Apostila

Resposta a Incidente e Plano de Continuidade

Prof. Sérgio Castilho

Resposta a Incidente e Plano de Continuidade

Sumário

Índice de ilustrações

Índice de tabelas

1 Entendendo Resposta a Incidente e Plano de Continuidade RIPC

Neste Capítulo:

Entender como os diversos tipos de desastres que afetam os negócios

Iniciando seu plano de recuperação de desastres

Tomando um rápida visão sobre ciclo de vida e planejamento do RIPC

1.1 Introdução

O planejamento de RIPC está preocupado com reparação e resposta quando ocorrer um desastres. O objetivo do planejamento é a sobrevivência de uma organização. Como o planejamento é um assunto amplo, o foco desta matéria se concentra apenas nos sistemas de TI e os usuários que suportam os processos críticos de negócio.

Neste capítulo, descreve a necessidade de um planejamento de recuperação de desastre e quais os benefícios de passar por este planejamento. Você pode ser surpreendido ao descobrir que os benefícios vão muito além de apenas o planejamento para o desastre.

O planejamento inicia na análise, para planejar o desenvolvimento e testes, a revisão dos planos periódicos baseados em eventos de negócios.

Alguns exemplos dos desastres que podem ocorrer em uma organização:

Incêndios; Incidente de Segurança; Falhas de equipamentos; Furacões; Falhas de energia Falha de Utilitário; Tempestades de vento e gelo; Tempestades severas; Sabotagem; Deslizamentos greves e paralisações; Avalanches ; Distúrbios civis; Terremotos; Terrorismo; Vulcões; Guerra entre vários outros.

1.1.1 Tempo de Inatividade e Tempo de atividade

Apresenta o quadro principal para as chamadas "economia de tempo de inatividade", fornecendo vários dados empíricos sobre os efeitos negativos financeiras de inatividade do sistema. Uma falha grave no sistema de computador, erro humano, ou qualquer tipo de desastre natural (incêndio, terremoto, enchente) pode parar a empresa desligando aplicativos suportados por esse sistema de computador, na maioria dos casos servidor corporativo. Tal evento pode causar indisponibilidade total ou parcial de dados e aplicativos corporativos. Quando o sistema não está operacional, por qualquer razão, diz-se: "tempo de inatividade."

Tempo de inatividade: refere-se a um período de tempo ou uma percentagem do período de tempo que uma máquina ou sistema (geralmente um servidor de computador) é desligada,

geralmente como resultado de qualquer falha no sistema (por exemplo, um acidente) ou a manutenção de rotina . O oposto é o tempo de atividade. Mesmo no início da época e-business, mais de uma década atrás, Datamation (1995) enfatizou a importância de o tempo de inatividade do sistema. Em agosto de 1995, Datamation citou os resultados de uma pesquisa com 400 empresas de grande porte, que revelou que, "... o tempo de inatividade de uma empresa custa 1.400 dólares por minuto, em média. Com base nesses números, 43 horas de tempo de inatividade por ano custaria US $ 3,6 milhões.

Tempo de atividade: é uma medida do tempo em que um sistema de computador está em operação. Ele é frequentemente usado como uma medida de confiabilidade do sistema operacional do computador e estabilidade. Este tempo representa o tempo que um computador pode ser deixado sozinho sem deixar de funcionar, ou a necessidade de ser reiniciado para muitos fins administrativos ou de manutenção. Nos negócios modernos, mesmo alguns minutos de tempo de inatividade do sistema pode causar milhares ou mesmo milhões em receitas perdidas. Além disso, tais situações podem resultar em decisões ruins, clientes insatisfeitos, imagem quebrada da empresa. Simplificando, quando aplicações de missão crítica são considerados, o tempo de inatividade do sistema (tanto planejado ou não) devem ser evitados ou minimizados. Este fato reforça a necessidade de sistema de confiabilidade, disponibilidade e escalabilidade. IDC (2006) ressalta o fato de que um modelo geral a alta disponibilidade elevada o conceito de disponibilidade para além de uma perspectiva de infra-estrutura, em termos de sistema ou de servidores. Existem muitas definições para a disponibilidade. Alguns consideram a disponibilidade dos dados apenas, enquanto outros falam em aplicações de disponibilidade ou indisponibilidade do servidor ou subsistema de armazenamento.

De acordo com o relatório apresentado por Adam Associates (Stanton, 2005), só no Reino Unido, o custo anual de interrupção de negócios está estimado em £ 3,9 bilhões. O tempo de interrupção média causado por incêndio é de 28 dias, 26 dias para um roubo e 10 por inundação. Falhas de TI levam uma média de 10 dias para se recuperar, e até mesmo uma falha de energia pode levar até 24 horas.

Tempo de inatividade zero significa que o servidor estava disponível o tempo todo. Para servidores que têm o tempo de inatividade acima de 1% por ano que pode ser considerado como inaceitável, tal como o que significa um tempo de manutenção de mais de 3 dias por ano.

Um estudo de 2002 do Standish Group (Graham & Sherman, 2003) descobriram que a aplicação de missão crítica média teve a seguinte estimativa de inatividade:

9% das empresas - maior do que 99,99% (menos do que uma hora para baixo por mês)

24% - 99,91% e 99,99% (uma hora a menos de nove horas)

67% - 99,9% ou menos (nove horas ou mais).

Tabela 1: Estimativa de tempo de Inatividade

Tempo de Atividade Estimado (%)	Tempo de inatividade por dia	Tempo de inatividade por mês	Tempo de inatividade por ano
95	72 minutos	36 horas	18,26 dias
99	14,4 minutos	7 horas	3,65 dias
99,9	86,4 segundos	43 minutos	8,77 hoas
99,99	8,64 segundos	4 minutos	52,6 minutos
99,999	0,86 segundos	26 segundos	5,26 minutoa

Maiores Causas de Tempo de Inatividade

- Defeitos ou falhas de software
- Tempo de inatividade
- Erro do operador
- Hardware: interrupção ou manutenção
- Construção: local do desastre (incêndio)
- Desastre Metropolitano: inundação, tempestade, etc

1.2 Os efeitos dos desastres

Os eventos listados anteriormente têm o potencial para causar danos aos edifícios, equipamentos e sistemas de TI. Eles afetam as pessoas, ferindo e deslocando-os, para não mencionar impedindo-os de comparecer ao trabalho. Os desastres podem ter os seguintes efeitos sobre as organizações:

Dano direto: Muitos desses eventos podem danificar diretamente os edifícios, equipamentos e sistemas de TI, tornando inabitável edifícios e sistemas inutilizável.

Inacessibilidade: Muitas vezes, um evento danifica um edifício, de tal forma que não é seguro para entrar. Autoridades civis podem proibir o pessoal de entrar em um edifício, até mesmo para recuperar artigos ou equipamentos.

Queda dos serviços: Mesmo em incidentes que não causam danos diretos, energia elétrica, água e gás natural são frequentemente interrompido para grandes áreas por horas ou dias. Sem serviços públicos, os edifícios são muitas vezes inabitável e sistemas incapaz de funcionar.

Interrupção nos Transporte: incidentes generalizados, muitas vezes têm um efeito sobre o transporte regional, incluindo as principais rodovias, estradas, pontes, ferrovias e aeroportos. Interrupções nos sistemas de transporte podem impedir os trabalhadores de comparecimento ao trabalho (ou indo pra casa), evitar o recebimento de suprimentos, e impedir a expedição de produtos.

Interrupção nas Comunicação: A maioria das organizações dependem comunicação de dados e voz para as necessidades diárias operacionais. Desastres frequentemente causam interrupções generalizadas na comunicação, seja por danos diretos à infra-estrutura ou picos repentinos no uso relacionados ao desastre. Em muitas organizações, a perda de comunicações - comunicações de dados em especial - é tão devastador como fechar os seus sistemas de TI.

Evacuações: Muitos tipos de catástrofes representam uma ameaça direta às pessoas, resultando em evacuações obrigatórias de determinadas áreas ou regiões inteiras.

Ausência do Trabalhador: Quando ocorre uma catástrofe, os trabalhadores muitas vezes não podem se apresentar ao trabalho, por muitas razões. Trabalhadores com as famílias muitas vezes precisa de cuidados para as famílias se o desastre afetar a mesma. Só depois de cuidarem de suas famílias que os trabalhadores consideram comparecer ao trabalho. Além disso, a interrupção no transporte pode impedi-los de chegar ao trabalhar.

Estes efeitos podem devastar empresas, fazendo com que deixem de operar por horas, dias ou períodos mais longos. Na maioria dos casos, as empresas simplesmente não podem sobreviver depois de experimentar tal falha. As empresas fornecem bens e serviços para os clientes que, em sua maior parte, só querem esses bens e serviços, se os clientes não podem obter esses produtos ou serviços de uma empresa, muitas vezes eles simplesmente vão para outra que pode fornecê-los. Muitas empresas não se recuperam de tal êxodo de clientes.

1.3 Desastres menores ocorrem com mais frequência

Não cometa o erro de justificar a falta de um plano de RIPC por pensar que furacões ou ventanias raramente visitam sua área de trabalho, terremotos ocorrem apenas a cada cem anos, ou apagões nunca vão ocorrer. Todas essas afirmações podem tornar-se verdade.

No entanto, os desastres em escalas menores acontecem com muito mais frequência, muitas vezes centenas de vezes mais do que os grandes.

Desastres menores como incêndios de construção, tubos com ruptura que inundam escritório, falha no servidor que resultam em dados corrompidos, falta de energia prolongada, tempestades , graves, e assim por diante ocorrer com regularidade muito maior do que grandes desastres.

Qualquer um desses pequenos eventos potencialmente pode interromper processos críticos de negócios por alguns dias. Nas empresas de serviços de tempo crítico, esta interrupção pode ser um golpe fatal. O artigo: “The Business Case For Disaster Recovery Planning: Calculating The Cost Of Downtime” constata que 40% (quarenta por cento), das empresas fecharam por três dias ou mais devido a falhas em 36 meses. Uma interrupção não planejada pode ser o começo do fim de uma organização, tudo começa a ir ladeira abaixo a partir desse ponto em diante. Esse pensamento preocupante deve incutir preocupação na gerência.

1.4 RIPC Obrigatórios

A implementação de planos de recuperação de desastre e resposta a incidente parecer ser uma boa ideia, mas padrões e regras tem aparecido através de normas e padronizações.

PCI DSS (Payment Card Industry Data Security Standard): apesar de não ser uma lei governamental, é obrigatório em empresas que prestam serviços financeiros. Trata-se de “legislação privada”, ou seja criada por empresas e não pelo governo. Todos os bancos e empresas de cartoão de crédito as utilizam.

NBR ISO/IEC 27001: utilizada em larga escala, esta norma internacional de segurança da informação possui um bom reconhecimento entre as empresas de TI.

BS25999: trata-se de uma norma internacional emergente para continuidade de negócio.

NR 23 - Proteção Contra Incêndios : É uma norma regulamentadora do trabalho urbano, cujo título é “Proteção Contra Incêndios”, estabelece as medidas de proteção contra incêndios de obrigatória nos os locais de trabalho, para proteger a saúde e integridade física dos trabalhadores. A NR 23 tem a sua existência jurídica assegurada em nível de legislação ordinária, no inciso IV do artigo 200 da CLT (Consolidação das Leis do Trabalho).

1.5 Os benefícios do RIPC

Além da prontidão óbvio para sobreviver a um desastre, as organizações podem desfrutar de vários outros benefícios de planejamento de DR:

Melhoria dos processos de negócios: Como os processos de negócio passam por essa análise pode-se encontrar áreas para melhoria.

Tecnologia melhorada: Muitas vezes os sistemas de TI apoia os objetivos do projeto de

recuperação. A atenção utilizada para implementar a recuperação também deixa os seus sistemas de TI mais consistente e portanto, mais robusto e gerenciável.

Menos interrupções: Como um resultado da tecnologia melhorada, sistemas de TI tendem a ser mais estáveis que no passado. Além disso, quando você faz alterações em arquitetura de sistema para atender a objetivos de recuperação e continuidade, eventos que costumavam causar interrupções não o fazem mais.

Serviços de maior qualidade: devido a melhoria de processos e tecnologias, os serviços, tanto internamente quanto para clientes e parceiros também melhoram.

Vantagens competitivas: Ter um bom RIPC dá à empresa vantagens sobre seus concorrentes. Preço não é necessariamente o único ponto em que as empresas competem. Um plano de RIPC permite que uma empresa reivindique maior disponibilidade e confiabilidade nos serviços.

A empresa muitas vezes não espera esses benefícios, a menos que implemente seu plano de recuperação de desastres.

1.6 Iniciando um Plano de Recuperação de Desastres Provisório

Sua empresa possui muitos processos críticos? quantos processos de negócios sensíveis ao tempo que a sua organização tem? A sua organização tem um plano de recuperação de desastres?

Se a organização não tem um plano de RIPC, a implementação de um plano completo pode levar um ou dois anos, deixando sua empresa exposta. Embora isso possa ocorrer, você pode começar com uma plano provisório que fornece algum valor para a organização, enquanto o plano é completado.

1.6.1 Começando com um plano provisório

É possível desenvolver um plano provisório, projetado como um plano a ser substituído, rapidamente. Ele deve aproveitar as capacidades atuais e não aborda todas as mudanças de tecnologia necessárias durante o longo curso.

Um plano provisório é um plano de resposta à pergunta: "Se ocorrer um desastre amanhã, que medidas podem ser tomadas para recuperar os sistemas?"

Embora um plano completo leva muitos meses ou até anos para ser concluído, o desenvolvimento de um plano provisório leva apenas dois a quatro dias do início ao fim. O procedimento para o desenvolvimento de um plano provisório é simples: Coloque dois ou três especialistas em determinado assunto em uma sala por um dia. Normalmente, essas especialistas são funcionários de linha ou gerentes de nível médio que estão familiarizados com os processos

críticos do negócio e os sistemas de suporte de TI. Com os meios existentes, a equipe desenvolve o plano de RIPC provisório, seguindo estes procedimentos:

Construir a equipe de resposta de emergência. Identificar especialistas em temas-chave da matéria que podem construir o ambiente a partir do zero, caso a empresa tenha uma necessidade.

Procedimento para declarar um desastre. Um procedimento simples que a equipe de resposta de emergência pode usar para decidir se os eventos garante declarar um desastre.

Invoque o plano de RIPC. O procedimento para a obtenção do esforço de resposta a desastres em curso.

Comunicar durante um desastre. Quem a equipe de resposta a desastres precisa se comunicar com e o que dizer. Esta lista de pessoal pode incluir outros funcionários, clientes e os meios de comunicação.

Identificar planos de recuperação básicos. Estabelecer procedimentos que podem colocar sistemas críticos funcionando novamente.

Decretar medidas preventivas. Que passos a organização pode tomar rapidamente, com antecedência, para tornar a recuperação mais fácil, assim como medidas para evitar um desastre.

D**ocumentar o plano de DR provisório**. Anote todos os procedimentos, listas de contatos e outras informações vitais que a equipe desenvolve durante o processo de planejamento.

Treinar os membros da equipe de resposta de emergência. Treinar os membros de emergência de resposta da equipe que a equipe escolhe.

A organização não deve contar com este plano por um longo período. É um substituto pobre para um plano de RIPC completo, mas pode fornecer alguma capacidade de resposta a desastres no curto prazo. O plano provisória não é um plano um completo, e não gera a confiança de um plano real. Os peritos que criam o plano provisório devem revê-lo a cada três ou quatro meses, até deixa-lo completo.

1.7 O projeto completo

O mais cedo possível depois de desenvolver o plano provisório, é necessário iniciar o plano completo. O tempo para desenvolver um plano completo varia consideravelmente com base no tamanho da organização, o número de funções críticas de negócios, e do nível de comprometimento que a empresa está disposta a fazer.

Estima-se que o desenvolvimento de um projeto leve três meses para organizações menores (menos de 100 empregados com apenas uma ou duas aplicações críticas) e dois anos para uma grande organização (milhares de funcionários e várias aplicações críticas). Mas existem muitas

outras variáveis, além do tamanho da empresa a considerar.

1.7.1 Ter apoio da gerencia

Plano de recuperação são perturbadores. Ele exige os melhores e as mais brilhantes mentes do negócio, isso mantem estes profissionais longe dos projetos. Do ponto de vista estritamente financeiro, planejamento de recuperação de desastres não oferece rentabilidade, nem torna a organização mais eficiente ou eficaz (embora ambos pode acontecer).

Um plano de RIPC não tem um ROI (retorno sobre investimento). Tanto o planejamento de recuperação de desastre como a política de segurança da informação são preparação para e evitar eventos que nunca espera-se que aconteça (o fato dos eventos não acontecer é o retorno do seu investimento). Um plano é um bom investimento para qualquer (ou todas) as seguintes razões:

Preparação para emergências e sobrevivência: O benefício mais óbvio de um plano é a sobrevivência da organização de um desastre, sobrevivência que vem como resultado de um planejamento e preparação.

Prevenção de desastres: planejamento de recuperação de desastres, muitas vezes leva à melhoria de processos e sistemas de TI, fazendo com que os processos e sistemas se tornem mais resistentes. Eventos que possam resultar em uma interrupção de negócios grave após o plano de RIPC tornar-se, em muitos casos, apenas um evento menor. Tabela 1-1 inclui alguns exemplos de eventos e seu impacto sobre as organizações.

Devido cuidado: Poucas organizações nunca tiveram um acidente ou evento que resultou na perda de dados. Negligenciar a necessidade de planejamento de recuperação de desastres pode ser tão grave quanto um crime. O planejamento protege os dados contra perda. Se uma organização não consegue exercer esse devido cuidado, pode enfrentar processos cíveis ou criminais se um desastre evitável destrói informações importantes.

Tabela 2: Exemplos de Eventos sem e com um plano de DR

Evento	sem um plano de RIPC	Com um plano de RIPC
Queda do servidor e corrupção de dados	Vários dias para reconstruir os dados da mídia de backup	Recuperação de servidor de backup ou mídia de backup baseado em disco
Fogo	Servidores danificadas por fumaça ou materiais de extinção; vários dias para reconstruir os dados da mídia de backup	Supressão precoce de incêndio, resultando em danos mínimos e baixo tempo de inatividade

Mau tempo, resultando em quedas de energia prolongadas	Capacidade de energia insuficiente para realizar backup, resultando em vários dias de tempo de inatividade	Energia de reserva suficiente ou transferência para servidores em centro de processamento alternativo
Sabotagem e Virus	Queda por vários dias para reparar os dados corrompidos	Recuperação de mídia de backup recentes
Grandes incêndios ou inundação	Evacuação de pessoal; servidores encerrado devido à falta de gerência no local	Transferência para servidores em centro de processamento alternativo

1.7.2 Compreender a frequência de eventos relacionados com o desastre

Ter uma ideia precisa da frequência que algumas desastre ou eventos ocorrem pode ser difícil. Alguns eventos, como vulcões e tsunamis, acontece tão raramente que torna-se difícil quantificar a probabilidade, para não mencionar a estimativa do impacto, quase impossível.

É possível prever estatisticamente outros eventos, tais como inundações, um pouco mais fácil (principalmente porque ocorrem com mais frequência e é previsível), mas mesmo assim estes eventos variam em intensidade e efeito. Se a sua organização tem algum tipo de apólice de seguro que cobre desastres, a companhia de seguros pode ter algumas informações úteis sobre a cobertura de desastres. Além disso, as companhias de seguros podem oferecer um desconto de prêmio para organizações que têm um plano de recuperação de desastres bem implementado.

1.7.3 Primeiros passos importantes em um projeto de RIPC

Depois de ganhar o apoio da diretoria ou gerência, é preciso tomar algumas medidas importantes antes de iniciar o projeto:

Criar uma carta do projeto. É um documento formal que define um projeto importante. A abertura do projeto típico inclui as seguintes seções:

- Definição do projeto
- Os nomes dos patrocinadores executivos
- Os objetivos do projeto
- O escopo do projeto
- Os principais marcos
- Principais responsabilidades
- Fontes de financiamento
- Assinaturas

Selecione um gerente de projeto. Um indivíduo com experiência de gestão de projetos e alguém com habilidades que possa desenvolver e acompanhar o plano, trabalhar com os membros da equipe do projeto, criar relatórios de status, executar projeto.

Criar um plano de projeto. Uma descrição muito detalhada de todos os passos necessários para completar o projeto - a sequência necessária de passos, quem vai executar essas etapas que passos são dependentes de outros passos, e que custos (se houver) estão associados com cada etapa.

Formar uma comissão de direção. Os executivos e gerentes seniores que estão patrocinando e apoiando o projeto deve escolher membros para um comitê de direção formal. O comite de direção deve ter a supervisão do executivo sobre a equipe do projeto.

1.8 Gerenciando o Projeto de RIPC

Comece o projeto com uma reunião inicial que pode durar de uma a três horas. Devem participar a equipe do projeto inteiro, os membros do comitê de direção, todos os patrocinadores executivos, e todas as outras partes envolvidas.

O comitê gestor deve declarar seu apoio ao projeto. Após a reunião inicial, a equipe do projeto provavelmente deve reunir-se toda semana para discutir questões de progresso, e quaisquer ajustes que precisam ser feitos no projeto. O gerente de projeto deve publicar um relatório sobre o estado a cada semana que houver reunião. O relatório de status deve sr enviado para todos os membros do comitê de direção para mantê-los atualizados sobre a forma como o projeto está progredindo. É necessário gerenciar muitos detalhes emr um projeto que se estende por muitos departamentos.

1.8.1 A realização de uma Análise de Impacto no Negócio

A primeira tarefa importante em qualquer projeto de recuperação de desastres envolve a identificação das funções de negócio, na organização, que requerem planejamento. Pode ser necessária uma análise de risco de cada função de negócio fundamental para quantificar o efeito na organização se algo interromper cada uma dessas funções por um longo tempo. Esta atividade é conhecida como Análise de Impacto no Negócio (BIA), porque ele analisa o impacto que cada processo crítico tem sobre o negócio.

1.8.2 Definir o tempo de inatividade máximo tolerável (TIMT)

Para cada processo crítico, a equipe precisa determinar uma medida importante - a maior quantidade de tempo que o processo pode não estar disponível antes que a indisponibilidade ameaça a própria sobrevivência do negócio.

Este valor é conhecido como o tempo de inatividade máxima tolerável (TIMT). É possível

medir uma TIMT em horas ou dias. Definir o TIMT para um determinado processo pode parecer arbitrária, e é. Os membros do comitê de direção envolvidos devem definir os números para cada TIMT.

Pode ocorrer alguns problemas de definição de uma TIMT:

Rigorosamente falando, um TIMT é hipotético.

Pode existir dificuldade em encontrar exemplos válidos de organizações pares que falharam por causa de um incidente crítico.

1.8.3 Definir os objetivos de recuperação

Depois de definir o TIMT para cada processo crítico, é necessário definir alguns objetivos de recuperação específicos para cada processo. Definir os objetivos de recuperação também é arbitrário. Os dois objetivos principais de recuperação que normalmente definidos em uma BIA são:

Objetivo do tempo de recuperação (OTR): O período máximo de tempo que um processo de negócio não estará disponível antes de reiniciá-lo. Por exemplo, definir um RTO de 24 horas. Se desastre teve início às três horas, com um RTO de 24 horas, significa que o processo de negócio deve reiniciar às três horas do dia seguinte.

O OTR deve ser menor do que o TIMT deve ter menos de dois dias,em outras palavras, se o negócio irá falhar caso um determinado processo de negócio torne-se disponível por dois dias, o tempo de recuperar esse processo deve ser menos de dois dias.

Objetivo do ponto de recuperação (OPR): A quantidade máxima de perda de dados que sua organização pode tolerar se um desastre interrompe um processo de negócio crítico. Por exemplo, digamos que o OPR para um processo seja de uma hora. Quando reiniciar o processo de negócio, os usuários não perdem mais de uma hora de trabalho.

1.8.4 Desenvolver a análise de risco

Depois de definir objetivos de recuperação, é necessário completar uma análise de risco. Para cada processo de negócio crítico, é preciso determinar o seguinte:

Prováveis cenários de desastre: A lista dos desastres graves que podem eventualmente ocorrer. Não detalhe cenários altamente improváveis, como um tsunami.

Probabilidade de ocorrência: A probabilidade que cada cenário pode realmente acontecendo. Pode ser usar uma escala de alta-média-baixa.

Vulnerabilidades: Identificar todas as vulnerabilidades razoáveis dentro de cada processo de negócio. Vulnerabilidades são fragilidades que contribuem para a probabilidade de que um evento

como uma inundação ou terremoto causem um dano significativa.

Medidas atenuantes: para cada vulnerabilidade lipoucos processos críticos de negócio. Um modo de agilizar o processo de análise de risco: Em vez de desenvolver uma lista de todos os cenários de desastre para cada processo de negócio, a equipe pode listar todos os cenários para cada local de negócios.

1.8.5 Uma visão geral

Depois de concluir o TIMT, OTR, OPR e a análise de risco para cada processo de negócio, é necessário condensar as informações em uma planilha simples para poder ver todos os processos de negócios em uma página, juntamente com seu respectivo TIMT, OTR e OPR.

Caso a lista seja ordenar a partir do OTR, é possível ver quais os processos precisam se recuperar primeiro após um desastre. Se ordenar por OPR, pode ver quais processos são os mais sensíveis à perda de dados.

Você pode adicionar uma coluna que expressa o custo ou esforço necessário para atualizar cada processo, para que o mesmo possa ser recuperado dentro do prazo estabelecido pelo seu OTR e OPR. Essas quantidades necessárias podem ser expressas usando símbolos como $, $ $, $ $ $, e $ $ $ $, onde cada $ representa milhares de dólares. A $ representa milhares de dólares, $ $ significa que dezenas de milhares, e assim por diante.

