UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE ADMINISTRAÇÃO GERAL E APLICADA
DAGA

Proposta de PROCEDIMENTOS

PARA A CRIAÇÃO DE UM

BUSINESS CONTINUITY PLAN (BCP)

no Ambiente de Telefonia IP em Empresas

CURITIBA

2011

EWERTON MIYOSHI TAKAMATU

Proposta de

PROCEDIMENTOS para a CRIAÇÃO de um

BUSINESS CONTINUITY PLAN (BCP)

no Ambiente de Telefonia IP em

Empresas Corporativas

Trabalho de Conclusão de Curso apresentado ao Curso de MBA em Gerenciamento de Projetos, da Universidade Federal do Paraná, como requisito para obtenção do título de especialista.

Orientador: Prof.ª Mirian Palmeira

CURITIBA

2011

PUBLIC

ÍNDICE

I INTRODUÇÃO 5
1.1 Problema de Pesquisa 5
1.2 Objetivo Principal: 5
1.3 Objetivo Específicos: 5
1.4 Justificativa 6
II BASE TEÓRICO-EMPÍRICA 6
2.1 Elaboração de um Plano de Continuidade do Negócio 7
2.1.1 Início e Administração do Projeto 8
2.1.2 Avaliação e Controle de Riscos 8
2.1.3 Análise de Impactos nos Negócios (BIA) 11
2.1.4 Desenvolvimento da Estratégia de Continuidade do Negócio 13
2.1.5 Resposta e Operações de Emergências 15
2.1.6 Desenvolvimento e Implantação do Plano de Continuidade do Negócio 16
2.1.7 Implementações de Programas de Treinamento 16
2.1.8 Manter e Exercitar o Plano de Continuidade do Negócio 17
2.1.8.1 Papéis e Responsabilidades 18
2.1.9 Políticas de Testes 18
2.1.9.1 Estratégia de Testes 19
2.1.9.2 Plano de Testes 20
2.1.9.3 Revisão do Plano de Testes 20
2.1.10 Relações Públicas e Gerenciamento de Crises 20
2.1.11 Parcerias com Entidades Públicas e Particulares 21
2.2 Telefonia com Tecnologia VoIP em um Ambiente Corporativo 21
2.2.1 A Tecnologia VoIP. 21
III METODOLOGIA DE PESQUISA 23
3.1 Designação de um Plano de Continuidade do Negócio 23
3.1.1 Lista de Notificação de Contatos 23
3.1.2 Revisão Documento 24
3.1.3 Escopo 24
3.1.4 Delimitação do levantamento 24
3.1.5 Sites Envolvidos 24
3.1.6 Prós-condições 26
3.1.7 Grupo de Recuperação e suas Responsabilidades 27
3.1.8 Lista de Atualizações do Plano de Contingência 27
3.1.9 Instruções para Uso deste Plano. 28
3.1.9.1 Acionamento do Plano. 28
3.1.9.2 Declaração do Desastre 28
3.1.9.3 Notificação 28
3.1.9.4 Comunicação Externa 28
3.1.9.5 Política de Backup dos Dados 28
3.1.9.6 Política de atualização dos Ramais Telefônicos e suas Facilidades 28
3.1.9.7 Procedimentos para Gestão das Emergências 29
3.1.9.8 Impossibilidade de acesso ao Ambiente 29
3.1.9.9 Revisão e Manutenção do Plano de Contingência. 30
3.1.9.10 Alerta / Verificação / Fases da declaração 31
3.1.9.11 Plano Checklist 31
3.1.9.12 Notificação do Incidente no Site 32
3.1.9.13 Prover Status ao EMT. 32

3.1.9.14 Tomada de Decisão. 33
3.1.9.15 Repasse aos Membros dos Grupos. 33
3.1.9.16 EMT Notifica as Equipes e Clientes 33
3.1.9.17 Contato Geral com os Parceiros. 33
3.1.9.18 Declaração do Desastre 34
3.1.9.19 Avaliação detalhada dos Estragos 34
3.1.9.20 Contato com EMT - Decide em continuar na fase de Recovery do Negócio 34
3.1.9.21 Fase da recuperação do Negócio (05 horas – recuperação Completa) 35
3.1.9.22 Requisitos de operação das Instalações e Sistemas 35
3.1.9.23 Notificado do Staff de Engenharia Técnica 35
3.1.9.24 Planejamento Prévio para a Realocação 35
3.1.9.25 Notificar o EMT e as Unidades de Negócio da Corporação para Inicio da Recuperação 35
3.1.9.26 Recuperação das Operações 35
3.1.9.27 Atualização da Documentação 35
IV CONCLUSAO 36
VI REFERÊNCIAS BIBLIOGRÁFICAS 37

I INTRODUÇÃO

A estratégia de Negócio e as suas decisões são baseadas na previsão de continuidade deste Negócio. Qualquer evento que transgrida esta hipótese é uma ameaça à saúde de qualquer empresa, violando diretamente sua sobrevivência.
Entre as variáveis que comprometem a sobrevivência da empresa, seja ele financeiro tecnológico, humano, ambiental ou legal/jurídico, temos que nos preocupar com vulnerabilidade e ameaças envolvidas com relação a evento que comprometam a interrupção do seu "core business". Ameaças que necessitam serem mapeadas e tratadas quando ocorrerem e com o menor tempo e impacto possível.
A Gestão de Continuidade do Negócio baseada num Plano de Continuidade do Negócio visa mitigas estas variáveis, inicialmente intangíveis, tornando-as mensuráveis e preditivas, criando procedimentos e mecanismos de reação ao evento indesejável.

1.1 Problema de Pesquisa

Segundo a Disaster Recovery Institute International (DRII), órgão certificador e de programas gerencias de continuidade do Negócio, são 11 as etapas a serem implementadas para a criação de um Plano de Continuidade do Negócio conforme apresentamos a seguir:
Identificar e analisar os procedimentos de um Plano de Continuidade do Negócio dando subsídios às implementações em um ambiente Corporativas como alternativas á Comunicação de Voz garantindo a sobrevivência da Empresa em um evento catastrófico.

