documentados.

Convém que as pessoas ou grupos cobertos por um plano sejam claramente definidos.

COMENTÁRIOS DE 8.3.3

Os planos também podem conter, quando for apropriado, procedimentos e listas de verificação que suportem o processo de análise crítica pós-incidente.

8.3.4 Ativação de planos

Convém que o método pelo qual um plano de gerenciamento de incidentes, continuidade de negócios ou recuperação de negócios é colocado em prática seja claramente documentado. Convém que esse processo permita que os planos ou partes pertinentes sejam executados no menor tempo possível após uma interrupção de negócios.

Convém que a organização estabeleça e documente claramente os procedimentos e conjunto de critérios sobre os quais os indivíduos possuem a autoridade de colocar em prática os planos e em quais circunstâncias.

O processo de ativação pode necessitar de mobilização imediata dos recursos organizacionais. Convém que o plano inclua uma descrição clara e precisa de:

a) como mobilizar as equipes;

b) pontos de encontro imediatos; e

c) pontos de encontros subseqüentes edetalhes de locais de encontro alternativos (emorganizações maiores, esses locais podem ser conhecidos como centros de gerenciamento de incidentes ou de comando).

A organização deve documentar um processo claro de desativação das equipes e retorno aos negócios, uma vez que acabe o incidente.

COMENTÁRIOS DE 8.3.4

O tempo perdido durante uma resposta é irrecuperável. É sempre melhor mobilizar a equipe de resposta e depois pará-la do que perder a chance de conter um incidente em seu começo e prevenir que tome proporções maiores.

Convém que as organizações levem em conta os procedimentos definidos e internacionalmente acordados para esses casos, de acordo com as recomendações de outras fontes especializadas, como, por exemplo, a Organização Mundial de Saúde, no caso de pandemias.

8.3.5 Proprietário e mantenedor do documento

Convém que a organização nomeie o principal responsável pelo plano e identifique e documente os responsáveis pela análise crítica, correção e atualização do plano em intervalos regulares.

Convém que um sistema de controle de versões seja empregado, as modificações sejam formalmente notificadas a todos os interessados e um registro formal de distribuição do plano seja mantido e atualizado.

8.3.6 Detalhes de contato

Convém que cada plano possua ou forneça uma referência aos detalhes essenciais de contato de todas as principais partes interessadas.

COMENTÁRIOS DE 8.3.6

Os detalhes de contato podem incluir informações externas ao escritório. Porém, nos casos em que os planos contenham esses detalhes particulares, deve-se ter a máxima consideração pela proteção dos dados.

8.4 Plano de gerenciamento de incidentes (PGI)

O propósito de um PGI é permitir que a organização gerencie a fase inicial (crítica) de um incidente. Convém que o PGI:

a) seja flexível, viável e relevante;

b) seja de fácil leitura e compreensão; e

c) forneça 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.

Convém que o PGI também:

1) tenha o apoio da alta direção, incluindo um patrocinador no nível de diretoria, quando for aplicável; e

2) seja suportado por um orçamento apropriado para seu desenvolvimento, manutenção e treinamento dos envolvidos.

8.5 Conteúdo do PGI

8.5.1 Geral

Além do recomendado em 8.3, convém que o PGI inclua as informações contidas em 8.5.2 a 8.5.8.

8.5.2 Lista de tarefas e ações

Convém que o PGI inclua listas de tarefas e de ações, de forma a administrar as conseqüências imediatas de uma interrupção de negócios. Convém que essas tarefas:

a) garantam que a segurança das pessoas está em primeiro lugar;

b) tenham como base o resultado da BIA da organização;

c) sejam estruturadas de forma que seja possível a execução das opções estratégicas e táticas escolhidas pela organização (como descrito na Seção 7); e

d) ajudem a prevenir maiores perdas ou indisponibilidade de atividades críticas e dos recursos que as suportam, como definido na Seção 7.