Com esta planilha de alta qualidade, é possível ver todos os processos críticos de negócio, as medidas chave para cada um, classificar os processos e quais processos são os mais críticos na organização. Os processos críticos, é claro, exigem mais trabalho, em termos de planejamento de recuperação de desastre.

1.8.6 Tempo para decisões

Às vezes, uma equipe pode ficar sobrecarregada pelo número de processos críticos e o custo cumulativo estimado de cada processo para obter um ponto em que a organização pode recuperá-lo dentro dos prazos estabelecidos. Algumas soluções:

Rever objetivos de recuperação. Quando o objetivo de recuperação e investimento estimado estão lado a lado, os gerentes seniores podem tomar algumas decisões sobre a quantidade de investimento para um determinado processo. As estimativas iniciais pode colocar o custo da adaptação de recuperação a um valor mais elevado do que o valor do próprio processo. Os gerentes podem ajudar a colocar limites sobre o valor a ser gasto.

Combine capacidades de recuperação. É possível combinar o investimento provavelmente

para melhorar o tempo de recuperação para várias aplicações, o que pode reduzir os custos. Por exemplo, o investimento em um sistema de armazenamento único grande custa muito menos do que os sistemas de armazenamento separados.

Melhoria dessas estimativas. A equipe do projeto podem fazer um trabalho mais detalhado sobre os investimentos necessários para melhorar o tempo de recuperação para aplicações através da elaboração de arquiteturas reais e planos e em seguida, obter estimativas reais para investimento.

Faça um investimento multi-ano em recuperação. Após a obtenção de estimativas precisas para melhorar a recuperação de aplicativos, é possível planejar um investimento de vários anos que melhore as aplicações mais críticas no primeiro ano e menos aplicativos críticos em anos subsequentes.

Faça o mais crítico agora e o resto mais tarde. A equipe pode desenhar uma linha sobre o gráfico, manipulando processos acima da linha (aqueles que são os mais críticos) no projeto atual e os processos abaixo da linha (aqueles que são menos críticos) em projetos futuros RIPC.

1.9 Desenvolvimento de procedimentos de recuperação

Depois que a equipe de planejamento de RIPC concordam com objetivos de recuperação (OTR e principalmente OPR) e escolhe a lista de processos, é necessário desenvolver os procedimentos de recuperação de desastres para cada processo.

1.9.1 Mapeamento de processos em infra-estrutura

Antes de começar a preparar os procedimentos de recuperação reais para aplicativos, é preciso saber exatamente quais aplicativos e infra-estrutura subjacente apoiam os processos.

Embora parte das estimativas de custo para recuperação da BIA já tenha sido feita, é necessário mais detalhes agora.

Quando uma organização sabe todas as partes e peças que suportam um aplicativo, então é possível começar a desenvolver planos de recuperação de aplicação, caso ocorra uma catástrofe.

1.9.2 Desenvolver planos de recuperação

Quando se pensa sobre isso, é necessário fazer uma incrível quantidade de trabalho inicial e planejamento antes de começar a elaboração de planos de recuperação reais. A recuperação de desastres tem muitos aspectos, pode ser necessário recuperar porções diferentes de um ambiente, dependendo do escopo e magnitude do desastre que os ataques. O pior cenário (como um terremoto, furacão, greve, inundação, ou qualquer tipo de desastre pode acontecer em sua parte do mundo), isso provavelmente pode tornar o seu estabelecimento de trabalho completamente danificado ou

destruído ,exigindo que o negócio continue em outro lugar. Assim, durante o planejamento RIPC, podem ser considerados vários aspectos do negócio e sua infra-estrutura:

Os usuários finais: A maioria dos processos de negócio dependem de empregados que executam suas funções de trabalho. Essas estações de trabalho dos funcionários pode precisar de recuperação após um desastre. No pior caso, todas as estações de trabalho são danificados ou destruídos (por água, cinzas vulcânicas, ou qualquer outro). Os funcionários também precisam de um lugar para trabalhar. Quando se desenvolve planos de contingência para a localização de servidores críticos, incluem acomodações de trabalho para os seus colaboradores críticos.

Instalações: É necessário recuperar o prédio(s) em que a organização abriga seus sistemas de TI. Se esses prédios estão danificados, é necessário repará-lo ou identificar instalações alternativas. Não, não ir às compras para o espaço durante um desastre é necessário resolver tudo com antecedência.

Sistemas e redes: O coração dos sistemas de TI são os servidores que rodam os aplicativos ou armazenam as informação. Em cenários de pior caso, os servidores são danificados, por isso é necessário reconstruí-los a partir do zero.

Nenhum servidor é uma ilha, então é preciso e recuperar a capacidade de um servidor para se comunicar com outros servidores e estações de trabalho do usuário final.

Dados: é o coração da maioria dos aplicativos de negócios. Sem dados, a maioria das aplicações são praticamente inúteis. A recuperação de dados é complicada, porque os dados muda o tempo todo, até o momento em que um desastre ocorra. É possível recuperar dados de muitas maneiras diferentes,

Medidas preventivas: Dentro do contexto do desenvolvimento de planos de recuperação, a empresa terá muitas oportunidades para melhorar as aplicações, sistemas, redes e dados tornando-os mais resistentes .

2 Necessidades para Inicializar um plano RIPC

Neste capítulo:

Iniciando um plano de RIPC

Compreender os recursos necessários

Planejando Operações de emergência

Desenvolver e testar um plano provisório

Colocar uma plano de recuperação de desastres em funcionamento em uma organização pode levar um ano ou dois, desde o início com a Análise de Impacto no Negócio, para planejar o desenvolvimento até os testes.

Um plano de RIPC adequado deve envolver todo o negócio (ou, pelo menos, as partes do negócio escolhidas para o projeto).

Deve ser realizada uma profunda análise de processos de negócio; desvendar e analisar as dependências entre os processos, sistemas de informação, bens e fornecedores, para finalmente iniciar o plano. Para desenvolver um bom plano é necessário um esforço considerável. É possível tomar algumas abordagens diferentes para começar, como formas de lidar com falhas operacionais ou riscos:

Conduzir um projeto completo: Começar com a Análise de Impacto no Negócio (BIA), análise de criticidade, análise de risco e planos de recuperação específicos para sistemas de TI.

Comece com um projeto de curto prazo: Pode-se decidir construir uma operação de emergência primeiro, apenas no caso de ocorrer um desastre antes de concluir o plano principal. Criação de um plano de emergência – basicamente é estabelecida uma estrutura de comando-e-controle para um plano de comunicação sem qualquer procedimento de recuperação real - pode ajudar a identificar e documentar estruturas hierárquicas (top-down), de gestão e de comunicação que precisam ocorrer durante um desastre.

Desenvolver um plano provisório: É possível elaborar um plano de DR provisória que trata de medidas específicas para manter os sistemas de TI que suportam os processos críticos de negócios em funcionamento o mais rápido possível. Um plano provisório não é um plano completo, e não é um substituto para um, mas isso fornece alguma proteção no caso de uma catástrofe, antes de terminar o plano completo.

Antes de iniciar um esforço para a criação de planejamento para o plano de RIPC, é necessário imaginar os efeitos que um desastre poderia causar em sua organização. Planejamento de um PRIPC é sobre prevenção e resposta a desastres, e para planejar adequadamente, é necessário

saber o que planejar. A seguir serão mostrados os efeitos dos desastres, e como usar prevenção e planejamento para reduzir seus efeitos.

2.1 Compreender o papel da prevenção

Não se pode evitar catástrofes naturais ou desastres feitos pelo homem. No entanto, é possível controlar um pouco o impacto que um desastre tem nas operações de sua empresa, reduzindo o impacto do desastre sobre o negócio.

No planejamento de recuperação de desastres, prevenção significa aprovar medidas de antecedência que diminuam ou eliminar os efeitos que um desastre pode ter em processos críticos de negócio. A seguir estão alguns exemplos:

Energia de emergência: Uma organização pode ser capaz de mitigar os efeitos de um desastre, investindo em equipamentos de geração de energia de emergência que pode produzir eletricidade, mesmo quando os serviços públicos não estão disponíveis por vários dias ou mais.

Vários caminhos de comunicação: Se reconhecer que muitos desastres são causados por interrupções de comunicação, o risco pode ser mitigado, investindo em capacidades secundárias e terciárias de comunicação que podem continuar funcionando, mesmo se as instalações principais estão danificados.

Computadores de backup em outra cidade: uma empresa que atende clientes através da Internet pode ser capaz de fornecer esses serviços a partir de praticamente qualquer lugar, se esses recursos podem ser concebidos em desde o início.

Apesar de nenhuma das medidas na lista anterior prevenir desastres, essas medidas podem ajudar uma organização a continuar a operar depois de um desastre acontece. Todas essas medidas exigem planejamento prévio e de investimento. O tempo para equipar um transatlântico com coletes salva-vidas é antes de deixar o porto, não depois que o navio começa a afundar.

2.2 Compreender o papel do planejamento

As seção anteriores falam sobre as medidas que podem ser tomar para diminuir os efeitos dos desastres. Estas medidas são a essência do planejamento de recuperação de desastre. Planejar-se para cenários com antecedência, e se preparando para eles através do investimento em equipamentos e treinamento, constituem a maior parte do planejamento do plano de RIPC.

A parte de planejamento do planejamento envolve descobrir o que o pessoal deve fazer quando um desastre ocorrer. Quando o terremoto, tsunami, furacão, deslizamento de terra, ou até mesmo uma greve ocorrer, o que as pessoas precisam fazer para manter os sistemas críticos em

execução? Se um centro de processamento dinundar, destruindo equipamentos, como a organização pode continuar a manter os seus sistemas críticos de TI funcionando? Estes e muitos outros cenários exigem antecedência planejamento para o pessoal de operações de emergência saber como manter esses sistemas. O planejamento prévio é a chave para a sobrevivência quando ocorre uma catástrofe.

2.3 Recursos para começar o planejamento

Para colocar o projeto de recuperação de desastres em andamento, muitos recursos de diferentes partes do da empresa são necessários. O projeto requer pessoas com uma ampla variedade de habilidades, assim como uma grande quantidade de informações e para obter essa informações é necessário envolver ainda mais pessoas.

Iniciar um projeto não é tarefa fácil. Planejamento de recuperação de desastres é complicado e multi-disciplinar. É provável que seja um dos maiores projetos que a maioria das organizações se comprometem, e reúne muitas pessoas que normalmente não se associam entre sio. Por essas e outras razões, é preciso muitos recursos importantes antes de iniciar um projeto como:

Um Executivo ou dono de empresa interessado no projeto: Um gerente sênior, executivo ou dono de empresa que está disposto a ir até o fim do projeto e disposto a colocar seu dinheiro no projeto.

Orçamento: Nos estágios iniciais de um projeto, é necessário um gerente de projeto, especialistas em tecnologia, especialistas de processo, ou ajuda suplementar de alguns departamentos. Nas fases posteriores do projeto, será necessário investir em melhorias de tecnologia para apoiar os objetivos de recuperação.

Gerente de projeto: Um gerente de projeto forte em tempo parcial ou total para um projeto multidisciplinar que pode envolver dezenas de pessoas ou mais.

Especialistas no assunto: um especialistas em processos de negócios que a organização tem em jogo, particularmente os processos que tratam com os clientes ou serviço. Podem ser necessários especialistas em tecnologia que compreendem as aplicações de TI e infra-estrutura que suportam esses processos.

Pessoas com habilidades de escrita: nas fases posteriores do projetos exigem que pessoas que possam escrever os processos e procedimentos de forma que qualquer um possa entender.

Um projeto típico pode levar de três meses (para a menor organização) a bem mais de um ano para ser concluído. A rapidez com que um plano é criado depende da prioridade e quanta verba extra a empresa tem disponível para gastar. Segue abaixo algumas sugestões quando não existe um bom controle sobre a quantidade de recursos que o projeto vai consumir:

Contratar um consultor: trazer um consultor experiente para um compromisso de curto prazo por não mais do que alguns dias, para dar um "olhada" e fazer algumas estimativas no dimensionamento do projeto.

Desenvolver um plano provisório: é necessário desenvolver um plano provisório, de qualquer maneira, para escrever este plano, será necessário saber o número de processos críticos, sistemas, fornecedores, e assim por diante. Essas informações podem ajudar a estimar o tamanho e o escopo do plano do real.

2.4 Planejamento das Operações de Emergência

Depois de um desastre, a equipe de resposta a incidente ou desastres começa a desempenhar as suas várias tarefas que se relacionam com a avaliação, reiniciar e recuperação dos sistemas críticos de TI que suportam os processos de negócios críticos.

Resposta a desastres envolve mais do que apenas as pessoas que estão recuperando de sistemas, o pessoal de resposta a outros desastres têm que executar uma variedade de atividades, incluindo comunicação com os clientes, gestão de empresa, fornecedores e parceiros.

Como a resposta a desastres se desenrola, um grande número de pessoas vão trabalhar, comunicar e tomar decisões.

Controlar todas essas atividades requer considerável gestão, liderança e planejamento. Planejamento de Operações de Emergência é a parte do planejamento de recuperação de desastre associado com a configuração e as operações de de emergência durante e imediatamente após um desastre.

O objetivo principal do Planejamento de Operações de Emergência é garantir que a gestão da empresa possa continuar a gerir as operações do dia a dia, incluindo esforços de reação a catástrofes, durante e imediatamente após um desastre. Um plano de Planejamento de Operações de Emergência podem incluir:

Listas de contatos de emergência: O pessoal precisa saber como entrar em contato uma com a outra quando um desastre ocorrer.

Procedimento de declaração de desastre: O pessoal precisa saber reconhecer quando um evento atrapalha as atividades chave de negócios, o suficiente para iniciar a resposta a desastres.

Comunicações de emergência: procedimentos de comunicação, informações de contato pessoal e recursos adicionais, e talvez um roteiro de comunicações para os clientes ou acionistas.

O plano de operação de emergência pode também incluir o estabelecimento de um Centro de Operações de Emergência (COE). As grandes organizações, muitas vezes configuram um comando de emergência e centro de controle como o centro nervoso para suas operações de emergência

durante um desastre.

2.5 Preparar um plano provisório

A maioria das organizações pode reconhecer os riscos associados com a ausência de um plano de recuperação de desastres. Se uma empresa não pode ter um plano completo testado por mais de um ano, então ela pode pode querer ter algo no lugar enquanto completar o plano de RIPC completo. Muitas vezes, um plano RIPC provisório pode preencher esta lacuna. Este plano pode ser criado de forma rápida e com o mínimo esforço. Não é, evidentemente, tão amplo como um plano de completo. É como rebocar um carro com uma corda quando na realidade o motor está com defeito, mas pode ajudá-lo a sair de uma situação ruim.

As seções seguintes descrevem uma forma de construir um plano provisório. A seguir estão as características gerais de um plano provisório:

É construído de forma rápida, normalmente em menos de 15 a 20 horas-homem.

Ele é construído com uma quantidade relativamente baixa de esforço.

Ele fornece ao negócio alguns recursos limitados, se uma catástrofe ocorrer antes do plano completo estar concluído

Não é nenhum substituto para o plano completo que a sua organização deve (ou deveria) a trabalhar.

Por que a organização deve construir um plano provisório? Estatisticamente falando, os desastres raramente ocorrem, mas quando ocorrem são graves. Por exemplo, se sua organização está localizada em uma área de inundação que ocorrem a cada dez anos ou mais, as chances são de 1 em 25 de que uma enchente vai ocorrer nos próximos dois anos , este incidente ocorrerá antes de completar o plano completo, para lidar com o dilúvio. O plano provisório abordará o que fazer se a inundação acontece nos próximos dois anos. Este plano ajuda a manter o negócio à tona, mas não é um substituto para um plano real.

2.6 Pessoal da equipe do plano provisório

Os membros da alta administração ou executivo que estão patrocinando o esforço para a realização do plano provisório devem selecionar dois ou três gerentes experientes para a elaboração do plano provisório. Esses gerentes devem ter conhecimento pragmático e conhecimento das operações e processos de negócios atualmente em vigor. Trata-se de um grupo provisório. A alta administração deve encontrar este grupo e coloca-los em uma sala de conferência, proporcionando-lhes um quadro branco, um par de computadores portáteis, e carta branca na elaboração.

Em uma visão geral o objetivo da equipe de planejamento do plano provisórios é montar um plano de RIPC provisório que consiste no seguinte:

- Uma Equipa de Resposta de Emergência (ERE): um grupo de indivíduos que são chamados à ação, se uma catástrofe ocorer
- Um procedimento para declarar um desastre, durante ou fora do horário normal de trabalho
- Um procedimento para invocar o plano provisório
- Um plano para manter a comunicação durante um desastre
- Identificar alguns requisitos básicos para a recuperação das instalações empresariais
- Determinar formas alternativas para continuar as operações críticas de negócios durante um desastre
- Identificação de medidas preventivas para proteger informações de negócios, registros e ativos críticos em um desastre
- Documentar o plano provisório certificando-se de que todos os membros da equipe têm cópias do mesmo prontamente disponíveis, independentemente de onde eles estão
- Identificação de um local fora fora da área de empresa onde o plano pode ser armazenado
- Garantir que a Equipa de Resposta de Emergência (ERE) está familiarizada com o plano provisória e pode implementá-lo caso ocorra um desastre

Criar o plano provisórios não deve levar mais do que um ou dois dias de dedicação de duas ou três pessoas na equipe. A equipe pode, no entanto, precisa passar algumas horas por dia durante um período de uma ou duas semanas para colocar este plano em conjunto.

3 Construindo o Plano Provisório

A equipe de planejamento do plano provisórios é montada, esta equipe têm disposição e cafeína suficiente para desenvolver o plano provisório.

Mas agora, o que você fazer?

As seções seguintes descrevem os passos que Equipa de Resposta de Emergência (ERE) precisa fazer para construir o plano provisórios. As etapas seguintes descrevem os passos que os planejadores precisa fazer para obter o plano provisórios. As etapas são as seguintes:

1. Construir a Equipa de Resposta de Emergência (ERE).
2. Definir o procedimento para declarar um desastre.
3. Invoque o plano de RIPC provisório.
4. Manter a comunicação durante um desastre.
5. Identificar planos de recuperação básicos.
6. Desenvolver alternativas de processamento.
7. Adotar medidas preventivas.
8. Documentar o plano provisório.
9. Treinar os membros de ERE.

3.1 Passo 1 - Construir a Equipa de Resposta de Emergência (ERE).

Os planejadores do plano intermediário primeiro devem identificar uma equipe de indivíduos dentro da organização que pode ser posta em ação, a qualquer hora do dia ou da noite, quando uma catástrofe ocorrer. Esta equipe é chamado de Equipa de Resposta de Emergência (ERE).

Os planejadores devem escolher os membros da ERE entre o pessoal, levando em consideração o seguinte ao fazer suas escolhas:

Os Membros ERE tem autoridade de gestão.

Os Membros ERE (a maior parte) residem perto o suficiente do estabelecimentos comercial, que possam provável chegar ao local se um desastre ocorre.

Os Membros ERE estão acessíveis em caso de um desastre. Eles têm mais de um meio de comunicação disponível (por exemplo, um telefone de casa e um celular).

Os Membros ERE estão familiarizados com os processos de negócios atuais e com a tecnologia que suporta esses processos.

Os Membros ERE precisa saber como trabalhadores individuais fazer seus trabalhos do dia a dia,

em detalhe.

Um desastre pode interromper o transporte e infra-estrutura de comunicações, matar ou ferir membros da equipe ou de seus familiares, levando danos aos membros do pessoal. Por qualquer uma destas razões (e outras), os funcionários podem estar indisponíveis por períodos curtos ou longos de tempo após um desastre.

Portanto, um suplente deve ser selecionado para cada membro da ERE. Esses membros suplentes da equipe devem ser tratados como membros da equipe completa, porque podem ser chamados em ação, quando ocorrer um desastre.

3.2 Passo 2 - Definir o procedimento para declarar um desastre

Os planejadores do plano intermediário precisa descobrir como os membros da ERE vão declarar um desastre.

Quando declarar um desastre, eles lançam o plano de RIPC provisório em ação.

Determine o Tempo de Interrupção Máximo Tolerável (TIMT) com antecedência ao desastre, o TIMT pode ser um período que varia de algumas horas a vários dias ou mais. O TIMT é o mais longo período de tempo entre o início de um desastre e a retomada de um processo de negócio crítico. A ERE deve avaliar o desastre e determinar se os processos críticos do seu negócio vão ultrapassar o TIMT. Se a ERE acha que vai exceder o TMIT, então deve ser declarado um desastre. Saber quando declarar um desastre não é realmente difícil, mas não é óbvio. Dizer que uma região tem experimentado uma tempestade de vento grave. Este tipo de acontecimento natural geralmente tem lugar durante um período de várias horas. Em tal caso, os danos da tempestade pode ser altamente localizado: Prédios podem ser danificados, a energia pode ser interrompido por queda de árvores em linhas de energia, e algumas estradas pode ser fechadas. Mas não é possível saber imediatamente se a tempestade de vento causou danos diretos às instalações, a tal ponto que a sua empresa não poder realizar suas funções normais. As instalações da empresa em si não pode não ser danificada em tudo, mas um vento causou queda de energia prolongada pode evitar que o negócio funcione. Ou a obstrução de estradas podem impedir que os funcionários sejam capazes de apresentar-se ao trabalho, o que também pode precipitar um desastre. Se ocorrer esse tipo de situação, então a ERE deve decidir por declarar um desastre.

Quando um evento causado pelo homem ou natural ocorre que podem perturbar ou prejudicar as operações de negócios, os membros ERE deve comunicar um com o outro,realizar uma avaliação rápida (por exemplo, determinar se o prédio está danificado, a energia elétrica ainda está em execução, os funcionários serão capazes de apresentar ao trabalho, e assim por diante), e

fazer um julgamento sobre se a empresa deve iniciar o plano provisório. Capacitar dois ou mais membros ERE com capacidade de declarar um desastre é uma abordagem simples e razoável.

3.3 Passo 3 - Chame o plano de DR interino

Depois que a ERE decide que o TIMT (Tempo de Interrupção Máximo Tolerável) foi excedido para processos críticos, ela ativa o plano provisório.

Segue abaixo os passos necessários para colocar o plano de RIPC em funcionamento:

1. Nomear um dos membros da ERE para fazer um relatório do ocorrido. O membro da equipe deve tomar nota do seguinte:

• Descrição geral do evento que ocorreu .

• Danos às instalações, ativos, sistemas e instalações de comunicações

• Pessoal disponíveis e pessoal desaparecidos, feridos ou mortos

2. Organizar uma reunião de emergência inicial. A equipe precisa fazer o seguinte:

• Nomear um líder ERE.

• Atribuir funções, tais como avaliação de danos e de comunicações.

• Estabelecer um Centro de Operações de Emergência (COE).

3. Tomar decisões. O ERE precisa determinar se deve manter pessoal suficiente para mudar-se para outro local, por exemplo.

4. Iniciar os planos de recuperação. O ERE precisa começar a executar os planos, ou parte dele.

Dependendo do tipo de negócio e da natureza do desastre, a ERE pode funcionar continuamente, ou em turnos.

3.4 Passo 4 - Mantenha comunicações durante um desastre

Neste ponto, dois ou mais membros ERE devem ter determinado que a empresa teve parte do processo interrompido ou perturbado, sinalizando o início das atividades do RIPC. Quando os membros da ERE se reunirem para discutir e declarar o desastre, já superaram uma série de desafios potenciais, incluindo lidar com falhas na comunicação (o que pode tornar difícil para os membros da ERE se comunicaremo).Em muitos cenários de desastres, as redes de comunicação estão danificados ou congestionadas devido ao pico de uso, o que torna difícil a comunicação entre os membros. Existe a probabilidade de que as comunicações estarão congestionadas, segue abaixo algumas possíveis contingências de comunicações:

- Ter pelo menos dois números de telefone diferentes para cada membro da ERE.
- Certifique-se que os membros ERE estão em várias redes de telefone diferentes, de modo

que uma falha em qualquer rede não afete as comunicações entre todos os membros ERE.

- Evite depender de apenas um fornecedor de comunicações sem fios.
- Evite colocar nos sistema de telefone (PABX), correio de voz, e-mail e recursos de conferência no caminho crítico. Em outras palavras, evite gargalos de comunicação provocadas pelo desastre.
- Uso de e-mail não pertencentes à empresa é uma alternativa no caso de servidores de correio eletrônico corporativos não disponíveis.
- Use sistemas de mensagens instantâneas como uma alternativa para suplementar de comunicação.
- Usar mensagens de texto via celular como um meio suplementar a transmissão de atualizações do status.
- Definir sistemas ou equipamentos de teleconferência com antecedência ao desastre.

Um sistema de teleconferência é um serviço telefônico que permite a várias pessoas participarem de uma chamada de telefone em grupo. Incluir um segundo fornecedor de teleconferência com um provedor diferente no caso de o prestador de serviço principal teleconferência estar inacessível.

Algumas dessas contingências podem demorar um pouco de tempo para ser configurada.

Durante o desenvolvimento do plano provisório, a equipe deve concordar que contingências de comunicação são necessárias para a sua organização. Além disso, um cartão impresso com os procedimentos do plano deve ser fornecido para cada um dos membros da ERE, preferivelmente em pequenas placas laminadas. Com este cartão, cada membro da ERE tem essa informações de contato na mão quando um desastre ocorrer.

3.5 Passo 5 - Identificar os planos de recuperação básicos

Esta etapa centraliza ainda mais o plano.

Nas seções anteriores, foi criada a ERE, o trabalho sobre o procedimento para a declaração de um desastre, discutida questões relacionadas às comunicações durante um desastre.