1.2 Objetivo Principal:

Elaborar um procedimento para a Criação de um Plano de Continuidade do Negócio utilizando as melhores práticas para sua viabilização no tocante a Contingência de Comunicação de Voz contemplada com a tecnologia IP (VOIP).

1.3 Objetivo Específicos:

a) Descrever os procedimentos previstos para a elaboração de um Plano de Continuidade do Negócio voltado à comunicação de Voz no Ambiente Corporativo;
b) Demonstrar a importância da atividade de testes para a Gestão da Continuidade de Negócio;
c) Propor algumas técnicas e métodos para o desenvolvimento de novos Planos de Testes e Validação de Sistemas de Comunicações de Voz via tecnologia VoIP;
d) Elaboração de um Plano de Continuidade do Negócio garantindo a operacionalidade do ambiente durante um incidente em função de problemas de acesso ao ambiente original da Empresa:
    - Auxiliar a evitar questionamentos e dúvidas durante um evento, documentando, testando e revisando estes procedimentos de recuperação;
    - Subsidiar o Time de recuperação para que tenha um guia de referencia sobre os possíveis danos e ações a serem tomadas em caso de eventos mapeados;

- Apresentar os procedimentos e recursos necessários para auxiliar na recuperação;
- Identificar os Fornecedores e Clientes que devem ser notificados em caso de um Desastre;
- Identificar alternativas de fontes de suprimentos, recursos e locais;
- Aprimorar novos itens de avaliações e procedimentos vivenciando com os testes;
- Atualizar procedimentos de Armazenamento de Documentos essenciais.

1.4 Justificativa

Estamos vivenciando um novo momento na economia brasileira e com isto empresas afloram no mercado nacional.
O Plano de Continuidade do Negócio visa atender aos preceitos de proteção contra desastres, ameaças e incidentes que a Empresa pode ser atingida e como reagir a estes eventos.
Empresas consolidadas, que possuem uma visão do seu Negócio devem engajar-se não somente uma visão estratégica voltada para o futuro, mas também uma visão do passado e do seu presente.
Como em qualquer projeto, faz-se necessário uma revisão dos gestores, no tocante a sua estrutura, cultura, valores, custos e investimentos para serem agregados ao Plano de Continuidade do Negócio . Tornando-o mais fidedigno à realidade de sua Empresa. Toda a Empresa deve estar comprometida na construção deste documento, principalmente as áreas estratégicas - Finanças, Crédito, RH, Tecnologia, Controle, Transporte, Jurídico, Marketing e planejamento entre outros.
Elaborado o documento BCP, este deve ser testado, praticado e atualizado continuamente.

Justificativa teórica – é apresentar um modelo teórico que mais espelha as necessidades de implementação de um produto de Business Continuity Plan (BCP), no tocante a contingencia do ambiente frente a um evento inesperado e catastrófico.

Justificativa prática – dar subsídios ao Core Business sobre as alternativas destinadas ao processo de Contingência de Voz em caso de ocorrência de um evento inesperado, abrindo alternativas para a Continuidade do Negócio com o mínimo de impacto à comunidade, imagem e colaboradores e garantindo a sobrevivência do seu Negócio.

II BASE TEÓRICO-EMPÍRICA

O processo do Plano de Continuidade de Negócio envolve a Recuperação, Retomada e a Manutenção de todo o Negócio da Empresa, não somente do segmento tecnológico, pois não adianta somente a recuperação do ambiente tecnológico, mas se a operação não estiver no mesmo nível de operacionalidade.
O Plano de Continuidade de Negócio envolve o desenvolvimento de um plano para toda a área da Empresa, priorizando os objetivos do negócio e as operações críticas que são essenciais para a sua recuperação.
Esta estrutura deve considerar todos os processos críticos, as unidades de negócio, os departamentos e os sistemas, devem ser implementadas, tanto a curto como em longo prazo. Caso não o tenhamos, estaremos expostos a possíveis prejuízos financeiros, danos de imagens, legislativos, perda de Clientes, entre outros.

Este Plano deve ser atualizado periodicamente, garantindo a sua abrangência de toda a Empresa, atualizando novos BCP's setoriais, atualizações tecnológicas e as novas diretrizes das Empresas com relação ao seu Negócio. Agregar a este processo as informações de auditorias realizadas periodicamente e as experiências adquiridas durante o período.
Este plano auxiliará a gerenciar os riscos resultantes de um evento catastróficos, minimizando a probabilidade de ocorrência de um desastre, reduzindo o tempo de retorno e minimizando os riscos do processo de retorno prevendo as decisões críticas em momento de stress.
Decisões críticas tomadas durante uma crise de stress elevam os riscos de fracasso bem como a exposição a erros, ineficiências e consequentemente a custos desnecessários.
Apesar da probabilidade de um desastre ocorrer ser baixo, está sujeito à ocorrência do mesmo. O problema consiste em ter em mente o que fazer frente a este evento com um mínimo de tempo de prejuízo.
Segundo Fernando Marinho (p12):

O Plano de Continuidade do Negócio não é a despesa vinculada a um evento improvável. É um investimento que garante a Continuidade e a redução de prejuízos diante de possíveis ocorrências. Caro não é o investimento em um seguro, E sim, o custo de reposição de um bem que perdemos indicado pelo seu valor e pelo esforço necessário para que atenda exatamente as nossas necessidades.
Resumindo: "referencia de preço é o custo de parada do Negócio.".

O Plano de Continuidade do Negócio possui três características básicas:

1. Redução dos Riscos - A Gestão dos Riscos para se evitar a catástrofe deve ser realizada através da identificação e avaliação dos riscos da Empresa mediante a possibilidade de ocorrência de um desastre;
2. Plano de Emergência – Gestão da Crise quando da ocorrência de um incidente (Controle de Incidência – Incident Control) para evitar que evolua para uma catástrofe, diminuindo seu impacto. Priorizar o ser humano em caso de ocorrências, pois objetos e informações valiosas podem ser recuperados sem riscos para a segurança do ser humano;
3. Plano de Continuidade do Negócio (BCP) – Um plano, rápido e de retorno eficiente, para a operação do negócio está diretamente relacionado com as ações de recuperação de um time especifico de recuperação. Existem 03 elementos a serem considerados para a continuidade:

- Serviços de escritório - instalações, mobiliário, artigos de papelaria, etc.
- Tecnologia da informação - as comunicações e serviços computacionais, e;
- Recursos humanos e outros - garantindo que o pessoal:
    - Cientes do ambiente alternativo;
    - Possuem recursos necessários;
    - Utilizados produtivamente.

