GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

IPPF – Guia Prático

Gestão de Continuidade de Negócios

Tradução ao Português Patrocinada pela:

FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

The Institute of Internal Auditors

Global Technology Audit Guide (GTAG)

Redigida em linguagem clara de negócios para abordar uma questão tempestiva relativa ao gerenciamento, controle ou segurança da TI, a série GTAG serve como pronto recurso para *chief audit executives* sobre diferentes riscos associados à tecnologia e práticas recomendadas.

Controles de Tecnologia da Informação: Os tópicos discutidos incluem conceitos de controle de TI, a importância dos controles de TI, os papéis e responsabilidades organizacionais para garantir controles eficazes de TI e técnicas de análise e monitoramento de riscos.

Controles de Gestão de Mudanças e *Patches*: descreve as fontes de mudança e seu possível impacto sobre os objetivos do negócio, além de como os controles de gestão de mudanças e *patches* ajudam a gerenciar os riscos e custos de TI e o que funciona e não funciona na prática.

Auditoria Contínua: Aborda o papel da auditoria contínua no ambiente de auditoria interna atual; a relação de auditoria contínua, monitoramento contínuo e avaliação contínua; e a aplicação e implementação da auditoria contínua.

Gerenciamento da Auditoria de TI: Discute os riscos relacionados à TI e define o universo de auditoria de TI, bem como a forma de executar e gerenciar o processo de auditoria de TI.

Gerenciando e Auditando os Riscos de Privacidade: Discute princípios e estruturas globais de privacidade, modelos e controles dos riscos de privacidade, o papel dos auditores internos, as dez principais perguntas de privacidade a serem feitas durante o curso de uma auditoria e mais.

Gerenciando e Auditando Vulnerabilidades de TI: Entre outros tópicos, discute o ciclo de vida do gerenciamento de vulnerabilidades, o escopo de uma auditoria de gerenciamento de vulnerabilidades e as métricas para mensurar as práticas de gerenciamento de vulnerabilidades.

Terceirização da Tecnologia da Informação: Discute como escolher o fornecedor terceirizado de TI correto e as principais considerações de controle de terceirização sobre a operação do cliente e sobre a operação do prestador de serviços.

Auditando Controles de Aplicativos: Aborda o conceito de controle de aplicativos e sua relação com os controles gerais, além de como definir o escopo de uma revisão de controle de aplicativos baseada em riscos.

Gestão de Identidades e Acessos: Abrange os principais conceitos relacionados à gestão de identidades e acessos (*identity and access management* – IAM), riscos associados ao processo de IAM, orientações detalhadas sobre como auditar processos de IAM e uma amostra de checklist para auditores.

Desenvolvendo o Plano de Auditoria de TI: Fornece orientações passo a passo sobre como desenvolver um plano de auditoria de TI, desde a compreensão do negócio, a definição do universo de auditoria de TI e a realização de uma avaliação de riscos, até a formalização do plano de auditoria de TI.

Visite o site do The IIA em www.theiia.org/technology para baixar toda a série.

Gestão de Continuidade de Negócios

Autores

David Everest, Key Bank

Roy E. Garber, Safe Auto Insurance Co.

Michael Keating, Navigant Consulting

Brian Peterson, Chevron Corp.

Julho de 2008

Copyright © 2008 The Institute of Internal Auditors, 247 Maitland Ave., Altamonte Springs, FL 32701-4201, EUA. Todos os direitos reservados. Impresso nos Estados Unidos da América. Nenhuma parte desta publicação pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma por qualquer meio — eletrônico, mecânico, fotocópia, gravação ou outro — sem a permissão prévia por escrito do editor.

O The IIA publica este documento para fins informativos e educacionais. Este documento destina-se a fornecer informações, mas não substitui a consultoria jurídica ou contábil. O The IIA não fornece tais conselhos e não oferece qualquer garantia quanto a quaisquer resultados jurídicos ou contábeis por meio da publicação deste documento. Quando surgirem problemas jurídicos ou contábeis, deve-se procurar e manter assistência profissional.

Índice

1. SUMÁRIO EXECUTIVO....5

2. INTRODUÇÃO....7
2.1 Definição de BCM....7
2.2 Planejamento de Gestão de Crises....7
2.3 Recuperação de Desastres de TI....7

3. ELABORANDO UM CASO DE NEGÓCIOS....8
4. Riscos do Negócio....9
4.1 Cenários Comuns de Desastres....9
4.2 Impactos Comuns de Desastres....10

5. REQUISITOS DE BCM....11
5.1 Apoio da Administração....11
5.2 Avaliação de Riscos e Mitigação de Riscos....12
5.3 Análise de Impacto Sobre os Negócios....14
5.4 Estratégia de Recuperação e Continuidade de Negócios....15
5.5 Recuperação de Desastres para TI....16
5.6 Conscientização e Treinamento....18
5.7 Manutenção do Programa de BCM....18
5.8 Exercício de Continuidade de Negócios....19
5.9 Comunicações da Crise....22
5.10 Coordenação com Agências Externas....22

6. RESPOSTA A EMERGÊNCIAS....24

7. GESTÃO DE CRISES....25

8. CONCLUSÃO/RESUMO....26

9. ANEXO....27
9.1 Amostra de Guia de Auditoria de BCM....27
9.2 Normas e Diretrizes de BCM....27
9.3 Modelo de Maturidade da Capacidade de BCM....28

10. GLOSSÁRIO....37

11. SOBRE OS AUTORES....38

1. Sumário Executivo

A maioria dos profissionais de negócios concordaria que, no decorrer da condução de um negócio bem-sucedido, os executivos corporativos passam bastante tempo analisando o mercado, desenvolvendo e implementando estratégias, estabelecendo metas financeiras e de desempenho, desenvolvendo e executando planos de operações de negócios, reportando resultados financeiros e se comunicando com os stakeholders. A maioria também concordaria que, antes da preparação mundial para o ano 2000, a gestão de continuidade de negócios (*business continuity management* – BCM) não estava necessariamente no topo da lista de prioridades de todos os executivos corporativos. Embora os desastres na história recente tenham aumentado a conscientização sobre os riscos de continuidade de negócios (BC) e seu impacto sobre as finanças e operações corporativas, ainda há empresas que não deram ouvidos aos sinais de alerta e estão despreparadas para um desastre ou uma interrupção de seus negócios. Interrupções naturais e causadas pelo homem podem ser imprevisíveis, mas seu impacto pode ser gerenciado, se um programa eficaz de BCM fizer parte do framework geral de governança corporativa.

O objetivo da BCM é permitir que a organização restaure processos críticos de negócios depois que um desastre for declarado. A BCM é uma simples questão de gerenciamento de riscos, projetada para criar recursos de continuidade de negócios para cada risco provável com base no valor comercial. Existem empresas grandes, médias e pequenas que não se prepararam adequadamente para os incidentes que poderiam tornar seus negócios ou parte de seus negócios inoperáveis inoperantes por um longo período de tempo. Casos documentados demonstram como empresas ou indústrias inteiras sofreram danos financeiros significativos, devido à falta de preparação para desastres imprevistos, incluindo a indústria de companhias aéreas dos EUA após os ataques terroristas de 11 de setembro de 2001; o TfL (*Transport for London*) após os atentados de Londres; e a indústria da pesca comercial no Sri Lanka e na Tailândia após o tsunami em 2004. Danos a uma organização podem incluir a perda de clientes, lucros, reputação, licenças/aprovações governamentais, etc. A falta de preparação expõe a empresa a um grau de risco que é relativo para cada tipo de negócio.

Seja por conta das desacelerações econômicas em uma indústria, falta de uma gestão informada ou outras decisões de custos corporativos, os defensores dos programas de BCM, como os *chief audit executives* (CAEs), muitas vezes têm suas recomendações à gerência executiva sobre melhorias na BCM ignoradas ou adiadas para um futuro distante. O CAE tem a responsabilidade de reportar as deficiências de BCM à administração e ao comitê de auditoria do conselho, por exemplo, quando uma auditoria ou outro meio de descoberta revelar que a administração não pode fornecer evidências para garantir que, no caso de um desastre declarado, as operações e sistemas comerciais serão recuperados de uma maneira que atenda aos objetivos comerciais, financeiros e operacionais da organização, com base na probabilidade de eventos disruptivos.

Este *Global Technology Audit Guide* (GTAG) foi escrito com uma compreensão da perspectiva do CAE. Os CAEs foram desafiados a educar os executivos corporativos sobre os riscos, controles, custos e benefícios da adoção de um programa de BCM. Embora os desastres recentes em todo o mundo tenham motivado alguns líderes corporativos a dar atenção aos programas de BCM, outros falharam em reconhecer e/ou abordar esse risco. O principal desafio é fazer com que os executivos corporativos tornem a BCM uma prioridade. Na superfície, qualquer executivo é capaz de expressar que a BCM é uma boa ideia, mas quando se trata de agir, alguns terão dificuldade de encontrar o orçamento necessário para financiar o programa, bem como um patrocinador executivo que tenha tempo para garantir seu sucesso. Este guia ajudará o CAE a conscientizar sobre o risco de continuidade dos negócios e a apoiar a administração no desenvolvimento e manutenção de um programa de BCM.

Como mostrado na Figura 1, o CAE deve entender o papel da BCM como um dos três elementos de um Programa de Gestão de Emergência (Observação: O termo Programa de Gestão de Emergência pode ser usado globalmente em vários setores governamentais e empresariais, mas não é necessariamente

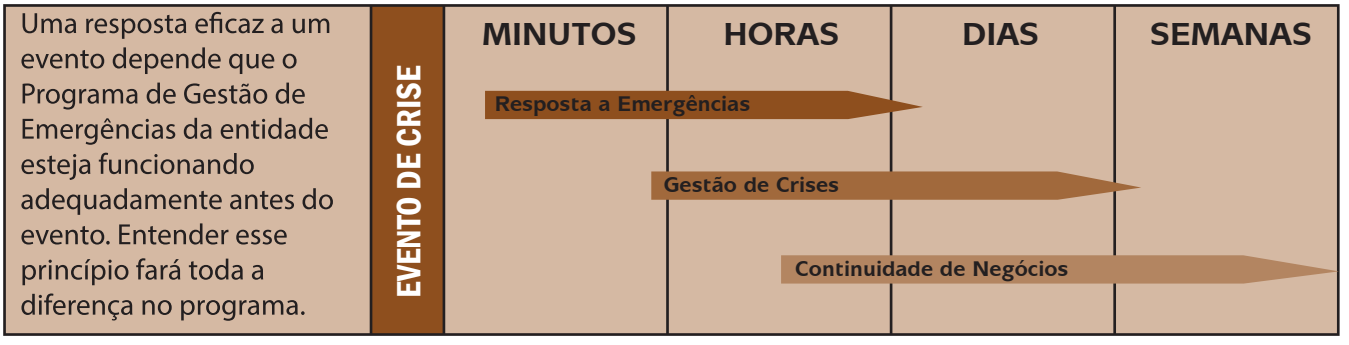

Figura 1. Programa de Gestão de Emergências

um termo profissional padrão). A Resposta a Emergências (*emergency response* – ER) é a primeira ação que busca evitar, dissuadir e prevenir desastres e preparar a organização para reagir a um desastre. O objetivo da ER é salvar vidas, garantir a segurança e realizar esforços iniciais para limitar o impacto de danos aos ativos. A gestão de crises (*crisis management* – CM) busca gerenciar as comunicações externas – e, em algumas empresas, internas – e as atividades da alta administração durante um desastre. Mesmo em um ambiente em que a ER e a CM são maduras e eficazes, a BCM pode permanecer inadequada. Os recursos de BCM estão focados na recuperação dos processos críticos do negócio, para minimizar os impactos financeiros e outros impactos causados a um negócio durante um desastre ou interrupção comercial. A BCM deve ser integrada à ER e à CM, mas deve ser um programa separado.

O ponto principal é que o CAE deve ser capaz de responder a três perguntas simples e importantes relacionadas à continuidade do negócio:

1. A liderança da organização compreende o nível atual do risco de continuidade de negócios e os possíveis impactos dos prováveis níveis de perda?
2. A organização pode comprovar que os riscos de continuidade dos negócios são mitigados a um nível aceitável aprovado e que são recertificados periodicamente?
3. Se existe um risco inaceitável de continuidade de negócios, mas a gerência executiva decidiu assumir o risco, os proprietários, parceiros de negócios e outros constituintes da organização sabem que a administração decidiu não reduzir o risco? Além disso, a decisão de aceitar o risco foi devidamente documentada?

Se a resposta a qualquer uma dessas perguntas for "não", esse GTAG poderá ajudar. Especificamente, este guia tem como objetivo ajudar os CAEs a entender o programa, os riscos e os controles da BCM e prepará-los com informações para as discussões no nível executivo e do conselho. Este GTAG agrega valor por meio da apresentação de um resumo de alto nível, em linguagem clara de negócios para leitores executivos, e orientações detalhadas para auditores internos em avaliações de auditoria. Esse GTAG se concentra em como a BCM, como programa ou estrutura, é projetada para permitir que os líderes empresariais gerenciem o nível de risco que a organização poderia encontrar, se ocorresse um evento disruptivo natural ou causado pelo homem que afetasse a ampla operacionalidade da organização. O guia inclui um planejamento para recuperação de desastres (disaster recovery planning – DRP) para a continuidade da infraestrutura crítica de tecnologia da informação e dos sistemas de aplicativos de negócios, porque muitas funções de negócios são predominantemente automatizadas. Isso ajudará o CAE a estabelecer a base para a condução de uma avaliação eficaz e para reportar as principais informações aos stakeholders.

2. Introdução

Esse GTAG descreve o conhecimento necessário para membros de órgãos governamentais, executivos e auditores internos, para abordar a eficácia dos recursos de recuperação de negócios e o impacto que eles têm sobre os negócios. Outros profissionais também podem achar as orientações úteis e relevantes. Este guia fornece informações relacionadas à avaliação dos recursos da BCM e descreve as diferentes partes de um programa abrangente e como estabelecer o plano correto para uma organização.

2.1 Definição de BCM

A gestão de continuidade de negócios é o processo através do qual uma organização se prepara para futuros incidentes que poderiam comprometer a missão central da organização e sua viabilidade a longo prazo. Tais incidentes incluem eventos locais como incêndios em edifícios, eventos regionais como terremotos ou eventos nacionais como doenças pandêmicas. Os principais componentes da BCM são:

- **Apoio da Administração** – A administração deve demonstrar seu apoio à preparação, manutenção e prática adequadas de plano de continuidade de negócios (*business continuity plan* – BCP), por meio de alocação dos recursos, pessoas e fundos orçados adequados.
- **Avaliação de Riscos e Mitigação de Riscos** – Os riscos em potencial devido a ameaças como incêndios, inundações, etc., devem ser identificados e a probabilidade e possível impacto sobre o negócio devem ser determinados. Isso deve ser feito no nível do local e da divisão, para garantir que os riscos de todos os eventos críveis sejam compreendidos e adequadamente gerenciados.
- **Análise de Impacto Sobre os Negócios (*business impact analysis* – BIA)** – A BIA é usada para identificar processos de negócios que sejam essenciais para manter a unidade de negócios em funcionamento durante um desastre e para determinar em quanto tempo esses processos integrais devem ser recuperados após um desastre.
- **Estratégia de Recuperação e Continuidade de Negócios** – Essa estratégia aborda todas as etapas, pessoas e recursos verdadeiramente necessários para recuperar um processo de negócios crítico.
- **Conscientização e Treinamento** – A educação e a conscientização do programa de BCM e dos planos de BC são fundamentais para a execução do plano.
- **Exercícios** – Os funcionários devem participar regularmente dos exercícios agendados do programa de BCM e dos planos de BC.
- **Manutenção** – Os recursos e a documentação de BCM devem ser mantidos para garantir que permaneçam eficazes e alinhados com as prioridades do negócio.
-

2.2 Planejamento de Gestão de Crises

O planejamento da gestão de crises aborda como a entidade corporativa informará o público em geral, a seus funcionários e diversos stakeholders sobre a crise e as medidas que estão sendo tomadas para colocar o negócio em funcionamento novamente. A CM consiste em métodos usados para responder tanto à realidade quanto à percepção das crises, documentadas em um plano de CM. A CM também envolve estabelecer métricas para definir quais cenários constituem uma crise e, consequentemente, desencadear os mecanismos de resposta necessários. Consiste na comunicação que ocorre dentro da fase de resposta dos cenários de gestão de emergências.

2.3 Recuperação de Desastres de TI

A recuperação de desastres de componentes de tecnologia da informação (TI) apoia a restauração de operações críticas para a retomada dos negócios, incluindo a recuperação do acesso a dados (registros, hardware, software, etc.), comunicações (e-mail, telefone, etc.), espaço de trabalho e outros processos de negócios após um desastre. Um plano de recuperação de desastres bem estabelecido e plenamente testado deve ser desenvolvido em harmonia com o plano de BCM, para aumentar a probabilidade de recuperar com sucesso os registros vitais da organização.