A abordagem sugiro nesta seção é um pouco mais metódica do que aqueles em seções anteriores, e está dividida em 3 passos:

1. Identificar todas as funções de negócio da organização. Listando as funções básicas como: produtos, serviços, clientes, facturas, suporte ao cliente, processamento pagamentos entre outras.
2. Desenvolva uma lista de todos processos de negócios que compõem as funções de negócios

identificadas na etapa anterior.

3. Organize as funções de negócio em uma lista, colocando os processos mais críticos na parte superior.

Serão necessárias pelo menos meia hora em cada etapa anterior. Devem ser consideradas todas as funções desempenhadas na organização. Uma lista típica de alto nível poderia ser algo como mostrado abaixo:

- Marketing
- Setor de vendas
- Setor de Suporte
- Envio e recebimento de mercadoria
- Jurídico
- Instalações físicas
- Tecnologia da Informação (TI)
- Engenharia
- Recursos Humanos (RH)

Usar uma cópia do organograma da empresa pode ajudar a identificar as principais funções da sua organização.

Depois de criar sua lista de processos de negócio, siga estes passos:

1. Identificar quais processos você precisa reiniciar o mais cedo possível depois de ocorrer um desastre.

2. Para cada processo, identificar quanto tempo é necessário para reiniciar o processo após um desastre.

3. Para cada processo, identificar os recursos necessários para reinicia-lo. Abaixo seguem algumas questões a considerar quando verificar a lista anterior numerada:

- Dependendo do tipo de desastre, apenas uma pequena fração do pessoal normal pode estar disponível.
- Fornecedores e parceiros da cadeia de abastecimento podem ter dificuldade em manter os níveis de serviço que os processos críticos da organização necessitam.
- Evite listar muitos processos críticos que devem iniciar ao mesmo tempo, porque uma quantidade razoável de recursos podem ser lnecessária.
- Dependendo da natureza das atividades comerciais da organização, a demanda por bens ou

serviços sua empresa podem dramaticamente subir ou cair (ou não podem serem afetados). Por exemplo, uma loja de venda de água engarrafada estará em alta demanda depois de quase qualquer tipo de desastre natural, enquanto que uma empresa que fabrica fontes de energia pode ver uma queda nos negócios.

- Comunicações será prejudicado, afetando a capacidade de reiniciar processos críticos, bem como a comunicação com os clientes e parceiros da cadeia de suprimentos.

A final dos processos que precisam reiniciar logo após um desastre deve levar em conta as questões na lista anterior. Não desenvolva uma lista excessivamente ambicioso de processos para começar imediatamente após um desastre, pois provavelmente a ERE não será capaz de realmente coloca-los em funcionamento por falta de pessoal e outros recursos. No planejamento de um plano provisório, apenas planos leves estão em foco.

3.6 Passo 6 - Desenvolver alternativas de processamento

Em muitos cenários de desastres, pode ser que a ERE não seJA capaz de reiniciar OS processos críticos. Se os sistemas ou bens que Que apoiam um processo de crítico são danificados ou destruídas, ou se o pessoal responsável por reinicia-lo simplesmente não estão disponíveis, iniciando o processo crítico no local afetado pelo desastre pode não ser possível, pelo menos, não imediatamente.

Os planejadores do plano provisório precisam identificar locais próximos onde as operações críticas de negócios podem retomar em caso de um desastre altamente localizado, como um incêndio, de preferência em edifícios próximos que permanecem intactos.

Em um desastre regional, como uma inundação ou furacão, locais a uma curta distância também podem ser danificados. Nesta situação, é necessário identificar os locais de maior distância do local da empresa.

Ao considerar qualquer localização alternativa, a equipe precisa se preparar para a possibilidade de colocar no local escolhido todos os bens necessários ou sistemas alternativos que a empresa necessite para continuar as operações de negócios.

Ativos ou sistemas localizados no local da empresa pode ser danificado pelo desastre, e portanto pode ser que não possam ser utilizados no local alternativo.

- Considerar os fatores a seguir quando a equipe está à procura de localizações alternativas: Pode abrigar os ativos, sistemas e pessoal necessários para continuar os processos críticos de negócio?
- Se o local for uma distância significativa do local original do negócio, existe

habitação temporária disponível para os funcionários que precisam apresentar-se ao trabalho no local alternativo?

- Os clientes e parceiros da cadeia de suprimentos podem ajustar suas rotas e horários para utilizar o local alternativo?

A organização também pode ter outras questões a considerar quando se procura locais alternativos. Um plano provisório é desenvolvido em um ou dois dias. O esforço necessário para fazer acordos comerciais formais com um site alternativo cai fora do âmbito de um plano provisório pois leva muito mais tempo. Após um desastre, uma organização pode ter de fazer concessões a fim de continuar as suas atividades críticas ou processos. Os planejadores precisam levar em conta esses outros fatores, quando considerar alternativas de tratamento possíveis:

- A redução dos níveis de serviço ou de produção temporária
- Substituir componentes
- Utilização de pessoal temporário
- Compartilhando instalações com outras empresas
- Usar mais processos manuais e confiar menos nos sistemas de informação
- Utilizar fornecedores alternativos e prestadores de serviços

A equipe que está elaborando o plano provisório conhece a organização muito bem. O modelo de negócio e os cenários de desastre que ela está planejando devem ditar as alternativas do plano provisório. Muito do que foi elaborado no plano provisório será aplicado no plano formal.

3.6.1 Passo 7 - Decretar medidas preventivas

A perda de informações importantes e ativos ter um efeito devastador se um desastre ocorrer. O plano provisório precisa identificar informações críticas, registros, bens e chegar as medidas de prevenção que podem ser rapidamente e facilmente implementadas, a fim de reduzir a probabilidade e impacto e perda desses registros e ativos.

A lista a seguir contém dicas sobre as medidas preventivas que podem ser adequados para uma organização:

Medidas preventivas em TI

- Certifique-se de que os backups são realizados e que os de dados críticos fazem parte dos mesmos. Confirmar que os sistemas, diretórios e arquivos estão sendo copiados e se eles realmente podem ser restaurados.
- Guarde as fitas de backup fora do prédio ou local dos equipamentos . Desenvolver um plano

de armazenamento de backup de mídia que inclui armazenamento “off-site”. Para que servem os backups se os mesmos forem danificaos estão danificados pelo fogo, inundação, terremoto ou qualquer outro motivo

- Verifique se as estantes são seguras. Certifique-se de que os sistemas de prateleiras estão firmemente seguras, de forma que um evento tal como um tremor não causarão danos. Estas medidas também pode garantir a segurança do pessoal que trabalham nessas áreas, evitando lesões caso um equipamento caia.

Medidas de registros preventivas, tais como

- Centralize o armazenamento de registros. Um primeiro passo lógico para proteger registros vitais é tirá-los de gavetas dos trabalhadores e coloca-los em um local central.
- Escanear documentos e guardar em arquivos. Considerar a implantação de um projeto para digitalizar eletronicamente registros em papel, tais como arquivos pessoais e contratos.
- Fotocópia de registros importantes. Existem registros vitais que devem ser armazenados em fotocopias e as mesmas devem ser guardadas em um local externo e seguro, longe o suficiente, que um desastre regional não danifica tanto os originais como as cópias.
- Use armários resistente ao fogo para arquivos. Considere o uso de armários corta-fogo para arquivo de documentos vitais. No caso de um incêndio, os registros armazenados nesses gabinetes sofrem menos danos do que os registros armazenados em arquivos mais tradicionais.

Utilize medidas preventivas, tais como:

- Use armários resistentes a fogo. Considere atualizar estes tipos de armários para armazenamento de ativos críticos, a fim de protege-los do fogo.
- Verifique se existe detecção de incêndio e sistemas de supressão. Certifique-se de que os extintores de incêndio, detectores de fumaça, sistemas de aspersão, e outras medidas para a detecção e combate a incêndios estão atualizados e funcionando corretamente. Em muitos locais, as autoridades locais impõe essas medidas. Em áreas onde as autoridades locais não realizam inspeções em sistemas de ROTECÇÃO contra fogo, as empresas locais precisam tomar a responsabilidade dessas inspeções para si mesmas.
- Configurar um modo de ajuda de emergência e planos de evacuação. Estabelecer e testar periodicamente as medidas de segurança pessoal, como material de primeiros socorros, iluminação de emergência e planos de evacuação. Ativos mais importantes de uma organização são o seu pessoal, e os planejadores às vezes esquecem de plano global de

gestão de risco.

3.7 Passo 8 - Documentar o plano Provisório

Depois de desenvolver o plano provisório, o mesmo deve ser documedo claramente. A estrutura do plano pode incluir qualquer uma ou todas as seguintes características:

- Quem promoveu e patrocinou (gerente ou diretoria), os desenvolvedores do plano provisório, quem realmente escreveu, e quem trabalhou como os planejadores.
- Equipe de Resposta de Emergência (ERE): Os membros do ERE e os departamentos que representam. Incluir informações de contato completo.
- Procedimento de declaração de desastre: Descreve a empresa declara um desastre. Este procedimento deve incluir o TIMT (Tempo de Interrupção Máximo Tolerável), bem como uma justificativa para o seu valor.
- Procedimentos de Comunicação: descreve a forma como a ERE e o pessoal de outras empresas deverão se comunicar, entre si e com o mundo exterior.
- Procedimentos de recuperação que constam no plano: Estes procedimentos são o centro plano provisório. Eles descrevem os procedimentos de recuperação, locais alternativos, e informações de contingência para cada processo de negócio.
- Medidas preventivas: Estas medidas não são realmente uma parte do plano em si, mas é necessário documentar as medidas preventivas na forma de itens de ação para que as pessoas e departamentos de fato as levem a cabo.

Armazenamento e distribuição do plano

Quando a documentação do plano provisório estiver completa, é preciso armazena-la e distribuir-la de tal forma que esteja devidamente protegida em caso de um desastre. No mínimo, tenha cópias nos seguintes lugares:

- Cópia Impressa: Cada membro ERE deve ter pelo menos duas cópias impressas do plano: uma para manter no local de trabalho e outra em casa.
- Cópia impressa fora da empresa: Manter uma cópia do plano disponível em um local externo, longe o suficiente que ela não estará em risco em caso de uma catástrofe regional.
- Cópia eletrônica: Cada membro TRE também deve ter cópias do plano em formato eletrônico.
- Online: Coloque o plano em um local seguro online, acessível por todos os membros do ERE. A localização on-line não deve ser hospedado pela própria organização.

3.8 Passo 9 - Treinar os membros ERE

Quase pronto! O Plano foi desenvolvido e documentado, mas que os membros da ERE se conhecem e sabem o que fazer quando um desastre ocorre? Todos os membros do ERE, e seus suplentes, precisam passar por um treinamento formal, em que todos os princípios do plano de RIPC provisório serão testados, incluindo os passos abaixo:

- Os membros da ERE precisam saber que o plano não é de longo prazo, é apenas um paliativo até que possa ser totalmente desenvolvido e implementado o plano completo
- Declaração de desastre: Provavelmente a parte mais difícil de um plano é realmente declarar um desastre. Eles precisam estar familiarizado com o procedimento e os critérios usados para determinar se devem invocar um desastre. Certifique-se de que os membros da ERE sabem serão perdoados se declararem um desastre desnecessariamente
- Centro de Operações de Emergência (COE): Os membros ERE precisa saber como configurar e gerenciar operações de emergência no COE. Cada membro ERE precisa entender que ele ou ela pode ser o líder do COE, dependendo de quem está disponível e em uma situação de desastre. Cada membro ERE precisa estar familiarizado com as operações de recuperação no plano provisório.

A equipe deve estar preparada para a possibilidade de novas questões que podem surgir durante o treinamento ou situação real, este fato pode levar a necessidade de pequenas alterações para no plano. Mas lembre-se, o plano de RIPC provisório não salvará a empresa de todo e qualquer desastres , pois é um plano mais simples, um “tapa-buraco” .

3.9 Testando o plano provisórios

Uma organização que emprega recursos para o desenvolvimento de um plano provisório quer saber se o mesmo vai funcionar em caso de um desastre. Abaixo segue uma lista dos tipos de testes que podem ser feitos para garantir se o plano vai funcionar:

Lista de verificação (teste no papel): Funcionários individualmente devem rever o plano com exatidão e integridade.

- Passo a passo: Funcionários se reúnem para percorrer os locais que o plano cobre em grupo, discutindo cada passo ao longo do caminho.
- Simulação: Funcionários devem executar um passo a passo no contexto de um desastre. Anúncios periódicos de eventos devem ser publicados e verificados à medida que ocorrem na região. Os membros ERE na verdade não vão executar todas as etapas de recuperação.
- Paralelo: A ERE realiza as etapas de recuperação reais, para mover os processos de negócios

para locais alternativos. A ERE constrói ou inicia servidores de recuperação e executa algumas transações comerciais reais através dos servidores de recuperação, enquanto os servidores principais estão trabalhando. Os principais processos de negócios devem continuar de forma ininterrupta todos os dias.

- Interrupção (de transição de teste): O negócio deixa de realizar processos críticos de negócio, como se um desastre real tivesse ocorrido. Os membros da equipe ERE e outros realizam operações de negócios de acordo com o plano provisório.
- Testes: Cada membro da ERE, além de outros membros selecionados na organização (particularmente aqueles estarão ajudando com as operações de negócios durante um desastre real), devem analisar cuidadosamente todo o plano provisório. Peça-lhes para fazer sugestões para mudanças ou melhorias no plano. Os autores do plano devem fazer as alterações recomendadas e distribuir o plano para comentários mais uma vez, para ter certeza de que todos concordam que o plano é precisos e completos.
- Testes passo a passo: A ERE inteira deve levar tanto tempo quanto necessário (metade de um dia a um dia inteiro ou mais) para verificar o plano, passo a passo. Deve haver muita discussão, incluindo perguntas e respostas. As pessoas que desenvolveram o plano devem estar presente, mesmo que eles não sejam membro membros da ERT. Dessa forma, os autores do plano pode responder a todas as questões levantadas.
- Testes de simulação: Se o planejamento de recuperação de desastres é novo para a sua organização (e provavelmente é se você está desenvolvendo um plano provisório), testes de simulação devem ser realizados no novo plano. Um teste de simulação permite que a ERE tenha respostas reais caso ocorra um desastre.

A principal diferença entre o teste passo a passo e testes de simulação é onde o mesmo é feito. Em um teste passo a passo, a equipe está em uma sala de conferências com quatro paredes e um quadro branco, em um teste de simulação, a equipe anda por todo o edifício com o plano na mão, observando, fazendo perguntas, e apontando questões que podem ser vistas pessoalmente.

4 Desenvolvendo e usando a Análise de Impacto nos Negócios.

As empresas que pretendem desenvolver um plano de RIPC possuem recursos limitados. À primeira vista, faz sentido que todos os processos de negócios e sistemas de informação devem ter capacidades de recuperação de desastres.

No entanto, uma organização apenas não pode ter planos para todos os seus processos e sistemas, pois não tem recursos suficientes ou tempo suficiente. Então como é que uma organização decidir quais processos e sistemas justificam a despesa e esforço relacionado com o desenvolvimento de planos de RIPC?

A maioria das empresas usa uma Análise de Impacto nos Negócios (BIA) para ajudá-la a tomar esta decisão.

4.1 Entender o propósito de uma BIA

Análise de Impacto no Negócio (BIA) é um inventário detalhado dos processos primários, sistemas, ativos, pessoas e fornecedores que estão associados com atividades e negócios principais de uma organização.

A BIA começa como uma lista, mas torna-se uma teia, ela acaba como um conjunto interconectado de listas em que as entradas em uma lista possuem dependências de outros processos, sistemas, recursos, pessoas e fornecedores.

Processo depende de sistemas K, L, e M, requer o uso de Ativos S e T; é operado por pessoal chave nos departamento Q, e depende de produtos entregues por fornecedores Y e Z.

Pense da BIA como uma espécie de três dimensões interligando os pontos, na qual as entradas de várias camadas tem conexões com entradas em outras camadas. Como na própria organização, tudo está interligado.

O objetivo principal de uma BIA é identificar quais processos e sistemas são os mais críticos para a sobrevivência de uma organização.

Dois termos utilizados na frase anterior:

Crítica: Esta palavra refere-se aos processos e sistemas necessários para a empresa desempenhar de suas funções principais.

Sobrevivência: Salvar o seu negócio ou a empresa de sofrer um golpe catastrófico que poderia resultar em danos significativos para o negócio, inclusive fechando as suas portas definitivamente.

Abaixo está identificado o que a Análise de Impacto Negócio realmente faz:

- Determina processos que são negócios para se recuperar e reiniciar processos o mais cedo possível depois de um desastre
- Determina quanto investimento é necessário para reiniciar os processos de negócios
- Identificar os recursos necessários para reiniciar os processos de negócios

Sem uma BIA, não é possível saber quais os processos são de missão crítica (crucial para o sucesso contínuo da organização), ou tempo crítico (aqueles processos que afetam negativamente a organização quando eles não estão sendo prontamente realizado), requerem atenção no planejamento de recuperação de desastre e fases de testes. Sem uma BIA ao invés de utilizar critérios ideais de identificação, os gerentes vão apenas adivinhar, normalmente seguindo um dos motivos abaixo:

- Seus favoritos
- Aqueles com os quais está mais familiarizado
- Os que os executivos mais gostam
- Os mais novos
- Os favoritos de outros
- Os mais fáceis

Os critérios listados acima não fazem sentido nos negócios. A BIA utiliza critérios objetivos para selecionar os processos que são verdadeiramente os mais críticos para a organização, em vez de se basear em critérios subjetivos.

4.2 Definir o objetivo do projeto

Logo no início, deve-se estabelecer claramente o objetivo de todo o projeto. Se o escopo do projeto de um plano de RIPC é claro, os membros da equipe de projeto pode arbitrariamente cortar componentes importantes ou aumentar o alcance para além do que os patrocinadores do projeto inicialmente previram.

Primeiro é necessário estabelecer os limites do projeto da BIA, abordando as seguintes questões:

Equipe do projeto: quais membros da vão compor a equipe do projeto? Quanto tempo por semana espera-se que cada membro da equipe para trabalhar no projeto? Da mesma forma, se algum membro da equipe vier por empréstimo, 0 que é necessário para obter os colaboradores para o projeto.

Escopo: Quais os conjuntos de funções que estão no escopo do projeto, e que estão fora?

Deve ser estabelecida uma rápida análise de dependências, a fim de estabelecer firmemente o escopo

Plano de projeto: estabelecer um plano de projeto de alto nível que inclui datas importantes

Orçamento: O orçamento está estabelecendo para cada fase do projeto? Os resultados da BIA podem ser utilizados para estabelecer o orçamento para o esforço para o plano, depois de conhecer a quantidade de investimento é possível cumprir os critérios estabelecidos de recuperação?

Suporte dos executivos: Qual o nível de apoio executivo necessário para o projeto? Os executivos da companhia apoiam o projeto firmemente?

4.3 A realização de uma BIA: uma abordagem comum

A fase de coleta de informações do BIA envolve um grande número de entrevistas que uma ou mais pessoas realizam. É preciso desenvolver uma abordagem comum para que cada entrevistador reúna as mesmas informações de cada pessoa que ele ou ela entrevistar sobre todos os processos, o sistema, de ativos e fornecedores.

Entrevistas e outras atividades de coleta de informações deve ter um um plano, passar algum tempo desenvolvendo procedimentos e modelos para fazer o processo de entrevista (provavelmente a mais trabalhosa de todas as atividades BIA) o mais eficiente e eficaz possível.

A BIA deve se concentrar em identificar e inventariar vários aspectos e características essenciais de uma organização, incluindo:

Processos de negócio: Este termo genérico refere-se a atividades empresariais que o pessoal de sua empresa realiza, muitas vezes com a ajuda de máquinas, incluindo sistemas de informação. Processos são constituídos por um ou vários procedimentos. Processos de negócio pode ser bastante simples, uma ou duas pessoas transportando-os para fora com dependência mínima em outros recursos, ou eles podem ser bastante complexa, envolvendo pessoas em muitas partes da organização, bem como fornecedores e outros recursos externos.

Sistemas de informação: Este termo genérico, os sistemas de computador, aplicativos, bancos de dados e dispositivos. Um sistema de informação pode ser tão simples como uma planilha em um computador ou tão complexo como uma aplicação rodando em dezenas de servidores em locais em todo o mundo.

Ativos: O equipamento necessário para facilitar a produção de produtos ou serviços qualquerr que uma organização produz. Ativos podem consistir de máquinas ou ferramentas que são essenciais para o negócio. Os ativos podem ser servidores; dispositivos mecânicos, como fresadoras ou tornos, ferramentas, tais como empilhadeiras e geradores elétricos ou equipamentos; máquinas

de raio X e scanners.

Pessoal: As pessoas que executam os processos ou apoiam os mesmos de alguma forma direta. Essas pessoas podem estar localizados em qualquer lugar, e podem incluir empregados, contratados e temporários.

Fornecedores: As organizações externas que fornecem o seu negócio com bens ou serviços de que necessita para produzir seus bens ou serviços. Fornecedores incluem organizações que fornecem matérias-primas, como aço, madeira, ou CDs virgens; uma utilidade pública o fornecimento de eletricidade, gás natural, ou água, e uma organização de serviços, como um local de colocação de Internet ou um provedor de armazenamento de dados.

4.3.1 Coleta de informações através de entrevistas

A melhor abordagem para a inventariação de todos os itens listados anteriormente é agendar discussões com pessoas chave na empresa. Processos de negócio e sistemas de informação não pode explicar-se, por isso a entrevista com as pessoas que são responsáveis por esses processos e sistemas.

Quando as pessoas descrevem seus processos e sistemas, eles podem apontar mais nomes que precisam para adicionar à sua lista de entrevistados.

Poucas organizações têm um único indivíduo que tem uma visão muito clara de cada processo crítico, sistema e fornecedor.

Usando formas consistentes e planilhas pode-se fazer o estágio de coleta de informações do BIA mais eficaz perguntando os mesmos tipos de informações de cada processo ou proprietário do sistema. É possível capturar uma maior quantidade de detalhes em entrevistas, incluindo detalhes nos formulários, além disso se várias pessoas estão conduzindo as entrevistas, eles são mais propensos a fazer as mesmas perguntas a cada momento, se usarem um formulário.

Abaixo estão algumas dicas de como desenvolver formulários de coleta de informações e procedimentos:

- Usar um formulário para cada processo, não um por entrevista. A menos que um entrevistado é responsável por apenas um processo, use um formulário separado para cada processo (ou sistema, ativos, pessoa, fornecedor, e assim por diante). Assim as informações estarão focadas nos processos e não no pessoal que está entrevistando.
- Referência cruzada. Em um formulário listar os fornecedores críticos, pessoal, bens e sistemas. Um fornecedor essencial de consumo, cruzando os processos e sistemas que fornecedor suporta.

- Incluir metadados. Inclui informações como o nome do entrevistado, as informações do entrevistado contato, que conduziu a entrevista, e quando isso ocorreu. Será possível rastrear dados caso surjam mais perguntas depois

Para ajudar a esclarecer os modelos de entrevistas abaixo segue uma lista que pode servir de ponto de partida:

- Entrevistado
- Título do Entrevistado
- Informação de contato do entrevistado
- Departamento do entrevistador
- Informação de contato do entrevistador
- Data
- Nome do processo
- Nome do proprietário do processo e de contato
- Finalidade do processo entradas do processo
- Saídas do processo
- Voltados para o cliente (Y / N)
- Quem ou o que executa esse processo
- Dependências (este processo depende do de ou quem)
- Dependências nas Comunicações: telefone, Internet, fax, e assim por diante
- Dependências dos ativos
- Dependências das instalações
- Dependências dos fornecedores
- Dependência de pessoal
- Dependências de informação de sistema

4.3.2 Captura de dados para o BIA

A BIA é totalmente baseada no recolhimento e análise de informações. Reunir informações para a BIA deve ser feita de forma metódica consistente e passível de ser repetida.

Em um projeto maior, em que mais de uma pessoa reúne informações, os mesmos detalhes devem ser obtidos, independentemente de quem está fazendo o recolhimento das informações.

Pode-se reunir uma grande quantidade de informações sobre uma variedade de temas para a

Análise de Impacto no Negócio. Mesmo se concentrando no lado de planejamento de recuperação de desastre para TI, não se pode ignorar o fato de que os sistemas de TI suportam os processos de negócios. É necessário saber quais processos de negócio são os mais críticos e a rapidez com que precisam ser recuperados. A BIA ajuda a descobrir os processos da organização.

Como definido anteriormente, Processos de negócios, ou apenas processos, são as atividades que a organização realiza em apoio do seu principal objetivo como a produção e entrega de bens e / ou serviços. Todas as empresas têm processos, embora eles não podem ser chamados de processos. A lista a seguir inclui alguns recursos possíveis de processos de uma empresa:

- **Processos que contem um ou mais procedimentos:** Os procedimentos são geralmente instruções escritas que consistem de uma ou mais tarefas, que são as etapas individuais que precisam ser executar em um procedimento. Processos simples pode conter um único procedimento, enquanto que processos complexos podem ter muitos procedimentos. Exemplo de tarefas incluem sair da aplicação, desligar o fornecimento de energia, entre outros. Um projeto de RI pode expor fraquezas nos processos de negócio, inclusive quando não existe procedimentos por escrito. Em uma organização menor. Uma organização que quer estabelecer um plano de recuperação de desastres eficaz precisa documentar seus procedimentos.
- **Processos são realizados por pessoas:** Exemplos de pessoas que realizam processos incluem caixas de banco, administradores de banco de dados, e mecânica. Em processos altamente automatizados, tais como refinarias de petróleo, a máquina faz a maioria do trabalho real, mas os opera.
- **Os processos podem depender de sistemas de informação:** Os colaboradores podem realizar alguns processos sem o uso de um sistema de informação, mas cada vez mais, os processos de negócio requerem sistemas de informação, de alguma forma direta ou indireta. Exemplos de estas dependências incluem a disponibilidade de um sistema de registos de pacientes; a disponibilidade de um sistema de inventário, a fim de identificar a localização de uma peça de substituição, e a disponibilidade de um servidor de diretório para efetuar cópias de segurança
- **Processos podem demandar ativos:** Processos muitas vezes dependem de um ou mais ativos. Por exemplo, um posto de abastecimento tem tanques e bombas, Uma empresa de fabricação precisa de suas empilhadeiras. Algumas organizações listam seus sistemas de computador no ativo, em vez de em sistemas de informação. É possível classificá-los de

qualquer maneira desde que faça sentido para a sua organização.