2.1 Elaboração de um Plano de Continuidade do Negócio

Segundo a Disaster Recovery Institute International (DRII), órgão certificador e de programas gerencias de continuidade do Negócio, são 11 as etapas a serem implementadas para a criação de um Plano de Continuidade do Negócio, conforme apresentamos a seguir:

1) Início e Administração do PROJETO;

2) Avaliação e Controle de Riscos;

3) Análise de Impactos nos Negócios (BIA);

4) Desenvolvimento Estratégias de Continuidade do Negócio;

5) Resposta e Operações de Emergências;

6) Desenvolvimento e Implementação do Plano de Continuidade do Negócio (BCP)

7) Implementação da Consciência e os Programas de Treinamento;

8) Manter e Exercitar o Plano de Continuidade do Negócio (BCP);

9) Relação Pública e Gerenciamento de Crise;

10) Parceria com Entidades Públicas e Particulares.

A seguir exploraremos cada etapa do processo de Plano de Continuidade do Negócio:

2.1.1 Início e Administração do Projeto

Nesta primeira etapa, de uma forma global, deve-se estabelecer o escopo para desenvolvimento do Plano de Continuidade do Negócio, incluindo as questões administrativas internas, a cultura da Empresa, o gerenciamento do projeto com o intuito de elaborarmos os prazos e custos.
Inicialmente devemos ter uma pessoa dedicada exclusivamente para a elaboração deste projeto dentro da Empresa.
Este profissional responsável deve tem os seguintes objetivos:

a) Definir os objetivos, as políticas e fatores críticos de sucesso, onde devem analisar o escopo e os objetivos, atendimentos aos preceitos legais e normativos, históricos e práticas da Empresa;
b) Coordenar, organizar e gerenciar o projeto de Plano de Continuidade do Negócio , através da convocação de um comitê administrativo e de uma força-tarefa, definindo os diferenciais entre Recuperação de desastre e Continuidade do Negócio, Respostas à crise e gerenciamento de crises e reduzir e impedir os ricos de ocorrência do evento.
c) Supervisionar o processo de Plano de Continuidade do Negócio, através de métodos de controles efetivos e gestão de mudanças;
d) Divulgação deste projeto aos gestores e aos funcionários;
e) Desenvolvimento de um plano do projeto e seus custos para inicio do projeto;
f) Definir e recomendar a gestão e a estrutura dos processos recomendados;
g) Gerir o projeto para desenvolvimento e implementação do processo de Plano de Continuidade do Negócio.

2.1.2 Avaliação e Controle de Riscos

O processo de avaliação dos Riscos é uma etapa crítica para analise e validação do Plano de Continuidade do Negócio, pois, durante esta analise serão verificados os processos da

Empresa e os ensaios do Business Impact Analysis (BIA). Frente aos diversos cenários de ameaças, resultando inclusive nas alterações e revisões destes documentos.
As Instituições Financeiras devem desenvolver vários cenários de ameaças que, como a própria finalidade do BCP rege abranger as várias descontinuidades do Negócio mitigando-as além de atender as expectativas dos vários Clientes (internos, externos e parceiros). O principal objetivo desta analise é focar na ameaça e seus impactos e não na natureza desta ameaça baseando-se em experiências praticas e circunstancias evidenciada do evento.
Caso o cenário seja pouco abrangente, os resultados também serão pobres em termos de benefícios e resultados de operacionalidade.
Para o cenário de ameaças deve ser considerada a severidade do desastre, o qual é baseado no impacto e na probabilidade de descontinuidade do Negócio, resultando na identificação desta ameaça. Estas ameaças seguem o regime de Probabilidade X Impacto, onde temos, por exemplo, uma ocorrência que queda de energia de pequena duração classificada, dependendo da Unidade, de baixo impacto e alta probabilidade. Portanto todos os recursos devem ser direcionados para os problemas de Alto Impacto e Alta Probabilidade de ocorrência. Caso a ameaça não seja identificada ou não especifica, vale trata-la como um problema de alto risco e o BCP deve contemplar este item.
Após analise do Impacto, Probabilidade e a Severidade Resultante da ameaça identificada, a Empresa pode priorizar os processos de Negócio, respondendo como interromper esta ameaça sob os vários cenários. A probabilidade de ocorrência deve ser mensurada através de um sistema de alta, media e baixa impacto.
Sob o ponto de vista de processo de BCP, as instituições devem confrontar o seus processos internos com as normativas BCP, garantindo uma compatibilidade de ações e procedimentos mitigando os riscos e atualizando o documento BCP.
Algumas ferramentas podem ser utilizadas para auxiliar cada uma das fases da gestão de risco, tais como, a APR (Análise preliminar de riscos), a TIC (Técnica de incidentes críticos), a SR (Série de Riscos), a AE (Arvore de Causas), o WIF (What IF/Checklist), a AAF (Análise de árvore de falhas), a AMFE (Análise do modo de falha e efeitos), HAZOP (Estudo de operabilidade e riscos) entre outras. Entretanto, é importante ressaltar que para um plano de gerenciamento de riscos serem eficaz este deve fazer parte da cultura interna da empresa e ser integrado a todos os níveis.
Este item define os prováveis eventos e cenários que fazem parte do cenário corporativo e que podem afetar a organização e suas instalações, tanto com interrupções quanto como desastres. São descritos os principais e possíveis danos acarretados de cada evento e quais a as medidas necessárias para prevenir e reduzir os efeitos de uma perda potencial. Oferece a possibilidade de incluir una análise de ROI (Return of Investment) para justificar os custos no controle de redução de riscos.
Ela é fundamental para orientar a abrangência das atividades de planejamento do PLANO DE CONTINUIDADE DO NEGÓCIO e deve ser baseada na vivência e experiência dos gestores dos processos de negócio. Os riscos são inerentes a processos, pessoas e ambientes que serão sempre peculiares e característicos de cada organização.