3. Elaborando um Caso de Negócios

A preparação para emergências não é mais a única preocupação de empresas localizadas em áreas propensas a terremotos ou tornados do mundo. A preparação deve, agora, levar em consideração desastres provocados pelo homem, como ataques terroristas, além de pandemias e desastres naturais. Saber o que fazer durante uma emergência é uma parte importante de estar preparado e pode fazer toda a diferença quando cada segundo conta. O objetivo da preparação é retomar as operações de negócios com a maior transparência possível, do ponto de vista do cliente. Exemplos de eventos catastróficos recentes que afetam grandes e pequenas empresas incluem:

- O surto mundial de SARS (novembro de 2002 a julho de 2003) consistiu em 8.096 casos infectados confirmados e 774 mortes. A quase pandemia causou um grande declínio de clientes nos restaurantes de culinária chinesa na América do Norte, com uma queda de 90% em alguns casos. A maioria das conferências e convenções agendadas nas principais cidades foi cancelada. Além disso, a intervenção do governo interrompeu as funções normais de negócios (ex., viagens, cadeia de fornecimento, etc.) para muitas empresas em países com infecções confirmadas.
- Os ataques terroristas de 11 de setembro de 2001 contra o Pentágono e o World Trade Center foram os ataques mais devastadores contra os EUA desde o bombardeio de Pearl Harbor. Além de perturbar os processos militares, os ataques de 11 de setembro também tiveram como alvo os processos civis e as empresas dos EUA.
- Os atentados de 7 de julho de 2005 em Londres foram uma série de explosões planejadas por terroristas no sistema de transporte público de Londres. Os ataques, responsáveis por mais de 50 mortes e 700 feridos, afetaram seriamente o sistema de transporte público de Londres, bem como o sistema de telecomunicações móveis do país.
- O furacão Katrina (formado em 23 de agosto de 2005) pode ser o desastre natural de maior custo da história dos EUA. Pelo menos 1.836 pessoas perderam a vida no furacão e nas inundações subsequentes. O Katrina causou danos estimados em US$ 81,2 bilhões, incluindo danos significativos a instalações industriais (principalmente petróleo, refinaria e produtos químicos), comerciais (principalmente de hospitalidade) e agrícolas.

Desde 1983, agências reguladoras, como a *American Bankers Association* e o *Banking Administration Institute*, exigiram que seus membros contribuintes executassem práticas de continuidade operacional (posteriormente apoiadas por manuais mais formais de BCP) que protegem o interesse público. As normas mais recentes foram frequentemente baseadas em normas formalizadas definidas sob o ISO/IEC 25002.

Muitas vezes, o valor de um programa de BCM não é apreciado até que seja necessário. Talvez seja porque é difícil calcular o retorno sobre o investimento de um programa de BCM até que um desastre ocorra. A gerência precisa entender que, se tal situação ocorrer, os negócios devem continuar, mas sob circunstâncias muito diferentes. O custo de um desastre pode ser o fim do negócio. Os líderes empresariais precisam ponderar o custo de se preparar contra o custo de fechar as portas do negócio por uma semana, um mês ou para sempre, dependendo da catástrofe. Muitos governos ao redor do mundo exigem que certas indústrias tenham um BCP testado em vigor. Nos Estados Unidos, todas as empresas dos setores financeiro, de serviços públicos e de saúde são obrigadas a manter um BCP atualizado. Existem normas e diretrizes gerais e específicas do setor para uma BCM eficaz (consulte o Anexo: Normas e Diretrizes de BCM, na página 27).

Durante o primeiro ataque ao World Trade Center, em 1993, a Morgan Stanley (MS) aprendeu uma lição importante. Nenhum dos funcionários da MS perdeu a vida, mas foram necessárias quatro horas para que todos os funcionários evacuassem o prédio. Como resultado, a gerência decidiu que o BCP precisava ser atualizado. A MS examinou atentamente as suas operações comerciais e o risco de possíveis desastres e desenvolveu um novo plano. Em 11 de setembro de 2001, o planejamento compensou. Depois que o primeiro avião sequestrado colidiu com a primeira torre do World Trade Center, a segurança da MS evacuou todos os funcionários. A evacuação levou apenas 45 minutos, permitindo que a MS continuasse a recuperar as operações diárias. As melhorias nos recursos de ER provavelmente salvaram inúmeras vidas. Os recursos de BCM também foram aprimorados como parte da revisão.

4. Riscos do Negócio

Desastres naturais acontecem em todo o mundo regularmente. Furacões, inundações, terremotos e incêndios destroem vidas e devastam empresas. Desastres provocados pelo homem, como incêndios, falhas de energia e terrorismo, não são menos destrutivos. Juntos, esses eventos imprevistos representam riscos para as operações normais dos negócios. Às vezes, as consequências financeiras persistem por anos. Algumas empresas nunca voltam ao que eram antes e outras simplesmente vão à falência. No entanto, esses resultados podem ser evitados em quase todos os casos.

Quase todos os locais do mundo estão em uma zona de perigo de furacões, tornados, terremotos, incêndios florestais e/ou inundações. Incêndios podem tomar conta de um edifício em qualquer cidade, em qualquer estado. Da mesma forma, o terrorismo pode ocorrer em qualquer parte do mundo.

4.1 Cenários Comuns de Desastres

Desastres comuns experimentados em todo o mundo incluem: O **incêndio** pode ocorrer em um único edifício comercial, complexo ou instalação industrial, ou em uma área inteira próxima a uma floresta. A cada ano, mais de 4.000 cidadãos dos EUA morrem e mais de 20.000 são feridos em incêndios, muitos dos quais poderiam ter sido evitados. A perda direta de propriedade devido a incêndios é estimada em US$ 10 bilhões por ano (somente nos Estados Unidos), o que não inclui a perda financeira que as empresas sofrem pela interrupção de suas operações.

A **pandemia** é um surto de doença global. Uma pandemia de gripe ocorre quando emerge um novo vírus influenza A, para o qual há pouca ou nenhuma imunidade na população humana. Em seguida, ele começa a causar doenças graves e se espalha facilmente de pessoa para pessoa. Muitos governos ao redor do mundo começaram a se planejar para pandemias. Eles identificaram setores críticos de infraestrutura nacional, como: finanças, bancos, energia, transporte, governo, etc. Estão pedindo a essas indústrias que preparem planos de BC para garantir que as funções críticas dos negócios continuem em operação durante uma pandemia. O impacto econômico de uma pandemia pode ser devastador, devido à indisponibilidade de funcionários, o que pode levar à suspensão das funções de negócios. Se ocorrer uma pandemia, é provável que seja um surto prolongado e generalizado, o que pode exigir mudanças temporárias em muitas áreas da sociedade, como escolas, escritórios, transporte e outros serviços públicos. Um público informado e preparado pode tomar medidas apropriadas para diminuir seu risco durante uma pandemia.

O **terrorismo** é o uso de força ou violência contra pessoas ou bens, em violação das leis criminais dos países do mundo todo para fins de intimidação, coerção ou resgate. Os terroristas costumam usar ameaças para:

- Provocar medo no público.
- Tentar convencer os cidadãos de que seu governo é incapaz de impedir o terrorismo.
- Obter publicidade imediata por uma causa.

Atos de terrorismo incluem ameaças de terrorismo, assassinatos, sequestros, ameaças de bombas e bombardeios, ataques cibernéticos (por computador) e o uso de armas químicas, biológicas, nucleares e radiológicas. Ataques terroristas devastaram grandes áreas metropolitanas, interromperam negócios nessas áreas gerais e tiveram grande impacto sobre os níveis de estruturação de equipe das empresas na região afetada.

Ataques biológicos são a liberação deliberada de germes ou outras substâncias biológicas que podem deixar as pessoas doentes. Muitos agentes devem ser inalados, entrar através de um corte na pele ou ser ingeridos para fazer efeito. Alguns agentes biológicos, como o antraz, não causam doenças contagiosas. Outros, como o vírus da varíola, podem resultar em doenças que podem ser transmitidas através do toque, da tosse, etc. Um ataque químico é a liberação deliberada de um gás tóxico, líquido ou sólido, que pode envenenar as pessoas e o meio ambiente. A ameaça de um ataque biológico pode ter um impacto devastador sobre uma empresa (ex., evacuação das instalações), mesmo que não haja um ataque real.

Tornados são as tempestades mais violentas da natureza. Eles podem aparecer sem aviso e ficar invisíveis até que poeira e detritos sejam captados ou até que surja uma nuvem funil. Embora tornados sejam mais comuns em certas áreas do mundo, eles podem ocorrer em qualquer lugar e em qualquer época do ano, tornando a preparação com antecedência especialmente importante. Os tornados podem danificar instalações de negócios e levar à indisponibilidade de funcionários.

Furacões/tufões são tempestades tropicais severas, que se formam em águas tropicais ou subtropicais no mundo todo. Os cientistas já podem prever muitos ciclones tropicais. Organizações localizadas em comunidades costeiras ou nas proximidades afetadas por ciclones devem planejar uma evacuação, o que pode prejudicar significativamente suas operações.

Inundações são desastres naturais comuns em muitas partes do mundo. No entanto, as inundações não são iguais. Algumas podem se desenvolver lentamente, durante um longo período de chuva, ou em uma tendência de calor após uma forte nevasca. Outras, como enchentes, podem ocorrer rapidamente, mesmo sem sinais visíveis de chuva. A maior parte do mundo precisa estar preparada para inundações, mas principalmente em áreas baixas, perto da água ou a jusante de uma represa. Mesmo um riacho muito pequeno ou o leito de um córrego seco pode transbordar e criar inundações. A inundação pode interromper a disponibilidade da equipe, mesmo que a instalação comercial principal não seja diretamente afetada.

Os Custos Crescentes dos Desastres Naturais

Embora desastres naturais tenham causado danos ao longo da história, há fortes indícios de que se tornaram mais frequentes e severos nas últimas décadas e que essa tendência ascendente deva continuar. Em parte, essa tendência pode ser explicada pela crescente urbanização, que levou a uma concentração crescente da população em áreas vulneráveis (veja Freeman, Keen e Mani, 2003). Também reflete as mudanças nos padrões climáticos – em especial, aqueles associados com o aumento das temperaturas da superfície global – que parecem ter aumentado a frequência e a intensidade de eventos climáticos adversos, como furacões, inundações e secas (veja IPCC, 2007). Com desastres naturais mais frequentes e intensos, que afetam áreas cada vez mais densamente povoadas, seus custos aumentaram fortemente ao longo do tempo (veja abaixo).

	1950-59	1960-69	1970-79	1980-89	1990-99	1996-2005
Número de eventos	21	27	47	63	91	57
(em bilhões de dólares; preços constantes de 2005)						
Perdas gerais	48.1	87.5	151.7	247.0	728.8	575.2
Perda média2	2.8	3.2	3.2	3.9	8.0	10.1

Figura 2. Os Custos Crescentes dos Desastres Naturais[1]

4.2 Impactos Comuns de Desastres

Vários desastres que ocorrem comumente podem resultar na perda de:

- **Pessoas.** Se houver grande perda de vidas humanas ou indisponibilidade significativa de pessoal, as organizações podem não ter o pessoal adequado para executar as operações diárias.
- **Instalações e equipamento.** Vários dos desastres descritos têm o potencial de destruir ou danificar gravemente as instalações operacionais, fábricas, escritórios e outros locais críticos para o negócio.
- **Infraestrutura de comunicação.** As organizações podem não conseguir se comunicar com seus funcionários, fornecedores e clientes.
- **Suprimentos.** Isso pode incluir o fornecimento de energia, os serviços de fornecedores, suprimentos de produção, etc.
- **Informação e sistemas de TI.** Aplicativos comerciais críticos podem não funcionar corretamente.

[1] David Hoffman, "*Innovations in insurance can help countries manage the fiscal impact of natural disasters,*" revista *Finance & Development*, março de 2007, Vol. 44, No. 1.

5. Requisitos de BCM

A Figura 3 mostra as ações necessárias para atender aos requisitos de BCM.

5.1 Apoio da Administração

O apoio da administração é fundamental para o sucesso da BC em todas as organizações. A alta administração deve garantir que existam políticas em vigor que exijam que as equipes de gestão de toda a organização implantem um programa de BCM

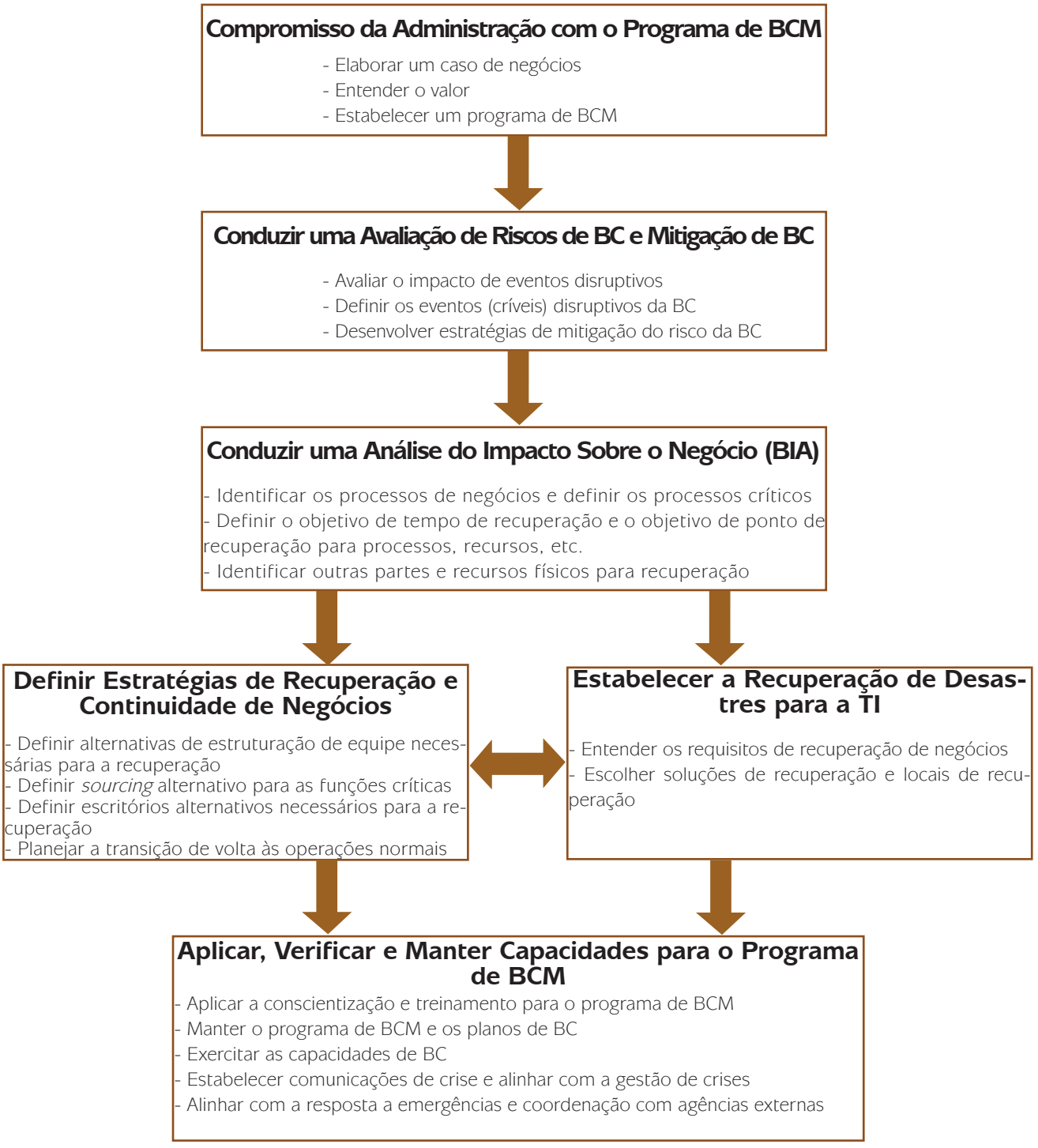

Figura 3. Fluxograma de Requisitos de BCM

para suas unidades de negócios. Todas as políticas de gestão de emergência devem estar alinhadas, para garantir que a CM, a ER e a BCM trabalhem juntas durante um desastre real.

A. Apoio da Alta Administração

A alta administração deve demonstrar apoio visível à BCM e ao programa de gestão de emergência. Isso pode ser feito de diversas formas, inclusive por:

- Definição de um grupo central dentro da organização responsável pelas atividades de BCM e de gestão da governança (ex., definição da padronização necessária), compartilhamento de conhecimentos, coordenação de melhores práticas, consultoria e atividades de BCM entre as unidades de negócios.
- Criação de um sistema de BCM que cada unidade de negócios (business unit – BU) deva implantar.
- Garantia de financiamento adequado para as atividades de BCM de toda a organização, por meio do plano de negócios anual da organização, testando e garantindo que as BUs incluam financiamento para seus esforços de BCM.
- Comunicação da importância da BCM e como ela agrega valor aos negócios.
- Participação em exercícios de BC, sessões de treinamento e outros eventos de gestão de emergência.