- **Processos pode depender de fornecedores ou prestadores de serviços:** A maioria dos processos requerem fontes ou matérias-primas, fazendo com que a empresa muitas vezes dependa de fornecedores externos.

O BIA contém uma lista detalhada de todos os processos (pelo menos, os mais importantes) que a organização realiza com as características listadas anterior sobre os processos de negócios, com um alto nível de detalhe, podendo conter várias planilhas que listam os processos de negócio da organização, um por linha (ou mesmo um por planilha). É um resumo de tudo o que a organização faz.

4.3.3 Sistemas de informação

A BIA contém um inventário dos sistemas de informação da organização. Como a lista de processos (discutida na seção anterior), a lista de sistemas de informação deve ser bastante detalhada. O sistema de informação é um termo que inclui alguns ou todos os componentes em um ambiente de TI. Por exemplo, uma grande clínica médica tem um sistema de informação do paciente que gerencia todas as informações sobre seus pacientes. Se o sistema de informação do paciente for imaginado como um aplicativo, o sistema contém não apenas a aplicação, mas os servidores que residem em servidores de banco de dados separados, e outros elementos, tais como servidores de diretório, servidores de impressão e servidores de arquivos. Sem todos esses outros elementos, o sistema de informações do paciente não iria funcionar, além da rede de computadores bem como as estações de trabalho e outros equipamentos.

O modelo de negócios dos sistemas de informação, arquitetura de aplicações, e até mesmo a estrutura de seu organograma podem ditar os caminhos para cortar todos os ativos de informação. Não deve haver uma preocupação com a maneira certa ou errada de identificação e classificação de como os seus sistemas de informação trabalham.

4.3.4 Ativos

A BIA contém uma lista de ativos importantes que a empresa utiliza, particularmente aqueles ativos que estão direta ou indiretamente relacionados com a produção de quaisquer bens ou serviços. Bens de uma organização pode ser qualquer um dos seguintes itens: veículos de entrega, guindastes, prensas, impressoras, etc. Independentemente dos itens específicos, uma BIA deve conter os ativos que estão relacionadas com atividades primárias da organização.

4.3.5 Pessoal

Cada organização tem seu pessoal substituível, bem como aqueles que não são. Uma lista de pessoal deve identificar aquelas pessoas que são críticas do ponto de vista dos serviços. Identifique dentro dos processos de negócios mais críticos o pessoal responsável. Em desastres graves, o pessoal chave podem falecer, ferir-se ou ser incapaz de comparecer ao trabalho por causa de interrupções de transporte.

4.3.6 Fornecedores

Identificar os principais fornecedores dentro de cada processo de negócio. Como processos, sistemas de informação, bens e pessoal, a empresa provavelmente tem vários fornecedores chaves, sem o qual os produtos ou serviços não podem ser realizados. Se a organização é altamente dependente de fornecedores externos, a BIA pode incluir uma lista separada destes fornecedores, se os mesmos forem colocados em uma única lista,é possível vê-los em um só lugar. Se for incluída uma uma lista separada de fornecedores na BIA, de ser feita uma referência cruzada de cada fornecedor.

4.3.7 Declarações de impacto

Nas seções anteriores, estão descritas as listas que devem ser adicionadas a BIA: processos, sistemas de informação, recursos, pessoal (opcional), e fornecedores. Essas listas contêm uma grande quantidade de detalhes sobre cada um dos processos, sistemas de informação, e assim por diante, incluindo dependências entre processos e fornecedores.

É necessário acrescentar algo mais a essas listas: o impacto da indisponibilidade. Em outras palavras, o impacto sobre a organização como um todo, se um processo, fornecedor ou ativo é interrompido ou torna-se indisponível por um período de tempo, a BIA, deve conter a declaração de impacto com frases curtas que descrevem o impacto se cada processo (ou fornecedor ou ativo) é interrompido ou não está disponível.

Exemplos incluem a incapacidade de processar dados, incapacidade de transferir bens do inventário, e incapacidade de acessar o histórico médico do paciente. Cada processo de negócio é de alguma forma, direta ou indiretamente, relacionado com a produção de bens e serviços.

A BIA também pode mostrar um valor do custo associado com cada processo. Este valor representa o custo para o negócio por unidade de tempo, como real por hora, se o processo não está disponível.

Calcular o custo do impacto pode ser bastante complicado, daí a necessidade de pessoal

com experiência financeiras.

4.3.8 Avaliação da criticalidade

Além de declarações de impacto um rankings de criticidade de cada processo deve ser incluído na BIA.

A criticidade de cada processo como sistemas de informação ou fornecedores pode ser feita através de uma escala: B, M, A e C (para baixo impacto, médio, alto ou crítico) ou uma escala numérica classificado de 1 a 4.

A criticidade tem um enorme impacto sobre os resultados da BIA. Quando todos os processos de negócios forem colocados em uma planilha e classificado por criticidade, surgirá um lista de classificação de processos mais críticos da organização

Um dos principais objetivos da Análise de Impacto no Negócio é o ranking de criticidade, ou seja, uma estimativa bem informada do impacto global, se as operações de negócios vão continuar caso um processo seja interrompido.

4.3.9 Tempo de Interrupção Máximo Tolerável (TIMT)

É o comprimento máximo de tempo que um processo de negócio pode ser interrompido ou não estar disponível sem causar falhas na própria empresa.

Aqui estão alguns exemplos:

- Um vendedor on-line pode falir se o seu catálogo on-line não está disponível por vários dias.
- Uma companhia aérea pode falir se não pode reservar voos por mais de 48 horas.
- Falhas de negócio que ocorrem por causa de desastres não são ocorrências diárias.

Para cada processo na BIA, é necessário determinar o tempo máximo tolerável que um processo pode ficar ocioso. TIMT é o tempo após o qual um processo para ou se tornar disponível, gera danos irreversíveis (e muitas vezes fatais), como mostra a Figura 1.

Em geral, um tempo superior ao TIMT conduz a graves danos à viabilidade do negócio. Dependendo do processo, o TIMT pode ser expresso em horas, dias, ou mês.

Chegar a um TIMT razoável para um processo não é nada fácil. Talvez respondendo a pergunta: "A última vez que esse processo tornou-se indisponível para a organização, por quanto tempo a empresa parou falhou?"

Se tais ocorrências acontecem tão raramente, até mesmo entre outras organizações semelhantes, que existem poucos dados para fazer referência ao estimar um TIMT.

4.3.10 Objetivo do Tempo de Recuperação (OTR)

Após determinar TIMT para processos é necessário fixar as de metas para a recuperação. Um alvo importante é o OTR. O Objetivo do Tempo de Recuperação é o período de tempo em que a organização pretende que o processo interrompido funcionando novamente. Para um determinado processo, o OTR é menor do que o TIMT.

A empresa quer que seu processo crítico seja restaurado e esteja operando bem antes do ponto em que seu tempo de inatividade poderia ameaçar a própria viabilidade do negócio.

Caso contrário, é uma espécie de como esperar três minutos e meio para começar a administrar plano de RIPC a uma vítima de afogamento.

Por exemplo, se o MTD para um processo crítico é de sete dias, você pode definir o seu RTO a quatro dias.

Por definição, tem de ser. Um OTR de 14 dias para um processo com um TIMT de 7 dias, o seu negócio faliu antes do processo crítico funcionar novamente.

Um processo constitui a base para qualquer planejamento de RIPC, por exemplo, se um processo tem um OTR de 30 dias, para fazê-lo funcionar novamente pode ser necessário comprar um novo servidor, instalar o software, e restaurar os dados de backup em um ritmo calmo. No entanto, um processo com uma OTR de uma hora requer um local com um servidor de espera e replicação de dados em tempo quase real.

Os custos para estes dois cenários variam muito, um OTR inferior exigir mais investimento em sistemas de espera, bem como a eventual necessidade de replicação de dados ou outras tecnologias de alto custo. Estabelecer OTR e então determinar os custos necessários para alcançar esses objetivos.

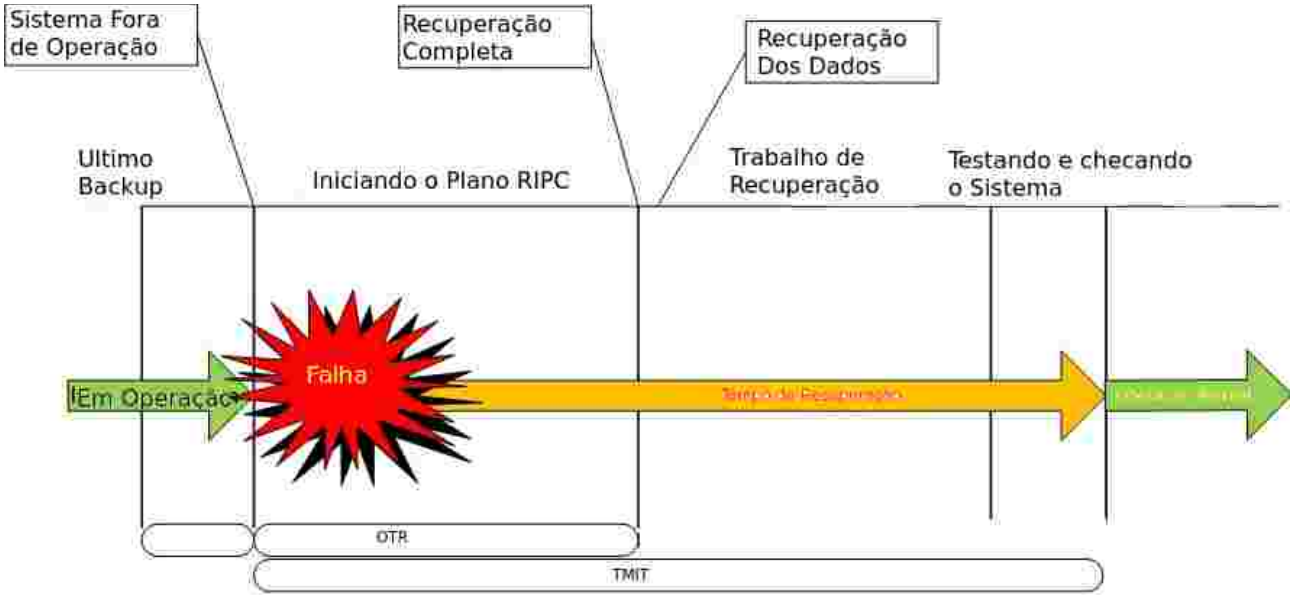

Figura 1: Tempo Máximo de Interrupção Tolerável e Objetivo do Tempo de Recuperação

4.3.11 Objetivo do ponto de recuperação (OPR)

O Objetivo de ponto de recuperação (OPR), como o OTR, é um tanto arbitrária e baseada em suposições que os executivos e gerentes seniores fazem. O objetivo do ponto de recuperação é a quantidade máxima de dados que você pode perder se um processo é interrompido e posteriormente recuperado.

Dizer que uma organização quer estabelecer um OPR de quatro horas para um sistema de entrada de pedidos. A fim de atender a essa figura a organização tem de implementar um mecanismo de backup ou replicar os dados da transação para que não perca mais de quatro horas de transações em um cenário de desastre. Similar ao OTR, definir o OPR determina que tipo de medidas que você precisa tomar para garantir não perder informações relacionadas a qualquer processo de negócio. OPR menores geralmente requerem um maior investimento na replicação de dados ou tecnologia de backup.

Se a organização quer encurtar o OPR, ela pode fazê-lo, executando backups com mais frequência ou replicando transações para outro servidor em outro local.

4.4 Determinando o Tempo de Recuperação Máximo Tolerável

É possível desenvolver qualquer sistema de categorias que funciona, mas como com todos os sistemas de classificação, certifique-se que as categorias são claramente definidas e que haja um entendimento comum do alcance de cada uma. A seguir é apresentado um sistema de classificação utilizado para avaliar a criticidade:

Categoria 1: Missão Crítica - 0-12 horas

Categoria 2: Vital - 13-24 horas

Categoria 3: Importante - 1-3 dias

Categoria 4: Processos de Negócios de Pouca Importância- mais de 3 dias

4.4.1 Processos de Negócios de Pouca Importância:

Processos de Negócios de Pouca Importância são muitas vezes aqueles que têm sido desenvolvidos ao longo do tempo para lidar com questões ou funções pequenas e recorrentes. Eles não vão desaparecer no curto prazo e, certamente, não são processos de negócios importante. Eles terão de ser recuperados no longo prazo, se necessário.

Alguns Processos de Negócios de Pouca Importância podem ser perdidos após uma perturbação significativa e, em alguns casos, isso é ótimo. Muitas empresas desenvolvem vários processos que devem, em algum momento ser analisados, revistos e muitas vezes descartados , mas que raramente ocorre durante as operações normais de negócios , devido ao trabalho mais exigente.

Ao realizar a BIA, recomenda-se o enxugamento dessas funções de negócios, preocupando-se com a missão crítica e vital.

4.4.2 Importante

Processo importantes dos negócio ou empresas não levam a mesma a parar no curto prazo, mas eles geralmente têm um impacto a longo prazo. Quando ausente, esses tipos de funções e processos causam alguma perturbação, implicações legais ou financeiras. Podem estar relacionados com funções entre sistemas de negócios.

A partir de uma perspectiva de TI, estes sistemas podem incluir e-mail, acesso à Internet, bancos de dados e outras ferramentas de negócios que são usados como apoio. Se desativado, estes sistemas pode tomar uma quantidade moderada de tempo e esforço para ser compensado.

4.4.3 Vital

Algumas funções de negócio pode cair em algum lugar entre de missão crítica e importante , então uma categoria intermediária como "vital" ou "essencial" pode ser utilizada. Como distinguir entre de missão crítica e vital?. Caso não seja possível precisar, esta categoria não será necessária.

No entanto, se decidir que determinadas funções são absolutamente de missão crítica e outros são extremamente importantes, mas devem ser tratadas imediatamente após as funções de

missão crítica esta classificação é importante. Funções vitais podem incluir processos como folha de pagamento por exemplo, não é uma missão crítica capaz de parar o negócio, mas que pode ser vital para a capacidade da empresa funcionar.

A partir de uma perspectiva de TI , sistemas vitais podem incluir aqueles que fazem interface com sistemas de missão crítica. Caso não utilize esta categoria, a classificação vai acabar com apenas três, de missão crítica, importante e de menor importância. O requisito de tempo de recuperação desta categoria pode ser medido em termos de horas, um dia ou dois.

4.4.4 Missão Crítica

Processos de negócios de missão crítica são aqueles que causam maior impacto sobre as operações e potencial de valorização de sua empresa. Quase todos os que trabalham em uma empresa tem uma compreensão inata das operações de missão crítica dentro de seu departamento.

A chave é reunir todos os dados e desenvolver uma visão abrangente de seus processos de missão crítica em uma perspectiva organizacional.

Quais são os processos que devem estar presentes para sua empresa para continuar os negócios? Estas são as funções de missão crítica. Uma forma de levar as pessoas a concentrarem-se nas funções de missão crítica é pedir (seja por meio de questionário, entrevista, ou oficinas), quais as primeiras três ou cinco coisas que seu departamento fariam após ou em uma eminência de interrupção dos negócios para continuar suas funções. Isso muitas vezes dá uma visão mais clara das funções de negócios de missão crítica em cada departamento.

De uma perspectiva de TI, a interrupção de rede, sistema ou aplicativos de missão crítica causam extrema interrupção dos negócios. Tal interrupção muitas vezes tem sérias implicações legais e financeiras. Este tipo de interrupção pode ameaçar a saúde, o bem-estar e a segurança das pessoas (sistemas hospitalares). Estes sistemas podem exigir esforços significativos para restaurar, esforços que quase sempre prejudicam para o resto da empresa. A tolerância para esse tipo de falha, seja do sistema de TI ou processo que proporciona é muito baixa, seu tempo de recuperação é muitas vezes descrito em termos de horas, e não dias.

5 Mapeando funções de negócios e Infra-estrutura

Este capítulo apresenta:

O uso de inventários para descobrir sistemas e dispositivos

Desenvolver arquiteturas de alto nível

Encontrar as dependências entre sistemas

Este capítulo ajuda a entender melhor a tecnologia pois planejamento de recuperação de desastres não é sobre a tecnologia, é sobre o negócio

Este capítulo explica as funções de negócio, seu mapeamento para a infra-estrutura e vice-versa. Os Sistemas de TI não executam os processos de negócio fazendo a empresa funcionar, os processos de negócio fazer as empresas trabalharem.

O desenvolvimento de planos específicos de RIPC para a infra-estrutura de TI estará no caminho certo se os desenvolvedores compreenderem que os sistemas de informação apoiam os processos de negócios.

A fim de desenvolver planos de RIPC para os sistemas de TI, é necessário saber no que os sistemas de TI atualmente consistem.

Primeiro é necessário descobrir se existe um inventário para todo o hardware, software e aplicações de TI que os colaboradores usam.

5.1 Encontrar e utilizar Inventários

Inventário são listas de equipamento e software de TI que uma empresa possui. Abaixo segue uma lista que ajuda a descobrir o que o a empresa possui na infra-estrutura:

- **Inventário de ativos de hardware:** As partes e peças de uma infra-estrutura. Todos os servidores, roteadores, firewalls e outros componentes físicos, incluindo o seu estado ou condição, categorizar cada um apropriadamente, por exemplo: a marca, modelo, número de série, e local (quarto, rack, o que for), como mostrado na Tabela 4-1, sem se esqueça de componentes de rede, cabos, fibra, entre outros
- **Inventário de software:** Saber que programas e onde estão em execução, além de outros dados que fazem sentido tais como: opções de configuração principais, localização de mídia, e assim por diante.
- **Aplicações de negócio:** Conversar com os chefes de departamento para descobrir quais aplicações internas e externas seus departamentos usam. Perguntar como acessam e fazer login para estas aplicações. Com esta informação,é possível começar a mapear aplicativos

de negócios para ativos de hardware e software.

5.2 Usando arquiteturas de alto nível

Um dos segredos em muitas organizações é a falta de diagramas de alto nível, são diagramas de caixas-e-flechas que retratam sistemas de dados de uma organização ou entre várias organizações. Esses diagramas mostram as relações entre os componentes e camadas de um ambiente de aplicação. Quando uma empresa está planejando um plano de RIPC, ela deve ter uma visão do nível de estoque de seus sistemas e aplicativos. Este diagrama deve ter:

- O fluxo de dados e armazenamento
- Infra-estrutura

Muitas vezes, estes diagramas são a única maneira de obter uma visão fim a fim completa de uma única aplicação ou um ambiente inteiro.

Tabela 3: Inventário de Hardware

Marca	Localização	Fabricante	Modelo	Número de Série	Número do Ativo	Rack
RV082	Sala1	CISCO	Roteador 8x portas	1234	101234	2

5.3 Diagrama de fluxo de dados e de armazenamento.

Diagramas de fluxo de dados e de armazenamento de dados fornecem as representações centralizadas do fluxo de informações dentro das aplicações e entre as aplicações. Em quase todos os casos, as aplicações recebem, armazenam, enviam informações. Ter uma visão centrada em de um aplicativo pode ajudar no planejamento do plano de RIPC, entender melhor como o aplicativo funcionam e como eles suportam os processos de negócio, proporciona um bom ponto de partida para o desenvolvimento de planos de recuperação.

Criar estes diagramas de fluxo de dados e de armazenamento ajudam a identificar os sistemas que contêm informações e como a informação se move entre eles. Para desenvolver planos para a recuperação de processos de negócios vitais e críticos, é preciso saber quais os sistemas que apoiam cada processo e como esses sistemas e processos estão interligados. Sem esse conhecimento, não é possível desenvolver bons planos de RIPC. A imagem destes fluxo muitas vezes fornece um caminho para a identificação de detalhes. em outras palavras, depois de ver a

imagem, pode-se selecionar partes do fluxograma e explorar os detalhes sobre como funcionam aplicações específicas e são suportados. A seguir seguem dois exemplos de montagem de fluxogramas um apara e-mail e o outro para aplicações cliente servidor:

5.3.1 O ambiente de e-mail

A figura 4.1 mostra um exemplo simples de fluxo de informações principais de um aplicativo de e-mail, que muitas empresas usam. O e-mail circula entre o servidor de e-mail e a Internet passando pelo filtro de firewall e spam que aparecem no diagrama, outros dispositivos de rede podem estar no caminho mas não aparecem no diagrama, incluindo um roteadores, switches e dispositivos de segurança. Mas com a finalidade de e-mail, os outros dispositivos de rede são alheias - eles são apenas o encanamento.

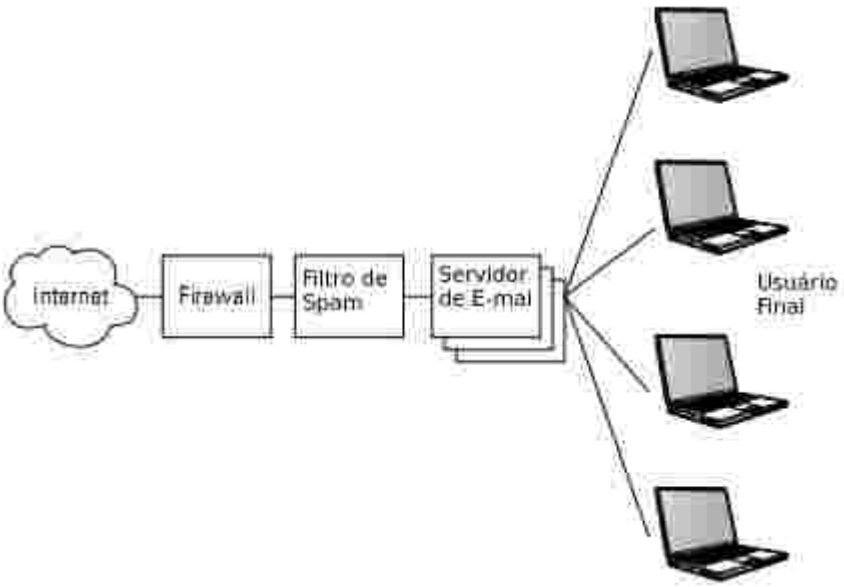

Figura 2: Fluxograma do aplicativo de E-mail

5.3.2 Aplicação cliente / servidor

Esta seção discute uma aplicação um pouco mais complexa, que tem mais peças e partes, para mostrar como descrever os componentes de um ambiente de aplicativo em um diagrama de fluxo de dados. Figura 3 mostra uma aplicação de gestão financeira que a organização executa. Este exemplo mostra um conjunto mais complexo de servidores, armazenamento e fluxos de dados entre a aplicação assunto e aplicações externas. O diagrama inclui um servidor de banco de dados, servidores de aplicativos e web, um servidor de relatórios, um armazenamento de dados, e os usuários finais. O servidor de e-mail também aparece no diagrama porque o aplicativo gera alertas para os usuários finais. O diagrama também inclui uma estação de trabalho de checagem de impressão, que também é uma estação de trabalho do usuário final, mas é um especial porque a impressora está diretamente ligada a ele.

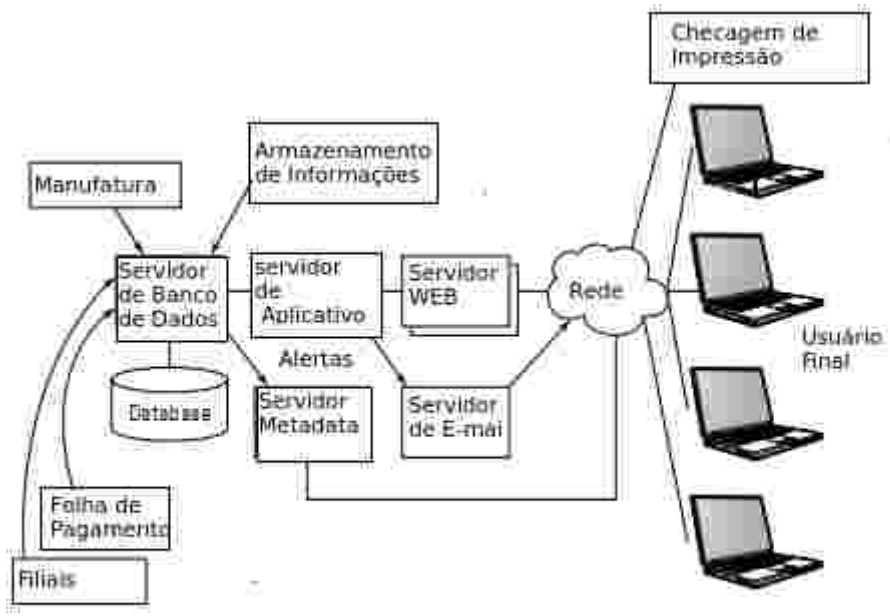

Figura 3: Aplicação de gestão financeira

O diagrama mostra também informações externas, dados que fluem a partir de fontes externas (de fabricação, opções de ações, folha de pagamento, e filiais de negócios, neste exemplo), para o sistema financeiro. Saber sobre estas ligações de ou para o mundo exterior é essencial se ter o conhecimento completo não apenas das aplicação, mas todas as entidades internas e externas com o qual um fluxo deve se comunicar em uma base regular, a fim de funcionar corretamente. Nunca coloque todos os componentes de um sistema complexo para uma só folha de papel. Em vez disso, é interessante utilizar várias ilustrações que cobrem todos os detalhes.