8.5.3 Contatos de emergência

Convém que uma descrição de como e em que circunstâncias a organização se comunicará com sua equipe, seus familiares, amigos e contatos de emergência seja incluída. Em alguns casos, pode ser apropriado incluir detalhes em um documento separado.

Convém que contatos de familiares e de emergência para todos os empregados estejam atualizados e prontos para uso.

COMENTÁRIOS DE 8.5.3

Dependendo do tamanho da organização e do tamanho do incidente, pode ser necessária uma grande quantidade de pessoas competentes e treinadas para responder às ligações telefônicas sobre o incidente.

8.5.4 Atividades das pessoas

Convém que o PGI satisfaça os interesses daqueles cujo bem-estar possa ser colocado em risco como resultado de um incidente, levando em conta as considerações socioculturais pertinentes (ver 7.8.2).

Convém que o PGI identifique as pessoas que vão definir a responsabilidade por problemas de bem-estar após um incidente (ver 7.8.3), incluindo:

a) a evacuação do local (incluindo abrigos no local);

b) a mobilização de equipes de segurança, primeiros-socorros ou assistência à evacuação;

c) a localização e prestação de contas daqueles que estavam no local ou na vizinhança;

d) a manutenção das comunicações com empregados e clientes, bem como relatórios de segurança.

Convém que a organização coloque em ação equipes que possuam os níveis de autoridade apropriados para estabelecer contato com os serviços de emergência, quando for apropriado.

NOTA Os serviços de emergência possuem o papel principal na proteção da vida e alívio do sofrimento durante as emergências. Logo, uma comunicação ágil, pré-planejamento e coordenação dos incidentes em tempo real entre a organização e estas autoridades podem melhorar a eficiência de uma resposta a incidentes.

Convém que a organização possua um meio de fornecer serviços de forma a aconselhar e confortar aqueles afetados pelo incidente. Os serviços podem ser terceirizados ou fornecidos como uma extensão dos programas existentes de saúde do trabalho e assistência aos empregados.

COMENTÁRIOS DE 8.5.4

As organizações são diretamente responsáveis por proteger o bem-estar de empregados, prestadores de serviço, visitantes e clientes nos casos em que um incidente causar um risco de vida e do bem-estar. É necessária uma atenção especial quando houver grupos com deficiências ou outras necessidades específicas (por exemplo, gravidez, invalidez temporária, etc.). Um planejamento adequado, de forma a atender a esses requisitos, pode reduzir o risco e tranqüilizar as pessoas afetadas.

Não se deve subestimar os impactos a longo prazo de um incidente. O desenvolvimento de estratégias apropriadas que promovam o bem-estar humano pode promover diretamente a recuperação física e emocional na organização.

8.5.5 Comunicação à mídia

Convém que a estratégia de comunicação da organização com a mídia seja documentada no PGI, incluindo:

a) a estratégia de comunicação de incidentes;

b) a interface com a mídia escolhida pela organização;

c) um guia ou modelo para a criação de uma minuta de declaração a ser fornecida à mídia na primeira oportunidade viável após o incidente;

d) uma quantidade apropriada de porta-vozes competentes que sejam nomeados e autorizados a liberar as informações autorizadas para a mídia;

e) a definição, quando for viável, de um local apropriado para realizar o contato com a mídia ou com grupos de pessoas interessadas.

Em alguns casos, pode ser apropriado:

— fornecer detalhes de suporte em um documento separado;

— estabelecer um número apropriado de pessoas competentes e treinadas para responder a ligações telefônicas da imprensa.

— preparar material sobre a organização e suas operações (convém que esse material seja pré-aprovado para divulgação);

— garantir que toda a informação à mídia esteja disponível sem uma demora indevida.

COMENTÁRIOS DE 8.5.5

Informações previamente preparadas podem ser especialmente úteis nos primeiros estágios de um incidente. Elas permitem que a organização forneça detalhes sobre ela e seu negócio enquanto os detalhes do incidente ainda estão sendo descobertos. Uma organização pode usar todos os meios aplicáveis de compartilhamento de informações durante e após um incidente. Estas fontes podem incluir páginas na internet, porta-vozes, fontes de notícias e comunicados genéricos.