O sistema de BCM que cada BU deve implantar deve incluir:

- Uma definição de BCM e seu valor comercial dentro da empresa.
- Uma descrição das etapas necessárias para implantar e manter um programa de BCM em uma BU.
- O estabelecimento da propriedade da BCM em cada BU (consulte "Apoio da Gerência da Unidade de Negócios" a seguir).
- A definição das métricas de BCM que podem ser usadas para avaliar o progresso do programa no nível da organização e na BU ou no nível regional (por exemplo, cada BU cria suas próprias métricas locais).
- Implantação de um programa de qualidade contínua de BCM, que possa ser atualizado por cada BU para implantar e manter a BCM.

B. Apoio da Gerência da Unidade de Negócios

- A gerência da BU ou regional também deve demonstrar apoio visível à BCM e ao programa de gestão de emergência. Isso pode ser feito de diversas formas, inclusive por:
- Implantação do sistema de BCM definido pela organização.
- Garantia de participação de todas as equipes da BU nos esforços de BCM, para que criem recursos de BC que correspondam a seu risco e valor comercial.
- Identificação de alguém para participar das atividades de governança de BCM da organização (ex., definir a padronização necessária), compartilhamento de conhecimentos, coordenação de melhores práticas, consultoria e atividades de BCM entre as unidades de negócios.
- Comunicação da importância da BCM e como ela agrega valor aos negócios.
- Participação em exercícios de BC, sessões de treinamento e outros eventos de gestão de emergência da BU.
- Garantia de financiamento adequado para as atividades de BCM da BU, através do plano de negócios anual da BU.

Ao implantar o sistema de BCM, a BU ou a gerência regional deve:

- Atualizar a seção de definição de BCM, para definir o valor comercial específico da BU.
- Entender as etapas necessárias para implantar e manter um programa de BCM em uma BU.
- Estabelecer a propriedade da BCM na BU, incluindo alocar pessoas para funções-chave, como patrocinador de BCM da BU (para obter financiamento e atuar na liderança de BCM), gerente de BCM da BU (para liderar e manter as capacidades de BCM) e coordenador de BCM da BU (para organizar as atividades de BCM sob a direção do gerente de BCM).
- Definir métricas de BCM para a BU que possam ser usadas para avaliar o progresso do programa.
- Implantar um programa de qualidade contínua da BCM para a BU.

5.2 Avaliação de Riscos e Mitigação de Riscos

A gerência da BU ou regional deve realizar uma avaliação de riscos de BC para cada uma das suas funções de negócios e locais associados (cidade ou região). O objetivo deste exercício é identificar riscos prováveis que poderiam interromper os processos críticos do negócio realizados em locais específicos de operação. A avaliação de riscos de BC é usada para moldar o escopo geral do programa de BCM, fornecendo uma lista de eventos prováveis e consequências associadas que devem ser abordados em um plano de mitigação de riscos (ex., prevenção) e no programa de BCM. Não há como prever todos os riscos ou mitigar todos os riscos conhecidos que talvez precisem ser aceitos. Os participantes da avaliação de riscos de BC devem incluir indivíduos, como funcionários da empresa, além de funcionários dos departamentos de saúde, segurança e meio ambiente; gestão de instalações; jurídico; recursos humanos; e pessoal da área médica.

É *muito provável* que ocorram alguns eventos disruptivos, como furacões e/ou falhas de serviços essenciais em algumas partes do mundo, ou outros eventos que ocorram regularmente. Planos táticos específicos de BC podem ser necessários para esses eventos previsíveis. A maioria dos eventos é *relativamente provável* de ocorrer, como terremotos. Embora um terremoto ocorra em algumas regiões, há uma boa chance de afetar outra parte da região mais ampla. Portanto, se o local das operações estiver em uma zona sísmica, isso deve

ser considerado um evento disruptivo provável, o que é geralmente chamado de *evento crível.*

É impossível erradicar todos os riscos de um ambiente e ainda executar operações eficazes. O equilíbrio é a chave para o gerenciamento de riscos de BC. Ao avaliar eventos disruptivos, é importante identificar aqueles que são críveis e buscar todos os possíveis eventos que possam afetar as operações de negócios. Possíveis métodos para prever futuros eventos disruptivos incluem:

• Observar dados históricos associados a organizações semelhantes na mesma região.
• Usar dados do governo ou do setor sobre possíveis riscos.
• Recorrer a especialistas no assunto, quando o modelo de negócios mudar ou quando dados limitados estiverem disponíveis para realizar uma avaliação de riscos detalhada.

A. Exemplos de Eventos Disruptivos

Abaixo, estão alguns exemplos de eventos disruptivos que podem afetar processos críticos de negócios.

- Desastres naturais, como terremotos, furacões, chuva/inundação e raios.
- Eventos industriais, como incêndios, explosões, derramamentos e contaminações.
- Falhas dos fornecedores, como interrupções no fornecedor de componentes e serviços essenciais de eletricidade.
- Outras catástrofes, como acidentes de avião.
- Epidemia médica, como uma pandemia ou outros riscos médicos.
- Interrupções trabalhistas, incluindo greves, interrupção dos transportes e conflitos civis.
- Instabilidade econômica ou política, incluindo terrorismo/bombardeios e guerra.
- Fatores humanos, como erros de funcionários, atos criminosos e fraudes.
- Riscos de TI, como terrorismo cibernético, vírus, ataques de hackers e ataques de negação de serviço.
- Riscos de produção e fabricação, tais como:
  - Interrupções nos fornecedores, incluindo energia, materiais brutos e serviços críticos.
  - Falha de equipamentos de produção em oleodutos, caldeiras e correias transportadoras.
  - Indisponibilidade de serviços de utilidade pública, como estações de tratamento e equipamentos de descarte.
  - Falhas de armazenamento, transporte e distribuição de produtos.
  - Indisponibilidade de processos críticos de laboratório, testes e/ou controle de qualidade.
  - Falhas no sistema de automação de processos (sistemas de TI, como SCADA e DCS) que parem a produção.
  - Atrasos do governo em licenças, alfândega, visto de funcionários e/ou certificação.

B. Avaliando o Impacto de Eventos Disruptivos

Depois de identificar os eventos críveis que possam afetar cada um dos locais ou regiões de operação da organização, é necessário um esforço adicional para entender o evento. Alguns dos fatores que devem ser avaliados para entender melhor o escopo e o impacto do evento em potencial incluem:

- **A extensão geográfica do impacto:** Um único edifício (ex., incêndio), complexo inteiro de instalações (ex., derramamento químico), área metropolitana (ex., greve de transporte), região ampla (ex., terremoto) ou possivelmente o mundo (ex., gripe pandêmica).
- **Dias de impacto:** O número de dias antes que as operações provavelmente retornem 75% da funcionalidade, o que significa que 75% das pessoas, recursos e produção estão funcionando. Os dias de impacto podem ser o período após o qual a organização poderá substituir os recursos perdidos, como alugar um novo prédio e torná-lo funcional após um incêndio no prédio.
- **Disponibilidade de pessoal (em dias):** Porcentagem da equipe que provavelmente seria capaz de trabalhar com base em cada evento provável de catástrofe (em dias: 0, 3, 7, 14 ou 30). A equipe pode precisar voltar para casa por um longo período, no caso de alguns desastres, como terremotos, que podem danificar as residências.
- **Disponibilidade de operações e/ou escritórios:** Porcentagem provável de operações e/ou espaço funcional de escritório (durante os dias de impacto).
- **Disponibilidade de TI (durante os dias de impacto):** Disponibilidade provável dos principais componentes de TI para cada evento de desastre. Isso inclui a infraestrutura de TI (recursos de logon), rede de TI, aplicativos de TI, etc.

A avaliação de riscos de BC pode ser usada para determinar o impacto sobre os processos críticos de negócios. Algumas instalações operacionais, como escritórios de pesquisa e desenvolvimento, podem ter poucos processos críticos de negócios realizados no local. A avaliação de riscos de BC para todos os locais deve se concentrar, no mínimo, na saúde e segurança da equipe, na segurança geral e nos possíveis impactos ambientais, para garantir que as funções de CM e ER tenham os recursos necessários para obter êxito.

C. Desenvolvimento de Estratégias de Mitigação de Risco

O desenvolvimento e a implementação de estratégias de mitigação de riscos de BC ajudarão a minimizar o impacto de eventos disruptivos e melhorarão as capacidades de resposta. Exemplos de riscos e suas estratégias de mitigação correspondentes incluem:

- **Riscos de segurança de diversos desastres:** Alavancar a ER e/ou a equipe de saúde, segurança e meio ambiente e/ou planos operacionais.
- **Falhas operacionais:** Alavancar os procedimentos operacionais padronizados e as atividades normais de

manutenção.

- **Perda do escritório principal:** Organizar a transferência de funcionários para um escritório alternativo ou permitir que eles trabalhem de casa, supondo que sua residência seja funcional (ou seja, não esteja danificada, se o evento for regional e a residência tiver recursos necessários como equipamentos, computador, conexão de rede, etc.)
- **Perda de conectividade de rede:** Desenvolver planos de recuperação de sistemas TI e de informações (recuperação de desastres) para criar redundância ou recuperação de rede.
- **Perda do data center de TI:** Desenvolver um plano para executar manualmente os processos de trabalho até que os sistemas de TI possam ser restaurados. Além disso, desenvolver planos de recuperação de desastres de TI para restaurar os sistemas de TI em locais alternativos.

O patrocinador de BCM e uma equipe adequada de gerentes devem revisar e aprovar as estratégias de avaliação e mitigação do risco de BC. Visto que a administração deve agir para lidar com os riscos, é essencial que a administração aprove a avaliação de riscos de BC e garanta que o plano de mitigação do risco de BC seja financiado, implementado e testado periodicamente.

5.3 Análise de Impacto Sobre os Negócios

Uma BIA é usada para identificar processos críticos de negócios que precisem ser recuperados após um evento de desastre. A BIA pode incluir uma discussão inicial sobre as soluções de recuperação necessárias para retomar os processos críticos de negócios (consulte "Estratégia de Recuperação e Continuidade de Negócios", na página 15). Os participantes da BIA devem incluir funcionários da empresa, bem como principais fornecedores. A BIA deve ser realizada com o conhecimento da avaliação de risco de BC que definiu os eventos críveis que poderiam prejudicar o negócio. Normalmente, as reuniões da BIA são realizadas individualmente para cada equipe. Então, ocorrem discussões com outras equipes identificadas como prestadoras críticas após cada reunião da BIA.

A. Identificando os Processos de Negócios

O primeiro passo em uma BIA é identificar os processos de negócios executados pela equipe funcional, os recursos necessários para executar a função e a equipe crítica que executa o trabalho. Os processos comerciais não devem ser divididos inicialmente em subprocessos individuais excessivos. Os processos de negócios devem ser identificados separadamente, se tiverem equipes diferentes (ex., papéis da equipe), prestadores de serviços (ex., externos, terceirizados, etc.) ou recursos (ex., sistemas de TI).

B. Determinando o RTO e o RPO com Base no Impacto Sobre os Negócios

A segunda etapa de uma BIA é identificar o tipo de impacto sobre os negócios, se o processo de negócios não puder ser executado. Abaixo, estão alguns tipos de impactos sobre os negócios:

- Saúde e segurança (ex., lesão).
- Ambiental (ex., derramamento).
- Atendimento ao cliente (ex., perda de clientes).
- Financeiro (ex., penalidades).
- Regulatório/jurídico (ex., ação governamental).
- Reputação (ex., prejuízo à imagem).

Em seguida, determine um objetivo de tempo de recuperação (*recovery time objetive* – RTO) com base nos tipos de impacto sobre os negócios. Um RTO é um período de tempo e de nível de serviço dentro do qual um processo de negócios deve ser restaurado (após um desastre), para evitar consequências inaceitáveis associadas à disrupção da continuidade. Um RTO é normalmente identificado com base em marcadores de tempo padronizados de 0, 3, 7, 14 ou 30 dias. A

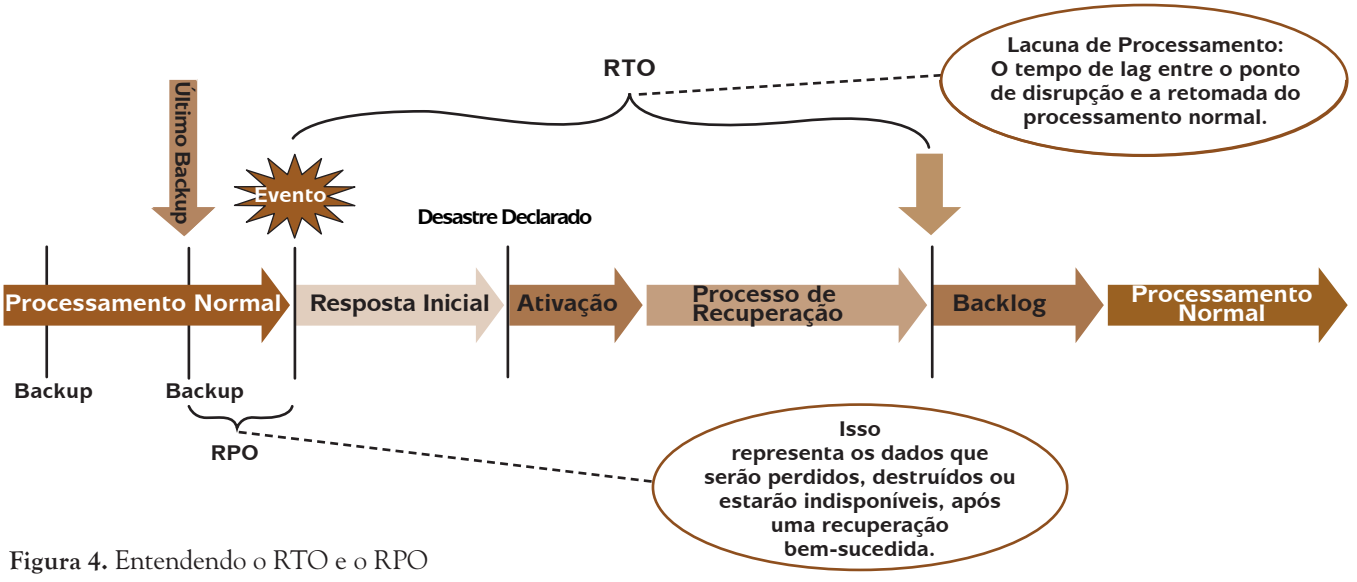

Figura 4. Entendendo o RTO e o RPO

administração do negócio determina, em última instância, o RTO correto para cada processo de negócios. Normalmente, o custo da solução de recuperação aumenta à medida que o RTO diminui (ou seja, se o processo de negócios precisar ser restaurado imediatamente, o custo poderá ser muito alto).

Em seguida, determine um objetivo de ponto de recuperação (*recovery point objective* – RPO) para sistemas de informação. O RPO é a quantidade de dados que pode ser perdida se um desastre destruir os sistemas de informação. A equipe de negócios deve determinar quantos dias de dados podem ser razoavelmente perdidos e recriados manualmente. Os dados geralmente podem ser recriados a partir de outras fontes, como sistemas externos que trocam dados com o sistema da organização (ex., sistemas bancários). Em última análise, a administração do negócio determina o RPO correto para cada processo de negócios. Normalmente, o custo da solução de recuperação aumenta à medida que o RPO diminui (ou seja, se o processo de negócios não puder perder qualquer dado, o custo da replicação de dados poderá ser muito caro).

C. Identificando as Outras Partes e Recursos Físicos

A terceira etapa da BIA é identificar as outras partes e os recursos físicos que são críticos para o processo de negócios, o que poderia incluir outros departamentos, fornecedores, terceiros, equipamentos críticos e registros físicos. Uma BIA pode precisar ser executada com a participação de outras partes que apoiem os processos críticos de negócios, para garantir que estejam preparadas para dar apoio à recuperação de negócios.

D. Obtendo a Aprovação da BIA pelo Patrocinador e Gerente

O patrocinador e os gerentes de BCM de cada equipe devem revisar e aprovar a BIA para seu escopo de operações. Como os gerentes de toda a organização são responsáveis por garantir que as soluções de continuidade e recuperação de negócios sejam implementadas, eles devem ser os proprietários da BIA em sua equipe.

5.4 Estratégia de Recuperação e Continuidade de Negócios

Estratégias de recuperação e continuidade de negócios devem ser desenvolvidas para os processos críticos de negócios identificados durante a BIA. A BIA pode incluir uma discussão inicial sobre as soluções de recuperação necessárias para retomar os processos críticos de negócios (consulte "Análise de Impacto Sobre os Negócios", na página 14). Os participantes da reunião estratégica de recuperação e continuidade de negócios podem incluir funcionários da empresa, principais fornecedores e organizações de sistemas de informação.

As estratégias de recuperação e continuidade de negócios podem incluir alguns dos seguintes tipos de soluções:

- **Processos de trabalho manual:** O trabalho pode ser feito manualmente, enquanto os sistemas de TI estiverem inativos.
- **Terceirização:** Alguns trabalhos podem ser executados por empresas externas, concorrentes (acordo recíproco) ou fornecedores secundários.
- **Recuperação de desastres para TI:** Uma solução de recuperação de TI será necessária para os sistemas críticos, mas como isso pode ser muito caro, os processos de trabalho manual podem ser usados inicialmente após um desastre.
- **Estruturação de equipe alternativa:** Identifique outros membros da equipe que possam desempenhar a função do cargo.
- **Instalações alternativas:** Identifique instalações alternativas nas quais a equipe principal possa trabalhar.