5.4 Diagramas e esquemas de infra-estrutura

Diagramas de infra-estrutura, muitas vezes referenciados como esquemas de infra-estrutura, mostram cada peça e como ela faz parte em um ambiente.

Dependendo do tamanho do meio ambiente de trabalho, de um único indivíduo pode ser capaz de realizar todas estas atividades. Mas em um ambiente maior, é necessário uma equipe de pessoas para fazê-lo, ou seja, para começar a desenhar o esquema de infra-estrutura global, é importante entrevistar os responsáveis pelo sistemas ou rede.

O grupo de TI pode usar ferramentas de gerenciamento de rede e de sistemas que fornecem algumas informações da arquitetura de rede para descobrir equipamentos nela contido, esta informação pode usar como ponto de partida. Alguns exemplos de ferramentas de mapeamento que podem ajudar na descoberta da arquitetura de rede:

- **Quéops** (www.sourceforge.net / projects / cheops-ng): Ferramenta Grátis para mapeamento e monitoramento de uma rede. Figura 4 mostra uma tela com esta ferramenta.

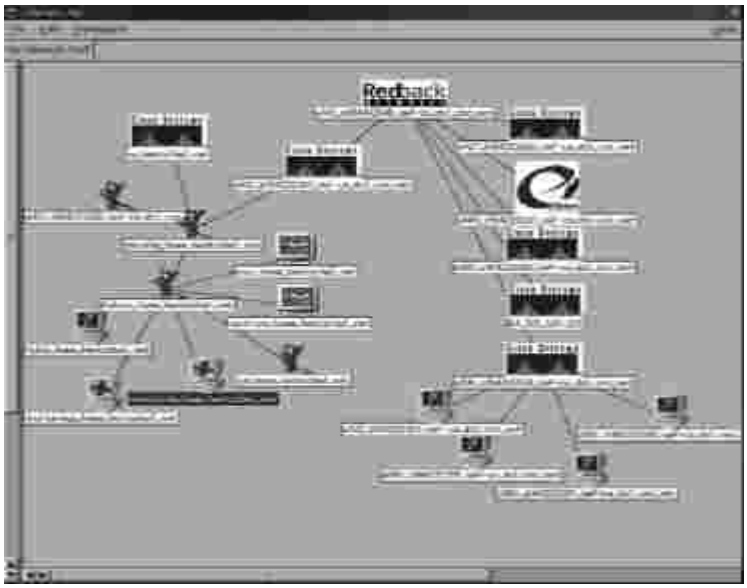

Figura 4: Ferramenta Quéops

- **FreeMap** (www.qualys.com /produtos/testes): Esta ferramenta gratuita é executado a partir de uma localização central, a rede tem de ser acessível através da Internet. Com esta ferramenta, provavelmente, não é possível mapear a partes da rede que estão por trás de um firewall. (Veja a figura 5).

Figura 5: Ferramenta FreeMap

Até mesmo as boas ferramentas de mapeamento rede não consegue identificar cada dispositivo ou sistema em uma rede, algumas omissões podem ocorrer por uma variedade de razões técnicas, incluindo:

- Dispositivos não gerenciados e não-rede: Um dispositivo na rede que não tem conectividade IP, como um servidor de discagem terminal, modem, e assim por diante.
- Dispositivos invisíveis: ferramentas de mapeamento provavelmente não vai ver um hub não gerenciado que não tem um endereço IP.
- Bridging firewalls: Firewalls são como hubs, sem endereços IP. Por essa razão, eles são invisíveis. (Se possuir porta de gerenciamento separada, pode ser visível na rede.)
- Não ligado: Claro, ferramentas de mapeamento ou de gestão não pode ver os dispositivos que não estão ativos.

Ferramentas de gerenciamento de rede e mapeamento pode não detectar sistemas e dispositivos do outro lado de um firewall, assim essas ferramentas precisam ser utilizadas a partir de diferentes lugares lógicos na rede para descobrir tudo.

Verificando a lista de inventário é possível encontrar as listas de equipamentos, pode ser um ponto de partida. As listas de inventário também pode complementar outros métodos de coleta de dados, tais como entrevistas com especialistas no assunto e criação de diagramas e esquemas. Aqui estão algumas vantagens potenciais de listas de inventário:

- Listas de inventário pode conter dispositivos e sistemas não encontrados por ferramentas
- O funcionário que criou a lista de inventário pode ser capaz de ajudar a explicar como tudo funciona em conjunto.

- A criação de uma lista de inventário pode ajudar a entender o fluxo ou funções de várias redes ou sistemas.
- As listas de inventário não pode diferenciar sistemas e dispositivos que estão em uso, produção versus, desenvolvimento, teste ou uso em laboratório.
- Listas de inventário não pode indicar que sistemas e dispositivos que não estão mais em uso. Só porque o dispositivo está listado ou presente, não significa que é fundamental.

Apesar da listas de inventário não são a melhor maneira de determinar quais componentes são essenciais para o desempenho de uma aplicação, listas bem feitas bons podem agregar valor ao esforço. Mesmo utilizando sistemas de gerenciamento de rede e ferramentas de mapeamento, comparar o resultado desses programas com o inventáriopodea validar a integridade dos resultados desses programas.

5.5 Identificando Dependências

Criação de inventários é muito simples, mas desenvolver um de diagramas de fluxo de dados é um pouco mais difícil porque é necessário descobrir por onde os dados circulam. A identificação de dependências entre os sistemas, dispositivos e componentes, é mais complicada, porém é possível identificar respondendo a questão: "Se esse equipamento for desligado, o que vai parar de trabalhar" . Logicamente não é possível desligar equipamentos, mas seguem algumas recomendações:

- **Entrevistas:** Identificar especialistas no assunto e conversar com eles sobre sistemas, redes e aplicações. Especificamente, pergunte o que o sistema representa para a organização e as dependências se externas existir.
- **Configurações:** Alguém com privilégios administrativos precisa examinar as configurações do sistema, dispositivos e aplicações, e identificar os serviços externos, sistemas, dispositivos e assim por diante.
- **Ferramentas de gestão e aplicações:** É possível que a organização já está utilizando ferramentas e aplicativos para configurar e gerenciar sistemas e dispositivos. Por exemplo, pode existir um banco de dados de gerenciamento de configuração e aplicação, isso significa que a maioria ou todos os servidores são configurados de forma quase idêntica. Esta consistência faz com que a tarefa de identificar dependências se torne

consideravelmente mais simples.

Por identificar dependências?

A missão nesta fase do projeto de recuperação de desastres é identificar os sistemas que são fundamentais para o apoio aos processos de negócios. Os sistemas que suportam os processos de negócios não são apenas os sistemas com as aplicações, mas também os que precisa manter-se funcionando corretamente.

5.5.1 Dependências Entre sistemas

Dependências podem existir dentro e entre os sistemas em uma organização. É importante conhecer essas dependências para criar um planos de RIPC de alta qualidade. É possível encontrar muitas camadas de dependências em ambientes de aplicativos. Abaixo seguem algumas categorias de dependência:

- Dependências nos Sistema
- Dependências nas comunicações
- Dependências Rede de serviço
- Dependências dos Gerenciamento de serviços
- Dependências da segurança
- Dependências das aplicação

Dependendo da natureza de seu negócio ou suas aplicações pode ser necessário categorias adicionais de dependências. Por exemplo, ter dependências com nível de segurança, departamento da organização, clientes e assim por diante.

5.5.2 Dependências de sistemas

Dependências do sistema incluem recursos, ferramentas e outros componentes necessários para este funcionar adequadamente, como:

- **Configuração de hardware:** O básico - a quantidade de memória, espaço em disco, outros componentes, e também CMOS / BIOS e outras configurações de hardware em nível de cada sistema contém.
- **Opções de Inicialização:** Será que cada servidor precisa de configurações fora do padrão para sua inicialização ou opções para funcionar corretamente? A Inicialização do servidor pode ser feita a partir de uma imagem armazenada em rede ou armazenamento em disco externo.

- **Clustering:** Organizações muitas vezes criam clusters de servidores com balanceamento de carga ou não para aplicações críticas.
- **Comunicação entre processos:** memória compartilhada, mensagens, entre outros, quantos, qual o seu tamanho e quais são suas configurações de segurança
- **Configuração de serviço:** cada servidor com serviços ou configurações fora do padrão, exemplos incluem serviços de deficiência que são normalmente ativadas, serviço diferente para reiniciar parâmetros,
- **Configuração de armazenamento:** Minimamente, aplicativos ou serviços podem depender de disco e configurações do arquivo de configuração do sistema. Se o sistema tem RAID on-board ou anexo.
- **Contas de usuário:** contas de usuários específicos que precisam estar no sistema que funcione corretamente, ou contas configuradas de forma particular.
- **Ferramentas de software:** As possibilidades são praticamente infinitas. Alguns exemplos podem incluir: ferramentas de gerenciamento de disco, ferramentas de autenticação de usuário, ferramentas de Segurança entre outras.
- **Serviços de rede no sistema:** recursos de rede e ferramentas. Estas dependências incluem entrada e saída de e-mail (existe um serviço ou daemon para execução no sistema de comunicações do correio eletrônico), Servidor de nome de domínio (DNS), console remoto (entrada, saída , ou ambos), entre outros.

Quando estão implementadas ferramentas de gerenciamento do sistema, estas conseguem lista mais dependências, o que torna a verificação de servidores e outros dispositivos um pouco mais fácil.

5.5.3 Dependências nas comunicações.

Praticamente tudo está em rede hoje em dia. Os servidores de aplicativos comunicam-se com os usuários, serviços e outras aplicações. Esta categoria inclui as seguintes comunicações dependências:

- **Configuração de rede:** Algumas das configurações podem incluir o servidor DHCP, DNS, máscara de sub-rede, gateways, tabelas de portas de entrada e de saída, entre outras
- **Comunicação Host-to-host:** Por exemplo, é IPSec, tunelamento ou SSH.
- **Fibre Channel para SAN**: A configuração de comunicações a um Storage Area Network (SAN) pode ser crucial em alguns sistemas.

5.5.4 Dependências de serviço de Rede

Esta seção lida os serviços de rede que existem em algum lugar dentro da organização. Esses serviços podem ou não ser hospedados em qualquer sistema que está sendo analisando. Exemplos desses serviços incluem:

- **Gerenciamento de identidade:** as questões de gerenciamento de identidade, se o sistema autentica os usuários usando um serviço baseado em rede. O sistema deve ser configurado para se conectar corretamente ao serviço
- **E-mail**: aplicações críticas muitas vezes dependem de e-mail para comunicar o status aos usuários e às vezes até mesmo a transferência de dados entre aplicações.
- **Serviços da Web:** interfaces de aplicativos baseados servidor web ou outras tecnologias.
- **PBX (sistemas de telefonia), VoIP:** o PBX está cada vez mais digital e em rede. VoIP, ou voz sobre protocolo TCP / IP dependem totalmente da rede. Embora os sistemas de si não podem depender do sistema VoIP, alguns sistemas VoIP dependem de servidores de comunicações ou de portas específicas para seu funcionamento
- **Fax:** Normalmente possui um colaboradir operado em um ou em ambos os lados
- **Os servidores de proxy e gateways:** na apenas Web ou qualquer outra função
- **Backup:** Organizações geralmente executar um back central, usando um servidor de backup dedicado
- **Replicação de dados:** Pode ou não ser uma parte de um servidor de banco de dados ou cluster. Mas a informação vai para outro servidor ou sistema de armazenamento em tempo real.
- **O horário da rede:** NTP (Network Time Protocol), o protocolo usado para sincronizar os relógios de tempo em sistemas e dispositivos de rede.

5.5.5 Gerenciamento de serviços de dependências

Serviços que são específicos para a gestão de sistemas, dispositivos, aplicativos e assim por diante têm suas próprias dependências.

- **Agentes para gerenciamento de patches:** detectar corretamente a presença de patches de software.
- **Agentes para gerenciamento de capacidade:** quando o sistema estiver com pouca memória ou espaço em disco.
- **Agentes para a gestão de alerta:** quando o sistema apresenta um erro (como falha do

serviço ou falha de hardware).

5.5.6 Dependências da segurança

Quando se fala sobre dependências de segurança, quer dizer mecanismos de segurança ou configurações que as aplicação ou serviço necessitam para serem executadas. Algumas possibilidades incluem:

- **Firewall:** Crítica em alguns ambientes, uma ótima ideia em outros. Protege as aplicações de tráfego de rede contra acessos indesejados.

Anti-vírus: Talvez alguns aplicativos não necessitem de um programa anti-vírus, mas vários outros necessitam

- **IDS/ IPS** (Intrusion Detection System / Intrusion Prevention System): IDS normalmente funciona como uma espécie de um daemon ou serviço. Ele ouve o tráfego de rede e alertas sobre anomalias.
- **Monitoramento da integridade dos arquivos** (FIM - File Integrity Monitoring) é um controle interno ou processo que realiza o ato de validar a integridade do sistema operacional, arquivos de software ou aplicativos, utilizando um método de verificação entre o estado atual do arquivo e o próximo estado após seu uso. Este método de comparação, muitas vezes envolve o cálculo de um checksum criptográfic, outros atributos do arquivo também pode ser usado para monitorar a integridade
- **PKI** (Public Key Infrastructure): Alguns aplicativos podem depender de chaves de criptografia externa, que podem estar em um servidor de chaves ou um aparelho.

5.5.7 Dependências de aplicação.

Às vezes, um aplicativo depende do outro para o bom funcionamento. Exemplos que ajudam a identificar as dependências específicas em ambientes:

- **Inserção de Dados:** Um aplicativo pode exigir uma inserção contínuo de transações de outras aplicações, a fim de funcionar corretamente (ou apenas para evitar resultados nulos).
- **Interfaces:** Aplicações frequentemente comunicam-se umas com as outras em tempo real, a fim de funcionar corretamente.

5.6 Dependências Externas

Aplicações e serviços podem requerer serviços ou funções externas à empresa, a fim de funcionar corretamente. Esses serviços e funções incluem:

- **E-mail:** A plataforma de mensagens onipresentes usado para transportar não apenas mensagens, mas também dados entre as entidades.
- **Comunicações de voz:** As pessoas precisam ser capazes de se comunicar uns com os outros através de voz. Nem sempre ligado diretamente aos aplicativos, mas muitas vezes diretamente ligada aos processos.
- **Fax:** Comunicações de voz, comunicações de fax pode ser essencial ou mesmo fundamental para a recuperação de processos de negócios.
- **Serviço de nome de domínio (DNS):** Absolutamente necessário para qualquer comunicação de rede. O DNS traduz nomes de domínio para os endereços IP que os sistemas realmente usam para se comunicar uns com os outros.
- **Prestadores de serviços externos:** As funções que os aplicativos usam em prestadores de serviços externos e podem estar no caminho crítico de aplicações e serviços internos.

6 Planejamento de Recuperação de Usuário Final

Neste capítulo:

- Certificar-se que as estações de trabalho dos usuários finais vão continuar trabalhando
- Manter a comunicação dos usuários finais

Os usuários são uma parte essencial de todos os processos críticos de negócio. Processos de negócios, mesmo quando altamente automatizados, logo quebram sem envolvimento humano, sua orientação e intervenção.

Recuperar usuários significa recuperar seus postos de trabalho e sua capacidade de se comunicar com as pessoas dentro e fora de sua organização. É necessário analisar vários detalhes para entender o papel de estações de trabalho dos usuários finais e as necessidades de comunicações em processos críticos de negócio.

Neste capítulo, é discutido vários aspectos de recuperação de estações de trabalho de usuários e as necessidades de comunicação, incluindo:

- Terminais de Web (usado principalmente como um navegador da Web)
- Aplicações cliente servidor e ferramentas
- O acesso à informação localizadas nas centrais
- Comunicações de voz
- E-mail
- Fax e mensagens instantâneas (IM)

Recuperar esses recursos requer planos de recuperação que rapidamente restauram a capacidade dos usuários para realizar suas tarefas e apoiar processos de negócios críticos.

As pessoas desempenham um papel vital na operação de processos de negócios e cada vez mais, envolve o uso de computadores ou notebooks.

Sistema de computação de usuário final varia muito, dependendo das tarefas que cada funcionário executa durante seu dia de trabalho. Alguns exemplos incluem:

- Uso e-mail para enviar e receber notificações de aplicativos de outros usuários
- Acessar da empresa aplicativos baseados na Web
- Acessar aplicativos externos baseados na Web
- Acessar aplicações cliente servidor
- Acessar e trabalhar com documentos em servidores de arquivos

- Acessar e trabalhar com documentos na estação de trabalho

Para algumas das funções na lista anterior, a estação de trabalho do usuário é pouco mais do que um terminal. Para outras funções, a estação funciona como um local de transformação ou recurso de dados.

A maioria dos usuários usam tanto os aspectos de terminais como os aspectos locais de processamento de suas estações de trabalho, mas as duas funções não são necessariamente críticas para todas as pessoas, processos ou tarefas.

Um dos propósitos da Análise de Impacto nos Negócios (BIA), é a análise cuidadosa dos processos de negócios. Essa análise ajuda a descobrir quais funções são essenciais para qualquer processo ou tarefa.

Como os funcionários podem utilizar suas estações de trabalho de muitas maneiras diferentes, a gestão e recuperação dessas estações de trabalho envolve uma grande variedade de abordagens.

As seções seguintes abordam as diferentes abordagens para a gestão e recuperação de estações de trabalho, como se fossem ambientes separados:

- Como terminais
- Como um meio de acesso à informação centralizada
- Como clientes de aplicativos
- Como os computadores locais

Independentemente de qual das funções na lista anterior estão em jogo, deve-se de descobrir como administrar e recuperar os sistemas operacionais de estação de trabalho.

A maioria dos usuários utilizam os postos de trabalho para uma combinação de tarefas e uma variedade de modos, porém é preciso considerar apenas os usos que são fundamentais para os processos de negócios.

6.1 Estações de trabalho como terminais Web

Do ponto de vista de recuperação de desastres, a melhor função para recuperar em estações de trabalho do usuário final é o seu uso como terminais, especialmente se essas funções terminais utilizam componentes nativos, como navegadores.

Mesmo neste caso simples, vários fatores requerem algumas considerações como: Aplicação de “Plug-ins” , abordada abaixo e a Configuração do Navegador.

6.1.1 Aplicação de “Plug-ins”

Caso o usuário acesse um ou mais de seus aplicativos críticos através de navegadores da

Web não significa que um planejamento de RIPC não seja necessário. Ao mapear todas as partes e peças móveis de um ambiente de aplicação fim a fim, deve-se identificar o Navegadores Web e os “plugins” que seus aplicativos da Web necessitam para funcionar corretamente.

Alguns exemplos de “plug-ins”:

- Adobe Acrobat: Para ler arquivos PDF
- Apple Quicktime: Para reproduzir vídeo e clipes de áudio
- Adobe Flash: Para exibir conteúdo de páginas da Web
- Shockwave: Para exibir conteúdo de páginas da Web 'Shockwave
- Windows Media Player e outros players de mídia: Para reproduzir vídeo e clipes de áudio
- Visualizadores de documentos: Para visualizar documentos, planilhas, apresentações, planos de projetos, desenhos técnicos, e assim por diante
- Java Virtual Machine (JVM): Para executar applets Java
- Plug-ins personalizados: Desenvolvido pela sua organização ou de um terceiro

Se uma ou mais aplicação Web crítica usar plug-ins, existem questões relacionadas com que podem precisar de atenção são, como:

- Instalação e atualização: Qual a origem do plug-ins, onde eles estão hospedados, em seu servidor de aplicativos ou de um terceiro, ou eles vêm de fontes externas?
- Configuração: Será que algum plug-ins requerem configuração, ou seja, não usa configuração padrão?
- Gestão: Os plug-ins requerem uma gestão central através de ferramentas de TI ou os próprios usuários finais os gerencia?
- O controle de acesso: Os plug-ins requerem acesso a outros recursos, como arquivos na estação de trabalho do usuário final ou em outro lugar?

É necessário dissecar a estação de trabalho do usuário final, para responder às perguntas da lista anterior e identificar outras questões que podem fazer a diferença entre, facilmente recuperar as estações de trabalho do usuário final e aqueles que simplesmente não vai funcionar, apesar de uma série de tentativas de solução.

6.1.2 Recomendações para a recuperação das Estações de Trabalho que operam como terminais Web

A fim de fazer com que as estações de trabalho que operam como terminais Web voltem a funcionar o mais rapidamente possível, durante ou depois de um desastre, deve-se seguir as

recomendações a seguir, alguns dos conceitos são proativos, ou seja, tarefas que precisam ser feitas com muita antecedência, antes de ocorrer um desastre.

- Use configurações padrões para as estações de trabalho que trabalham como terminais Web. Desenvolver e aderir a configurações padrão tem benefícios em muitos negócios, incluindo recuperação. Garantir que as configurações padrão incluem todos os plug-ins necessários, documentos, configurações de rede, configurações de autenticação e outros itens necessários para que as mesmas funcionem adequada
- Use tecnologia de imagem para as configurações padrão. Usando imagens padrão permite que o departamento de TI realize rapidamente sua substituição (o que significa instalar e configurar o sistema operacional, aplicativos e ferramentas para as estações de trabalho).
- Construir imagens da estação de trabalho para uma variedade de configurações de hardware. Tendo estas imagens, aumenta a probabilidade de que a equipe de TI será capaz de reconstruir estações de trabalho usando não só o hardware que sua organização possui em sua base regular, mas também outro hardware que podem ser usados com menos frequência.
- Considere o uso de um modelo de estação de trabalho Computador Cliente para uso, bem como para fins de recuperação. Computador Cliente permite que as estações de trabalho atuem como terminais, mesmo quando a estação de trabalho utiliza programas como editor de texto ou planilha eletrônica, na verdade são executados em um servidor central, em vez de localmente na estação de trabalho. Um ambiente de Computador Cliente simplifica o gerenciamento, centralizado a configuração de software do lado do cliente.
- Backup das imagens das estações de trabalho, de modo a recupera-la e reconstruí-la rapidamente em um desastre. Esses backups facilitam a rápida recuperação das estações de trabalho do usuário final.

6.2 Estações de trabalho com acesso às informações centralizadas

Uma organização preocupada com recuperação de desastre promove (se não exige) que os documentos, planilhas e outros arquivos sejam armazenados centralmente em servidores, e não apenas em estações de trabalho do usuário.

Estações de trabalho que funcionam como terminais web, clientes de aplicações distribuídas ou plataformas de computação independentes também precisam acessar as informações centralizadas, muitas vezes de maneiras semelhantes e exigindo algumas características comuns como servidores. Os tipos de servidor que as estações de trabalho acessam são: Servidores de arquivos e de impressão, Servidores Web e Servidores de aplicativos, descritos à seguir.

6.2.1 Acesso a servidores de arquivo e impressão

Servidores de arquivo armazenam informações para grupos de trabalho, departamentos e organizações, muitas vezes, muitas vezes estes servidores organizam as informação de hierarquias de pastas.

Os departamentos de TI muitas vezes configuram o mapeamentos das unidades em letras, mapear uma unidade do tipo PC, por exemplo como M. Um nome de servidor de arquivos normalmente é mapeado como: \\server2\departamento\legal. Sistemas Linux e Mac usam mecanismos diferentes do Windows, mas o efeito é o mesmo. Servidores de impressão funcionam de forma semelhante, exceto que facilitam o acesso diretamente a impressora, plotters e outros dispositivos de saída.

A seguir estão as principais questões relacionadas com o acesso a servidores de arquivo e impressão:

- Mapeamento: Seja através de mapeamento de unidade do Windows, os atalhos e links, Samba ou NFS (Network File System), estações de trabalho de usuários finais necessitam de algumas informações de configuração para que possam encontrar o servidor.
- Autenticação: Os usuários precisam se autenticar na rede, ou diretamente nos servidores, a fim de acessar arquivos e impressoras.
- Controles de acesso: arquivos e servidores de impressão usar controles de acesso que determinam quais usuários podem acessar diretórios, arquivos e impressoras.
- Serviço de diretório: Aplicações precisa de serviço de nome de domínio (DNS) ou do Windows Internet Name Service (WINS), para as estações de trabalho do usuário poder localizar sistemas na rede corporativa, tais como servidores de aplicativos, servidores de arquivos e servidores de impressão, bem como sistemas na Internet.

6.2.2 Acesso a servidores Web

Servidores Web facilitam o acesso tanto ao conteúdo estático como informações em aplicativos. As questões relacionadas ao acesso ao servidor Web incluem:

- Autenticação: Os usuários muitas vezes precisam ser autenticados para as redes ou aplicações, a fim de acessar o conteúdo em servidores web.
- Controles de acesso: servidores Web usam controles de acesso para determinar quais usuários e grupos têm permissão para acessar informações específicas do servidor web.
- Serviço de diretório: estações de trabalho precisa de serviço de nome de domínio (DNS)

para que eles possam localizar servidores Web na rede.

6.2.3 Acesso a servidores de Aplicativos

Os servidores de aplicativos executar programas de software que são parte de um aplicativo de negócios. Cliente/servidor e ambientes de aplicativos distribuídos também possuem componentes de aplicativos separados, instalado em estações de trabalho do usuário final.

Este software de cliente tem de ser capaz de se comunicar com servidores de aplicação. Questões relacionadas com o acesso ao servidor de aplicação incluem:

- Autenticação: Os aplicativos precisam saber quem está solicitando acesso. Normalmente, o componente do lado do cliente recolhe as credenciais do usuário e passa-os para o aplicativo, que então deve consultar um banco de dados interno ou um serviço de autenticação baseada em rede para validar o usuário.
- Serviço de diretório: estações de trabalho precisa de serviço de nome de domínio (DNS), desta forma a estação do o usuário final pode encontrar servidores e outros recursos na rede.