8.5.6 Gestão de partes interessadas

Convém que um processo de identificação e priorização da comunicação com as principais partes interessadas seja incluído. Pode ser necessário desenvolver um plano de gestão das partes interessadas de forma a estabelecer critérios e alocar uma pessoa para cada parte interessada ou grupo de partes interessadas.

COMENTÁRIOS DE 8.5.6

Pressões ou grupos de ação comunitários que coletivamente possuem poder ou influência sobre a organização também devem ser considerados.

8.5.7 Localização para o gerenciamento de incidentes

Convém que a organização defina previamente um local, sala ou espaço resistente a partir do qual um incidente será gerenciado. Uma vez estabelecido, convém que esse local seja o foco da resposta da organização. Convém que um ponto de encontro alternativo em um local diferente também seja estabelecido, caso não seja possível obter acesso ao local primário. Convém que cada local tenha acesso aos recursos apropriados, por meio do qual a equipe de incidentes possa iniciar as atividades de gerenciamento de incidentes sem atrasos.

Convém que o local escolhido seja apropriado e inclua:

a) meios primários e secundários eficientes de comunicação;

b) facilidades para acessar e compartilhar informações, incluindo monitoramento de notícias na mídia.

COMENTÁRIOS DE 8.5.7
Uma localização para o gerenciamento de incidentes é um ponto focal conhecido, a partir do qual um incidente pode ser gerenciado. É importante capturar e compartilhar as principais informações e definir objetivos, designar tarefas, gerenciar recursos, identificar a rastrear problemas e tomar decisões. É essencial manter boas comunicações. O uso de um ponto de encontro elimina o problema de situações em que as redes telefônicas estejam sobrecarregadas.

Esse local pode ser tão simples quanto um quarto de hotel ou a casa de um membro da equipe. Também pode ser complexo como um "centro de comando" dedicado, com PC, videoconferência e vários telefones.

Inicialmente, pode ser necessário fazer uma reunião virtual, via telefone, teleconferência ou videoconferência, de forma que as principais decisões possam ser prontamente tomadas.

8.5.8 Anexos

Convém que o PGI inclua informações de contato e mobilização de todas as agências, organizações e recursos pertinentes que possam ser necessários para o suporte das estratégias de resposta da organização.

Convém que o PGI inclua registros ou formulários para armazenar informações vitais sobre o incidente, como a cronologia do incidente, detalhes de fatalidades, decisões tomadas, recursos gastos, avaliações de danos, comunicações realizadas e todas as outras informações que sejam consideradas essenciais à organização para dar suporte à análise crítica pós-incidente.

O PGI também pode incluir ou referenciar:

a) mapas, tabelas, plantas, fotografias e qualquer outra informação que possa ser relevante em caso de incidente;

b) estratégias de resposta documentadas, acordadas com terceiros, conforme apropriado (parceiros de negócios, prestadores de serviços, fornecedores etc.);

c) detalhes de armazenamento de equipamentos e áreas de instalação;

d) planos de acesso ao local; e

e) um procedimento de gerenciamento de solicitações que garanta que todas as requisições legais ou de seguro, a favor ou contra a organização, atendam às regulamentações e aos requisitos contratuais.

8.6 Planos de continuidade de negócios (PCN)

O propósito de um plano de continuidade de negócios (PCN) é permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.

Os PCN são ativados para dar suporte às atividades críticas necessárias para cumprir os objetivos da organização. Eles podem ser executados integral ou parcialmente e em qualquer etapa da resposta a um incidente.

COMENTÁRIOS DE 8.6

O conteúdo e os componentes dos PCN variam de organização para organização e possuem diferentes níveis de detalhe, dependendo da escala, ambiente, cultura e complexidade técnica da organização.