Ao desenvolver estratégias de recuperação e continuidade de negócios, os eventos críveisidentificados durante a avaliação de riscos de BC devem ser considerados, juntamente com seus possíveis impactos sobre os recursos. As opções de instalações alternativas podem ser muito limitadas para desastres regionais, como furacões, que poderiam impactar as instalações da organização e as residências dos funcionários ao mesmo tempo.

A. Atividades de Recuperação de Estruturação da Equipe

Como a estruturação de equipe limitada é um resultado provável para a maioria dos eventos críveis, o recrutamento de equipes alternativas é sempre necessário para a BC. A melhor opção é identificar pessoas externas à provável área impactada, com base nos eventos críveis. Se não houver pessoas externas à área, considere aumentar os níveis de estruturação de equipe na região primária. Se for assumido que 80% da equipe não estará disponível se ocorrer um desastre, considere quantas pessoas serão necessárias para realizar um determinado trabalho e multiplique esse número por cinco:

- Se uma pessoa é necessária para realizar o trabalho, identifique cinco pessoas que poderiam fazer o trabalho.
- Se duas pessoas forem necessárias para realizar o trabalho, identifique 10 pessoas que poderiam fazer o trabalho; e assim por diante.

Os profissionais que normalmente executam o trabalho podem saber outras maneiras de executar os processos críticos de negócios. Essas opções podem incluir a execução manual das funções do trabalho, o que já pode ser feito ocasionalmente quando os sistemas estiverem inativos. Outras opções podem incluir o uso da equipe existente em outro local, se a equipe principal não estiver disponível. Algumas funções podem ser terceirizadas, se necessário.

B. *Sourcing* Alternativo de Funções Críticas

Considere diversas opções em que o trabalho seja executado por um prestador externo. Avalie o nível de consistência e de qualidade que é necessário para cada função crítica. Em

um desastre, a organização pode ser capaz de funcionar com produtos e serviços de padrão industrial que não atendam às especificações exatas da organização. Outra opção é terceirizar o trabalho interno para outros fornecedores. Muitas funções podem ser realizadas externamente por diversas empresas que prestem serviços padronizados. Considere estabelecer um acordo recíproco com concorrentes, se houver altos custos de capital ou funções regulamentadas que sejam executadas consistentemente por diversas empresas.

Muitos dos riscos identificados durante a BIA podem incluir fornecedores de bens e serviços que são críticos para a cadeia de fornecimento geral da organização. Esses fornecedores podem fornecer matérias-primas críticas ou componentes usados para fabricar produtos ou usados na embalagem, armazenamento ou distribuição dos produtos. Termos contratuais podem ser usados para garantir que os principais fornecedores cumpram com suas obrigações, presumindo que o negócio continue em funcionamento. Fornecedores alternativos (diversidade de fornecedores) podem ser necessários, se o fornecedor principal falhar.

Outra opção é determinar como fornecer produtos no caso de uma falha completa na produção. A aquisição de produtos de concorrentes em um desastre pode ser uma opção, mas um acordo recíproco antecipado pode ajudar a controlar os custos. Outra opção é priorizar o atendimento ao cliente com base nos compromissos contratuais e, então, futuras oportunidades de negócios, etc. A identificação antecipada de alternativas de produção pode ajudar a maximizar a produção geral da empresa com base em diversos eventos de desastre. Os dados incluiriam a utilização de recursos, a produção de subprodutos e outros fatores que poderiam ser usados para otimizar a produção com base nos recursos e serviços (dos fornecedores e das concessionárias) disponíveis.

C. Escritórios Alternativos Necessários para Atividades de Recuperação

Podem ser necessários escritórios alternativos em quase todos os desastres que exijam a ativação do BCP. Há muitas opções para fornecer escritórios para a equipe, mas o custo dessas soluções varia muito. Abaixo, estão algumas das opções alternativas de escritório.

- Outra instalação da organização que fique fora da zona de desastre, mas perto do escritório principal, é geralmente uma solução de baixo custo. Isso exige que a unidade de negócios do escritório alternativo da organização aplique seu BCP para enviar para casa os funcionários que não forem críticos.
- Atualmente, muitas pessoas usam o acesso remoto para executar muitas funções relacionadas ao escritório a partir de casa ou de um hotel. O principal requisito é que os funcionários tenham as ferramentas de segurança adequadas (ex., token de acesso remoto) e hardware apropriado (ex., laptop ou computador pessoal) de que precisem para trabalhar remotamente. Ao avaliar as soluções de acesso remoto, o impacto sobre a produtividade deve ser considerado, especialmente no que se refere à falta de colaboração e comunicação, se a equipe estiver distribuída em diversos locais.
- Locais de recuperação comercial também oferecem escritórios, mas geralmente a altos custos e, geralmente, com conexões de rede limitadas aos sistemas de TI da organização.

Qualquer solução de escritório alternativo deve ser testada pelos usuários, para garantir que consigam fazer logon. Alguns testes de volume (desempenho) também devem ser realizados para verificar se a solução suportará o número desejado de usuários. A equipe não crítica deve ser instruída a não se conectar durante um desastre, para que os recursos permaneçam disponíveis para aqueles considerados críticos.

D. Planejando a Transição de Volta às Operações Normais

Um plano deve ser desenvolvido para fazer a transição da organização para um estado normal, depois que as soluções de recuperação não forem mais necessárias. Isso pode ser um desafio, porque a organização opera em estado anormal durante um desastre. Os dados coletados manualmente devem ser inseridos nos sistemas, assim que eles forem restaurados. Exceções financeiras e regulamentares que tenham ocorrido durante o desastre devem ser resolvidas, arquivando a documentação apropriada e obtendo as aprovações. As trocas de produtos (emprestados) que ocorreram durante o desastre precisam ser reabastecidas ou a outra parte deve ser paga por esses produtos.

O patrocinador de BCM e uma equipe apropriada de gerentes devem aprovar as estratégias de continuidade para seu escopo de operações. Como os gerentes de toda a organização são responsáveis por garantir que as soluções de continuidade e recuperação de negócios sejam implementadas, eles devem ser os proprietários das estratégias de continuidade em sua equipe.

5.5 Recuperação de Desastres para TI

Dependendo das funções de negócios que estão sendo executadas e de sua dependência de TI, parte dos processos críticos de negócios pode ser recuperada sem a TI ou sem informações. Em outros casos, são necessários sistemas e informações de TI para apoiar a recuperação de alguns processos críticos de negócios. Cada organização deve determinar o tempo de inatividade máximo dos sistemas de TI, antes que se torne um problema que poderia colocar em risco toda a organização, sejam horas, dias, semanas ou mais.

O *planejamento de recuperação de desastres* (*disaster recovery planning* – DRP) é um termo usado para descrever a recuperação de TI. Algumas empresas usam termos diferentes, para incluir a recuperação de sistemas de TI, dados, sistemas e processos de gestão de informações e outros sistemas relacionados. O documento de recuperação de desastres deve descrever as estratégias de recuperação dos sistemas de gestão de informações e TI. O DRP deve incluir instruções detalhadas de

recuperação, que podem incluir referências a procedimentos, referências de fornecedores, diagramas do sistema e outros materiais de recuperação relacionados. Os procedimentos detalhados de recuperação devem ser atualizados quando os processos do sistema e de negócios forem alterados.
Abaixo, estão alguns exemplos dos componentes que podem ser recuperados como parte do DRP.

- Sistemas de TI, incluindo:
  - O *data center* de TI.
  - Aplicações e dados necessários para a organização.
  - Servidores e outros hardwares.
  - Comunicações, como telefone, rádio, etc.
  - Rede, incluindo conexões externas (de terceiros).
  - Infraestrutura de TI (ex., serviços de logon e distribuição de software).
  - Serviços de acesso remoto.
  - Sistemas de controle de processos (ex., SCADA/DCS).
- Sistemas de gestão de informações, incluindo:
  - Salas de arquivos.
  - Sistemas de gestão de documentos (elétricos e manuais).

A. Considerações ao Escolher Estratégias de DRP

Há várias coisas a considerar ao escolher estratégias de recuperação de TI:

- O documento do DRP deve descrever as estratégias para recuperar sistemas e informações com base na orientação da equipe após seus membros terem realizado uma BIA.
- As capacidades de recuperação dos fornecedores críticos de serviços de TI e informações devem ser avaliadas, para garantir que atendam aos requisitos do negócio.
- A recuperação dos componentes de TI e de informações geralmente devem ser combinadas, para criar o sistema completo necessário para apoiar os processos críticos de negócios. Por exemplo, a recuperação de um aplicativo pode exigir a recuperação do aplicativo de desktop, do aplicativo do servidor, do hardware do servidor, do sistema operacional do servidor, dos servidores de infraestrutura, do *data center*, das conexões de rede de terceiros, etc.
- Os prestadores de serviços internos e externos de TI e serviços de informação devem descrever os serviços de recuperação que prestam, incluindo informações sobre:
  - As atividades de recuperação pelas quais o prestador de serviços é responsável e quaisquer limitações de recuperação que possam existir.
  - As atividades de recuperação (ex., reconstrução de dados perdidos) pelas quais a organização é responsável.
  - A maneira pela qual a organização e o prestador de serviços se comunicarão durante um desastre.
  - Contratos de terceiros (ex., prestadores de serviços de aplicativos) ou contratos de nível de serviço para o prestador interno.
  - O escopo de seus esforços de recuperação (ex., sistemas, dados, rede, etc.).
  - Sua estratégia de recuperação.
  - Seus RTOs e RPOs.
  - O custo de suas soluções de recuperação, serviços, testes e declaração de desastre.
  - A frequência de seus testes de recuperação.
- Componentes do ambiente podem ser recuperados usando soluções que normalmente não seriam usadas em um *data center* de produção. Por exemplo, alguns dados podem não ser recuperados inicialmente (ex., grandes bibliotecas de imagens), o que significa que não estariam disponíveis (ex., podem gerar mensagens de erro).
- Estratégias de recuperação para cada sistema ou componente de TI devem ser desenvolvidas independentemente, sem a necessidade de consistência com outros sistemas de TI. No entanto, é importante que os componentes que trabalhem juntos para formar um sistema sejam hospedados no mesmo local ou em vários locais que tenham largura de banda de rede suficiente. Por exemplo, os e-mails podem ser recuperados em um grande *data center* central, a replicação de arquivos pode ocorrer em outro local em um servidor dentro da região local, aplicativos e serviços (ex., engenharia) podem ser terceirizados temporariamente durante um desastre, a recuperação de aplicativos locais pode ser feita usando um PC, em vez de um servidor, etc. O objetivo é encontrar a melhor e mais econômica solução de recuperação para cada sistema, mesmo se as soluções estiverem espalhadas pelo mundo. O único requisito é que os sistemas estejam acessíveis para os usuários, independentemente de onde sejam recuperados, e que todos os componentes do sistema funcionem juntos.
- Os padrões de segurança e conformidade da informação precisam ser considerados ao projetar soluções de recuperação. As soluções de recuperação não devem introduzir níveis não razoáveis de segurança ou riscos de conformidade. Alguns controles de segurança e conformidade serão relaxados se ocorrer um desastre real, mas é necessária uma decisão consciente para entender os riscos que existem no ambiente de recuperação. As soluções de recuperação visam reduzir o risco associado à perda de disponibilidade, mas devem ser equilibradas com a necessidade de integridade e confidencialidade.

B. Soluções de Recuperação e Locais de Recuperação

A seguir, uma lista de soluções de recuperação e locais de recuperação comumente usados.

- Plano/capacidades de recuperação quentes.

  - Existe um plano de recuperação.
  - Os recursos de recuperação estão disponíveis no(s) local(is) de recuperação e os dados são sincronizados em tempo real, para permitir que o sistema seja recuperado imediatamente ou em questão de horas.
  - O tempo de recuperação típico é de minutos a um dia.
- Plano/capacidades de recuperação mornas.
  - Existe um plano de recuperação.
  - Recursos de recuperação (ex., sistemas de não produção, hardware de reposição, etc.) estão disponíveis no(s) local(is) de recuperação, mas podem precisar ser configurados para suportar o sistema de produção quando o desastre ocorrer.
  - Alguns dados podem precisar ser restaurados (provavelmente, a partir de fitas ou outros backups).
  - O tempo de recuperação típico é de dois a 13 dias.
- Plano/capacidades de recuperação frias.
  - Existe um plano de recuperação.
  - O(s) local(is) de recuperação foi(ram) identificado(s) com a infraestrutura básica e de espaço necessária para realizar a recuperação.
  - Os recursos de recuperação (ex., servidores) não estão disponíveis no(s) local(is) de recuperação e provavelmente precisam ser adquiridos.
  - Provavelmente, os dados precisam ser restaurados (provavelmente, a partir de backups em fita).
  - O tempo de recuperação típico é de 14 a 30 dias.
- Nenhum plano/recurso de recuperação.
  - Não há plano de recuperação.
  - Os recursos de recuperação e os processos de restauração de dados não foram definidos.
  - Existem planos de backup de dados para garantir que os dados críticos possam ser restaurados em algum momento no futuro.
  - Existe o risco de que os sistemas e processos de negócios que eles suportam nunca sejam recuperados ou possam resultar em uma recuperação demorada.

O patrocinador de BCM e uma equipe apropriada de gerentes devem aprovar as soluções de recuperação de TI para seu escopo de operações. Como os gerentes de toda a organização são responsáveis por garantir que as soluções de BC e de recuperação sejam implementadas, eles devem ser os proprietários das soluções de recuperação de TI em sua equipe.

5.6 Conscientização e Treinamento

A educação e a conscientização são eficazes na preparação da equipe para a recuperação. O treinamento de conscientização deve ser feito anualmente, no mínimo, para garantir que os membros da equipe compreendam suas funções de BC e as atividades de resposta a emergências em seu local ou região. O treinamento de CM, incluindo a tomada de decisões da equipe de liderança e a gestão das comunicações, também é de vital importância.

O programa de BCM exige diferentes níveis de conhecimento, com base no papel dos indivíduos participantes e nas estratégias de terceirização. Abaixo, estão alguns dos papéis e o nível de conhecimento necessário para cada função:

- O patrocinador de BCM deve:
  - Compreender os conceitos de BCM e a proposta de valor de BCM.
- O gerente de BCM deve:
  - Compreender a gestão de emergência (CM, ER, BCM).
  - Conquistar uma certificação *Certified Business Continuity Professional* (CBCP) da DRI International (DRII), do Business Continuity Institute (BCI) ou equivalente. (Essa qualificação é opcional para gerentes de BCM da unidade de negócios, mas é necessária para o gerente de BCM da organização como um todo.)
  - Criar programa e/ou implantação de processo de BCM (melhor se estiver alinhado com a metodologia da organização, como eficiência operacional, segurança e/ou outros processos relacionados).
- Os coordenadores de BCM devem:
  - Possuir forte conhecimento da metodologia do processo de BCM da organização (normalmente, entregue por meio da organização ou por treinamento externo).
- O consultor de BCM (interno ou externo) deve:
  - Obter um certificado CBCP ou *Master Business Continuity Professional* (MBCP) da DRII, BCI ou equivalente.
  - Ter vasta experiência na realização de: avaliação de risco de BCM, BIA, planejamento de recuperação, exercícios, etc.
- A equipe de BCM deve:
  - Compreender os conceitos de BCM e a proposta de valor de BCM.
  - Compreender os procedimentos de comunicação de emergência.
  - Conhecer a ER para seu local ou região.

Os exercícios são o principal método de treinamento da equipe para a execução real dos planos de recuperação e de suas funções, bem como para a identificação de lacunas e fraquezas. Consulte “Exercício de Continuidade de Negócios” (na página 15) para obter uma descrição dos diferentes tipos de exercícios.

5.7 Manutenção do Programa de BCM

Um dos obstáculos mais comuns que impedem as organizações de atingir a prontidão da BC é a negligência. Frequentemente, as organizações investem muito tempo e dinheiro no desenvolvimento de planos que nunca são mantidos a partir de então. Como qualquer plano operacional, os planos de BC e de CM atrofiam ao longo do tempo e se tornam menos

eficazes à medida que mudanças nas prioridades de negócios, pessoas, processos, tecnologia e ambiente operacional deixam de corresponder aos planos. Em alguns casos, a "manutenção" limita-se a alterar as datas de um plano sem alterar o conteúdo. Em todos os casos, o foco do grupo de auditoria interna deve ser a manutenção da capacidade de BC/CM, e não simplesmente a atualização de um documento.