6.2.4 Notas para a recuperação de estação de trabalho com acesso às informações centralizadas

Quando o usuário final das estações de trabalho precisam acessam de vários tipos de informações sobre a rede, servidores de arquivos, servidores Web e servidores de aplicativos, é necessário gerenciar esse acesso. Considere as recomendações abaixo para a preparação e recuperação:

- Configurar corretamente o DNS ou o WINS para o usuário final da estações de trabalho possa encontrar esses servidores na rede.
- Incluir um serviço de autenticação de rede para que os usuários possam identificar-se com servidores e outros recursos.
- Faça todo o conjunto de permissões de controle de acesso no servidores de modo a ser facilmente recuperáveis e transferível para servidores substitutos, desta forma os controles de acesso serão os mesmos para proteger as informações em um ambiente de recuperação.
- Regularmente realize backup de servidores ou dados, que devem ser replicados para fora do local dos servidores, para ser possível recuperar os dados em caso de um desastre.
- Configurar uma rede substituta que tenha um IP com numeração e arquitetura física e lógica diferente, de modo seja possível transferir todo o conjunto das estação de trabalho do servidor se for necessário.

- Considere a largura de banda nas interações entre servidores e estações de trabalho para otimização. Num ambiente de recuperação, os servidores e estações de trabalho podem ser separados por uma distância considerável ou redes lentas.

6.3 Estações de trabalho como clientes de aplicativos

Estações cliente servidor revolucionaram a computação no início de 1990, liberando valiosos recursos em computadores centrais e movendo IU lógica (interface de usuário) para o usuário final com estações de trabalho que tinham poder de computação relativamente amplo.

Muitas organizações implementadas aplicações cliente servidor, e muitos desses aplicativos ainda estão em uso hoje.

Uma das questões que foi muitas vezes negligenciada em computação cliente servidor era a carga do software de gerenciamento e as configurações relacionadas.

A gestão de estações de trabalho baseada em software de rede ainda estava em sua infância, mas hoje em dia é mais avançadas plataformas de gestão. A gestão de cliente por software ainda é uma tarefa importante para a TI e necessária como parte do plano de RIPC.

Software cliente servidor tem várias componentes do lado do cliente, incluindo:

6.3.1 Servidor de software para clientes

Alguns ambientes cliente servidor são usados para instalação de pacotes de software no cliente, além de programas separados ou scripts para cada aplicação de negócio.

Uma série de perguntas e questões sobre cliente servidor de base de software surgem:

- É possível instalar o software automaticamente através da rede?
- Para instalar o software é necessário um operador para introduzir um código de licença ou dados de configuração?
- Disponibilidade: Aversão usada ainda está disponível?
- Mídia de instalação: Existe uma mídia de instalação para o software?
- Compatibilidade com os sistemas operacionais mais recentes: O software trabalha com as versões mais recentes do Windows e outros sistemas operacionais?

A pergunta principal que deve ser feita sobre o seu cliente servidor de software é: "É possível reconstruir a estação de trabalho a partir do zero o usando o cliente servidor?"

6.3.2 Servidor de “patch” para clientes

Seu ambiente cliente servidor pode usar “patch[1]” nas atualizações de aplicativos de software, ou nas configuração do sistemas para do cliente.

O uso de “patch” pode gerar mecanismos de correção automatizados, ou pode usar um mecanismo centralizado, como o Microsoft SMS (Systems Management Server)

Considere as seguintes questões no uso de “patch” nos aplicativos dos cliente:

- O cliente servidor atualiza os aplicativos
- Pode-se usar uma visão de gestão para determinar quais “patches” devem ser instalados
- O registro das atualizações é bem documentado

As respostas para as perguntas anteriores pode dizer-lhe como fazer atualizações de software do lado do cliente, bem como determinar o histórico de atualizações feitas nas estações de trabalho do seu cliente.

6.3.3 Notas para recuperação de estações de trabalho clientes de aplicativos

A lista a seguir fornece algumas recomendações específicas e ações de recuperação que podem ser tomas para colocar as estações de trabalho cliente em operação a partir de um servidor de aplicativo ou atualização:

- Na medida do possível, usar as configurações padrões para estações de trabalho. As configurações padrões também ajudam a reduzir os custos de suporte. Garantir que as configurações padrões incluam todos os componentes necessários, a partir do código do aplicativo e das configuração. As configurações de qualquer sistema operacional são necessárias para suportar o software.
- Use tecnologia de imagem e ferramentas que podem ajudar a reconstruir rapidamente o servidor das estações de trabalho. Teste suas imagens em uma variedade de tipos de estações de trabalho. Em um cenário de desastre, pode ser necessário construir estações de trabalho em plataformas de hardware que normalmente não são utilizadas.
- Considere-se um ambiente de thin-cliente (estações de trabalho de tamanho reduzido reduzindo usada como terminais inteligentes), como cliente de software instalado em servidores. A tecnologia thin-client permite que a organização centralizar os software de instalação, configuração e manutenção nos servidores.
- Backup de imagens de estações de trabalho. É possível recuperar essas imagem de sistema

1 Patch é um pedaço de software projetado para corrigir problemas, ou atualizar um programa de computador ou os seus dados de apoio

em um desastre, utilizando-as para reconstruir as estações de trabalho, a partir do servidor conforme a necessidade.

6.4 Estações de trabalho como computadores locais

Muitos trabalhadores de uma organização utilizam suas estações de trabalho para compor e gerenciar documentos, planilhas, apresentações, desenhos técnicos e planos de projetos.

As estações de trabalho podem ter ferramentas de software adicionais para o desenvolvimento e teste de aplicativos, análise de dados e modelagem, modelagem gráfica, análise estatística, entre outas muitas aplicações. Muitas vezes, os usuários armazenam os dados (arquivos ou bancos de dados reais que eles criam e usam), localmente na estação de trabalho, especialmente quando a estação de trabalho é um laptop.

É necessário decidir se a utilização desses programas é verdadeiramente fundamental para os processos de negócios específicos da empresa ou se estes aplicativos são meros auxiliares para o usuário final das estações de trabalho.

As estações de trabalho atuam como computadores locais realmente críticas para um determinado processo, ou que elas têm um papel não-crítico?

A gestão e recuperação de estações de trabalho como computadores locais tem três aspectos importantes:

- Programas: Os programas ou aplicativos usados para criar e gerenciar documentos e dados.
- Dados: Os dados que os usuários criam e trabalham com em suas estações de trabalho.
- Procedimento: Documentos sobre o uso de programas locais, em termos de apoio aos processos de negócios críticos.

As três classes de informação na lista anterior são muito diferentes em termos de gestão e de recuperação. Ao determinar quais estações de trabalho estão no caminho crítico dos processos de negócio e os programas bem coo os dados são vitais, é preciso gerenciá-los de maneiras diferentes.

6.4.1 Software utilizados pelas estação de trabalho

É necessário gerenciar o local de software para que ocorra uma recuperação bem sucedida de desastres nas estações de trabalho que estão no caminho crítico dos processos de negócio. Considerar esses fatores abaixo nos seus planos de RIPC:

- Instalação: Qual o método que usado para instalar programas nas estações de trabalho locais? Os programas já fazem parte de uma imagem da estação de trabalho, ou serão instalados usando uma imagem de instalação em um servidor?

- Configuração: os parâmetros de configuração são gerenciados centralmente, ou não cada usuário final irá controlá-los? Se mais de um usuário final realiza tarefas semelhantes, todas elas usam configurações idênticas?
- Controle de versão: A TI controlar quais versões de ferramentas de software são instalados e mantidos em estações de trabalho? Fazer estações de trabalho tem as versões mais recentes ou algumas versões mais antigas?
- Patches: Os programas em estações de trabalho do usuário final tem patches instalados? Configuração: configurações de documentos está associada com a operação correta do programa

6.4.2 Os dados de negócios armazenados em estações de trabalho

Ao se deparar com uma situação em que estação das trabalho de um empregado está, de fato, no caminho crítico para de um processo de negócio crítico, a primeira pergunta a ser feita é: "Por quê?"

As principais preocupações nesta ocorrência são:

- Armazenamento de alta integridade: TI não pode (e não deve) garantir a integridade de armazenamento em estações de trabalho do usuário final. A organização deve armazenar informações de negócios em sistemas com alto nível comercial, talvez utilizar RAID (Redundant Array of Independent Disks), ou uma outra opção.
- Backups: informações de negócios regularmente possuem cópias de segurança, especialmente quando essa informações estão associada com os processos críticos de negócio. Normalmente, ele faz o backup de servidores de TI, mas raramente faz o backup de estações de trabalho do usuário final.
- Gestão: IT servidores geralmente são melhor geridos que as estações de trabalho do usuário final. Servidores de TI estão mais propensos a ter a configuração correta,
- Ambiente: estações de trabalho do usuário final são vítimas de abusos: os usuários as submetem a temperaturas extremas, ou as deixam cair. Servidores de TI, por outro lado, são alojados em instalações com temperatura e umidade controladas.
- Energia: uma fonte de alimentação ininterrupta, condicionadores de linha, ou geradores de energia pode assegurar os servidores.
- O acesso físico: As empresas costumam colocar servidores em salas trancadas com acesso controlado e limitado. Os laptops dos usuários finas estão em local aberto e frequentemente

são roubados

- Disponibilidade: em servidores os dados estarão disponíveis para todos os usuários quando eles precisam, quando comparado com os dados no laptop de um funcionário, o mesmo não ocorre.

6.4.3 Notas para recuperação de estações de trabalho de trabalho como computadores locais

Usar estações de trabalho como plataformas de computação locais tem alguns riscos operacionais. No entanto, é vantajoso e necessário, em muitas circunstâncias.

Abaixo segue umas instruções para preparar a recuperação e as funcionalidade das estações de trabalho caso ocorra um desastre:

- Melhore a capacidades de gerenciamento de configuração, instalações de software e ferramentas de configuração em estações de trabalho críticas.
- Documentar as tarefas e procedimentos dos processos de negócios são executadas em estações de trabalho. Essa documentação deve abranger não só as etapas processuais, mas também a estação de trabalho, versões de software de ferramentas e configurações necessárias para apoiar as tarefas.
- Tomar medidas para assegurar que as informações comerciais nas estações de trabalho pode ser facilmente recuperada.
- Certifique-se que existe controles suficientes no local da estações de trabalho do usuário final para evitar o acesso não autorizado a informações de negócios armazenadas e as ferramentas utilizadas para criar ou gerir essa informação.
- Certifique-se de que os operadores das estação de trabalho entendam os procedimentos associados à estação de trabalho de processamento de informação de base, bem como os procedimentos gerais de segurança e precauções.
- Use procedimentos de imagem ou ferramentas que podem rapidamente construir ou reconstruir estas estações de trabalho.
- Certifique-se de que a imagem da estação de trabalho e procedimentos de aprovisionamento incluem a licença de software e as etapas de ativação.
- Considere recuperar funções da estações de trabalho críticas em um ambiente Citrix-like.

6.5 Sistemas operacionais das estação de trabalho

Não importa que seja Windows, Linux, Mac OS, ou qualquer outro, os sistemas operacionais são o coração de estações de trabalho do usuário final.

Não importa se estas estações são usadas como terminais inteligentes da web, clientes de computação distribuída, plataformas de computação locais, ou qualquer outra, deve-se atentar para os seguintes itens: segurança, plataforma de hardware das estações de trabalho, autenticação em servidores, versão de sistemas operacional e conexão com a rede.

- Plataformas de hardware das estações de trabalho: No contexto do planejamento de recuperação de desastre, as plataformas de hardware para o usuário final é uma atividade crítica. As estações de trabalho devem alguma capacidade, durante e depois de um desastres para que seja possível recuperar as operações e processos críticos. Cada plataforma de hardware tem sua imagem própria, os arquivos, pastas e configurações instaladas. Os departamentos de TI pode ter que gerir dezenas de imagens. Em uma situação em que os escritórios comerciais sofreram significativa destruição, as equipes de recuperação podem ter que reconstruir as estações de trabalho inteiramente, para que o pessoal possa voltar a operar os processos de negócios críticos.
- Versão de sistemas operacional: Gerenciamento de sistemas operacionais em um pequeno número de servidores é um grande trabalho. Mas a gestão SOs em um grande número de estações de trabalho do usuário final apresenta muitos desafios. As estações de trabalho dos usuários finais estão na equação de recuperação de quase todas as empresas.
- Conexão com a rede: É preciso conhecer os métodos de conectividade de rede em uso na sua organização, independentemente da função uma estação de trabalho. Os navegadores da Web e aplicações devem ser capazes de comunicar com os sistemas dentro da empresa e, possivelmente, no mundo externo. Entender esses casos pode ajudar a entender melhor o ambiente de negócio.

6.5.1 Notas para recuperação para sistemas operacionais de estação de trabalho

Você precisa planejar para o sistema de estação de trabalho operacional (SO) de recuperação, independentemente de sua empresa usa essas estações de trabalho, terminais Web, clientes em ambientes distribuídos, ou plataformas de computação independentes. siga estespreparação e as etapas de recuperação para recuperar os sistemas operacionais de estação de trabalho:

1. Instalar um sistema operacional. Esta ampla categoria abrange o licenciamento, a mídia de instalação, ativação e imagem para estações de trabalho. Se existir uma versão mais antiga de um sistema operacional, certifique-se que poderá ativá-la no futuro. Um desastre não é o momento para descobrir que o fornecedor do sistema operacional não pode mais ativar uma

plataforma de sistema operacional necessário uma função crítica do negócio.

2. Configure o seu sistema operacional. Existe um gerenciamento centralizado dos sistemas operacionais ou os componentes do SO serão instalados manualmente, é necessário identificar e documentar todos os pontos salientes da configuração da estação de trabalho para apoiar as funções críticas de negócios.
3. Corrigir e atualizar seu sistema operacional. As atualizações precisam suportar as aplicações, acesso à rede, e outras funções.
4. Configure a autenticação e controle de acesso. Certifique-se que o SO suporta a autenticação local e baseado em rede para que os usuários possam acessar os recursos de que precisam para continuar funções críticas.
5. Configurar a rede e acesso remoto. Estações de trabalho recuperados devem ser capazes de acessar recursos através de redes, caso ocorra um desastre, incluindo redes novas ou temporárias.
6. Configure a segurança. Pode ser necessário o uso de chaves de criptografia, certificados digitais e outras configurações de segurança para facilitar o acesso ou o processamento adequado.

7 Gerenciamento e Recuperação das Comunicações do Usuário Final

Embora o sistema de computação utilizado pelos usuário finais é, definitivamente, um aspecto importante de apoio empregado nos processos de negócios, as comunicações são provavelmente ainda mais importante.

Mesmo em tempo de paz (ou seja, quando você não antecipar um desastre), as comunicações são um ingrediente vital no mundo dos negócios atualmente. Empregados rotineiramente invocam um ou mais dos seguintes elementos de apoio aos processos de negócios: Comunicações de voz ou de correio de voz; E-mail; Fax ou Mensagens instantâneas.

7.1 Comunicações de voz:

As organizações equipam os trabalhadores com as comunicações de voz em uma ampla variedade de maneiras como: serviço telefônico simples para ligação direta; telefone da empresa baseado em PBX (digital com gerenciamento discagem direta ou analógico); PBX-IP conectado a telefones digitais ou baseada em IP conectado softphones através de redes com ou sem fio.

Além dos serviços citados acima podem ser oferecido ao colaborador sistemas mais avançados como: serviço 0800 entrada com o balanceamento de carga de entrada e serviços de gerenciamento de capacidade que rotear chamadas recebidas para um ou mais centros; integração com operadoras de telefonia móvel, por meio de extensão de “trunking” (uma maneira de conectar filiais de escritórios principais); correio de voz ligado a gateways de e-mail; entre outros.

As listas anteriores leva a questão de que a capacidades de telecomunicações de voz, em si mesmas, já justifica projetos extensos RIPC.

Esses projetos podem obter especialmente ser complicado, porque podem existir níveis de integração entre aplicações corporativas, telecomunicações e as empresas de telefonia em si.

A complexidade desses sistemas requer um planejamento detalhado, a seguir é apresentada uma lista contendo dicas de preparação e recuperação para garantir uma recuperação rápida de comunicações de voz:

- Criar um sistema de gestão de recursos de voz, que inclui gerenciamento de mudanças, documentação, procedimento e gestão de configuração.
- Faça backup de todas as informações de configuração no PBX e equipamento de apoio, para poder recuperar esses sistemas.
- Identificar todos os pontos de integração entre PABX, equipamentos de apoio, e de outras redes internas, sistemas e aplicações. Documentar formalmente todas essas interfaces e

pontos de integração, tanto em termos de procedimentos de configuração como de operações.

- Identificar todos os pontos de integração entre PABX, equipamentos de apoio a outros prestadores de serviços externos, incluindo os prestadores de serviços de telecomunicações de outras entidades.
- Identificar pontos de integração entre a comunicação de voz e outras formas de comunicação, incluindo mas não limitado ao correio de voz, e-mail, e sem fio.
- Identificar nos esforços de planejamento de continuidade de negócios os centros de apoio ao cliente e outros eventos empresariais que dependem fortemente de comunicações de voz de entrada e saída. Certifique-se de que existe uma coordenação ampla entre a continuidade do negócio e os esforços de planejamento de recuperação de desastre.
- Considere os operadores alternativos, prestadores de serviços e outras contingências de voz para comunicações de emergência em caso de um desastre. Lembre-se que grande parte da capacidades comunicação de voz de uma organização dependem dos fornecedores e prestadores de serviços externos, cuja resposta a desastres podem ou não traduzir-se em restauração rápida dos serviços que sua organização necessita.
- Desenvolver listas de contato de emergências para o pessoal da ERE, incluir vários meios para entrar em contato com esses indivíduos. Uma catástrofe regional pode resultar na falha generalizada de várias formas de comunicações. Por causa da grande variedade de complexidade e integração com outros sistemas.

7.2 Comunicação por E-mail

O e-mail é considerado crítico na maioria das organizações. As pessoas usam e-mail, não só para comunicar mensagens de rotina, mas também como um mecanismo de transferência de arquivos e um mecanismo formal de alerta.

Cada vez os colaboradores enviam e recebem e-mails, como parte de sua função normal. Tire o serviço de e-mail e uma boa parte dos processos vão parar.

Alguns aspectos de e-mail que o projeto típico de RIPC precisa resolver ou incluir: Cliente de E-mail; Servidor de E-mail; Gateways de E-mail e Conectividade a Internet e Segurança de E-mail.

7.2.1 Clientes de E-mail

Na maioria das arquiteturas, os usuários que enviam e recebem e-mail o fazem usando

software cliente que está instalado nas estações de trabalho. Este software fornece a interface do usuário com o qual eles podem ler, criar e enviar e-mail, e muitas vezes também armazena-lo localmente. Algumas questões devem ser consideras sobre clientes de e-mail incluindo:

- Configuração: E-mail clientes muitas vezes têm vários itens de configuração que lidam com a identidade de um usuário, a localização de servidores de correio na organização, onde as mensagens locais são armazenadas na estação de trabalho, entre outras
- Armazenamento de e-mail local: Muitos clientes de e-mail armazenam localmente, permitindo ao usuário ler e escrever e-mails enquanto estiverem offline.
- Listas de endereços: clientes de E-mail, muitas vezes permitem que o usuário crie listas locais de destinatários, grupos e apelidos dentro de sua lista de endereços própria. Em alguns ambientes, estas listas locais também podem ser armazenados no servidor de e-mail.
- Filtros e regras de encaminhamento: Muitos clientes de email incluem a capacidade de armazenar, apagar ou encaminhar mensagens com base em critérios.

7.2.2 Servidores de E-mail

Servidores de E-mail recebem, armazenam e encaminham e-mail para outros servidores de e-mail e usuários. Grandes organizações têm vários servidores de correio eletrônico, com uma porção da força de trabalho atribuída a cada servidor.

Um desses servidores de e-mail também pode enviar e receber e-mails de entidades externas e à Internet, ou servidores separados podem ser dedicado para esta finalidade.

Devem ser verificados vários problemas quando se considera servidores de e-mail:

- Armazenamento de E-mail: E-mails nas caixas de correio dos usuários, muitas vezes são armazenados permanentemente todos os e-mails enviados e recebidos para todos os usuários na organização.
- Diretórios de destino: E-mail os usuários precisam ser capazes de localizar outros destinatários de e-mail nos livros de endereços online. Esses receptores consistem de outros usuários na organização, além de outras entradas, como endereços de grupo e destinatários externos que os administradores de e-mail colocam no diretório.
- Grupos, listas de distribuição e apelidos: servidores de E-mail muitas vezes contêm outros destinatários de correio eletrônico, incluindo grupos e listas de distribuição .
- Filtragem e encaminhamento regras: servidores de E-mail costumam usar regras para o arquivamento de encaminhamento bem como para excluir as mensagens recebidas.

7.2.3 Gateway de E-mail e conectividade a Internet

Além de transmitir e-mail entre os usuários dentro de uma organização, os usuários também podem enviar e-mail para destinatários fora da organização. Em alguns ambientes, os servidores de correio realizam todas essas funções, mas em outros, os sistemas são separados e é preciso lidar com essas funções:

- Configuração: Os gateways e outros sistemas que processam os e-mail possuem configurações que permitem que eles façam seu trabalho corretamente. Essas configurações incluem informações sobre servidores de correio e maneiras de obtê-los e envia-los para o mundo exterior.
- Armazenamento local: Muitas vezes os gateways armazenam estas informações temporariamente, enquanto esperam para ser transmitidas a seus destinos finais.

7.2.4 Interface de E-mail

Organizações cada vez mais usam e-mail para enviar mensagens e dados de e para aplicações, e não apenas pessoas. Muitos sistemas e aplicativos de servidor podem rotineiramente enviar e-mail por uma vasta gama de razões, incluindo:

- Status: Alguns aplicativos e ferramentas enviam informações sobre o seu estado para as pessoas que os gerenciam.
- Relatórios: Algumas aplicações enviam os resultados de relatórios e consultas via e-mail para as pessoas que solicitam.
- Erros: Os aplicativos podem enviar e-mail para pessoas específicas quando ocorrem erros.

Segurança de E-mail

Está se tornando uma prática comum para os departamentos de TI configurar sistemas de segurança para aplicar proteção de vários tipos aos e-mails:

- Criptografia: Para embaralhar o conteúdo de mensagens para que os curiosos não possam lê-los enquanto as mensagens estão em trânsito.
- Assinaturas digitais: sistemas de E-mail podem usar assinaturas digitais, também conhecido como hash, para protege-los. As assinaturas digitais não vão ocultar o conteúdo de mensagens de correio eletrônico, como a criptografia, mas elas dizem o destinatário se o conteúdo da mensagem foi alterado em qualquer lugar ao longo do caminho entre o remetente e o destinatário. As assinaturas digitais também fornecem uma maneira de verificar a identidade do remetente de uma mensagem.

- Anti-spam: E-mail muitas vezes empregam sistemas de filtros de spam que para bloquear e remover (ou quarentena) a entrada de e-mail que poderia ser spam.
- Anti-vírus: servidores de E-mail costumam ter software anti-vírus que remove os vírus e outros malwares antes de serem entregues aos usuários finais.

7.3 Notas de recuperação de e-mail

- Saber como o e-mail flui, ao redor, e fora da organização, incluindo servidores, clientes, gateways, entre outros
- Documentar todos os fatos sobre os registos de e-mail da organização. Fazer as configurações nos servidores de domínio pode levar algum tempo e é preciso estar preparado.
- Rastrear todos os usos de e-mail nos processos de negócios para determinar os endereços de e-mail, listas de distribuição, regras de filtragem, e outras características que essas mensagens necessitam para chegar aos seus destinos.
- Garantir que qualquer substituição de spam e vírus podem bloquear mecanismos utilizados em cenários de recuperação temporários
- Certifique-se de que o servidor de e-mail têm ampla capacidade de armazenamento durante um cenários de desastres. Em desastres, e-mail poderá acumular mais do que o normal, resultando em necessidades de armazenamento muito maior do que em um dia típico
- Considere um provedor de serviços de e-mail externo para receber e armazenar todos os e-mails recebidos em um cenário de desastre. Com este tipo de fornecedor, os usuários fazer login para ler e-mails através da Internet.
- Arquivo de todas as chaves de criptografia e ferramentas que sua empresa usa para criptografar e-mail
- Backup de e-mail para que possam ser recuperados. Em um cenário de desastre a capacidade de recuperar as mensagens já existentes e receber novas deve ser considerado.

7.4 As máquinas de fax

Muitas organizações ainda dependem fortemente de fac-símile (ou fax) para transmitir documentos de negócios, tais como contratos, recibos, facturas, etc. Embora muitas organizações estão fazendo a transição digital de imagem, máquinas de fax são, todavia, fundamentais para muitos processos de negócios. A seguir são apresentados alguns fatores para considerar em um ambiente de negócios:

- Diretórios: Pessoas que precisam enviar faxes precisa saber os números de telefone de destino.
- Números de fax: Algumas organizações usam números de fax amplamente divulgados ou publicados. Em um cenário de desastre, a organização pode precisar de ter os faxes recebidos encaminhado para outro aparelho de fax ou servidor de fax.
- Configuração do servidor de Fax: Servidores de fax são sistemas que estão ligados a linhas telefônicas ou circuitos E-1, e servidores de fax pode aceitar grandes volumes de faxes que as máquinas não podem.

7.5 Mensagens instantâneas

Ou MI, é uma ferramenta de comunicação em muitas organizações apesar de não estar no caminho crítico para processos de negócios, é útil para comunicações informais.