Em síntese, a Avaliação do Risco é uma fase importante para o desenvolvimento do Plano de Continuidade do Negócio , pois este auxilia a:
Identifica os Riscos de um departamento;

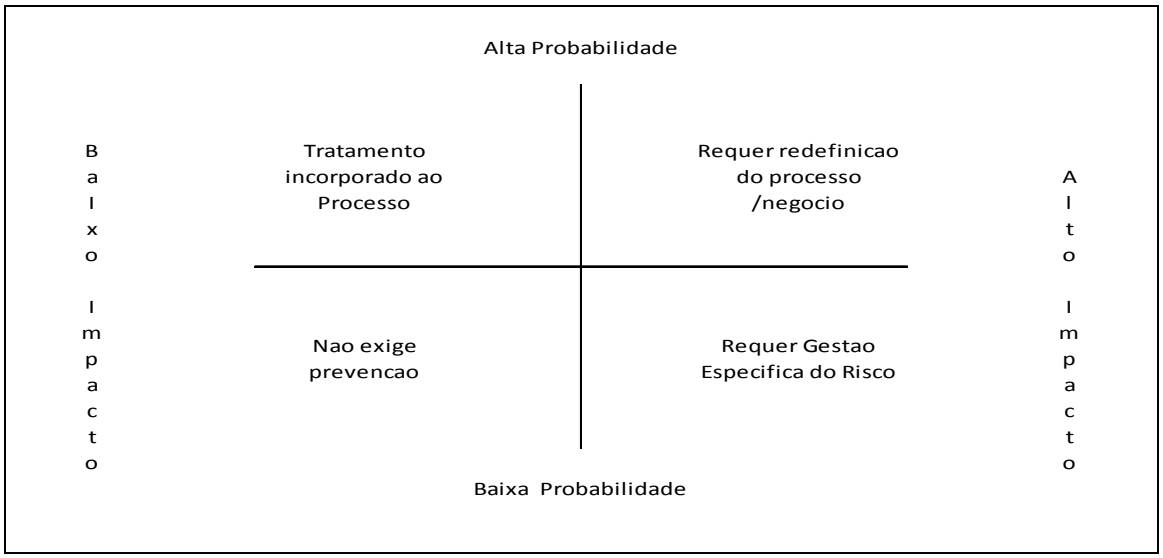
Identifica operações essenciais que deve ser restabelecido rapidamente após o evento ser deflagrado;

Identificar medidas de custo/beneficio que podem ser apresentados para prevenir os riscos ou minimizar os impactos;

Considerações sobre o Impacto do Desastre

Quando consideramos o Impacto de um Desastre, devemos lembrarmo-nos que este desastre nunca ocorre em um horário conveniente e normalmente não temos como prevermos, isto é, não temos quando acontecerá, de que forma este será, qual o estrago causara' e qual o seu impacto.

Figura 1 - Forma de Tratamento de Risco x Probabilidade de Ocorrência x Impacto



(Fonte Saldanha p 65)

FASES DE UM DESASTRE

Um Desastre pode consistir de parte ou de todas as fases descrevemos a seguir:

a) Crise – Compreende nos primeiros instantes após o inicio do evento Como exemplo, temos como causa os danos nas instalações que comprometam a segurança. O responsável pelo acione e ações é o Grupo de Controle de Incidentes, cujas ações preveem a aplicação de procedimentos de evacuação de emergência e a convocação de serviços de emergências;
b) Resposta à Emergência – Período com duração de alguns minutos a até poucas horas após o Desastre . Iniciada quando uma potencial situação de Ameaça é identificada. O responsável pelas ações é o grupo de Continuidade do Negocio o qual estará avaliando a situação e decidindo a declaração do Plano de Continuidade do Negócio . Neste período a fase de Crise pode ou não ter ocorrido mas o Desastre ter assumido magnitudes que envolva a necessidade de ações desta etapa;
c) Recuperação- Varia de alguns dias a até meses após a ocorrência do Desastre e retorno às operações normais. É responsabilidade do grupo de Recuperação e o qual deverá

reinicializar as operações essenciais aplicando os procedimentos do Plano de Continuidade do Negócio;

d) Recuperação - Retorno às condições normais com a avaliação dos estragos e danos. É responsabilidade do grupo de Controle de Incidente.

Abaixo apresentamos mais algumas práticas utilizadas para a manutenção do BCP:

a) Implementar o BCP em todos os processos de negócio da Empresa;
b) Implementar um profissional dedicado para a manutenção deste BCP;
c) Implementar um profissional dedicado para as revisões periódicas deste BCP;
d) Implementar auditorias periódicas para testes do BCP.

Um Plano de Continuidade do Negócio para as Empresas é tão importante quanto o seu objetivo ou sua missão, pois é deste que da a sustentabilidade para garantir o desenvolvimento da Empresa.

2.1.3 Análise de Impactos nos Negócios (BIA)

Nesta etapa identificamos e avaliamos os impactos resultantes da interrupção e dos diversos cenários de desastres que podem afetar a Empresa. Demonstramos também as técnicas para quantificar e qualificar estes impactos. Define a criticidade dos processos de negócio, suas prioridades de recuperação e interdependências, para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

Muito tempo e recursos são necessários para compor uma Analise de Impacto do Negócio (BIA) e depende principalmente do tamanho e da complexidade do ambiente.

Embora o restabelecimento dos meios de TI e de dados seja importante, tem-se que valorizar as operações e processos do negócio.

O Plano de Continuidade do Negócio envolve o desenvolvimento de um PLANO DE CONTINUIDADE DO NEGÓCIO Geral de toda a Empresa, priorizando os objetivos do negócio e as operações críticas que são essenciais para o ser restabelecimento. Esta empreitada deve considerar quão critico é cada processo, suas unidades de negócio, os departamentos e seus sistemas e como estes responderão a uma descontinuidade e suas possíveis falhas apontadas para correção contendo operações de curto e longo prazo.

Em uma Empresa que considera que todos os elementos são críticos não poderá identificar quais são os itens que melhor destaca a necessidade dos seus clientes á um nível aceitável de interrupção. Desta forma, o gerente de deve priorizar os objetivos e os seus respectivos processos críticos que são essências para a sobrevivência da instituição, pois a restauração de todo o ambiente da Empresa é praticamente inviável em função do custo sua estrutura física e as diversas circunstâncias em que o evento pode ocorrer.