Algumas técnicas para avaliar a manutenção de BC incluem:

- Avaliar o histórico de alterações do documento, para determinar se as atualizações do documento são registradas.
- Revisar os requisitos de manutenção, para garantir que a manutenção do componente seja atribuída a indivíduos específicos e que a administração fornece orientações que permitam que os indivíduos sejam eficientes na manutenção dos recursos de BC.
- Revisar as premissas de BC, para garantir que estejam bem alinhadas com os requisitos operacionais atuais. As premissas de BC devem mudar para abordar novas questões, como locais adicionais, novas concentrações de riscos (ex., um novo cenário de desastre se torna crível), confiança em terceiros novos/diferentes ou operações em novos países.
- Revisar as mudanças nas premissas de BC, para garantir que cada mudança seja fundamentada.
- Revisar a data da BIA, para garantir que a base dos planos de BC seja atual o suficiente para fornecer orientações adequadas.
- Entrar em contato com os responsáveis pelas tarefas do plano, para determinar sua compreensão dos requisitos e seu nível de confiança de que possam ter bom desempenho. Em muitos casos, as pessoas citadas nos planos (especialmente em planos que existem há vários anos) são simplesmente substitutos de seus predecessores, mas que não receberam o mesmo treinamento de quando o programa de BCM e/ou o plano de BC foi inicialmente apresentado.
- Revisar a estrutura/configuração do documento de BC, para determinar com que precisão ele reflete o modelo e a estrutura organizacionais atuais.
- Verificar palavras como "atual" e "hoje" e avaliar se o conteúdo associado realmente reflete a organização, especialmente se o documento estiver disponível eletronicamente.
- Revisar os resultados de exercícios/testes e seus relativos relatórios de ações para as exceções (ex., lacunas) que exigem correção.
- Avaliar o programa de BCM e as capacidades de recuperação de BC, para garantir que tenham sido atualizados para corrigir as lacunas necessárias e que tenham sido implementados de forma eficaz.

5.8 Exercício de Continuidade de Negócios

Exercícios, ou testes, são geralmente considerados a maneira mais eficaz de manter um programa de BCM e planos de BC atualizados e executáveis. Algumas organizações diferenciam os termos *exercício* e *teste*, mas não há necessidade de usar esses termos em circunstâncias específicas. Independentemente do vernáculo, a prioridade dos testes do plano deve

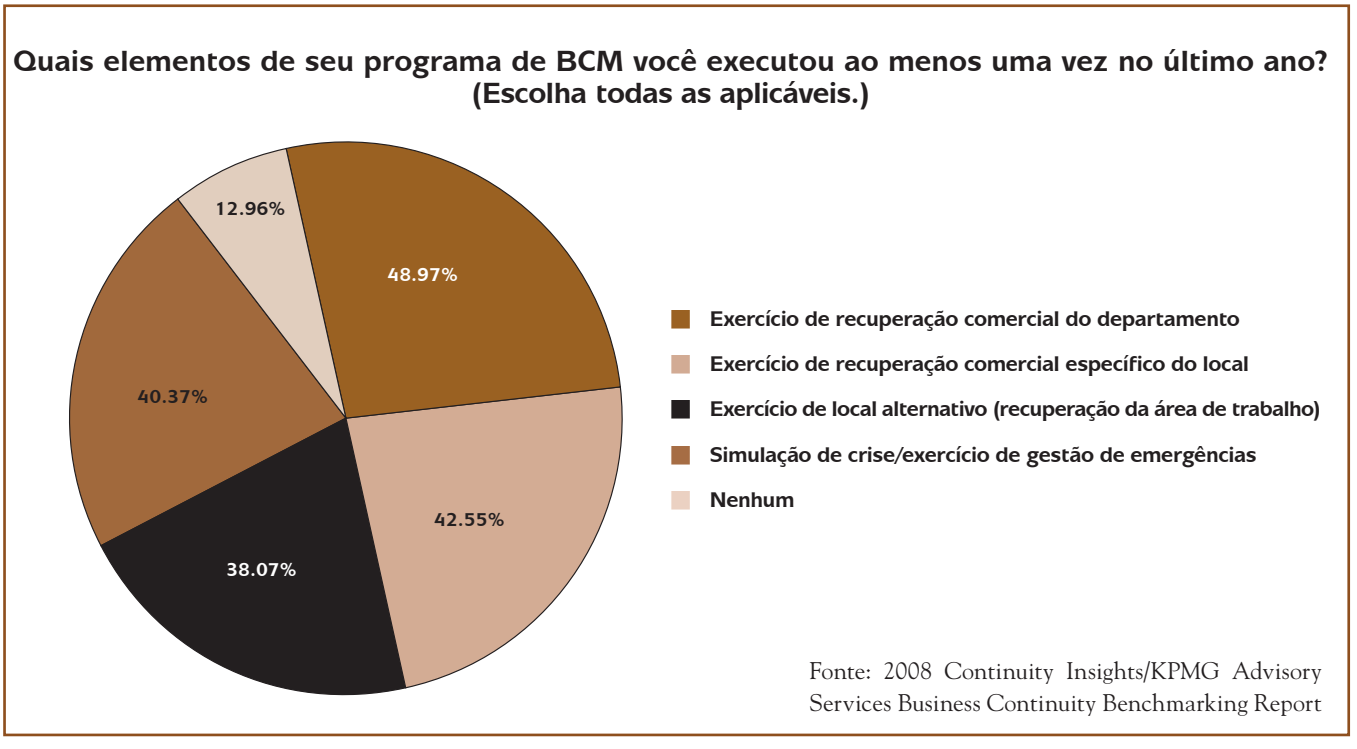

Figura 5. Executando os Elementos do Programa de BCM

ser melhorar o desempenho da organização em um evento real. É importante notar que existem muitos tipos de exercícios que, quando usados apropriadamente, podem fornecer segurança e agregar valor. Todos as principais normas de BC exigem que algum tipo de exercício/teste faça parte do programa de BCM. Geralmente, um exercício de grande escala dos programas de BCM e planos de BC deve ser realizado pelo menos anualmente. Testes mais frequentes podem ser necessários para ambientes complicados e de grande impacto (ex., perda) para a organização. Também devem ser programados diversos testes de componentes, em intervalos regulares ao longo do ano.
Os requisitos de exercício/teste devem ser documentados no próprio plano ou na política de BCM no nível da entidade.

A maioria das normas usadas para governar os programas de BCM exige três elementos básicos para um regime de testes:

- Os testes devem ser realizados em intervalos periódicos. O período real entre os eventos é determinado pelo Comitê Diretivo de BCM e é baseado nas metas e objetivos do programa.
- Os testes devem abordar uma variedade de ameaças/cenários e diferentes elementos dentro do programa de BCM. É possível abordar essas questões em uma série de exercícios anuais amplos ou através de testes em locais mais específicos ou testes no nível do componente.
- Deve haver algum método para rastrear problemas e lacunas descobertos no teste e para rastrear sua resolução.

A. Tipos de Exercícios

Tipo de Exercício	Descrição e Objetivos
Teste de Mesa ou Auditoria do Plano	Este é o tipo menos invasivo de exercício/teste, geralmente ainda considerado um teste. O teste de mesa normalmente envolve apenas o proprietário do plano e talvez uma terceira parte desinteressada. O objetivo desse tipo de esforço é simplesmente garantir que o conteúdo do plano não esteja desatualizado (ex., informações de contato) e que o impulso geral do plano ainda seja relevante. Normalmente, inclui uma leitura simples de página a página e a atualização do próprio plano. **Objetivos:** • Garantir que os membros da equipe sejam precisos. • Garantir que os números de contato internos e externos estejam atualizados.
Orientação ou Passo-a-Passo do Plano	Especialmente após a recente adoção ou aprimoramento significativo de um plano de BC ou CM, é útil repassar o passo-a-passo do documento informalmente, com aqueles de quem se espere sua implantação. O esforço incluiria uma reunião de equipe facilitada por um líder de equipe designado. Normalmente, esse tipo de evento de baixa intensidade não constitui um "teste" em termos dos requisitos da política de BCM de uma organização. **Objetivos:** • Garantir que os membros da equipe entendam seus papéis novos/atualizados. • Garantir que os membros da equipe entendam o conteúdo e o formato básico do plano.
Exercício *Tabletop* (Exercício no Estilo *Boardroom*)	Em muitos casos, é útil reunir toda a equipe de BC/CM para uma sessão, para trabalhar de forma colaborativa em um cenário realista, para identificar desafios e criar um bom relacionamento ao resolvê-los juntos. Geralmente, esses exercícios duram de duas a quatro horas e são facilitados pelo gerente de BC/CM ou por um terceiro independente. O esforço conclui com uma crítica formal do exercício, detalhando se os objetivos pré-estabelecidos para o exercício foram atingidos e delineando lacunas descobertas no evento, com um cronograma de remediação, bem como os próximos passos a serem realizados. **Objetivos:** • Ajudar os membros da equipe a entender a importância de seus papéis e responsabilidades. • Enxergar o benefício de resolver desafios de continuidade/crise como uma equipe. • Identificar as lacunas específicas de planejamento/treinamento nas áreas funcionais.

Tipo de Exercício	Descrição e Objetivos
Teste de Comunicação	A comunicação é um componente chave do processo de BCM. Na verdade, a falha em se comunicar com precisão com os principais stakeholders é uma causa frequente de respostas a crises malsucedidas. Esses testes variam muito, dependendo do escopo do planejamento de comunicação e do nível de automação usado no processo de comunicação de crise. As empresas que implantaram uma ferramenta de notificação em massa usufruem de um benefício duplo em seu exercício: avaliar o desempenho da ferramenta e expor os participantes a como a notificação será recebida. Normalmente, esse tipo de evento envolve, na verdade, entrar em contato com parceiros de negócios e funcionários, e não simplesmente revisar as informações da lista de contatos. **Objetivos:** • Validar as informações de contato dos principais stakeholders. • Treinar os participantes sobre como usar a notificação em massa e qualquer papel que eles tenham na resposta. • Configurar corretamente as ferramentas de notificação em massa. • Identificar lacunas/gargalos de comunicação, onde a comunicação tempestiva possa falhar em um evento.
Passo-a-Passo do Ambiente de TI (Sistemas e Aplicativos)	Este teste envolve a realização de uma simulação de desastre, anunciada ou não anunciada, e a execução de procedimentos documentados de recuperação de sistemas. Muitos ambientes de TI são extremamente complicados e os planos podem ser construídos em torno da recuperação de aplicativos ou sistemas específicos, em vez de recuperar todas as perdas do *data center*. Nessas circunstâncias, testar a perda de um *data center* pode ser altamente perturbador e caro. Um passo-a-passo bem projetado pode ser um exercício eficaz para reunir os diferentes envolvidos da única forma que possa ser feita na prática. **Objetivos:** • Verificar se os sistemas e dados críticos podem ser recuperados em um evento de grande escala. • Determinar se os recursos internos em sistemas individuais ou planos de aplicativos são capazes de cumprir com suas responsabilidades, devido à perda de diversos sistemas/aplicativos. • Coordenar o uso de recursos de resposta/recuperação em diversos locais/linhas de negócios. • Garantir a adequação dos recursos de suporte (ex., recursos humanos, aquisições) à resposta de TI.
Teste de Local Alternativo	Esse teste de todos os componentes de restauração/recuperação em um local alternativo deve incluir um teste da capacidade da organização de realocar a equipe para o local alternativo, bem como uma validação de que os processos de recuperação e ativos de TI operam no local alternativo conforme projetado. **Objetivos:** • Demonstrar a capacidade real de continuar os principais processos no local alternativo. • Identificar se a privacidade, a segurança e os controles financeiros podem ser mantidos no ambiente operacional alternativo. • Treinar os participantes quanto a quaisquer procedimentos revisados, para concluir os principais processos no local alternativo. • Avaliar a suficiência e eficácia dos ativos de TI no local alternativo. • Garantir que o plano para transportar os funcionários seja razoável, com base nos prováveis cenários de desastres identificados na avaliação de riscos de BCM.
Teste *End-to-End*	Esse teste das instalações de locais alternativos deve incluir tanto negócios quanto TI. Um teste end-to-end é diferente de um teste de local alternativo, porque os fornecedores/parceiros de negócios críticos e clientes – internos ou externos – estão incluídos no escopo. Esse teste geralmente valida a conectividade com o local de produção da organização. **Objetivo:** • Demonstrar a capacidade de executar os processos críticos em um nível pré-determinado sem grandes problemas. Não é necessário demonstrar 100% de capacidade operacional em testes end-to-end; no entanto, a melhor prática seria atingir, como capacidade efetiva da estratégia de continuidade, as expectativas de desempenho presumidas ou documentadas no plano de continuidade.

B. Frequência dos Exercícios

Os executivos de auditoria interna muitas vezes se perguntam se há uma frequência "certa" de exercícios/testes para o programa de BCM. A frequência de exercícios, por si só, não é a resposta, porque realizar o mesmo teste duas vezes por ano levará rapidamente a resultados estagnados e participantes entediados. Como em muitas áreas de controle, a melhor prática geralmente aceita é que a frequência seja suficiente para garantir que o programa esteja se tornando progressivamente mais maduro. A maioria das organizações maduras testa os processos de continuidade de negócios uma ou duas vezes por ano; no entanto, isso pode ser aumentado por fatores como:

- • Mudanças nos processos de negócios.
- • Mudanças na tecnologia.
- • Uma mudança na equipe de BCP.
- • Eventos antecipados que possam resultar em uma possível interrupção nos negócios (ex., o início da temporada de furacões ou a percepção de que uma pandemia possa ser iminente).

Independentemente da frequência real dos exercícios/testes, o foco do CAE deve ser garantir que os exercícios/testes realizados contribuam para a melhoria contínua do programa.

5.9 Comunicações da Crise

O planejamento da comunicação de crise é uma parte integrante de um programa holístico de BCM e é mais frequentemente coordenado pela comunicação interna, relações públicas ou outro departamento com profissionais de comunicação. Planos de comunicação de crise, quando existem, abordam como gerenciar as mensagens de mídia após um evento de crise. Em todos os casos, o processo de comunicação de crise deve ser uma função subordinada ao processo geral de CM, em vez de um esforço autônomo.

Infelizmente, abordar a mídia é apenas uma pequena fração da quantidade de comunicações de crise que ocorrem em um evento real. Embora o contato com a mídia seja importante e muito público, falhas em elementos "menores" da comunicação de crise podem ser igualmente devastadoras se forem mal gerenciadas ou executadas.

Planos eficazes de comunicação de crise são projetados para comunicar de forma proativa uma mensagem integrada a vários stakeholders, de uma maneira que seja relevante para as audiências individuais. Pontos de comunicação relevantes para a comunidade financeira podem não ser tão relevantes para funcionários ou vizinhos; no entanto, a mensagem principal deve ser consistente. Embora seja impossível antecipar todos os aspectos das comunicações de crise a serem implementadas durante um evento, alguns públicos que devem ser abordados nos planos e nos esforços de preparação incluem:

- Membros da equipe de resposta da organização.
- Gerentes responsáveis pela continuidade das operações e pelo contato direto com os funcionários.
- Funcionários de linha cuja compreensão dos problemas mais amplos possa ser menos completa do que a da equipe de administração.
- Membros da família de funcionários, especialmente os familiares dos empregados diretamente impactados pelo evento ou pela resposta da organização.
- Mídia nacional, incluindo a mídia financeira, cujo interesse na organização esteja focado principalmente na gestão do evento atual.
- Mídia local, impressa e transmitida, que cubra a organização regularmente em uma ampla variedade de tópicos.
- Investidores, especialmente investidores institucionais, que desejem transparência nas consequências de curto e longo prazo de um incidente.
- Governos locais e estaduais/provinciais que estejam interessados na viabilidade a longo prazo da base tributária e outros benefícios que a organização traga para seus constituintes.
- Agências reguladoras responsáveis por garantir a conformidade contínua, mesmo quando operando em modo de recuperação.
- Vizinhos que possam ser afetados negativamente pelo evento, pela resposta da organização ou pelos esforços das autoridades para minimizar o impacto geral sobre a comunidade.

5.10 Coordenação com Agências Externas

Nenhum dos aspectos de BCM pode existir sozinho. Além de coordenar as várias disciplinas entre si, é imperativo que os pontos de coordenação com entidades externas sejam refletidos no processo de planejamento. As entidades governamentais estão interessadas em organizações do setor privado devidamente preparadas. Por exemplo, os Estados Unidos aprovaram a Lei Pública 110-53 em 2007, que determina a criação de um padrão voluntário de prontidão para emergências, por meio do qual as organizações do setor privado possam medir seus esforços para se preparar para uma crise. A *Civil Contingencies Act* do Reino Unido aborda as maneiras pelas quais as autoridades trabalharão de maneira diferente com o setor privado durante um estado de emergência. Outros governos têm leis similares que abordam suas expectativas de si mesmos e do setor privado durante uma crise. Não existe uma maneira "certa" para documentar cada um dos pontos de contato com essas agências externas, mas, no mínimo, o planejamento deve abordar as seguintes questões:

- Quais entidades governamentais devem ser contatadas no caso de um evento?
- Quais os limites da notificação obrigatória e em que circunstâncias a organização faria uma notificação voluntária?
- Quais as áreas de preocupação de cada agência e como elas serão diferentes ou semelhantes?
- Como a organização pode envolver as entidades governamentais durante o processo de planejamento ou exercício, para se beneficiar de sua experiência sem

comprometer a independência da organização?
- Quais são os requisitos do programa de BCM das agências reguladoras e como a organização comunica sua conformidade?
- Existem agências externas que devam revisar ou aprovar as estratégias de continuidade, como a produção temporária de produtos em uma instalação não certificada, a execução de funções reguladas em uma geografia separada ou a alteração do modo como as matérias-primas ou produtos prontos entram no país?
- Dentro da organização, quem fará o contato com cada entidade governamental e como?