Algumas organizações de grande porte podem necessitar de documentos separados para cada uma de suas atividades críticas, enquanto as organizações menores podem ser capazes de abordar todos os aspectos críticos em um único documento.

8.7 Conteúdo do PCN

8.7.1 Geral

Além dos termos recomendados em 8.3, convém que um PCN contenha os elementos contidos em 8.7.2 a 8.7.5.

8.7.2 Planos de ação/Listas de tarefas

Convém que o plano de ação inclua uma lista estruturada de ações e tarefas em ordem de prioridade, destacando-se:

a) como o PCN é ativado;

b) as pessoas responsáveis por ativar o plano de continuidade de negócios;

c) o procedimento que esta pessoa deve adotar ao tomar esta decisão;

d) as pessoas que devem ser consultadas antes desta decisão ser tomada;

e) as pessoas que devem ser informadas quando a decisão for tomada;

f) quem vai para onde e quando;

g) quais serviços estão disponíveis, aonde e quando, incluindo como a organização mobilizará seus recursos externos e de terceiros;

h) como e quando esta informação será comunicada; e

i) se relevante, procedimentos detalhados para soluções manuais, recuperação dos sistemas etc.

COMENTÁRIOS DE 8.7.2

Os planos devem referenciar as pessoas, instalações, tecnologia, informação, suprimentos e partes interessadas identificados na fase de estratégias (ver Seção 7). Devem ser incluídas premissas claras e detalhamentos sobre quaisquer recursos necessários para implementar os planos. Caso a falta de um serviço ou recurso torne os objetivos desse plano inalcançáveis, um procedimento claro deve ser definido para que o problema seja escalado a um nível mais alto.

8.7.3 Recursos necessários

Convém que os recursos necessários para a continuidade e recuperação dos negócios sejam identificados em diferentes pontos no tempo. Estes podem incluir:

a) pessoas, o que pode incluir:

- segurança,
- logística de transporte,
- necessidades de bem-estar e
- gastos de emergência;

b) instalações;

c) tecnologia, incluindo comunicações;

d) informações, o que pode incluir:

- detalhes financeiros (por exemplo, folha de pagamento),
- registros de contas de clientes,
- detalhes de fornecedores e partes interessadas,
- documentos legais (por exemplo, contratos, apólices de seguro, escrituras etc.), e
- outros documentos de serviços (por exemplo, acordos de nível de serviços);

e) suprimentos; e

f) gestão das partes interessadas e da comunicação com estas.

8.7.4 Responsáveis

Convém que a organização identifique e designe um responsável para gerenciar as fases da continuidade e da recuperação dos negócios que ocorrem após uma interrupção de serviços.

COMENTÁRIOS DE 8.7.4

Em muitos casos, é desejável que a organização designe os mesmos indivíduos identificados no plano de gerenciamento de incidentes para gerenciar as questões de longo prazo.

8.7.5 Formulários e anexos

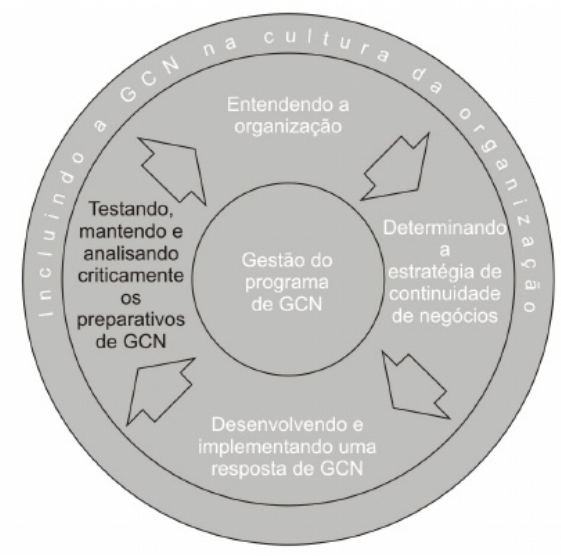
Quando apropriado, convém que o PCN possua detalhes de contato atualizados das agências pertinentes internas e externas, organizações e fornecedores que possam ser necessários para o suporte da organização.