8 Planejamento de Recuperação de Recursos

Este capítulo centra-se na recuperação de Instalações de Processamento de Informações e de locais críticos. Planejar exatamente onde os computadores e as pessoas vão trabalhar.

Apesar do foco em TIC, outras áreas da organização podem elaborar o plano de continuidade do negócio da empresa bem como o planejamento da recuperação de desastres, que inclui locais de trabalho alternativos para todas as categorias de pessoal

Proteger as instalações pode ajudar uma organização a reduzir ou eliminar os efeitos de um desastre, melhorando as chances de uma organização sobreviver a um desastre, objetivo global de planejamento de RIPC.

Este capítulo discute algumas estratégias para locais de processamento alternativos, ou seja, lugares onde colocar computadores e processos críticos de negócios que dependem de sistemas de informação para seu funcionamento.

Instalações de Processamento de Informações são altas concentrações de computadores e equipamentos de apoio que suportam processos críticos de negócio. Os equipamento de apoio praticamente suportam todos os processos críticos de uma organização e geralmente estão empilhados em racks de equipamentos especiais colocadas lado a lado em uma sala, com massas de cabos de energia e cabos de rede, conectando este equipamento para fornecimento de energia e redes.

Uma sala de tamanho modesto, digamos 5 metros por 5 metros, pode ser tão crítica como 50.000 metros quadrados de espaço de escritório. Não só é o equipamento caro, mas o valor comercial derivado do uso do equipamento que é potencialmente muito elevado.

8.1 Proteger as Instalações de Processamento

Em muitas empresas, a maioria das operações deixam de funcionar se os sistemas de informação que suportam os processos se tornar indisponível por qualquer motivo. Muitas das razões das operações parar tem muito a ver com as características ambientais (energia e refrigeração), ou outros (controle de acesso, detetor e supressor de incêndio), presentes nas instalação em que estes sistemas de informação estão alojados.

8.1.1 Controle de acesso físico

O alto valor dos sistemas de informação, tanto o valor do ativo desses sistemas como seu apoio aos processos de negócios, faz com que as instalações de processamento de informações

sejam altamente seguras. Os centros de dados são muitas vezes a mais alta concentração de riqueza de uma organização. Por conseguinte, o acesso a estes locais tem de ser firmemente controlado, de modo que apenas o pessoal autorizado, com uma razão de negócio válida pode ter permissão para entrar e sair.

Controles de acesso físico evitam catástrofes de origem humana provocados por sabotagem de indivíduos maliciosos ou acidentais,

Os centros de dados muitas vezes empregam vários controles de acesso físico que trabalham em conjunto para detectar e impedir a entrada indesejada de pessoas não autorizadas. Os controles mais comuns são: vigilância por vídeo, cartão ou chave de controles de entrada, controles biométricos de entrada, guardas de segurança, armários com tranca, rack equipamentos com tranca.

Mesmo em uma situação de desastre, é preciso proteger a confidencialidade das informações.

8.2 Energia elétrica

Eletricidade é o ingrediente fundamental para sistemas de informação e equipamentos de apoio. Servidores e equipamentos de rede param de funcionar ou não operam corretamente quando alguma anomalias elétricas comuns e não tão comuns ocorrem.

Estas anomalias incluem: queda no nível de tensão, surtos, picos, transientes, queda de energia, ruídos e falhas definitivas. Quedas e cortes de eletricidade, frequente, não só causa paradas não programadas, mas também pode ter um efeito significativo na expectativa de vida do equipamento. Equipamentos de TI requer energia limpa (sem ruido) e ininterrupta.

São necessários alguns equipamentos em uma instalações para proteger o seu equipamento de TI a partir de problemas de energia:

- Controladores de potência remoto: Estes equipamentos inteligentes, conectados à rede permitem alternar e desligar cada tomada. Eles são de valor inestimável para controlar remotamente equipamentos no “Lights-Out” (apagar da luzes) em data centers.
- Fonte de Alimentação Ininterrupta (FAI): são absolutamente essenciais, estes equipamentos só armazenar alguns minutos de eletricidade em baterias e geralmente filtram os ruídos de linha.
- Os estabilizadores de linha: uma possível adjuntos para FAI, estes equipamentos suavizam as saliências e depressões na alimentação de entrada.
- Gerador elétrico: Se uma organização não pode tolerar paralisações de serviços públicos ocasionais, um gerador elétrico é essencial. Geradores trabalham em conjunto com um no-

break: No caso de uma falha de energia da rede elétrica, a FAI começará imediatamente a fornecer energia a partir de suas baterias por segundos ou minutos, que o gerador necessita chegar a velocidade. Instalações maiores podem exigir mais de um gerador, por razões de capacidade e redundância.

- Alimentações de energia diversificada: Para instalações realmente críticas, considere ter duas alimentações de energia separadas que entram no prédio de lados opostos e que se alimentam de diferentes subestações.
- Equipamentos de comutação: grandes instalações com vários pontos de alimentação de energia, geradores e no-breaks precisa de equipamento de comutação que pode garantir o fluxo contínuo de energia elétrica para os sistemas em qualquer situação.

8.3 Detecção e supressão de incêndio

Detecção precoce de incêndio é fundamental para centros de processamento de informações. Detectar um incêndio em seus estágios iniciais, permite a sua extinção antes que um dano grave ocorra. Quando o fogo inicia, é necessário extingui-lo o mais rápido possível, com o mínimo de danos causados em equipamentos. O uso de água para extinguir um incêndio em um centro de dados não é uma ideia tão boa, a menos que todos os equipamentos serão substituídos.

8.3.1 Detecção de Fumaça e Incêndio

Onde há fumaça, há fogo. O velho ditado não está muito longe da verdade. Detecção de incêndio eficaz começa com a detecção de fumaça. Quando o fogo está em seus estágios iniciais, pode emitir fumaça em quantidades muito pequenas. As opções para detecção de fumaça e fogo são:

- Fotoelétrico: a fumaça espalha a luz no ar, detectores de fumaça fotoelétrico detectam essa dispersão.
- Ionização: Em uma pequena câmara de ionização, a fumaça altera o processo de ionização e desencadeia o alarme.
- Amostragem de Ar: uma rede de tubos de amostragem de ar em toda a instalação suga o ar para uma câmara de amostragem altamente sensível centralizada. Pelo projeto, essa configuração pode detectar fogo mais cedo do que outros tipos de detectores, porque ele pode ter uma amostragem de ar de maior qualidade, utilizando apenas um bom dispositivo de amostragem ao invés de muitas unidades menos caras.
- Temperatura: Quando o fogo se torna mais ativo, ele aquece o ar em torno dele. Os sensores de temperatura detectam a mudança na temperatura.

- Estações manuais: Pessoas na instalação podem acionar o painel de alarme de incêndio mais próxima informando que o fogo começou, da mesma forma que um vigilante.

8.3.2 Alarmes de incêndio e de evacuação

Como a vida humana e a segurança são as principais preocupações em qualquer situação de desastre, alarmes de incêndio precisam ser devidamente concebido e mantido para que o pessoal saiba quando um incêndio inicia e como evacuar rapidamente o local. As saídas devem ser bem sinalizadas, é claro, para ajudar as pessoas a encontrar seu caminho para fora de um edifício quando o alarme disparar.

Alarmes de incêndio em edifícios comerciais são comumente ligado ao corpo de bombeiros local. Esta conexão notifica automaticamente os bombeiros, acelerando a sua chegada e reduzindo os de danos.

8.3.3 Extintor de incêndio

Quando o fogo começa em uma unidade de processamento de informação, é preciso apaga-lo fogo o mais rápido possível, antes que ele danifique os equipamentos mais caros. É preciso utilizar vários meios de controle e extinção de incêndio, incluindo:

Extintores de incêndio: Estes dispositivos portáteis são geralmente localizados ao longo edifícios de escritórios e centros de dados. Existem vários tipos de extintores de incêndio para diferentes tipos de incêndios. Aqui estão os tipos disponíveis:

- Classe A: combustíveis comuns, tais como madeira e papel
- Classe B: Líquidos inflamáveis
- Classe C: energizado (ligado e ativo), equipamento eléctrico
- Classe D: Combustível metais
- Classe K: óleos de cozinha

Alguns extintores possuem diferentes tipos por exemplo, um extintor pode ser classificado como Classe A e Classe B.

8.3.4 Sprinkler

Estes sistema cria uma pulverização constante de água em grandes áreas, resfriando o fogo até que ele não possa mais se sustentar. A água provoca graves danos ao equipamento de processamento de informações, de modo que sprinklers não são bem vindos em combate a incêndios em centros de dados. No entanto, os códigos de construção muitas vezes exigem sistemas

de aspersão como um backup para outros tipos de repressão.

8.3.5 Gases como supressão de fogo

Na maioria das vezes os centros de dados, utilizam estes sistemas, inundando a área com um gás inerte, privando assim o fogo de oxigênio. O sistema funciona através de descarga de gás quando alguém aciona um alarme de incêndio na instalação ou quando um ou mais detectores de calor e fumaça são ativados. O gás é armazenado em grandes tanques dentro ou imediatamente fora do lado da área protegida. Gases frequentemente utilizados são: FM-200, Argonite e Inergen. O uso do gás Halon 1301, mas foi interrompido desde a assinatura do Protocolo de Montreal, em 1989, que proibiu o uso de substâncias que destroem a cama de ozônio.

8.3.6 Manter a Temperatura de Operação

Equipamentos de processamento de informação opera bem dentro de uma faixa bastante estreita de temperatura e umidade. Estas restrições ambiente se torna um desafio quando o equipamento consome muita eletricidade e gera muito calor.

Os equipamento de refrigeração devem livrar-se do calor com uma taxa maior ou igual ao produzido.

A expectativa de vida dos equipamentos de processamento de informações cai drasticamente (às vezes por mais de 90 por cento) com apenas um único pico de alta temperatura, portanto o controle de temperatura é tão vital em um centro de processamento de informações, a ponto de ter redundância Além disso, os sistemas de controle que gerenciam os sistemas de climatização devem ser robustos, assim eles nunca deixar de controlar os sistemas de ventilação, refrigeração e ar condicionádo.

8.4 Seleção de locais de processamento alternativos

Apesar de todos os meios razoáveis disponíveis para prevenir um desastre ou minimizar o impacto de um desastre, alguns eventos são tão intensos que não existe alternativa a não ser abandonar temporariamente ou permanentemente uma instalação de processamento de dados e retomar as operações em outros lugares.

Desastres naturais e provocados pelo homem ocorrem com maior ou menor intensidade dependendo da região. Portanto, a questão principal é: Se ocorrer um desastre, onde a empresa vai operar? As seções seguintes são dedicadas a ajudar a responder a essa pergunta para a sua organização.

- Cold sites: instalações de processamento sem computadores instalados

- Warm sites: instalações de processamento com os computadores que necessitam de instalação e configuração
- Hot sites: instalações de processamento com os computadores que estão prontos para executar o processamento de negócios
- Outros locais de negócios: Outras facilidades que a organização possui
- Mobile sites: instalações de processamento em reboques
- Contracted facilities: instalações de processamento de propriedade de outras organizações
- Reciprocal facilities: acordos de ajuda mútua
- As seções a seguir explicam alguns detalhes sobre as alternativas na lista anterior.

8.4.1 Hot Site

Um hot site é um local que está pronto para assumir o processamento de aplicativos de produção, com pouca ou nenhuma preparação. Sistemas, redes e aplicativos estão todos no lugar e prontos, talvez os dados em tempo real já estejam no site ou podem ser carregado rapidamente. De modo geral, um hot site pode assumir processamento com apenas alguns minutos a horas. Hot sites são os mais caros, porque manter um hot site pronto para assumir funções de produção exige um esforço contínuo. Mas, para as empresas com aplicações altamente sensíveis ao tempo, à custa de um hot site pode valer o custo.

8.4.2 Cold Site

Geralmente são apenas centros de processamento vazios com poucos ou nenhum equipamentos de rede e alguns sistemas (se houver). Facilidades de comunicação pode ou não estar ninstalada. Pense em um local frio como uma sala vazia, com controles físicos e ambientais no local, mas nenhum equipamento de processamento de informações. O tempo necessário para colocar um Cold Site é de pelo menos vários dias, possivelmente, uma semana ou mais.

8.4.3 Warm sites

Esye modelo está bem no meio entre os anteriores. Warm Sites pode ter servidores e equipamentos de rede no lugar, mas nenhum software ou dados carregados. Este modelo pode precisar de um a cinco dias para funcionar completamente.

A Tabela 4 mostra a prontidão, comunicação, estado das dados e custo para os diferentes tipos de locais alternativos explicados acima.

Tabela 4: Comparação entre diferentes tipos de Locais de trabalho

Categoria	Hot	Warm	Cold
Prontidão	Minutos ou horas	horas ou dias	dias ou semanas
Aplicação	Carregada e pronta	Presente, mas pronto	Ausente, deve ser comprado e instalado
Comunicações	Pronta	Capaz de atender	Pouca ou nenhuma
Dados da aplicação	Atualizados	Não atualizados	Não está presenta
Custo	Muito alto	Moderado	Baixo

8.4.4 Outros locais dos negócios

Algumas empresas já têm mais de um local de processamento secundário com a capacidade de processamento de suas instalações. A construção do seu próprio local de processamento alternativa pode custar menos do que serviços no exterior ou instalações compartilhadas. Alguns pontos a considerar quando se pensa em outros locais de negócios, locais de processamento alternativos incluem:

- Segurança física: O outro local de negócios têm controles de segurança física suficientes, tais como cercas, vigilância por vídeo, sistemas de cartões-chave, e assim por diante?
- Apoio de Ambiente: O site tem condicionamento de ar suficiente e capacidade de potência?
- Riscos: É o local livre de riscos associados com os aeroportos, ferrovias, materiais perigosos, inundações, tempestades, deslizamentos de terra e outros fatores?
- Proximidade ao local de processamento primário: É o local longe o suficiente de instalações de processamento de informações existente para não ser considerado na mesma zona de risco? Tal distância mínima pode variar de 100 a 800 quilômetros.
- Transporte: É o local alternativo suficientemente perto dos principais sistemas de transporte, tais como aeroportos, ferrovias, portos, rodovias, ou para tornar os sistemas de acesso em caso de emergência?
- Leis e códigos: os códigos de construção e as leis relativas à segurança e outros assuntos para o centro de tratamento alternativo são adequadas para as suas necessidades?

8.4.5 Centro de dados em uma caixa

Sites de móveis de organizações como a Sun Microsystems, e SunGard desenvolveram centros de

dados móveis de emergência que eles podem oferecer para um local de negócios. Essas empresas oferecem as seguintes funcionalidades:

- Sun Microsystems Projeto Blackbox: centro de dados auto-suficiente em um contêiner que pode ser enviado para qualquer lugar do mundo por caminhão, navio, trem ou ar. Equipado com alimentação integrada, refrigeração e uma seleção configurável de servidores e equipamentos de rede.
- SunGard: centro de dados móvel em uma plataforma semi-reboque do caminhão, que inclui um gerador, voz e acesso de comunicação de dados, terminais e impressoras, racks de equipamentos, áreas de trabalho, cozinha, banheiros, iluminação e segurança física. SunGard tem várias dessas unidades disponíveis para a expedição dentro de 48 horas.

8.4.6 Instalações compartilhadas - "*Colocation facilities*"

Centros de dados comerciais, também conhecido como instalações de *colocation*, são um grande negócio em quase todas as áreas metropolitanas do mundo.

Instalações compartilhadas são centros de dados "multi inquilinos" em que uma organização arrenda tanto espaço quanto um inquilino necessita, passando a fazer parte de um único local de centenas de metros quadrados, oferecendo recursos como:

- Segurança física: Os guardas de segurança, entradas principais com vídeo vigilância, cercas, e talvez outras medidas, tais como cães de guarda, barreiras de segurança, e assim por diante.
- Conectividade de Rede e Internet: Fornece conectividade com a Internet basta ligar o roteador, firewall, switches, e assim por diante.
- Energia, incluindo energia de emergência: Algumas instalações têm alimentações de energia redundante, geradores, no-breaks, e assim por diante.
- Ar-condicionado e controles de umidade redundantes para se livrar de todo o calor que seus servidores geram.
- Sistema de monitoramento e gerenciamento: monitoramento de sistemas, gerenciamento, backups, e assim por diante, aberta 24/7..

A vantagem dos custo de uma instalação compartilhada é potencialmente significativa. Em particular, elas são caros de construir e manter, e uma organização vaie pagar apenas a sua parte usada na forma de taxas mensais. Instalações compartilhadas têm uma desvantagem, elas são caras, embora menos do que a construção de uma particular.

8.4.7 Instalações com Facilidades Reciprocas

Antes de instalações compartilhadas (colocation), uma das poucas opções disponíveis para locais de processamento alternativo foi a Instalações com Facilidades Reciproca. A facilidade recíproca é um acordo legal entre duas partes, em que cada um se compromete a fazer uma parte de seu recurso disponível para a outra parte, no caso de a outra parte sofre um desastre que obriga a abandonar o seu próprio centro de dados.

Simplesmente é um acordo onde uma empresa deixa a outra utilizar o seu centro de dados se caso a primeira tenha um desastre e vice versa.

Na era dos computadores mainframe, o acordo de reciprocidade aplicva-se não somente ao espaço físico, mas oo uso de computador mainframe da organização. Assim, um acordo de reciprocidade também foi um “time-sharing”, porque uma organização permitiria uma outra organização executar seus programas em seu mainframe.

As duas organizações precisavam ter o mesmo tipo de computadores mainframe para que os programas de aplicativos em um também seja executado em outro e talvez realizar testes regulares para se certificar de que os sistemas continuam compatíveis.

No ambiente de hoje, um acordo recíproco pode ou não incluir o uso de sistemas da outra organização, podendo abranger apenas o espaço físico e energia para seus sistemas no centro de dados da outra organização. Ainda assim, um acordo de reciprocidade pode custar muito menos do que as alternativas ou instalações compartilhadas.

9 Planejamento e recuperação do sistema de rede

9.1 Gestão e Recuperação de servidores

Se os dados e aplicativos são a alma de um processo de negócios de TI, os sistemas são o corpo em que a alma reside. O sistema precisa ser um recipiente adequado que permite que o aplicativo seja executado corretamente e fornece acesso a dados da aplicação.

Resiliência de Sistemas é a chave para a recuperação em face do desastre, isso significa que o sistema terá a capacidade de restabelecer seu equilíbrio após este ter sido rompido por um distúrbio ou desastre.

Durante e após um desastre uma organização precisam desta resiliência.

A organização tem uma coleção de sistemas, em diferentes locais, que estão prontos para assumir funções operacionais, quando ocorre um desastre. Não significa ter um segundo conjunto de servidores prontos. Muitas organizações não podem pagar esse tipo de redundância. Pelo contrário, os sistemas devem estra prontos somente quando necessário, de acordo com as opções:

- Hot servers já compartilhando a carga de trabalho atual
- Hot Standby servers pronto para assumir a curto prazo
- Warm standby servers em espera passiva pronto para assumir com alguma preparação
- Cold standby servers prontos para instalação de aplicativos e dados

A opção que uma organização escolhe depende da sensibilidade de tempo e valor de negócio das aplicações que os servidores suportam, bem como se a organização pode investir em uma determinada capacidade de recuperação. Independentemente da opção deve-se identificar e gerenciar diversas questões técnicas. Em geral, quanto mais rápida é a recuperação da recuperar a capacidade de processamento, mais complicado e caro fica a solução.

9.2 Determinar a prontidão do sistema

Um PCRD define os processos de negócios mais críticos e, por isso, identifica as aplicações e bancos de dados associados a esses processos como crítica. Estas aplicações críticas e bancos de dados, por sua vez, identificam servidores críticos e infra-estrutura de apoio.

Ao determinar o Objetivo do Tempo e Recuperação (OTR), fica estabelecido quanto tempo uma organização tem para conseguir novos servidores prontos para executar as aplicações críticas.

Um OTR determinado em minutos para recuperar os sistemas em um desastre, implica em um local remoto que provavelmente já realiza o trabalho de produção com balanceamento de carga. Um OTR em horas ou dias, também necessita de um hot site, em dias ou semanas, o seu plano

provavelmente exigirá um Hot ou cold.

9.3 Arquitetura e configuração do servidor

No Capítulo 4, foi discutida a necessidade de informações de inventário em cada nível. Ao inventariar os sistemas, softwares, dispositivos de rede, e outros ativos de suporte, pode-se começar a identificar os componentes que suportam funções críticas de negócios. Depois de identificar esses ativos, é necessário olhar para os servidores de aplicativos críticos. Neste nível deve-se identificar cada pequeno detalhe e determinar as seguintes informações para cada servidor:

- A configuração de hardware: Saiba tudo sobre o hardware em um servidor, incluindo: marca, modelo, número de série, versões de firmware (BIOS / CMOS),número e tipo de CPUs, auantidade e tipo de memória, adaptadores de rede hardware, interfaces de armazenamento (por exemplo, adaptadores SCSI), exatamente como o hardware é montado (ordem de placas adaptadoras, cartões de memória, e assim por diante). dispositivos periféricos conectados (tipo, modelo, versão, e assim por diante), entre outros
- Sistema Operacional: saber tudo sobre o sistema operacional (OS) que está sendo executado no servidor, incluindo, mas não limitado a: versão, data de lançamento, nível de patch para o sistema operacional, componentes instalados e suas versões, configuração de inicialização, configurações de recuperação
- Recursos de configuração: memória virtual, as definições de utilização de disco, utilização de memória, como o sistema operacional faz com que os recursos disponíveis para aplicações e processos do sistema. No mundo UNIX, estes são os parâmetros do kernel, no Windows, estes são configurados principalmente no registro e em algumas funções de interface de usuário administrativo. Independentemente do sistema operacional, os administradores de sistema geralmente gerenciam essas configurações.
- Configuração de serviços de rede: Todos os ajustes usuais, incluindo a máscara de sub-rede, gateway, servidor DNS, servidor de diretório e servidor de tempo, bem como configurações de ajuste, tais como o número de conexões abertas e alocação de buffer.
- Configuração de segurança: lidar com registro de eventos, auditoria de sistemas, acesso em nível de sistema de controle de configuração, download de patches e de instalação e configurações de conta de usuário.
- Os componentes adicionais instalados no nível do sistema, incluindo: Firewall, detecção e prevenção de intrusão, anti-virus, anti-malware, agentes de gerenciamento do sistema

- Gerenciamento de acesso: toda a gama de nível de sistema de acesso que inclui: IDs de usuário, ID de usuário e senha de configuração, Configurações relacionadas a qualquer gerenciamento centralizado de usuários, recursos como LDAP ou Active Directory, recursos compartilhados, diretórios significado e outros recursos que os usuários podem acessar através da rede

9.3.1.1 Por este nível de detalhe é importante

Aplicações e dados críticos residem e são executadas em seus servidores. A configuração complexa de servidores permite a execução das aplicações no estado mais ou menos previsível que os administradores e os usuários estão familiarizados. Para assegurar que um servidor de recuperação pode apoiar o funcionamento correto e adequado de uma aplicação crítica, é necessário configura-loo para coincidir com o servidor original, tanto quanto possível. Caso contrário criam-se instabilidades ou mudanças potenciais em termos de funcionalidade.

9.3.2 Desenvolver a capacidade de construir novos servidores

Em um incidente é necessário fazer cópias ideênticas de servidores de aplicativos críticos e usar essas cópias para executar seus aplicativos quando ocorre uma catástrofe. Então, é necessário descobrir como construir novos servidores que são como os já existentes ou tao semelhante quanto possível aos já existentes para que os aplicativos possam ser executados com o mínimo de incompatibilidade. Construindo servidores quase idênticas para fins de recuperação é uma coisa, mas mantendo os servidores consistente é outra completamente diferente. Consistência Server requer duas disciplinas distintas, porém relacionadas:

- Gestão da mudança: O processo de negócio preocupados com o bom desenvolvimento, análise e aprovação das alterações feitas em um ambiente de produção, em todas as camadas. O objetivo da gestão da mudança é expor os riscos potenciais e outras questões que possam comprometer as alterações propostas antes que eles ocorram. Gestão da mudança adequada dará maior disponibilidade do sistema e menos interrupções não programadas.
- Gerenciamento de configuração: O processo de gravação de todas as alterações feitas a todos os componentes (em todas as camadas) em um ambiente. O repositório central é conhecido como o banco de dados de gerenciamento de configuração, que armazena todos os detalhes sobre os sistemas sob sua gestão.

  Normalmente, o gerenciamento de mudanças e gerenciamento de configuração se

relacionam entre si desta forma: O gerenciamento de configuração serve para documentar as mudanças analisadas e aprovadas pela gerencia de mudanças.

Como manter as configurações do servidor de recuperação consistente depende muito da sua velocidade de recuperação: Se o seu plano de RD utiliza-se de Hot Servers, é importante ter os meios para atualiza-los de modo automatizado quanto possível. Se você instalar patches ou fazer outras alterações no servidor principal, pode realizar essas mesmas alterações aos servidores de recuperação o mais rapidamente possível.

Servidores muito longe da sincronia pode gerar problemas durante uma operação de recuperação.

Um plano de RD pode especificar a compra de servidores em caso de desastre e em seguida, construí-los depois que eles chegam. Em uma situação como esta, é possível investir em um conjunto de ferramentas que podem ser usar para duplicar as configurações de um servidor para outro.

Como manter essa consistência depende da rapidez necessária para começar a usar seus servidores de recuperação em um desastre.