Geralmente, a melhor forma de abordar essas e outras preocupações é garantir que a administração seja responsável pelo programa de BCM e esteja realmente conversando com as agências externas sobre esse tópico. O fato de as agências externas não terem comunicado suas expectativas em relação ao desempenho de BCM à administração não significa que elas não tenham expectativas. A comunicação e a coordenação antecipadas com essas entidades é um passo crucial para assegurar sua parceria durante um evento real.

6. Resposta a Emergências

A resposta a emergências é geralmente descrita como o planejamento tático e atividades práticas destinadas a proteger a vida e a propriedade imediatamente após algum tipo de evento. A maioria das nações industrializadas tem algum requisito para desenvolver planos de ER para organizações maiores e os requisitos específicos relacionados às indústrias são abundantes. Em muitos casos, as agências governamentais definem requisitos específicos, mas há muitas diretrizes de grupos setoriais nacionais ou internacionais que tratam de questões de ER. Alguns dos principais elementos de um programa de ER incluem:

- Planejamento e providências de evacuação.
- Protocolos de escalonamento.
- Avaliação e reporte de danos.
- Resposta de Hazmat e controle de derramamento.
- Resposta médica.
- Salvamento e recuperação.
- Questões especializadas, como brigadas de incêndio, primeiros socorros, resgate de alto ângulo ou em espaço confinado, etc.

Geralmente, não é solicitado que o CAE revise esse aspecto de prontidão como um item independente. Portanto, o aspecto essencial a ser abordado em qualquer revisão ou consulta de BCM são os níveis adequados de integração e cooperação com os recursos internos responsáveis pela ER. Como muitos eventos de BC começam com um esforço de ER, a falha na coordenação de planos e atividades não apenas impede a capacidade da organização de abordar todos os impactos imediatos de um evento, mas também dificulta o processo de tomada de decisões de longo prazo, ao omitir desnecessariamente uma informação importante sobre a origem e as características da interrupção.

Como muitos planos de ER concentram-se em questões de preservação da vida – quase à exclusão de quaisquer outras considerações –, um dos desafios comuns na coordenação dos esforços de continuidade e de emergência é determinar como os responsáveis podem incorporar as prioridades de cada um, sem prejudicar o foco principal. Essa é uma área em que a auditoria interna pode agregar valor, devido à sua neutralidade e abordagem consultiva. Na maioria dos casos, as equipes de BC podem usar as informações já coletadas por uma equipe de ER para otimizar os planos de BC e para melhor informar as equipes de ER sobre como suas ações afetam a resiliência operacional, financeira e a reputação da organização.

Organizações com necessidades significativas de ER, devido à natureza de suas operações, quase sempre empregam uma abordagem estruturada para gerenciar o esforço de resposta. Um mecanismo popular é o modelo *Incident Command Team* (Equipe de Comando de Incidentes), no qual um comandante de incidentes é escolhido para supervisionar todos os aspectos de ER, incluindo logística, planejamento, relatórios situacionais e resposta operacional. A maioria das organizações que usa um modelo *Incident Command Team* personaliza sua abordagem para a organização, mas mantém os princípios fundamentais de unidades de comando e mantém as funções e responsabilidades claramente definidas. Informações adicionais sobre o modelo *Incident Command Team* podem ser encontradas em http://www.fema.gov/txt/nims/nims_ics_position_paper.txt.

Se a coordenação dos programas de BC e ER for incluída em um plano de auditoria, algumas questões principais devem ser consideradas:

- Com que frequência os proprietários do programa se encontram para discutir as questões e preocupações sobre o programa?
- Os proprietários do programa se reuniram com as autoridades locais de ER, para chegar a um consenso sobre como eventos de diversas magnitudes podem ser gerenciados da melhor forma, tanto para impactos imediatos e quanto de longo prazo?
- O coordenador de ER tem influência suficiente para alterar as estratégias de BC, se justificado, e vice-versa?
- A alta administração aprovou um detalhamento claro das responsabilidades de ER, em comparação com as de BC em uma organização?
- Existem protocolos concretos de transferência de informações e relações externas, à medida que a fase de ER é reduzida e a BC tem sua prioridade aumentada?
- Se um modelo de Equipe de Gestão de Incidentes for usado, o líder do programa de BC terá um papel na equipe?

7. Gestão de Crises

A gestão de crises é facilmente uma das expressão mais incompreendidas de todo o campo de BCM. Em algumas organizações, é o planejamento extremamente tático que acabamos de descrever como resposta a emergências. Algumas organizações usam para cobrir eventos relacionados a problemas de segurança física. Algumas organizações definem como sendo o plano de nível executivo para lidar com grandes eventos no nível da entidade, mas, na realidade, seus planos tratam apenas de problemas de comunicação de crise. Para os propósitos deste GTAG, usaremos o termo para descrever o planejamento no nível da entidade, projetado para abordar os impactos imediatos e de alto nível sobre a organização.

A maioria dos planos de gestão de crises é projetada para ser ativada em qualquer incidente, independentemente do impacto. Em muitos casos, são estabelecidos limites específicos antecipadamente para diversos tipos de impactos, para eliminar a subjetividade geralmente associada ao escalonamento de um evento. Esses critérios de escalonamento devem incluir impactos humanos, financeiros e operacionais e ser diretos o suficiente para permitir que os funcionários de nível gerencial, em qualquer lugar em que a organização atue, saibam se é necessário escalonar para a equipe de gestão de crises. Da mesma forma, o uso consistente dos limites em toda a entidade ajuda a equipe de gestão de crises a ter certeza de que, se ainda não tiver sido contatada, o evento não excedeu os limites pré-estabelecidos.

Outra vantagem importante desses limites é o valor que eles agregam ao separar um evento de BC de uma crise no nível da entidade. Um pequeno incêndio ou a perda de um fornecedor importante pode ter um impacto significativo sobre uma linha de negócios ou sobre um local de operação, mas isso não constitui necessariamente uma crise no nível da entidade que justifique a ativação da equipe de gestão de crises. Limites desenvolvidos adequadamente empoderam os gerentes das unidades de negócios (ou regionais) para atuar sobre problemas de retomada das atividades comerciais sem se perguntar se serão questionados pela alta administração.

Um tema consistente na maioria das empresas que operam programas maduros de gestão de crises é uma capacidade de comando e controle bem definida e ensaiada. Durante um evento real, especialmente um evento complicado, o caos é abundante. Não há informações confiáveis suficientes à disposição da administração no início do evento para tomar decisões completamente precisas 100% do tempo. Organizações que buscam a excelência na gestão de crises desenvolvem e testam com antecedência um sistema que possa ingerir informações disponíveis, filtrar o "ruído", disseminar informações de forma rápida e segura e maximizar a capacidade de tomada de decisões.

Além de protocolos de escalonamento e comando e controle de pessoas, processos e informações, outros aspectos de programas eficazes de gestão de crises incluem:

- Incorporar disciplinas especializadas, como extorsão/recall de produtos, incidentes de segurança (especialmente incidentes internacionais) e resposta a incidentes de emergência específicos do setor (ex., aviação) ao programa geral de gestão de crises. Geralmente, as empresas com exposição nessas áreas desenvolverão alguns planos para resolvê-las, mas podem não estar vinculados ao programa de gestão de crises no nível da entidade.
- Ajudar os funcionários afetados por um desastre, podendo incluir o fornecimento de apoio à saúde mental, apoio familiar ou assistência financeira durante eventos regionais. A assistência também pode incluir incentivos para viagem ou mudança temporária em caso de emergência.
- Incorporar as expectativas do conselho à resposta a incidentes e aos relatórios do conselho durante a resposta.
- Gerenciar as questões e responsabilidade dos acionistas após um evento, incluindo questões de erros e omissões e problemas de responsabilidade dos diretores e executivos.
- Testar a CM e a BC em conjunto, para que cada programa possa desenvolver os pontos fortes do outro e o esforço geral possa amadurecer de forma unificada.
- Detalhar as autoridades, quando algumas operações são gerenciadas como *joint venture* e/ou existem em diversos países. A responsabilidade jurídica pode ser transferida de uma *joint venture* ou de outro país, se as decisões forem tomadas por outra entidade legal ou em um país diferente. Essa questão é muito importante se a equipe de CM estiver nos Estados Unidos, por causa do ambiente litigioso do país.

8. Conclusão/Resumo

A BCM é um importante programa de gerenciamento de riscos, projetado para proteger as empresas de possíveis consequências significantes, relacionadas a eventos que possam interromper processos críticos de negócios. O CAE pode ajudar a organização a compreender os riscos e as opções para criar um programa eficaz de BCM. Os gerentes de toda a organização devem ser responsabilizados pelo gerenciamento adequado dos riscos associados à interrupção das operações de negócios e das funções associadas em sua organização.

Um programa de BCM fornece a estrutura para a tomada de decisões apropriadas de mitigação de riscos e para a construção da resiliência organizacional. Os processos comerciais críticos devem ser recuperados, para apoiar a recuperação das operações críticas de negócios. O programa de BCM permite que a organização mantenha seus recursos de recuperação, incluindo suas capacidades e conhecimento organizacional, a recuperação de sistemas e informações, a restauração e aquisição de recursos, a gestão de fornecedores e o alinhamento com processos de gestão de emergências.

O programa de BCM deve ser projetado para manter e aumentar continuamente os recursos de continuidade de negócios. A manutenção eficaz das capacidades de BCM deve incluir o treinamento regular da equipe, exercícios periódicos (incluindo a resolução de quaisquer lacunas identificadas e o compromisso da administração com o programa), avaliações de auditoria do programa de BCM e das capacidades das unidades de negócios, e a melhoria contínua do programa de BCM.

9. Anexo

9.1 Amostra de Guia de Auditoria de BCM

O *Federal Financial Institutions Examination Council* possui um excelente livreto de planejamento de continuidade de negócios (*Business Continuity Planning Booklet*, março de 2008). O guia pode ser encontrado no site do conselho, www.ffiec.gov. Abaixo, estão os principais objetivos discutidos no livreto.

- Determinar o escopo e os objetivos da revisão do programa de planejamento de BC.
- Determinar a existência de um plano de BC adequado que inclua toda a organização.
- Determinar a qualidade da supervisão e apoio ao plano de BC por parte do conselho de administração e da alta administração.
- Determinar se uma avaliação de riscos e BIA adequados foram concluídos.
- Determinar se há um gerenciamento de riscos apropriado sobre o processo de BC.
- Determinar se o (s) plano (s) de BC inclui (m) testes apropriados para garantir que os processos de negócios sejam mantidos, retomados e / ou recuperados como pretendido.
- Determinar se o ambiente de TI possui um plano de BC devidamente documentado que complemente os planos de BC corporativos e outros departamentos.
- Determinar se o(s) plano(s) de BC inclui(em) o backup e a recuperação de hardware apropriados.
- Determinar se o processo de BC inclui backup e recuperação de software e software de aplicativo apropriados.
- Determinar se o(s) plano(s) de BC inclui(em) a preparação adequada para garantir que os processos de recuperação do *data* center funcionem conforme pretendido.
- Determinar se o(s) plano(s) de BC inclui(em) procedimentos de segurança apropriados.
- Determinar se o(s) plano(s) de BC aborda(m) as atividades terceirizadas críticas.
- Discutir ações corretivas e comunicar os resultados.

9.2 Normas e Diretrizes de BCM

Organização/Órgão de Governança	Norma	Descrição da Norma
Business Continuity Institute(BCI)		Dez Competências do Business Continuity Institute
International Standards Organization (ISO)	ISO 9000	Gestão da Qualidade
	ISO 14001	Sistema de Gestão Ambiental
	ISO 25002	Código de Práticas para a Gestão da Segurança da Informação: seção de Gestão da Continuidade de Negócios
British Standards Institute (BSI) engloba: • **Reino Unido** • **Austrália** • **Nova Zelândia**	AS/NZ 4360	Gerenciamento de Riscos (AS/NZ: Normas da Austrália e Nova Zelândia)
	HB221	Guia para a Continuidade de Negócios: manual complementar da Norma 4360
	AS/NZ 4390	Gestão de Registros
	AS/NZ 4444	Segurança da Informação com Gestão de Continuidade de Negócios
Publicly Available Standard (PAS): Reino Unido e Nações da *Commonwealth*	PAS 56	Guia para a BCM (PAS, Reino Unido)

Organização/Órgão de Governança	Norma	Descrição da Norma
Os Bulletins do *Office of the Comptroller of the Currency* (OCC), dos EUA, aplicam-se às funções de serviços financeiros – especificamente, a questões de TI	Norma	Retomada de Negócios Corporativos e Planejamento de Contingência
	Bulletin 97-23	Resiliência
	Bulletin 2001-14	Planejamento de Continuidade de Negócios e Supervisão dos Fornecedores Tecnológicos
Bolsa de Valores de Nova York (NYSE) / Financial Industry Regulatory Authority (FINRA)	Bulletin 2003-18	*White Paper* elaborado em conjunto pela Securities and Exchange Commission, Office of the Comptroller of the Currency e Board of Governors of the Federal Reserve System sobre Boas Práticas de BCP http://www.sec.gov/news/press/studies/2006/soundpractices.pdf Programa de Registros Vitais (identificação, gestão e recuperação de registros críticos para o negócio) (2003).
American National Standards Institute (ANSI)	ANSI/ARMA 5	ARMA: American Records Management Association
American Society for Industrial Security (ASIS)	ASIS GDL BC 10	*Business Continuity Guideline: A practical approach to emergency preparedness, crisis management, and disaster recovery* (versão preliminar de 2004)
National Institute of Standards and Technology dos EUA (NIST)	NIST SP 800-34,45	*Contingency Planning Guide for IT Systems* (2002)
National Fire Protection Association dos EUA (NFPA)	NFPA 1600	*Standard on Disaster / Emergency Management and Business Continuity Programs* (referida como norma para BCP)

9.3 Modelo de Maturidade da Capacidade de BCM

Embora o seguinte modelo de maturidade de capacidade de BCM não seja precisamente correspondente a esse GTAG, ele é consistente com as práticas e normas do GTAG e de BC. É apresentado apenas como exemplo de uma maneira de avaliar a maturidade de um programa de BC.

Fonte: Protiviti Inc. (www.protiviti.com). Adaptado a partir de "*Capability Maturity Model: Guidelines for Improving the Software Process*," Software Engineering Institute da Carnegie Mellon University, 1994.

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade do Apoio e Patrocínio da Gerência Executiva		
	Características de Capacidade	**Método de Atingimento**
Em Otimização	As capacidades de BCM são aprimoradas contínua e sistematicamente. A alta administração utiliza os recursos de BCM para impulsionar outras eficiências internamente e construir relacionamentos estratégicos externamente.	As estratégias de BCM estão alinhadas com os objetivos estratégicos e as expectativas do cliente. A alta administração garante que o planejamento de BCM funcione como uma função central de negócios, com prestação de contas e responsabilidades claras.
Gerida	A alta administração definiu as principais métricas, de acordo com os requisitos regulatórios e diretrizes da indústria. Essas métricas são usadas para mensurar a eficácia e a qualidade das capacidades de BCM. A administração participa das atividades de teste e de treinamento e revisa as exceções à política interna e aos resultados de testes.	A alta administração está comprometida em gerenciar a qualidade da execução do programa de BCM. Métricas são coletadas e gerenciadas, para garantir a qualidade das estratégias e planos de BCM. Os objetivos relacionados à BC são registrados nas metas de desempenho.
Definida	É criado um comitê diretor de BCM, liderado por um membro da equipe da alta administração não relacionada à TI. O comitê diretivo é o melhor tomador de decisões em relação às estratégias e soluções de BCM. Um orçamento dedicado à BCM e os recursos necessários são alocados para garantir a eficácia dos recursos de BCM, e as disciplinas de BCM são integradas para fornecer uma solução geral de BCM para a organização.	A alta administração está plenamente envolvida na tomada de decisões de BCM, por meio de uma função de comitê diretivo. Além da política de BCM, a organização definiu frameworks específicos para garantir a integração da retomada de negócios, da CM e das capacidades de recuperação de desastres de TI, assim como manutenção, testes e processos de treinamento.
Repetível	A alta administração suporta o programa de BCM; no entanto, continua tendo envolvimento limitado na execução do processo. Embora a coordenação de CM, BC e recuperação de desastres de TI seja atribuída à gerência média, a coordenação geral de BCM é ad hoc ou ausente. Os eventos de falha são reconhecidos e corrigidos depois que ocorrem.	A alta administração está ciente da necessidade dos recursos de BCM. Uma política de BCM foi criada e os esforços de BCM são conduzidos com base nos resultados de uma BIA (formal ou informal).
Inicial	O patrocínio dos esforços de BCM por parte da alta administração é informal ou ausente. Nesta fase, as capacidades de BCM dependem de esforços individuais e de "heroísmo", e concentram-se principalmente no backup e restauração de sistemas de TI e em ER, como procedimentos de evacuação de edifícios.	Estes esforços são liderados pela gerência média e executados sem financiamento adequado e sem recursos suficientes. Consequentemente, quaisquer capacidades de continuidade existentes são definidas como medidas táticas.