Convém que o plano de continuidade de negócios inclua um registro de incidentes ou formulários para o registro de informações vitais, principalmente como conseqüência de decisões tomadas durante sua execução.

COMENTÁRIOS DE 8.7.5

O plano pode incluir também formulários para armazenar dados administrativos, como, por exemplo, os recursos usados, material para controle de despesas, mapas, desenhos e plantas do local e do escritório, especialmente aqueles relacionados a instalações alternativas, tais como áreas de recuperação do local de trabalho e de armazenagem.

9 Testando, mantendo e analisando criticamente os preparativos de GCN



Esse elemento do ciclo de vida da GCN garante que os preparativos para a GCN da organização estejam validados por testes e análises críticas e que sejam mantidas atualizadas.

9.1 Introdução

Os preparativos de continuidade de negócios e de gerenciamento de incidentes da organização não podem ser considerados confiáveis até serem testados e apenas se estiverem atualizados. A realização de testes é essencial para o desenvolvimento do trabalho em equipe, da competência, da confiança e do conhecimento, que são vitais quando ocorre um incidente.

Convém que os preparativos sejam verificados por meio de testes, auditoria e processos de auto-avaliação, de forma a garantir que estejam adequados.

9.2 Programa de testes

Convém que um programa de testes esteja consistente com o escopo do plano de continuidade de negócios,

levando em conta a legislação e as regulamentações em vigor. Os testes podem:

a) adiantar um resultado previsto, ou seja, que tenha sido antecipadamente planejado e incluído no escopo; ou

b) permitir que a organização desenvolva soluções inovadoras.

Convém que um programa de testes seja criado de forma que, ao longo do tempo, possa ser garantido objetivamente que o PCN funcionará como previsto quando necessário. Convém que o programa:

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

b) teste os preparativos e a infra-estrutura de GCN, incluindo papéis, responsabilidades e quaisquer locais de gerenciamento de incidentes e áreas de trabalho, entre outros;

c) valide a recuperação da tecnologia e das telecomunicações, incluindo a disponibilidade e remanejamento de pessoal.

Adicionalmente, os testes podem melhorar a capacidade de GCN da organização, pois permitem:

a) exercitar a capacidade da organização de se recuperar de um incidente;

b) verificar se todas as atividades críticas da organização, suas dependências e prioridades estão contempladas pelo PCN;

c) realçar premissas que devam ser questionadas;

d) gerar confiança nos participantes envolvidos no teste;

e) aumentar a consciência do processo de continuidade de negócios pela organização por meio da publicação do teste;

f) validar a funcionalidade e tempestividade do processo de restauração das atividades críticas; e

g) demonstrar a competência das equipes titulares de resposta a incidentes e de seus substitutos.

COMENTÁRIOS DE 9.2

Os testes fornecem evidência demonstrável da competência e capacidade de continuidade de negócios e gerenciamento de incidentes da organização. O tempo e os recursos utilizados para validar as estratégias de GCN por meio dos testes dos PCN levarão a uma capacidade adequada. Independentemente de quão bem pensada e desenhada possa ser uma estratégia de GCN para PCN, uma série de testes sólidos e realistas vai identificar áreas que necessitam de correções.

9.3 Testando os preparativos de GCN

9.3.1 Convém que os testes sejam realistas, planejados cuidadosamente e acordados com as partes interessadas, de modo que haja um risco mínimo de interrupção dos processos de negócio. Convém que os testes sejam planejados de forma a minimizar a chance de que ocorra um incidente como resultado direto do teste.

9.3.2 Convém que todo teste tenha objetivos claramente definidos. Convém que sejam elaborados relatórios e análises após o teste que demonstrem se os objetivos do teste foram alcançados. Convém que um relatório pós-teste seja elaborado. Convém que esse relatório contenha recomendações juntamente de uma previsão de tempo para a implementação destas.