9.3.3 Considerações de computação para servidor distribuídos

Muitos ambientes utilizam uma arquitetura de aplicação complexa que inclui componentes que residem em vários servidores, e nem todos os servidores são, necessariamente, localizado no mesmo local. Arquitecturas distribuídas (como esses tipos de arquiteturas são chamados), aumentam a complexidade de um ambiente no estado estacionário e introduzem outras questões que devem ser abordados no plano de RD. Esta complexidade é ainda mais exacerbado nos casos em que outros organismos possuem ou operam um ou mais dos componentes no ambiente de aplicação.

Com empresas conectadas à Internet a integração de aplicações que é alimentada por interoperabilidade nos negócio tornou-se possível, com a Arquitetura Orientada a Serviços (SOA), o planejamento de recuperação de desastres assume um nível muito mais elevado de complexidade. As organizações precisam fazer planos adicionais para a recuperação destes ambientes cada vez mais complexos.

9.3.4 Problemas de Arquitetura

É possível encontrar questões relacionadas à arquitetura do aplicativo durante a análise de um plano de RD e esforço de planejamento como:

- Interfaces: Interfaces personalizadas entre os componentes de seu ambiente distribuído, vai

demandar mais de esforço (por parte dos desenvolvedores de sistemas ou integradores) para melhorar a resiliência no ambiente em geral.

- Latência: Em um ambiente altamente distribuído, os sistemas que se comunicam através de grandes distâncias ou através de conexões de rede WAN lentas, pode experimentar latência (atrasos na transmissão de dados de um sistema para outro). O comportamento da aplicação podem mudar de forma inesperada em um cenário de desastre se a latência entre os componentes aumenta (ou diminui) por um montante significativo. Partes de um ambiente distribuído pode não ser capaz de tolerar a latência de outras partes.
- Considerações de rede: Um ambiente de aplicação distribuída que engloba a conectividade WAN precisa levar o projeto de rede em conta. Aplicações distribuídas que foram projetados para, e implementado em, redes locais rápidos podem sofrer degradação do desempenho em uma rede WAN. O efeito cumulativo de vários saltos longos através desta pode diminuir o tempo de resposta e até mesmo causar timeouts de rede.

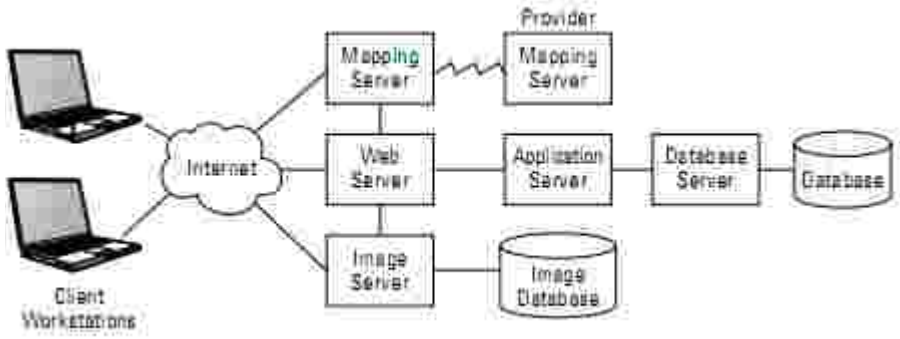

Figura 6: Típica aplicação de Arquitetura

9.3.5 A consolidação de servidores

A consolidação de servidores tem sido o assunto dos departamentos de TI por vários anos e representa um movimento de redução de custos ainda popular. O conceito é simples: em vez de instalar aplicações em servidores individuais, o que pode resultar em servidores subutilizados, instala-se vários aplicativos em poucos ou em um único servidor, utilizando forma mais eficiente o hardware e reduzindo assim os custos. Tudo deve ser feito para poupar dinheiro, energia elétrica, recursos naturais entre outros.

9.4 Gestão e Recuperação de Infra-estrutura de Rede

Redes e serviços de rede são canais de comunicação que permite que aplicativos se comuniquem uns com os outros e com as pessoas que os utilizam.

Embora as redes são geralmente muito menos complicadas do que as aplicações que suportam, elas são muito mais complicadas do que as arquiteturas empresas utilizadas em tempos passados.

A Figura 7 mostra uma arquitetura típica rede corporativa. As redes são muito mais do que apenas os dispositivos que movem o tráfego da rede.

Redes podem executar funções muitas vezes invisíveis , que permitem a comunicação dentro e entre empresas.

Noventa por cento de um bom planejamento RD é saber o que faz com ocorre o tráfego de dados na rede, especialmente quando você está lidando com as redes e serviços desconhecidos de terceiros. Na maioria das vezes as características de uma rede e os problemas com sua recuperação estão correlacionados. Depois de identificar os ativos e recursos, deve-se incorporar essa informação no planejamento RD.

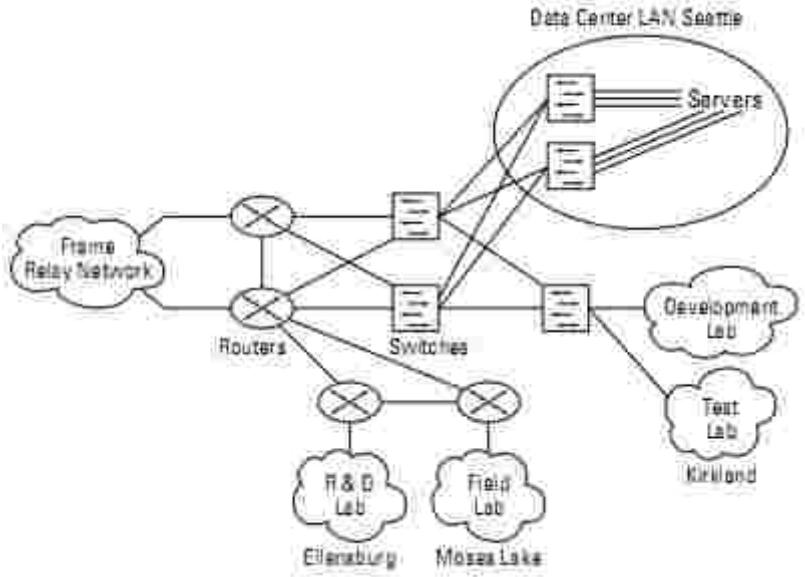

Figura 7: Típica Arquitetura de rede corporativa

Considere a rede de voz (ou seja, os telefones do escritório), como parte da rede, como por exemplo: telefones analógicos, digitais ou baseado em IP no ambiente. Comunicações de voz são tão vitais como a comunicação de dados na maioria das organizações, e talvez até mais.

9.4.1 Dependências de rede externa

A conexão de uma organização com a Internet depende de algumas definições de configuração que os prestadores de serviços externos mantêm, incluindo:

- Circuitos e troncos de dados: obter qualquer espécie de circuito de dados na Internet (um circuito de rede que conecta sua rede de dados interna com a Internet) ou tronco PBX (a conexão de rede entre o seu sistema interno de telefonia e rede telefônica pública). Sua instalação leva várias semanas.
- Serviço de nome de domínio (DNS): DNS é a cola dos nomes de domínio associados com os endereços IP que os sistemas utilizam. Alterar um endereço IP para um serviço bem conhecido, como um site, pode levar horas ou dias antes que os usuários da Internet posam visitar o site sobre o novo endereço IP.
- Números de rede publicamente roteáveis: a conexão de rede estabelecida entre um ISP (Internet Service Provider) e um negócio inclui alguns endereços fixos (não alterável) IP que estão associados a essa conexão de rede particular.
- Serviço de telefonia: Além dos troncos, existem outras considerações para construir ou recuperar a rede de voz em um ambiente RD. O provedor de serviço de voz pode ter uma ideia melhor do que é necessário considerar a fim de recuperar a rede de voz. DNS, endereços de rede e circuitos de voz podem levar muito tempo para recuperar as funções.
- Network Time Protocol (NTP): o uso do NTP para fornecer informações precisas de sincronização do relógio para servidores e estações de trabalho, certificar de que esta importante função continua funcionando.

9.5 Implementação de interfaces padrão

Muitas vezes é mais fácil estender e alterar uma arquitetura de aplicativos que é baseado em padrões abertos do que aquele que é construída com interfaces personalizadas. Os padrões abertos são a programação e tipos de comunicação no qual as aplicações e os sistemas são construídos.

Aqui estão alguns exemplos de padrões abertos:

- TCP / IP: O protocolo de rede da Internet. Dezenas de padrões abertos cair dentro de TCP / IP, incluindo SMTP (Simple Mail Transfer Protocol) que faz o trabalho de e-mail, DNS (Domain Name Service), que é usado para traduzir nomes em endereços IP, NTP (Network Time Protocol) que sincroniza o relógio do sistema , HTTP (HyperText Transfer Protocol) que os navegadores da Web usam para solicitar dados de servidores Web e SNMP (Simple Network Management Protocol), que é usado para gerenciar dispositivos e sistemas de rede.

- World Wide Web: Engloba protocolos e padrões que suportam a web.
- GSM: O padrão de comunicação de telefone celular usado na maior parte do mundo.

9.6 Implementar Cluster de Servidores

As aplicações que são críticas para os processos de negócios importantes muitas vezes exigem maior disponibilidade, precisando ser recuperadas rapidamente em outro local. Organizações que precisam recuperar esses aplicativos em poucos minutos em caso de uma falha frequentemente usam clusters de servidor.

Clustering é uma proposta cara, mas é o método de escolha para aplicações que requerem uma rápida recuperação. Um cluster de servidor é uma coleção fortemente acoplado de dois ou mais servidores que estão configurados para hospedar um ou mais aplicativos.

Em seu livro In Search of Clusters (Prentice Hall), Gregory Pfister descreve um cluster como "um sistema paralelo ou distribuído que consiste em um conjunto de computadores interligados, que são utilizados como um recurso de computação unificada." Em outras palavras, um cluster é um conjunto de computadores que aparecem como um único computador para os usuários finais.

Os servidores em um cluster pode coordenar com os outros para garantir que pelo menos um dos servidores irá executar os aplicativos. Eles coordenam, comunicando uns com os outros através de uma rede rápida, usando o software de clustering que administra um complexo conjunto de tarefas. Figura 8 mostra uma arquitetura de cluster de servidor.

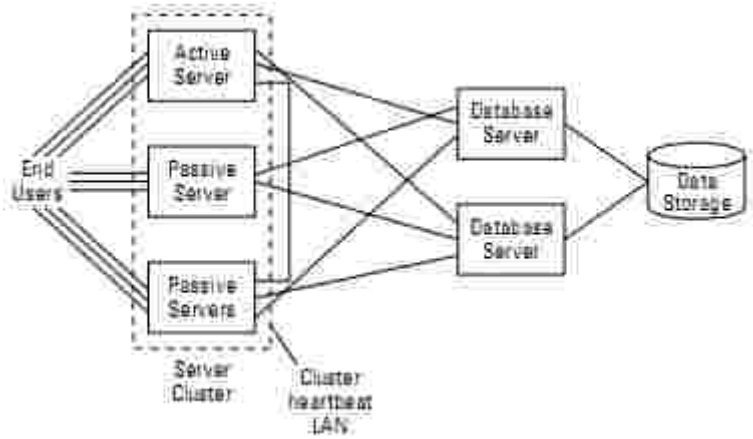

Figura 8: Típica Arquitetura de rede corporativa

9.6.1 Modos de operação do clusters

Os clusters de servidor geralmente operam em um dos dois modos básicos, que são baseados

em como os servidores são configurados para operar no dia a dia:

- Ativo / ativo: Nesta configuração, todos os servidores do cluster executam aplicações. Pode-se usar este modo para um cenário de compartilhamento de carga no qual um aplicativo é executado em vários servidores ao mesmo tempo.
- Ativo / passivo: Esta configuração é composta de servidores que são aplicativos de hospedagem (os ativos) e outros servidores que estão em modo de espera.

Se uma organização optar por executar em modo ativo / ativo ou ativo / passivo depende do desempenho, disponibilidade e necessidades de recuperação de desastres.

9.6.2 Arquitetura de cluster e armazenamento

A arquitetura de servidores em cluster, sistemas de armazenamento, e as próprias aplicações são fortemente acoplados. Aplicativos hospedados em um cluster de servidor deve ser concebido de forma a adequar a arquitetura de armazenamento com o conjunto do sistema.

Pode-se usar várias tecnologias para proteger os dados de aplicativos, incluindo o armazenamento resistente, espelhamento e replicação. Um aglomerado servidor precisa de uma ou mais destas tecnologias. A lista a seguir decompõe cluster e arquitetura de armazenamento em termos mais simples. Escolha uma tecnologia de cada um dos seguintes grupos para montar uma arquitetura de cluster completa:

- Arquitetura de cluster: Ativo / Ativo ou ativo / passivo
- Arquitetura de armazenamento: SAN (Storage Area Network), via SCSI, Loop Arbitrated Fibra, ou uma rede de fibra ou NAS (Network Attached Storage): sistemas de armazenamento na rede com o protocolo NFS (Network File System) ou SMB (Server Message Block) protocolos de rede.
- Replicação de dados: executar o espelhamento em que as alterações dos dados em um dispositivo de armazenamento sistema são copiados para um sistema de armazenamento remoto em tempo real, ou a cópia de transações de um sistema para outro.
- Arquitetura de rede: balanceadores de carga

10 Lista de Verificação de Plano de Continuidade

A verificação do estado que uma empresa se encontra em relação a existência ou não de um Plano de Continuidade é importante para iniciar o desenvolvimento do mesmo.

A Tabela 5 possui uma lista de verificação inicial.

Tabela 5: Sua Empresa está está prepara para o rompimento de suas atividade.

Procedimentos de emergência	Será que todos os colaboradores sabem como dar o alarme e pedir ajuda? Será que todos os colaboradores sabem os procedimentos de evacuação em caso de incêndio, bem como a rota de saida? Existe um ponto de encontro em caso de fogo? Os seus procedimentos são testados regularmente?
Segurança e bem-estar	Sua empresa tem provisões de primeiros socorros adequados no lugar? Sua empresa cumprir os aspectos da lei de saúde e segurança?
Lista de contato	Sua empresa tem detalhes de contato para os principais membros da equipe de resposta de emergência? É possível contatá-los a qualquer hora? Sua empresa verifica regularmente se os detalhes de contato estão atualizados?
Avaliação de risco	Você já pensou o que poderia ameaçar os negócios ou as operações na sua empresa? As empresas vizinhas possuem características que são uma ameaça? Você já tomou medidas para prevenir ou reduzir os riscos mais significativos na sua empresa?
Segurança	Sua empresa possui instalações seguras? Você sabe e controla quem entra e sai em suas instalações?
Manutenção e prevenção	Os sistemas de canalização, eletricidade, gás e aquecimento mantido são mantidos e revisados regularmente? Existem outros equipamentos importantes sujeitos a manutenção preventiva?
Seguro	O seu seguro possui cobertura a níveis adequados níveis adequados?

	O seu seguro possui cobertura cobre interrupção de negócios e perda de renda?
Plano de Continuidade	Você tem um plano de continuidade de negócios? Mesmo um esquema básico de como manter suas principais operações em execução irá dar-lhe uma vantagem caso o pior ocorra.
Informação	Você sabe para onde ir de modo a obter mais informações sobre o planejamento de continuidade de negócios caso ocorra um desastre? Você sabe como obter ajuda em caso de um incidente?
Consequência	Será que todo mundo entende o que precisar fazer no caso de um incidente e como eles podem contribuir para o processo de recuperação?

11 Gerenciamento de Plano de Continuidade BS 25999-1

Esta norma britânica foi desenvolvido por profissionais em toda a comunidade de continuidade de negócios, aproveitando as suas experiências acadêmicas, técnicas e práticas de gestão de continuidade de negócios.

Foi produzido para fornecer um sistema baseado em boas práticas para a gestão de continuidade de negócios. Destina-se a servir como um ponto de referência para a maioria das situações em que a gestão de continuidade de negócios é praticada.

É para ser usada por organizações de grande, médio e pequeno porte, em setores comerciais, públicos e voluntários industriais.

Consciência:

Será que todo mundo entende o que podem precisar fazer no caso de um incidente e como eles podem contribuir para o processo de RECUPERAÇÃO?

11.1 Características e aplicabilidade

Esta Norma britânica estabelece o processo, princípios e terminologia de gestão de continuidade de negócios.

O objetivo desta Norma é o de fornecer uma base para a compreensão, desenvolvimento e implementação de continuidade do negócio dentro de uma organização e para fornecer confiança nas relações da organização com os clientes e outras organizações. Ela também permite a organização medir sua capacidade de continuidade de uma forma consistente e reconhecida.

Esta Norma proporciona um sistema baseado em boas práticas e deve ser utilizado por qualquer pessoa com responsabilidade para as operações comerciais ou de prestação de serviços, desde a gestão de topo em todos os níveis da organização, desde aqueles com um único site até aqueles com uma presença global, a partir de empresários autônomos, pequenas e médio empresas à organizações que empregam milhares de pessoas. É, portanto, aplicável a qualquer pessoa que detém a responsabilidade de qualquer operação e portanto, a continuidade dessa operação.

Esta Norma não se aplica às atividades de planeamento de emergência na medida em que o assunto diz respeito a emergências civis.

Esta norma tem os foco os itens abaixo:

- Visão geral da gestão da continuidade do negócio
- A política de gestão de continuidade de negócios
- Gestão do programa de RIPC

- Compreender a organização
- Determinar a estratégia de continuidade de negócios
- Desenvolver e implementar uma resposta RIPC
- Exercitar, manutenção e revisão de acordos de RIPC
- Incorporação RIPC na cultura da organização

11.2 Visão geral da gestão da continuidade do negócio

Todas as organizações, sejam elas grandes ou pequenas, têm metas e objetivos, tais como o de crescer, de prestação de serviços e para adquirir outros negócios. Estas metas e objetivos são geralmente atendidas através de planos estratégicos para atingir a curto, médio e longo prazo.

A Compreensão PCRD corresponde ao mais alto nível da organização de modo a garantir que essas metas e objetivos não sejam comprometidas por interrupções inesperadas.

As consequências de um incidente variam e podem ser de longo alcance. Essas consequências podem envolver perda de vidas, perda de bens ou renda, ou a incapacidade de oferecer produtos e serviços, a reputação ou mesmo a sobrevivência pode depender da estratégia de recuperação da organização.

O PCRD precisa reconhecer a importância estratégica do conhecido das partes interessadas. Além disso, quando as consequências de uma interrupção se desenrolar, novas consequência surgem e têm um impacto direto sobre a eventual extensão dos danos.

11.2.1 RIPC e a relação com a gestão de riscos

RIPC é complementar a uma estrutura de gestão de risco que se propõe a compreender os riscos para as operações ou negócios, e as consequências desses riscos.

A gestão de risco visa a gerenciar o risco em torno dos produtos e serviços que a organização proporciona. Produto e serviço de entrega pode ser interrompido por uma ampla variedade de incidentes, muitos dos quais são difíceis de prever, ou analisar por causa.

Centrando-se sobre o impacto da interrupção, a RIPC identifica os produtos e serviços que a organização depende para sua sobrevivência, podendo identificar o que

é necessário para que a organização continue a cumprir as suas obrigações.

11.2.2 A política de gestão de continuidade de negócios

A política de BCM define os seguintes processos:

- A gestão e manutenção do negócio em curso.
- As atividades de criação de uma capacidade de continuidade de negócios.

As atividade de incorporar especificações de projeto fim a fim, construir, implementar e exercitar a capacidade de continuidade dos negócios.

As atividades de manutenção e de gestão em curso incluem a incorporação de continuidade de negócios dentro da organização, exercitar os planos regularmente , atualizar e comunicar as mudanças, especialmente quando há mudanças significativas nas instalações, pessoal, processo, mercado, tecnologia ou estrutura organizacional.

11.2.3 Desenvolvimento da política de continuidade de negócios

A organização deve desenvolver a sua política de continuidade de negócios que afirma os objetivos do PCRI dentro da organização. Inicialmente, esta pode ser uma indicação de alto nível de intenção que é refinado e reforçado ao longo do desenvolvimento.

A política de continuidade de negócios deve fornecer a organização princípios documentados a que ela aspira e contra a qual a sua capacidade de continuidade de negócios deve ser medido.

A política do PCRI deve ser de propriedade em um nível elevado, por exemplo, um diretor de bordo ou representante eleito.

A organização pode considerar o seguinte no desenvolvimento da sua política de RIPC:

- Definição do escopo do PSRI dentro da organização;
- PCRI recursos;
- Definição dos princípios, diretrizes e normas mínimas para a organização;

Referência a quaisquer normas, regulamentações ou políticas relevantes que

têm de ser incluído ou pode ser usado como um ponto de referência.

A organização deve manter e rever regularmente as suas políticas BCM, estratégias, planos e soluções em uma base regular, de acordo com as necessidades da organização.

O escopo da política do PCRI deve definir claramente as limitações ou exclusões que se aplicam, por exemplo, exclusões geográficas ou produto.

11.2.4 Gestão do programa de RIPC

A gestão do programa é o cerne do processo do PCRI.

A gestão eficaz do programa estabelece a abordagem da organização para a continuidade dos negócios.

A participação gerência é fundamental para garantir que o processo de PCDI está corretamente introduzido, devidamente apoiada e estabelecida como parte da cultura da organização.

Um programa de GCN deve ser posto em prática para atingir os objetivos definidos na política de continuidade de negócios (ver 4.3). Gestão do programa de GCN envolve três etapas:

Atribuição de responsabilidades.

Nomear ou designar uma pessoa com grande vivência apropriada e com autoridade para ser responsável pela política de RIPC além de sua implementação

Implementar a continuidade dos negócios da organização.

Atividades para implementar um programa de continuidade de negócios deve incluir o design, construção e implementação do programa.

O gerenciamento contínuo de continuidade de negócios.

Atividades de gestão em curso devem assegurar que a continuidade do negócio é incorporado dentro da organização. Cada componente da capacidade de continuidade dos negócios de uma organização deve ser revisto regularmente, exercitado e atualizado. Além disso, acordos e planos de continuidade de negócios também deve ser revisado e atualizado sempre que há uma mudança significativa no funcionamento da organização, que sejam: ambiente, pessoas, processos ou tecnologia, e quando um exercício ou incidente destaca deficiências.

Documentação do PCRI

Indivíduos com a tarefa de manter a continuidade do negócio deve criar e manter a documentação de continuidade de gegócios. Isto pode incluir o seguinte:

a) política de BCM:

- PCRI declaração do escopo,
- PCRI termos de referência;

b) análise de impacto nos negócios (BIA);

c) risco e avaliação de ameaças;

d) Estratégia de BCM / estratégias;

e) Programa de conscientização);

f) Programa de formação;

g) Os planos de gestão de incidentes;

h) Planos de continuidade de negócios;

i) Planos de recuperação de negócios; cronograma e relatórios

j) Exercício;

k) Os acordos de nível de serviço e contratos

11.2.5 Compreender a organização

O objectivo deste elemento do ciclo de vida do PCRI é ajudar o entendimento da organização através da identificação de seus produtos e serviços essenciais, as atividades críticas e recursos que lhes dão suporte. Isto garante que o PCRI está alinhado com os objetivos da organização, obrigações e deveres estatutários.

Business impact analysis (BIA)

Identificar qualquer atividades inter-dependente, bens, infra-estrutura de apoio ou recursos que devem ser mantido de forma contínua ou recuperado ao longo do tempo.

Estabelecer o período máximo tolerável de interrupção de cada atividade, identificando:

11.2.6 Determinar a estratégia de continuidade de negócios

Este elemento do ciclo de vida do PCRI logicamente vem após "o entendimento da organização." Como resultado da análise anterior, uma organização estará em uma posição para escolher as estratégias de continuidade apropriadas que lhe permitam cumprir os seus objetivos.

Opções estratégicas

A organização deve considerar opções estratégicas para as suas atividades críticas e os recursos que cada atividade vai exigir em sua reabertura. A estratégia ou estratégias mais adequado vai depender de uma série de fatores, tais como:

- O período máximo tolerável de interrupção da atividade crítica;

- Os custos de implementação de uma estratégia ou estratégias,
- As consequências da inação.

Estratégias pode ser necessária para a seguinte organizacional recursos:

- Pessoas
- Instalações
- Tecnologia
- Informação
- Suprimentos
- Partes interessadas

11.2.7 Desenvolver e implementar uma resposta RIPC

Este elemento do ciclo de vida do PCRI está preocupado com o desenvolvimento e implementação de planos e arranjos para assegurar a continuidade das atividades essenciais adequados, bem como a gestão de um incidente.

- Invocar o plano
- Lista de contato
- Atividade dos colaboradores
- Estratégia de comunicação na midia

11.2.8 Exercitar, manutenção e revisão de acordos de RIPC

Este elemento do ciclo de vida do PCRI garante que os arranjos da GCN da organização são validados pelo exercício e revisão e que são mantidos em dia.

Programa de Exercício

Um programa de exercícios deve ser consistente com o alcance do plano de continuidade de negócio (s), dando a devida atenção a qualquer legislação e regulamentação pertinente. Exercícios podem:

- Antecipar um resultado pré-determinado
- Permitir a organização desenvolver soluções inovadoras.

Um programa de exercício deve ser leva a certeza de que o PCRI vai funcionar como esperado, quando necessário. O programa deve:

- Exercitar os sistemas técnicos, logísticos, administrativos, processuais e outros operacionais do PCRI;

- Exercitar os arranjos de GCN e infra-estrutura (incluindo papéis, responsabilidades e todos os locais de gestão de incidentes e áreas de trabalho, etc);
- Validar a tecnologia e recuperação de telecomunicações, incluindo a disponibilidade e realocação de pessoal.

11.2.9 Incorporação do PCRI na cultura da organização

Para ter sucesso, a continuidade do negócio tem de se tornar parte do caminho como uma organização é gerenciada, independentemente de tamanho ou setor. Em cada etapa do processo do PCRI, existem oportunidades para introduzir e melhorar a cultura do PCRI de uma organização.