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade da Avaliação de Riscos e da Análise de Impacto Sobre os Negócios (BIA)		
	Características de Capacidade	**Método de Atingimento**
Em Otimização	Os resultados da avaliação de riscos e da BIA impulsionam a melhoria contínua das estratégias de recuperação. A execução e revisão de avaliações de riscos e BIAs são coordenadas com os processos organizacionais e tecnológicos de gestão de mudanças/*due diligence*.	A alta administração atua como um comitê diretivo, para identificar e aprovar conclusões de riscos e de impacto. O comitê diretivo recomenda mudanças ao processo de avaliação de riscos e BIA, com base nas necessidades e requisitos do próprio negócio.
Gerida	A alta administração apoia a abordagem formal da avaliação de riscos e da BIA. O estabelecimento de objetivos e a eficácia são mensuráveis. Tanto objetivos de tempo de recuperação (RTO) quanto objetivos de ponto de recuperação (tolerância a perda de dados) (RPO) são estabelecidos, assim como a capacidade no RTO. O processo de avaliação de riscos leva em consideração a avaliação dos controles. Esses processos são repetíveis e executados regularmente.	Os resultados das avaliações de riscos e BIAs orientam a definição e o desenvolvimento de estratégias e soluções de recuperação. Os principais processos de negócios e aplicativos/sistemas de TI foram abordados e são revisados durante a avaliação de riscos programada regularmente e as atualizações da BIA. A alta administração usa esses resultados para medir e gerenciar riscos em toda a empresa.
Definida	Uma abordagem mais formal foi implementada em relação à avaliação de riscos e impacto sobre os negócios. A administração identificou uma abordagem para definir níveis de criticidade, apoiando uma metodologia para coletar/estimar dados de impacto sobre os negócios. Os objetivos de tempo de recuperação foram definidos e foram selecionadas estratégias para atender a esses requisitos. A administração analisa e aprova a avaliação de riscos e os resultados da BIA.	Como parte de um processo formal de seleção e implementação da estratégia de BC, uma avaliação de riscos definida ou abordagem de BIA é estabelecida. O processo de seleção de estratégias também inclui objetivos de recuperação vinculados diretamente aos níveis de criticidade e aos impactos sobre a organização. A gerência executiva conduz e aprova formalmente essas análises.
Repetível	A administração desenvolveu informalmente conclusões de avaliação de riscos e prioridades de recuperação, tipicamente como resultado de discussões e sessões facilitadas, em oposição à análise formal. As prioridades estão normalmente focadas no nível do componente. A administração pode não conseguir justificar totalmente o financiamento da estratégia de recuperação, uma vez que as informações de impacto sobre os negócios (financeiras ou não financeiras) permanecem incompletas.	A gerência comercial e/ou de TI discutiu e resumiu os riscos de continuidade/disponibilidade ou impactos percebidos associados às interrupções nos negócios. Objetivos de recuperação preliminares/de alto nível são acordados; no entanto, não há um processo para mensurar a eficácia e a razoabilidade desses objetivos.
Inicial	Não foi realizada uma avaliação de riscos, formal ou informal, nem uma BIA. A gerência comercial e de TI podem ter desenvolvido prioridades de recuperação, mas essas são possivelmente limitadas a níveis percebidos de importância (foco em seu conhecimento isolado sobre o negócio). A organização não estimou os impactos (financeiros ou não financeiros) associados às interrupções nos negócios.	A gerência comercial e/ou de TI desenvolveu prioridades de recuperação "*ad hoc*", com base nos níveis percebidos de importância. Cenários de falhas e avaliações de controles permanecem incompletos. Não foram estabelecidos critérios de mensuração.

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade da Estratégia e Elaboração da Continuidade dos Negócios		
	Características de Capacidade	**Método de Atingimento**
Em Otimização	As estratégias de BC são revisadas como parte da tomada de decisões estratégicas e da gestão de mudanças tecnológicas. As estratégias são atualizadas conforme a necessidade.	Sessões estratégicas com os executivos seniores e/ou comitês de gestão de mudanças direcionam o design, a escolha, o financiamento e a implementação das estratégias de BC.
Gerida	Os resultados da avaliação de riscos e da BIA orientam a escolha das estratégias de BC. Um comitê diretivo multidisciplinar avalia as opções de CM, retomada de negócios e recuperação de desastres de TI com base em uma análise de custo-benefício. As estratégias de BC são revisadas periodicamente, normalmente a cada 12 meses (após uma avaliação de riscos e/ou atualização da BIA).	Um comitê diretivo de BC faz a escolha das estratégias de BC com base em uma análise de custo-benefício. Essa equipe multifuncional avalia e seleciona soluções comerciais e de TI complementares.
Definida	Soluções pontuais ou estratégias específicas à disciplina são projetadas e implementadas com base na orientação da administração. A organização não aproveitou os benefícios associados à escolha de uma estratégia para toda a organização que integre a CM, a retomada de negócios e a recuperação de desastres de TI. A organização continua se aproximando de implantar estratégias que atendam aos objetivos de recuperação estabelecidos.	A organização de tecnologia da informação (ITO) retém a tomada de decisões em relação às estratégias de recuperação de desastres de TI. O design e a escolha da estratégia de retomada de negócios e CM são tratados separadamente, orientados pelo gerenciamento de riscos, pela segurança, pela auditoria interna ou até mesmo pela ITO. A coordenação entre a empresa e a ITO é frequentemente ignorada.
Repetível	O controle de custos é o principal direcionador da escolha da estratégia de BC. As estratégias normalmente dependem de acordos de locais frios (internos ou de terceiros) e de recursos enviados pelos fornecedores. A organização continua em risco, dada a probabilidade de que as estratégias de BC possam falhar em atingir os objetivos de negócios mais agressivos.	A organização não aloca orçamento para a implantação e manutenção da estratégia de BC. Em vez disso, o mínimo percebido é implementado, e, quando é necessário financiamento, esses problemas são tratados como exceções de orçamento.
Inicial	Os planos de BC não têm uma estratégia de recuperação e definições de recursos, devido à falta de propriedade ou responsabilidade pelo programa de BC. A organização deposita grande confiança no suporte dos fornecedores após a crise ou interrupção de negócios.	O gerenciamento depende de ações *ad hoc* ou de estratégias de recuperação e resposta não testadas. A elaboração de estratégias de resposta e recuperação não é pré-planejada; Em vez disso, a administração espera que as experiências, a criatividade e a engenhosidade prevaleçam diante de uma situação de crise.

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade do Alinhamento dos Negócios		
	Características de Capacidade	**Método de Atingimento**
Em Otimização	A BCM está presente durante as sessões de revisão da gestão de mudanças, bem como durante as sessões de estratégia de negócios, a fim de manter a organização a par de todas as mudanças que podem afetar as estratégias existentes de resposta e recuperação. O comitê diretivo de BCM se reúne trimestralmente para avaliar a razoabilidade das estratégias existentes e propostas, assim como os gastos em comparação com o resto da indústria.	A BCM tira proveito da estratégia de negócios mais avançada e dos processos de gestão de mudanças em prática em toda a organização.
Gerida	Um comitê diretivo de BCM considera as exigências do cliente e/ou acordos formais do nível de serviço ao avaliar os resultados da BIA e o investimento na estratégia de BC. A auditoria interna está envolvida no esforço de BCM como consultora e analisa o programa com base na política interna e nos requisitos regulatórios (se aplicável). Quando a organização testa suas estratégias de BC, as soluções comerciais/de TI são testadas em conjunto.	A BCM é vista como um controle fundamental e a auditoria interna promove a conformidade com a política documentada existente. Todos os aspectos do ciclo de vida de BCM são implementados de forma conjunta com o comercial/TI. A BCM é usada como vantagem competitiva em outras iniciativas de negócios.
Definida	A organização integrou as três disciplinas de BCM e um único comitê diretivo de BCM toma decisões sobre estratégias e soluções. Um orçamento de BCM foi desenvolvido. Uma análise formal de BIA e custo-benefício orienta a tomada de decisões. As estratégias de resposta e recuperação internas e de terceiros são formalmente avaliadas, com as escolhas baseadas nos resultados da avaliação de riscos.	A responsabilidade pelo programa de BCM é tirada do *data center*. Um executivo com a capacidade de influenciar toda a organização patrocina o esforço. Os objetivos de BCM aparecem nos objetivos anuais de desempenho da gerência da unidade de negócios.
Repetível	A organização desenvolveu uma política formal de BCM para impulsionar o design, a implementação e a execução da BC. Embora a coordenação entre a CM, a retomada de negócios e os processos de recuperação de desastre de TI esteja imatura ou ausente, eles existem e estão posicionados para auxiliar nas operações de resposta e recuperação. A BIA orienta a elaboração das estratégias de BCM.	Embora o escopo do esforço de planejamento tenha se expandido para incluir os negócios, a propriedade e a responsabilidade permanecem dentro da TI, ou a auditoria interna atua como promotora do esforço de BCM. A BIA é a principal ferramenta usada para projetar estratégias de BCM.
Inicial	O programa de BC da organização aborda a ER e/ou a recuperação de desastres de TI, mas não aborda a CM estratégica e/ou recuperação de processos de negócios.	As soluções de BC, que podem estar limitadas à tática e a restaurações do sistema, são conduzidas no nível da gerência média e executadas a partir do excesso de financiamento existente (ou recursos internos disponíveis).

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade do Desenvolvimento do Plano e Implementação da Estratégia		
	Características de Capacidade	**Método de Atingimento**
Em Otimização	Os planos de crises, recuperação de desastres e retomada dos negócios estão integrados ao planejamento e à execução. A equipe é multifuncional e inter-regional. As expectativas são claramente entendidas por todos os stakeholders. A manutenção do plano é rigorosamente integrada aos processos organizacionais de gestão de mudanças.	A BCM tira proveito da estratégia de negócios mais avançada e dos processos de gestão de mudanças em prática em toda a organização.
Gerida	A coordenação entre os planos e equipes de CM, de retomada de negócios e de recuperação de desastres de TI é bem definida. Os planos são mantidos conforme a necessidade, em vez de com frequência mínima (ex., anualmente). A documentação do plano é revisada por uma autoridade central ou autorizada pela alta administração. Os resultados dos testes e as experiências diárias promovem a melhoria do plano. A documentação é devidamente protegida e disseminada conforme a necessidade.	A BCM é vista como um controle fundamental e a auditoria interna promove a conformidade com a política documentada existente. Todos os aspectos do ciclo de vida de BCM são implementados de forma conjunta com o comercial/TI. A BCM é usada como vantagem competitiva em outras iniciativas de negócios.
Definida	A CM (incluindo a ER e as comunicações de crise), a retomada de negócios e a recuperação de desastres de TI são documentadas e incluem detalhes organizacionais. Todos os planos são atualizados anualmente. Embora os papéis e responsabilidades sejam claros, a coordenação entre os planos é mal definida.	A responsabilidade pelo programa de BCM é tirada do *data center*. Um executivo com a capacidade de influenciar toda a organização patrocina o esforço. Os objetivos de BCM aparecem nos objetivos anuais de desempenho da gerência da unidade de negócios.
Repetível	O foco do esforço de planejamento é a documentação de recuperação de desastres de TI e o planejamento de ER (evacuação de edifícios, primeiros socorros, etc.). Existe alguma documentação de CM, mas seu foco está na resposta a incidentes de TI. A principal razão para a documentação do plano é evitar comentários da auditoria. Os planos costumam ser atualizados de maneira *ad hoc*.	Embora o escopo do esforço de planejamento tenha se expandido para incluir os negócios, a propriedade e a responsabilidade permanecem dentro da TI, ou a auditoria interna atua como promotora do esforço de BCM. A BIA é a principal ferramenta usada para projetar estratégias de BCM.
Inicial	Os planos, onde existem, são desenvolvidos em silos, sem detalhes de processos comerciais e tecnológicos. Os stakeholders de BCM não conhecem seus papéis e responsabilidades ou, em alguns casos, não sabem de seu envolvimento na execução da resposta e da recuperação. Os planos estão frequentemente desatualizados. A resposta e a recuperação dependem da memória e a execução é muitas vezes *ad hoc*, conduzida por alguns funcionários principais.	As soluções de BC, que podem estar limitadas à tática e a restaurações do sistema, são conduzidas no nível da gerência média e executadas a partir do excesso de financiamento existente (ou recursos internos disponíveis).

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade do Treinamento e Conscientização		
	Características de Capacidade	**Método de Atingimento**
Em Otimização	O programa de BCM e seu impacto sobre as operações diárias são entendidos profundamente por todas as camadas da organização. Os responsáveis pela execução das tarefas de BCM participam ativamente do treinamento de outros. As estratégias de BCM são avaliadas quanto ao seu impacto sobre o valor da empresa. O treinamento de BCM está incluído nas avaliações de desempenho (ex., *balanced scorecard*).	Os membros da equipe são treinados especificamente sobre como ser um proponente de BCM. A liderança de BCM coordena cuidadosamente os objetivos de BCM com os principais objetivos comerciais, para explorar sua publicidade. Os membros da equipe que receberam treinamento cruzado têm oportunidades de se exercitar fora de suas responsabilidades normais.
Gerida	A administração tem um amplo entendimento de como os elementos de BCM funcionam conjuntamente. Os funcionários sabem suas responsabilidades imediatas em um evento real e muitos conhecem suas atividades de longo prazo. Os membros da equipe podem articular suas responsabilidades individuais e como seu elemento está conectado aos outros elementos de BCM e aos objetivos de negócios da empresa como um todo. As questões de BCM são consideradas em todas as iniciativas de negócios.	Todos os membros da equipe são treinados quanto às suas tarefas e ao programa como um todo. A liderança de BCM fornece atualizações do programa à alta administração regularmente. Os programas de treinamento e conscientização são orçados separadamente, incluindo recursos externos, se necessário. Os membros da equipe participam de treinamento de terceiros ou de estudos de caso. O treinamento inclui questões sobre como executar o plano no meio de um evento que se estenda além da empresa.
Definida	Um programa estruturado para comunicar as metas e objetivos do programa de BCM é desenvolvido com todos os elementos participantes. Os funcionários externos às equipes de planejamento e execução entendem as metas e objetivos do programa. Há uma consciência geral na administração sobre a abordagem multifacetada de BCM.	Existe uma abordagem estruturada para o treinamento de BCM, sendo que a gerência de cada linha de negócios compreende o programa. O treinamento relacionado à tarefa é obrigatório para todos os membros da organização listados como principais ou membros da equipe de backup. Os recursos existentes, como a intranet da empresa ou a orientação de novos contratados, são usados para promover a conscientização geral do programa.
Repetível	Alguns treinamentos ou conscientização limitados estão presentes em um elemento do programa, mas não há treinamento cruzado sobre crises, retomada de negócios e recuperação de desastres. Componentes específicos do programa podem ter backups designados e os membros da equipe são incluídos na comunicação casual sobre o programa.	A gerência média, com responsabilidade tática pelos elementos do programa, compreende o perigo de depender de uma pessoa para executar uma tarefa crítica de BCM. Os testes e/ou atualizações de BCM são um tópico periódico das reuniões da equipe do departamento. É fornecido treinamento formal em tarefas específicas àqueles que devem fazê-las, mas nada mais. O treinamento é limitado à participação nos exercícios.
Inicial	Não há treinamento formal ou programa de conscientização. Somente aqueles com responsabilidade imediata conhecem as metas e objetivos do programa. Não há treinamento cruzado sobre crise, retomada de negócios e recuperação de desastre. Questões regulatórias orientam os esforços de treinamento e conscientização.	Produzido por uma combinação de silos de planejamento. Está presente onde esforços individuais extraordinários são a base de BCM. O treinamento, quando há, é limitado às atividades de ER.