9.3.3 Convém que a escala e a complexidade dos testes sejam apropriadas aos objetivos de recuperação da organização.

9.3.4 Convém que os planos de continuidade de negócio e de gerenciamento de incidentes sejam testados de forma a garantir que eles possam ser executados corretamente e estejam suficientemente detalhados, contendo as instruções necessárias para sua execução.

COMENTÁRIOS DE 9.3.4

Testes que demonstrem deficiências sérias ou imprecisões no PCN devem ser refeitos depois de as ações corretivas terem sido completadas.

Uma série de abordagens para testar as estratégias de GCN é exibida na Tabela 1.

Tabela 1 — Tipos e métodos de teste de estratégias de GCN

Complexidade	Teste	Processo	Variações	Freqüência recomendada[a]
Simples	Testes-de-mesa	Análise crítica/correção Questionar conteúdo do PCN	Atualização/Validação Auditoria/Verificação	Ao menos anualmente Anualmente
	"Walk-through" (repassar os passos) do plano	Questionar o conteúdo do PCN	Incluir interação e validar papéis dos participantes	Anualmente
Médio	Simulação	Usar situação "artificial" para validar se os PCN possuem as informações necessárias e suficientes, de forma a permitir uma recuperação com sucesso	Incorporar planos associados	Anualmente ou duas vezes ao ano
	Testar atividades criticas	Execução em ambiente controlado que não prejudique o andamento normal dos negócios	Executar algumas operações a partir de um local alternativo por um tempo determinado	Anualmente ou menos
Complexo	Testar todo o PCN, incluindo o gerenciamento de incidentes	Teste que envolve todo o prédio/campus/zona de exclusão		Anualmente

[a] Convém que a freqüência dos testes dependa das necessidades da organização, do ambiente no qual ela opera e das necessidades das partes interessadas. Porém, convém que o programa de testes seja flexível, levando em conta a freqüência de ocorrência de mudanças na organização e o resultado dos testes anteriores. Os métodos de teste acima podem ser empregados para cada componente de um plano ou para um ou mais planos.

9.3.5 Convém que o programa de testes considere o papel de todas as partes envolvidas, inclusive principais fornecedores, parceiros terceirizados e outros que seria esperado participar das atividades de recuperação. A organização deve incluí-los nos testes.

9.4 Manutenção dos preparativos de GCN

Convém que seja estabelecido um programa de manutenção do GCN claramente definido e documentado. Convém que esse programa garanta que quaisquer mudanças, internas ou externas, que causem um impacto à organização, sejam analisadas criticamente quanto à GCN. Convém também identificar novos produtos e serviços e suas atividades dependentes, para que sejam incluídos no programa de manutenção da GCN.

Como resultado do programa de manutenção de GCN, convém que a organização:

a) analise criticamente e questione quaisquer premissas adotadas para quaisquer componentes da GCN presentes na organização; e

b) distribua uma política de GCN atualizada, corrigida ou alterada, estratégias, soluções, processos e planos para os principais funcionários dentro de um processo formal de controle de alterações.

NOTA Se houver mudanças significativas no negócio, deve ser efetuada uma análise crítica da BIA. Os outros componentes do programa de GCN devem ser corrigidos para refletir estas mudanças.

Convém que os resultados do processo de manutenção da GCN incluam:

a) evidência documentada da gestão pró-ativa e da governança do programa de continuidade de negócios da organização;

b) verificação de que as principais pessoas designadas para implementar as estratégias de GCN e planos foram treinadas e são competentes;

c) verificação da monitoração e controle dos riscos de GCN enfrentados pela organização; e

d) evidência documentada das mudanças pertinentes relativas à estrutura da organização, seus produtos e serviços, atividades, propósito, equipe e objetivos que foram incorporados nos planos de continuidade de negócio e de gerenciamento de incidentes.