O processo do Plano de Continuidade do Negócio deve incluir regulares atualizações e estas atualizações devem mudar de acordo com as mudanças do processo do negócio baseadas em auditorias regulares e lições aprendidas com os testes. Mudanças no processo do negócio incluem avanços tecnológicos, o qual permite um processo mais rápido e eficiente para o tratamento deste Plano de Continuidade do Negócio e consequentemente reduzindo os tempos mínimos aceitáveis de paralisação.

Em resposta às demandas dos clientes e à competitividade, muitas Empresas estão diminuindo seu tempo no processo de recuperação utilizando os recursos tecnológicos mais avançados para sua recuperação.

A Análise do Impacto do Negócio (BIA) deve estimar o tempo máximo de paralisação para os processos e funções críticas da Empresa e o nível máximo aceitável de perdas dos seus dados, operação, finanças, reputação e mercado. Como parte da analise, o gestor deve decidir o quanto tempo os sistemas podem operar antes que a perda se torne muito grande e quando de dados a Empresa pode se dar ao luxo de perder para se manter operante.
O resultado deste passo auxiliará a estabelecer o RTO – Recovery Time Objective, isto é, o período de tempo dentro do qual o sistema, aplicações, ou funções devem ser recuperados após uma interrupção (dias/horas/minutos). É frequentemente usado como base para o desenvolvimento de estratégias de recuperação, e para determinar se serão ou não implementadas as estratégias de recuperação durante uma situação de desastre, e o RPO – Recovery Point Objective, que consiste no tempo na qual o sistema e dados serão recuperados após uma interrupção (último dado válido). É frequentemente usado como base de
Desenvolvimento de estratégias de backup, e para determinar o montante de dados que precisa ser recriado após os sistemas e as funções terem sido recuperados e também mapear os processos mais críticos. Estes objetivos para a recuperação devem ser considerados simultaneamente para determinar com maior precisão o tempo total de paralisação que a Empresa pode suportar face ao desastre. Com isto, o gestor deve determinar quais são os recursos necessários para a mínima operação dos seus processos e objetivos, sejam elas em termos de recursos humanos, tecnológicos, de comunicações e dados. Agregado a isto, definir quais processos são prioritários e ajustá-los a sequenciar as ações.
O gestor desta Analise de Impacto do Negócio (BIA) deve considerar o desenvolvimento uniforme de entrevistas e requisitos de inventários que podem ser utilizados como base para toda a Empresa, utilizando como ferramenta, nesta fase, para comparar e enriquecer as exigências do processo do negócio.
Esta fase deve prioriza os processos do negócio baseados em sua importância para os objetivos estratégicos, manutenção da segurança e boas práticas da Empresa.

Quando determinamos as necessidades criticas da Empresa, todas as funções, processos, recursos humanos devem ser analisados. Para documentar a missão critica das funções desempenhadas, cada departamento deve considerar os seguintes questionamentos:

a) Quais são as interdependências criticas existentes entre o sistema interno, aplicações, processos do negócio ou departamentos?
b) Qual equipamento especializado será necessário e como será utilizado?
c) Como o departamento funcionará se o mainframe, rede lógica e/ou acesso internet não estiverem disponíveis?
d) Qual é o ponto único de fala existente e quão significativo é este risco?
e) Quais sãos as relações criticas e suas dependências com terceiros?
f) Qual é a responsabilidade da Empresa em relação aos serviços de Terceiros pelo acordo no nível de serviço (SLA)?
g) Quais os critérios operacionais e os controles de segurança que são exigidos para priorizar o restabelecimento.
h) Qual o numero mínimo de funcionários em relação ao espaço necessário para um site de contingência?
i) Quais as formas especiais ou suprimentos necessários para este site de contingência?
j) Quais os equipamentos serão necessários para o site de contingência para a comunicação com os funcionários, vendedores e cliente?

k) Qual o impacto em potencial se utilizar o mesmo site de contingência para diversas áreas da Empresa?
l) Possui funcionários treinados para este site de contingência e possui funções de backup/ regras que os funcionários atuam se o principal responsável estiver ausente?
m) Todas as necessidades pessoais dos funcionários estão adequadamente consideradas?
n) Quais são as gestões financeiras criticas/questões de liquidez do projeto?

Uma vez que o BIA estiver completo, deve ser analisado durante o processo de avaliação do risco, incorporado e testado como parte do PLANO DE CONTINUIDADE DO NEGÓCIO . O BIA deve ser revisado por um gestor sênior periodicamente e atualizado para refletir as mudanças significativas na operação do negócio, pareceres da auditoria e lições aprendias durante o processo de testes.
Uma copia do BIA deve ser mantida em um site fora do ambiente da Empresa e de fácil acesso quando necessário.

2.1.4 Desenvolvimento da Estratégia de Continuidade do Negócio

Esta etapa visa, em linhas gerais, definir e orientar a seleção de estratégias operacionais alternativas para a recuperação dos processos e dos componentes do negócio dentro dos prazos de recuperação desejados enquanto processos corporativos críticos são mantidos em atividade.
Cuja missão é:

a) Identificar as possíveis alternativas para a Continuidade de Negócio disponíveis, suas vantagens e desvantagens, com as respectivas características de custo, incluindo a mitigação (redução de riscos) como estratégia de recuperação;
b) Identificação das estratégias de recuperação compatíveis com as áreas funcionais de negócio; cada ambiente e topologia possuem características e exigências de negócio próprias;
c) Consolidar as estratégias; reduzindo os riscos de compatibilidade ou de “gargalo estratégico”;
d) Identificação das necessidades de armazenamento remoto e instalações alternativas;
e) Desenvolvimento da unificação das varias estratégias e planos de continuidade do Negócio;
f) Obtenção do comprometimento da Gerência com as estratégias apresentadas.

Divididos em dois planos:

- Plano de Recuperação de Desastre – Destinado a indicar atividades relativas á recuperação ou substituição de componentes;

- Plano de Contingência Operacional – Destinado ás atividades de manutenção dos processos de Negócio.