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade dos Testes e Manutenção do Plano		
	Características de Capacidade	Método de Atingimento
Em Otimização	O teste de BC ocorre sem aviso prévio. Simulações são desenvolvidas usando riscos prováveis identificados em uma avaliação de riscos. Os testes são mensurados principalmente por uma recuperação esperada. Departamentos inteiros trabalham em um local alternativo por um determinado período de tempo, usando sistemas e recursos de backup. Parceiros de negócios e fornecedores externos participam dos testes. As atualizações do plano são integradas automaticamente, por meio de um processo de manutenção.	Os membros da equipe são precisamente treinados e sua resposta é meramente uma reação. É feito um planejamento mínimo na preparação para os testes, feito secretamente por alguns indivíduos. Os membros da equipe de resposta e recuperação têm confiança mínima na documentação do plano, além de alguns procedimentos técnicos ou listas de contatos atualizadas. Ferramentas automatizadas são empregadas para armazenar os planos e mantê-los atualizados, refletindo as operações comerciais.
Gerida	São realizados testes completos de BC, para negócios e TI, regularmente. Simulações são desenvolvidas usando riscos prováveis identificados em uma avaliação de riscos. Os testes são mensurados pela taxa de recuperação de componentes ou funções críticas, como conectividade, uso de aplicativos ou processamento de transações. Os planos são mantidos fora do local e as atualizações são feitas após a conclusão do teste. A auditoria interna observa o exercício e garante que os planos sejam atualizados.	O planejamento do teste engloba a CM, a retomada de negócios e a recuperação de desastres de TI. Os membros da equipe são treinados para todos os procedimentos relevantes. Há pouca dependência da documentação do plano, embora as imprecisões da lista de procedimentos e de contato devam ser tratadas em tempo hábil. A auditoria interna monitora os itens de planejamento, execução e itens de ação resultantes do teste. As atualizações do plano devem ser de responsabilidade dos proprietários do processo, com supervisão da auditoria interna.
Definida	Às vezes, os testes de BC e recuperação de desastre de TI são executados em conjunto, mas o foco geralmente está na recuperação dos componentes. Os procedimentos de continuidade são discutidos em sessões facilitadas, para identificar as lacunas de planejamento. Os testes são mensurados principalmente usando um cronograma esperado para recuperação e eficácia geral. Departamentos inteiros trabalham em um local alternativo por um determinado período de tempo, usando sistemas de backup. As lições aprendidas são documentadas e as atualizações do plano são feitas de forma programada.	A equipe comercial e de TI realiza testes de BC programados regularmente, projetados para lidar com processos de negócios e recuperação de ativos de TI. Os usuários testam a conectividade e o acesso aos aplicativos. O processo de planejamento para esses testes é extenso e envolve profissionais internos e externo como facilitadores e/ou monitores. A auditoria interna participa dos exercícios de teste e monitora o processo de atualização de planos com base nos resultados do teste. As atualizações do plano são de responsabilidade do proprietário do processo, com coordenação central.
Repetível	O teste é focado na recuperação de desastres de TI e pode envolver a validação do usuário final do ambiente recuperado e/ou dos resultados do teste. Em algumas organizações, o gerenciamento se envolve em exercícios baseados em cenários ou tabletop para suas capacidades de CM. Os testes de recuperação de desastre de TI estão focados na recuperação de componentes. A auditoria interna examina os procedimentos de continuidade, se a função existir. As atualizações do plano são feitas de forma programada.	A equipe de TI conduz regularmente testes de recuperação de desastre e recuperação de componentes de TI. O processo de planejamento para esses testes é extenso e deve envolver profissionais internos e externos como facilitadores e/ou monitores. A auditoria interna participa dos exercícios de teste e monitora o processo de atualização de planos com base nos resultados do teste. Um indivíduo é responsável pelas atualizações do plano.
Inicial	O teste de componentes de TI ocorre internamente no departamento de TI, com conhecimento limitado de gestão e sem a participação da comunidade usuária. Não há cronograma formal de testes e os resultados dos testes raramente são documentados. O teste não resulta em alterações ou melhorias na documentação dos procedimentos de resposta/recuperação. Os planos podem não ser bem mantidos ou atualizados, porque o processo de BCM é novo.	Os sucessos do planejamento de BC, normalmente limitados à TI, estão presentes onde esforços individuais extraordinários são a base. O treinamento, quando há, está limitado às atividades de recuperação de ER (primeiros socorros, evacuação, etc.) e de componentes de TI. As atualizações do plano são de responsabilidade dos proprietários do processo e não seguem um processo padrão monitorado.

MATURIDADE DO PROCESSO

Objetivo da Avaliação: Avaliação de Maturidade do Monitoramento e da Auditoria de Conformidade		
	Características de Capacidade	**Método de Atingimento**
Em Otimização	A auditoria interna, o gerenciamento de riscos e o conselheiro geral revisam a documentação do plano regularmente e também patrocinam auditorias de terceiros das capacidades de BCM, incluindo atividades de teste. A organização está envolvida em discussões do setor sobre conformidade regulatória e revisa regularmente as análises de *benchmarking*. Uma avaliação de riscos e BIA são realizadas e regularmente atualizadas, para garantir que os planos reflitam a realidade dos negócios e do ambiente regulatório.	É mantido contato proativo com os órgãos reguladores. Uma equipe dedicada lidera as atividades de BCM, apoiada por uma equipe de negócios e tecnologia multifuncional, incluindo a auditoria interna e prestadores terceirizados de serviços especializados. Uma avaliação de riscos (por localização) e uma BIA (por processo) devem ser conduzidas e usadas como base para a elaboração dos planos. Eles também devem ser atualizados periodicamente.
Gerida	Equipes multifuncionais, incluindo o conselheiro geral e a auditoria interna, realizam avaliações regulares das condições comerciais e dos requisitos regulatórios. A auditoria interna, o gerenciamento de riscos e o conselheiro geral também revisam a documentação do plano, de alguma forma, anualmente. Uma avaliação de riscos e uma BIA são usadas para garantir que os planos reflitam a realidade dos negócios e se concentrem nos riscos e impactos mais prováveis e graves.	Uma equipe dedicada lidera as atividades de BCM, apoiada por uma equipe multifuncional de negócios e tecnologia, incluindo a auditoria interna e prestadores terceirizados de serviços especializados. Uma avaliação de riscos (por localização) e uma BIA (por processo) devem ser conduzidas e usadas como base para a elaboração dos planos. Eles também devem ser atualizados periodicamente. A auditoria interna concentra-se na execução do programa de BCM, em vez de focar no conteúdo do plano.
Definida	Os regulamentos relacionados à BCM são considerados e incorporados aos planos de BCM. A responsabilidade de monitorar o panorama regulatório recai sobre o conselheiro geral, que se comunica com o comitê diretivo de BCM. A auditoria interna monitora o processo de manutenção do plano e influencia quando mudanças regulatórias justificam atualizações à documentação. Uma avaliação de riscos e uma BIA que consideram o ambiente regulatório foram realizadas nos últimos dois anos.	Uma pequena equipe multifuncional está em prática e a função de auditoria interna está ativamente envolvida nas ações dessa equipe. Uma avaliação de riscos (por localização) e uma BIA (por processo) são conduzidas e usadas como base para a elaboração dos planos e para a identificação do impacto da regulamentação sobre o desenvolvimento do plano.
Repetível	Regulamentações relacionadas à BCM são consideradas e incorporadas aos planos de BCM, quando financeiramente práticas. A auditoria interna revisa a relevância da documentação de acordo com um plano de auditoria de longo prazo e pode solicitar evidências dos testes do plano.	A auditoria interna, o gerenciamento de riscos ou o conselheiro geral compartilham atualizações regulatórias com a equipe de BCM ou com os responsáveis pela BCM.
Inicial	Os requisitos regulatórios ou normas do setor relacionados à BCM são raramente considerados e incorporados aos planos de BCM, ou são considerados muito caros para implementação. A atenção da auditoria interna não vai além de garantir que os planos tradicionais de recuperação de desastres de TI estejam sendo documentados.	Há um processo de planejamento de recuperação de desastres de TI. Existe uma função de auditoria interna em vigor e a recuperação de desastres está no plano de auditoria anual ou bianual.

10. Glossário

BC (*business continuity*) — continuidade dos negócios

BCM (*business continuity management*) — gestão de continuidade dos negócios

BCP (*business continuity plan*) — plano de continuidade dos negócios

BIA (*business impact analysis*) — análise de impacto sobre os negócios

BU (*business unit*) — unidade de negócios

CAE — *chief audit executive*

CBCP — *Certified Business Continuity Professional*

CM (*crisis management*) — gestão de crises

DRII — DRI International

DRP (*disaster recovery planning*) — planejamento de recuperação de desastres

ER (*emergency response*) — resposta a emergências

GTAG — *Global Technology Audit Guide*

MBCP — *Master Business Continuity Professional*

RPO (*recovery point objective*) — objetivo de ponto de recuperação

RTO (*recovery time objective*) — objetivo de tempo de recuperação

TI — tecnologia da informação

11. Sobre os Autores

David Everest, CISA
David Everest é vice-presidente de Revisão de Riscos Tecnológicos do Key Bank em Cleveland, Ohio. Everest concentra-se em oferecer expertise em consultoria interna para a divisão de tecnologia do Key Bank. Suas especialidades incluem projetos de infraestrutura e redes. Antes de ingressar no Key, ele foi auditor de tecnologia na General Motors em Detroit, MI. Everest tem vasta experiência em TI, tanto técnica quanto estratégica, e trabalhou em *data centers* e gerenciou departamentos de TI. Everest é bacharel em Sistemas de Informação de Computadores pela Baldwin Wallace College, em Berea, Ohio, e possui MBA pela The Weatherhead School of Management, da Case Western Reserve University, em Cleveland.

Roy E. Garber, CIA, CISA
Roy Garber é o diretor de Desenvolvimento de Aplicativos na Safe Auto Insurance Co. e é responsável pelo departamento de gestão de projetos (*project management office* – PMO) e entrega de soluções em aplicativos corporativos de TI. Suas responsabilidades atuais também incluem a implementação dos princípios e boas práticas de governança de TI.

Garber tem mais de 20 anos de experiência em gerenciamento de riscos operacionais, financeiros e de TI. Em sua função anterior de auditoria interna, foi o diretor corporativo responsável pela liderança em serviços corporativos de auditoria de TI para uma empresa internacional de seguros. Em sua função anterior de auditoria externa, Garber gerenciava trabalhos de avaliação de TI em empresas de grande, médio e pequeno porte e fazia parcerias com os executivos clientes, para ajudá-los a atender às necessidades de gerenciamento de riscos de TI.

Michael Keating
Mike Keating lidera a prática de gestão de continuidade de negócios da Navigant Consulting. Antes de ingressar na Navigant Consulting, ocupou vários cargos de liderança na área de gestão de crises e consultoria em continuidade de negócios, incluindo quase quatro anos como líder corporativo do Centro-Oeste da maior corretora de seguros do mundo e quatro anos como líder corporativo de gestão de continuidade de negócios do Sudeste para uma proeminente empresa de auditoria e consultoria interna. Keating também desenvolveu o programa BICEPP da Cruz Vermelha Americana, o primeiro programa do gênero a ajudar as organizações a se prepararem para desastres. É especializado em programas de continuidade de negócios que engajem toda a empresa e ajudou clientes de quase todos os tamanhos e setores a se prepararem para minimizar o impacto das interrupções nos negócios.

Brian Peterson
Brian Peterson é o líder da equipe global de consultores de gerenciamento de riscos da informação da Chevron Corp. e é responsável pela prestação de serviços de consultoria para empresas da Chevron no mundo todo. Suas responsabilidades atuais incluem o gerenciamento de consultores em quatro países, que prestam consultoria de gerenciamento de riscos. Peterson tem mais de 25 anos de experiência em gestão de projetos, TI e gerenciamento de riscos. Trabalhou em 55 países, auxiliando unidades de negócios da Chevron com várias iniciativas de gerenciamento de riscos. Peterson desenvolveu diversas ferramentas e processos que são usados em toda a Chevron para gerenciar riscos da informação.

Peterson ajudou a estabelecer o consórcio LOGIIC (*Link the Oil and Gas Industry to Improve Cyber-security*), que é uma parceria entre o governo e a indústria, na qual atua hoje como gestor de projeto.

Revisores

O The IIA agradece aos seguintes indivíduos e organizações que forneceram comentários valiosos e agregaram grande valor a este guia:

- Comitê de Práticas Profissionais:
  - Comitê de Tecnologia Avançada
  - Conselho de Regentes
  - Comitê de Qualidade
  - Conselho de Normas de Auditoria Interna
  - Comitê de Assuntos Profissionais
  - Comitê de Ética
- Lily Bi, The IIA
- Larry Brown, The Options Clearing Corp., EUA
- Faisal R. Danka, Londres, Reino Unido
- Christopher Fox, ASA, Delta, Nova York, EUA
- Nelson Gibbs, Deloitte & Touche, LLP, EUA
- Markus Künzel, Medizinische Universität Wien, Áustria
- Lemuel Longwe, Ernst & Young Chartered Accountants, Zimbábue
- Steve Mar, Resources Global, EUA
- Tom Margosian, Ford Motor Co., EUA
- James Reinhard, Simon Property Group Inc., EUA

A PROTIVITI

É LÍDER EM

CONSULTORIA INDEPENDENTE DE

RISCOS

A Protiviti é uma firma global de consultoria e auditoria interna, composta de especialistas em riscos e serviços de assessoria. A firma ajuda seus clientes a resolver problemas de finanças, operações, tecnologia, litígio e GRC. Os profissionais da Protiviti, altamente treinados e focados em resultados, atendem clientes das Américas, Ásia-Pacífico, Europa e Oriente-Médio e oferecem uma perspectiva única sobre uma ampla variedade de questões críticas de negócios. A Protiviti tem mais de 60 escritórios no mundo todo e é subsidiária integral da Robert Half International Inc. (símbolo da NYSE: RHI). Fundada em 1948, a Robert Half International é membro do índice S&P 500.

Para saber mais sobre nossos serviços ou fazer o download de cópias gratuitas de nossas publicações, por favor, acesse protiviti.com.

protiviti®
Independent Risk Consulting

Know Risk. Know Reward.®

© 2008 Protiviti Inc. Um Empregador com Oportunidades Igualitárias. A Protiviti não é licenciada ou registrada como uma firma de contabilidade pública e não emite opiniões ou demonstrações financeiras, ou presta serviços de certificação. 0608

RISCO

E POR QUE SABER ONDE ELE ESTÁ EM SEU NEGÓCIO É ESSENCIAL PARA

UMA BOA NOITE DE SONO

Muitos executivos passam noites em claro, perguntando-se "quando" e "se" seus processos de negócios falharão. Isso não é de surpreender, considerando que as organizações da atualidade precisam que diversos fornecedores, tecnologias, processos e pessoas trabalhem em conjunto para entregar o serviço contínuo que os consumidores esperam. Para encarar esse desafio, organizações do mundo todo e de todas as indústrias recorrem à Protiviti. Na Protiviti, adotamos uma abordagem pragmática ao planejamento de continuidade de negócios e avaliamos os riscos inerentes a todos os processos e partes interdependentes de suas operações.

Nós, então, trabalhamos com você para elaborar soluções práticas e práticos para gerenciar os incidentes que possam prejudicar seu desempenho financeiro e sua reputação. Isso dá a você uma vantagem em relação a seus concorrentes, que tentam gerenciar as interrupções devidas a erro humano, softwares falhos e fornecedores não confiáveis por meio de soluções pontuais e processos manuais. Isso também significa que, enquanto eles ficam acordados se preocupando, você estará dormindo como um bebê.

Para saber mais sobre as capacidades da Protiviti e fazer o download de uma cópia gratuita de nosso Guide to Business Continuity Management 2ª edição, por favor, acesse protiviti.com/bcm.

protiviti®
Independent Risk Consulting

Know Risk. Know Reward.®

© 2008 Protiviti Inc. Um Empregador com Oportunidades Igualitárias. A Protiviti não é licenciada ou registrada como uma firma de contabilidade pública e não emite opiniões ou demonstrações financeiras, ou presta serviços de certificação. 0206-9009206-9009

GTAG

Gestão de Continuidade de Negócios

Esse GTAG se concentra em como a gestão de continuidade de negócios (*business continuity management* – BCM) é elaborada para permitir que os líderes empresariais gerenciem o nível de risco que a organização poderia possivelmente enfrentar no caso de um evento disruptivo natural ou causado pelo homem, que afete a operacionalidade geral da organização. Esse guia inclui o planejamento de recuperação de desastres para a continuidade da infraestrutura crítica de tecnologia da informação e dos sistemas de aplicativos de negócios.
Os *chief audit executives* (CAEs) foram desafiados a instruir os executivos corporativos sobre os riscos, controles, custos e benefícios da adoção de um programa de BCM. Embora os desastres recentes em todo o mundo tenham motivado alguns líderes corporativos a dar atenção aos programas de BCM, a implantação de tais programas ainda está longe de ser universal. O principal desafio é envolver os executivos corporativos para tornar a BCM uma prioridade. Embora a maioria dos executivos provavelmente concorde que a BCM é uma boa ideia, muitos terão dificuldade de encontrar o orçamento necessário para financiar o programa, bem como um patrocinador executivo que tenha tempo para garantir seu sucesso. O guia Gestão de Continuidade de Negócios ajudará o CAE a conscientizar sobre o risco de continuidade dos negócios e a apoiar a administração no desenvolvimento e manutenção de um programa de BCM.

Acesse www.theiia.org/guidance/technology/gtag/gtag10 para classificar esse GTAG ou enviar comentários.

Número do Pedido: 1045
Membro do IIA US$25
Não Membro US$30
Evento do IIA US$22.50

The Institute of Internal Auditors

ISBN 978-0-89413-623-8
53000
9 780894 136238