COMENTÁRIOS DE 9.4

O propósito do processo de manutenção de GCN é garantir que a competência e a capacidade de GCN da organização continuem efetivas, apropriadas e atualizadas.

As atividades de manutenção buscam modificar os cronogramas atuais de teste quando ocorre uma mudança significativa na estratégia, solução ou processo de negócios.

9.5 Análise crítica dos preparativos de GCN

9.5.1 Convém que a alta direção da organização, nos intervalos que considerar apropriados, analise criticamente a capacidade de GCN da organização de forma a garantir sua aplicabilidade, adequação e funcionalidade. Convém que a análise crítica seja documentada.

9.5.2 Convém que a análise crítica verifique se a conformidade com a política de GCN da organização garante a conformidade com as leis, normas, estratégias, estruturas e boas práticas aplicáveis.

9.5.3 Convém que a análise crítica leve em conta uma eventual necessidade de mudanças na política, na estratégia, nos objetivos e nos outros elementos da GCN, considerando o resultado dos testes, eventuais circunstâncias de mudança e o compromisso com uma melhoria contínua.

COMENTÁRIOS DE 9.5.3

No contexto da melhoria contínua, a organização pode adquirir conhecimento em novas tecnologias e práticas relacionadas à GCN, incluindo novas ferramentas e técnicas, que devem ser avaliadas para estabelecer seus benefícios à organização.

9.5.4 A análise crítica pode ser realizada por meio de auditorias internas ou externas, ou auto-avaliações. A freqüência e a periodicidade destas análises críticas podem ser influenciadas por leis e regulamentações, dependendo do tamanho, natureza e situação legal da organização. Também podem ser influenciadas por necessidades das partes interessadas.

Convém que uma auditoria ou auto-avaliação do programa de GCN da organização verifique se:

a) 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;

b) a política de GCN da organização, suas estratégias, estrutura e planos refletem precisamente suas prioridades e requisitos (os objetivos da organização);

c) 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;

d) as soluções de GCN da organização são efetivas, atualizadas e adequadas, além de apropriadas ao nível de risco enfrentado pela organização;

e) os programas de manutenção e testes de GCN da organização foram efetivamente implementados;

f) as estratégias e planos de GCN incorporam as melhorias identificadas durante os incidentes e testes e no programa de manutenção;

g) a organização tem um programa contínuo de treinamento e conscientização de GCN;

h) os procedimentos de GCN foram efetivamente comunicados à equipe relevante e se esta equipe entende seus papéis e responsabilidades;

i) os processos de controle de alterações estão implementados e funcionam de forma eficaz.

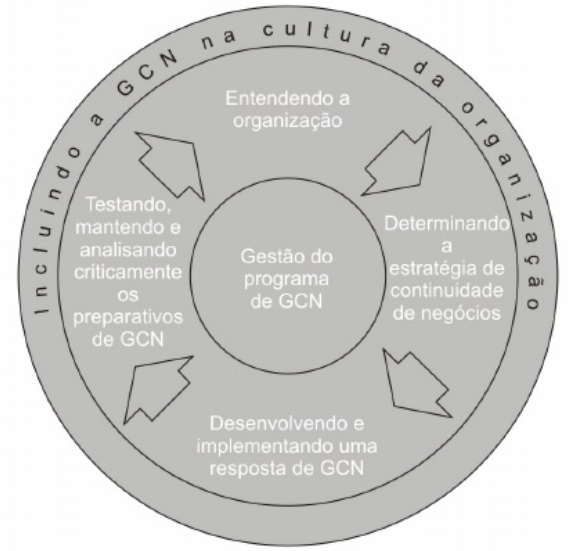
9.6 Auditoria

Convém que a organização providencie uma auditoria independente para avaliar sua competência de GCN e sua capacidade de identificar falhas reais e potenciais. Convém que a organização estabeleça, implemente e mantenha procedimentos para lidar com a auditoria independente. Convém que auditorias independentes sejam conduzidas por pessoas competentes, sejam elas internas ou externas.