Detalhando um pouco mais:

1) Plano de Recuperação de Desastre

A principal razão do Plano de Recuperação de Desastre é garantir que a Empresa seja capaz de operar em caso de algum desastre. Seja ela baseada em catástrofes naturais (furação,

vendaval, incêndios, inundações, etc.) ou falhas de equipamentos, processos, erros de julgamentos, ação de hackers, vírus ou pirataria.
Destacando a diferença entre o Plano de Prevenção de Perdas e o Plano de Recuperação de Desastre, o primeiro se preocupa em minimizar a exposição da Empresa a riscos que podem ameaçar o funcionamento normal da Empresa. Já o Plano de Recuperação de Desastre está voltado para o conjunto de ações que a Empresa deve realizar para restabelecer as suas operações normais, ou próximas a ele, após uma perda significativa com o mínimo de tempo de paralisação.

Consiste em três atividades:

- Identificação de elementos comuns que possam causar uma critica interrupção ou operações importantes da Empresa;
- Antecipar o impacto e os efeitos que devem resultar desta interrupção das operações;
- Desenvolver e documentar uma resposta de contingência para recupera esta interrupção para que possa retornar as operações o mais breve possível.

As principais vantagens sem criar um Plano de Recuperação de Desastre são:

- Estabelecer critérios e grau de severidade para a interrupção, baseado no impacto desta interrupção e o que causará nas funções criticas da Empresa;
- Determina as funções e sistemas críticos associando aos tempos necessários para sua recuperação;
- Determina os recursos necessários para suportar estes sistemas e funções críticos, inclusive a necessidade de um site de recuperação;
- Identifica as pessoas, competências, recursos e suprimentos necessários para ajudar no processo de recuperação;
- Identifica registros vitais, que devem ser armazenados em sites externos para prover a recuperação do negócio;
- Documentar os processos e as informações necessárias para recuperar após o desastre;
- Garantir que o plano esteja atualizado;
- Garantir que os procedimentos documentados asseguram a integridade e exatidão do plano.

2) Plano de Contingência Operacional

O principal objetivo de qualquer Plano de Contingência é assegurar que a capacidade da Empresa em operar após o evento de interrupção das suas funções após a perda de informações, perda de pessoas, perda de acesso á informações e instalações. Os objetivos do Plano de Contingência são:

- Continuidade das operações críticas e importantes da Empresa;
- A recuperação das operações normais após a interrupção;

- Notificar periodicamente o status do evento
- Disponibilidade dos componentes críticos - dados, pessoal, comunicações, documentações, suprimentos, lista de inventários, etc.
- Métodos alternativos de realizar as atividades eletronicamente ou manualmente;
- Qualquer alteração necessária no método, necessária acompanha um novo processo de atuação;
- Documentação do plano de negócio da Empresa para responder, recuperar, recomeçar, recuperação e retorno após interrupção do negócio;

O Plano de Contingência procura cumprir os objetivos acima, enquanto minimiza os riscos que comprometem a recuperação e a retomada do processo de negócio, incluindo:

- O número de decisão deve ser realizada imediatamente após o desastre ou a interrupção severa;
- Ponto único de falha na infraestrutura da Empresa;
- Dependência da participação de pessoa ou grupo de pessoas no processo de recuperação;
- Indisponibilidade de pessoal com competência para proceder à recuperação;
- Necessidade de desenvolver, testar, deputar novos procedimentos, programas ou sistemas durante a recuperação;
- Impacto negativo com a perda de dados, reconhecendo que a perda de algumas transações é inevitável.

2.1.5 Resposta e Operações de Emergências

Aqui são desenvolvidos e implementados os procedimentos de resposta e estabilização de situações por meio de um incidente ou evento, incluindo a criação e a especificação de normas para o gerenciamento de um Centro de Operacional de Emergência (COE), uma central de comando.
Se na etapa anterior define-se, através da avaliação dos riscos, quais os eventos deveram atuar, nesta etapa teremos a ação efetiva do Plano de Recuperação de Desastre e operacionalização do Plano de Contingência.
Para que se tenha uma otimização de recursos e eficiência no processo, é importante definir as atividades de cada um dos envolvidos e muito bem estruturada para as diversas situações de emergência.
Obviamente a sequencia dos grupos de atuações devem ter um nível técnico operacional e um conhecimento do seu papel e da Empresa a altura para a sua respectiva atuação.
O objetivo do líder de equipe deve:

a) Identificar os tipos potenciais de emergências e as respostas necessárias (por exemplo: incêndio, inundação, greves etc.).
b) Verificar a existência de procedimentos de resposta apropriados às emergências.
c) Recomendar o desenvolvimento de procedimentos de emergência quando não existam.
d) Integrar os procedimentos de resposta à emergência com os procedimentos de recuperação de desastres e de Continuidade de Negócios.
e) Identificar os requisitos de comando e controle para gerenciamento de emergências.
f) Sugerir a elaboração de procedimentos de comando e controle para definir o papel das autoridades e os processos de comunicação para o gerenciamento das emergências.
g) Assegurar que os procedimentos de resposta a emergências estejam integrados com os procedimentos de órgãos públicos.

2.1.6 Desenvolvimento e Implantação do Plano de Continuidade do Negócio

Nesta etapa consolidaremos todos os planos setoriais e departamentais em um único Plano de Continuidade do Negócio . Estes planos devem cobrir todo o ciclo de uma interrupção significativa, provendo ações e procedimentos para atuarmos sobre o evento, escalation list, inventários dos recursos críticos, contato dos responsáveis, etc.
É importante criara um Plano de Continuidade do Negócio que contemple o pior caso e ter em mente que estes recursos e suprimentos devem estar fora do local afetado.
Estes planos devem conter instruções sucintas e diretas, com no mínimo as seguintes informações:

a) Todos os passos executados, com designação de nomes, para a recuperação do negócio;

b) Atividades descritas como ordens de comando, não dando margem a questionamentos, pois se pressupõe que já foram testados e validados anteriormente;

c) Criação de lista de contatos contendo nome, fones, endereço celular. Definido como escalation list dos funcionários;

d) Criação de lista de contatos contendo nome, fones, endereço celular. Definido como escalation list dos clientes e fornecedores;

e) Inventario dos recursos necessários para a recuperação;

f) Plano devera ser amplamente divulgado para que todos saibam o que, quem, onde, por que e quem executará as atividades.