9.7 Auto-avaliação

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

10 Incluindo a GCN na cultura da organização



Para obter sucesso, a continuidade de negócios precisa se tornar parte da gestão da organização, independentemente de seu tamanho ou setor. Em cada estágio do processo de GCN, existem oportunidades de se introduzir e melhorar a cultura de GCN da organização.

10.1 Geral

O desenvolvimento, promoção e incorporação da cultura de GCN na organização garantem que a GCN se tornará parte dos valores básicos e da gestão da organização.

Uma organização com uma cultura positiva de GCN irá:

a) desenvolver um programa de GCN com mais eficiência;

b) passar confiança às partes interessadas (especialmente funcionários e clientes) quanto à sua habilidade de gerenciar interrupções de negócios;

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

d) minimizar a probabilidade e o impacto das interrupções.

O desenvolvimento de uma cultura de GCN é suportado por:

a) liderança dos níveis superiores da organização;

b) atribuição de responsabilidades (ver 5.2);

c) conscientização;

d) desenvolvimento de habilidades; e

e) planos de testes.

COMENTÁRIOS DE 10.1

A criação e inclusão de uma cultura de GCN na organização pode ser um processo longo e de difícil execução e pode encontrar um nível de resistência maior que o esperado. O entendimento da cultura atual da organização ajuda no desenvolvimento de um programa de cultura de GCN.

Toda a equipe deve entender que a GCN é de alta relevância para a organização e que cada um possui papel importante na manutenção da entrega de produtos e serviços aos clientes, em caso de incidente.

10.2 Conscientização

Convém que a organização tenha um processo para identificar e implementar os requisitos de conscientização de GCN e para avaliar a eficiência desta implementação.

Convém que a equipe de GCN esteja consciente quanto às informações externas de GCN. Isso pode ser realizado em conjunto com uma busca por informações junto a serviços de emergência, autoridades locais e agências reguladoras.

Convém que a organização crie, aumente e mantenha uma consciência por meio da educação permanente em GCN e de um programa de informações para toda a equipe.

Esse programa deve incluir:

a) um processo de consulta junto a toda a equipe sobre a implementação do programa de GCN;

b) discussão de GCN nos informativos, apresentações, programas ou reportes diários da organização;

c) inclusão da GCN nas páginas pertinentes da web ou da intranet;

d) aprendizado por meio de incidentes internos ou externos;

e) GCN como um tópico nas reuniões de equipe;

f) testes de planos de continuidade em locais alternativos, por exemplo, um local de recuperação; e

g) visitas a esses locais alternativos.

A organização deve estender seu programa de conscientização de GCN para seus fornecedores e outras partes interessadas.

COMENTÁRIOS DE 10.2

Criar e manter uma consciência quanto à importância da GCN com toda a equipe da organização é importante para garantir que todos entendam o motivo da importância da GCN para a organização. Deve ser mostrado que a GCN é uma iniciativa duradoura que tem o apoio permanente da alta direção.

10.3 Treinamento

Convém que a organização possua um processo para identificar e implementar os requisitos de treinamento de GCN e para avaliar a eficiência desta implementação.

Convém que a organização treine:

a) a equipe de GCN para tarefas como:

   — gestão do programa de GCN,

   — execução de uma análise de impacto nos negócios,

   — desenvolvimento e implementação de PCN,

   — execução de um programa de testes de PCN,

   — avaliação de riscos e ameaças, e

   — comunicação com a mídia;

b) o pessoal não relacionado diretamente à GCN que necessite de habilidades específicas para desempenhar seu papel em respostas a incidentes ou recuperação de negócios.

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

Bibliografia

[1] ABNT NBR ISO 9000, Sistemas de gestão da qualidade – Fundamentos e vocabulário

[2] ABNT NBR ISO/IEC 27001, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação*

[3] ISO/IEC 20000 (both parts), *Information technology – Service management*

[4] *Requirements PAS 77, IT Service Continuity Management*