Sugere-se, em função dos vários planos individuais e inter-relacionais a implementação de uma ferramenta de gestão especializada em PLANO DE CONTINUIDADE DO NEGÓCIO /BCP.

2.1.7 Implementações de Programas de Treinamento

Aqui estaremos desenvolvendo o programa para incrementar a cultura corporativa, incentivando as habilidades necessárias para elaborar, implementar, atualizar e executar um Plano de Continuidade do Negócio ,
Colocar na cultura interna da Empresa o conceito de Plano de Continuidade do Negócio deve ser auxiliado pelas áreas de Marketing e Recursos Humanos, para garantir uma abordagem eficiente e eficaz. Permitindo uma disseminação mais abrangente dentro da Empresa. Criação de espaço dentro da intranet corporativa, campanhas institucionais, quiz, treinamentos na intranet. Enfim, é necessário envolver e comprometer os colaboradores para a concepção da ideia e principalmente vinculá-lo para que suas ações dependam a sobrevivência da Empresa em caso de desastre.
A conscientização deve ser voltada não somente para o publico interno/colaboradores mais os parceiros /fornecedores e os Clientes. Sob o ponto de vista de Parceiros/Fornecedores, temos o comprometimento e a visão de um serviço garantido e para os olhos dos Clientes a segurança de fornecimento ininterrupto do produto/serviço.

2.1.8 Manter e Exercitar o Plano de Continuidade do Negócio

Para esta fase, estaremos elaborando um pré-plano e coordenação do exercício do PLANO DE CONTINUIDADE DO NEGÓCIO , avaliando os resultados e obtidos. Provendo uma rica base de informações para as melhorias do Plano de Continuidade do Negócio . Desenvolvendo processos para a manutenção das variáveis não descritas e reestudando com os objetivos da Empresa, auditando seus pontos fortes e pontos a melhorar.
É recomendável que os testes sigam um processo evolutivo, iniciando com os processos menos críticos e gradativamente com os processos mais complexos. Ganhando assim know-how e expertise para o processo evolutivo e apresentando aos Clientes, acionistas, colaboradores e fornecedores a capacidade de operar após um desastre.
A frequência com que os testes são executados depende da instituição, grau de complexidade da Empresa e das alterações realizadas no Plano de Continuidade do Negócio . Como boa pratica, sugere-se realizar estes testes uma vez ao ano, no mínimo.

O profissional responsável deverá atingir os seguintes objetivos:

a) Preparar o planejamento dos exercícios;

b) Coordenar os exercícios;

c) Avaliar os exercícios dos planos;

d) Implementar o exercício das atividades dos planos;

e) Documentar os resultados;

f) Avaliar os resultados;

g) Atualizar e adequar os planos;

h) Reportar os resultados e a avaliação dos exercícios aos gestores;

i) Assimilar as diretivas estratégicas do Negócio;

j) Acompanhar as reuniões de planejamento estratégico;

k) Coordenar as reuniões de planejamento estratégico;

l) Auxiliar o estabelecimento de um programa de auditoria para o Plano de Continuidade do Negócio .

Após a conclusão dos testes, deverá ser gerado um relatório contendo:
a) Escopo do teste;

b) Responsável pelo teste;

c) Tempo de recuperação – Previsto x Realizado;

d) Melhorias propostas no Plano;

e) Evidencias da destruição das informações utilizadas.

O relatório deve ser armazenado junto com os planos, servindo como referencia para outras possíveis consultas.
O grande desafio do gestor é desenvolver um programa de testes que proveja um alto grau de segurança para a continuidade dos processos críticos do negócio, incluindo infraestrutura de suporte, sistemas e aplicações que não comprometa o desenvolvimento da produção. Portanto, um programa de testes consistente deve incorporar papeis e responsabilidades, políticas de testes que incluam estratégia de testes e um plano de testes, a execução, evolução, avaliação das interdependências e a divulgação dos resultados dos testes e consequentemente atualizações no documento do Plano de Continuidade do Negócio e no programa de testes.

2.1.8.1 Papéis e Responsabilidades

O grupo de gestores seniores é responsável em estabelecer e revisar um programa de testes global da Empresa. Uma vez estabelecido estes dirigirão os grupos para desenvolver, implementar e avaliar o programa de testes de Continuidade do Negócio da Empresa:
a) Gestor da Linha do Negócio - Responsável pelos testes das operações do Negócio;

b) Gestor de IT – Responsável pelos testes de recuperação dos sistemas tecnológicos da Empresa;

c) Gestor de Crise – Responsável pelos testes dos processos de gestão da Empresa;

d) Gestor Facilitador – Responsável pelos testes de prontidão operacional da planta física da Empresa e equipamentos, controle de ambientes - acesso físico e segurança;

e) Auditor interno – Responsável pela avaliação da qualidade global do programa de teste e de seus resultados.

2.1.9 Políticas de Testes

Uma política de testes deve ser desenvolvida pelo grupo de gestores seniores e deve descrever a base para a criação e implementação da estratégia de testes e seu plano. Deve-se

implementar uma política de teste gradativa com relação ao escopo e sua complexidade, implementando e adaptando mudanças no Plano de Continuidade do Negócio como um todo.
Esta política de testes deve identificar os principais papeis e responsabilidades e estabelecer requisitos mínimos para a continuidade das atividades. A execução dos testes deve ser baseada no tamanho e no perfil dos riscos da Empresa, envolvendo Colaboradores, Fornecedores e Clientes, dependendo da abrangência dos testes.

2.1.9.1 Estratégia de Testes

A política de testes deve incluir a estratégia de teste de toda a Empresa. Que estabelece Perspectivas individuais de toda a sequência de negócio através de testes do ciclo de vida do planejamento, execução, medidas, relatórios e aperfeiçoamento do processo de teste. Esta estratégia deve incluir:

a) Perspectiva da linha de negócio e função de suporte que demonstram a realização dos testes com o objetivo de Continuidade do Negócio e consistente com Plano de Continuidade do Negócio e com a avaliação dos riscos;

b) Descrição detalhada dos testes a serem realizados;

c) Envolvimento do pessoal, tecnologia e dos facilitadores;

d) Perspectiva da interdependência dos testes internos e externos;

e) Validação dos recursos utilizados pela estratégia de testes.

A estratégia de Testes deve incluir os testes de escopo e de objetivo, o qual define claramente quais funções, sistemas ou processos serão testados e qual será a validação do teste. O objetivo de um programa de teste é assegurar que o processo do Plano de Continuidade do Negócio é preciso, relevante e viável sob condições adversas e conforme mencionado anteriormente, realizado pelo menos, anualmente. Os testes devem incluir aplicações e funções de negócio que foram identificados anteriormente na analise do BIA, o qual determina os pontos de recuperação e seus tempos. Com isto, poderemos determinas uma estratégia apropriada com seus tempos de RPOs e RTOS.
O objetivo dos testes deve iniciar-se dos mais simples e aumentado sua complexidade e âmbito de atuação e devem:

- Gradualmente serem implementada sua complexidade, nível de participação, funções e área física envolvida;
- Não prejudicar a operação normal do negócio;
- Demonstrar a variedade de gestão e respostas sobre condições de crise simuladas, progressivamente envolvendo mais recursos e participantes;
- Procedimentos e recursos ineficientes podem ser revisados;
- Considerar desvios do roteiro de testes para atender a eventos não planejados
- Envolver um volume suficiente de todos os tipos de transações assegurando-se da adequada capacidade e funcionalidade das facilidades de recomposição.

A Manutenção do Plano de Continuidade do Negócio é tão importante com a confecção do mesmo, pois garante a integridade, eficiência, segurança e operacionalidade do plano face às suas necessidades em termos de recursos, os envolvidos e o custo das atividades.

Qualquer teste desta magnitude gera um volume muito grande de informações e processos, para garantir que todas as etapas serão executadas, sugere-se que aplique ferramentas de gestão as atualizações, custos e operacionalidade.

2.1.9.2 Plano de Testes

A política de testes deve incluir um Plano de Testes, o qual é baseado no escopo de teste predefinido e com objetivos estabelecidos como parte do gerenciamento da estratégia de testes, onde temos além da revisão dos procedimentos de testes o desenvolvimento de métodos e cenários destes. O gestor deve avaliar as métricas e riscos de cada etapa e cenários dos testes em função das necessidades de recuperação identificadas.
Os cenários de teste devem incluir todas as ameaças, tipos de eventos, situações do gerenciamento de crises e deve abranger todos os tipos de eventos. Ainda sobre estes cenários, devem-se realizar inclusive testes com sites backups e contingenciados envolvendo a participação de terceiros e prestadores de serviços testando as suas interdependências internas e externas.
Novamente vale ressaltar a necessidade de atualização e testes de validação periódica, garantindo que o que foi editado foi cumprido.
O Plano de testes deve comunicar o escopo predefinido, os objetivos e prover os participantes de todas as informações necessárias:

- Cronograma previsto dos Testes englobando todos os objetivos;
- Descrição especifica dos métodos e objetivos dos testes;
- Regras e responsabilidades de todos os participantes;
- Designação dos participantes dos testes;
- Teste do comando de Emergências;
- Contato de todo o staff de Teste - Escalation list
- Acompanhamento da lógica dos processos e procedimentos;

2.1.9.3 Revisão do Plano de Testes

O Gestor deve elaborar e analisar um script para cada teste prioritário com o intuito de identificar os pontos fracos que podem culminar em testes ou procedimentos insatisfatórios. Como parte do processo de revisão o plano de teste deve ser revisado para identificar e sanar qualquer mudança nos itens abaixo:

a) Pessoas Chaves;
b) Políticas;
c) Procedimentos;
d) Infraestrutura;
e) Equipamentos;
f) Terceirizações;
g) Parceiros;
h) Componentes que comprometam o funcionamento normal da Empresa.

Esta revisão deve ser compartilhada com todos os envolvidos, através de copias, principalmente para os gestores das áreas criticas da Empresa, solicitando a revisão de sua parte, garantindo uma documentação completa do ambiente.

2.1.10 Relações Públicas e Gerenciamento de Crises

Faz-se necessário desenvolver, coordenar, avaliar e exercitar o contato com a mídia e documentos durante uma crise, isto pode minimizar os impactos durante uma crise perante a própria organização, funcionários e seus familiares, principais Clientes, Fornecedores, Sindicatos, Investidores e Gestores da Corporação. E consequentemente transmitir segurança nas ações tomadas pelo Comitê e à própria imagem da marca da Empresa.
Dentro desta óptica, deve-se:

a) Identificar os componentes de um programa de relações publica proativa, baseados em grupos internos à corporação, grupos externos e entidades externas;
b) Identificar órgãos públicos, tais como, serviços de emergências (guarda municipais) entidades de transito, defesa civil, para entidades financeiras a FEBRABAN, órgãos de cartões de créditos, parceiros e terceiros, BACEN, COBIT, Sarbanes-Oxley e Basiléia II;
c) Identificar os grupos de Investidores e Comunicações essenciais, tais como os Investidores, funcionários e familiares, principais Clientes, Fornecedores;
d) Desenvolver e exercitar as atividades de manuseios das mídias dos planos, através de Politicas e Procedimentos e também da Preparação e Manuseios destas mídias.

As mídias sociais estão fortemente vinculados à imagem da Empresa e é importante garantir que este recurso contribua com o BCP, principalmente quando da ocorrência deum desastre.

2.1.11 Parcerias com Entidades Públicas e Particulares

Sob a óptica das parcerias com entidades Publicas, é importante acompanharmos as diretrizes legais do país, referente ás normas financeira, trabalhistas, Procons, etc.
Vale salientar também entidades de infraestruturas, como os departamentos de transito municipais, departamento de policia, os bombeiros e hospitais dependendo do evento e que criam vínculos com o item BCP a ser sanado.
Já para as entidades privadas, temos também as empresas de transportes, operadoras de telefonia celulares (também a Nextel), empresa de fornecimento de alimentação coletiva, etc.

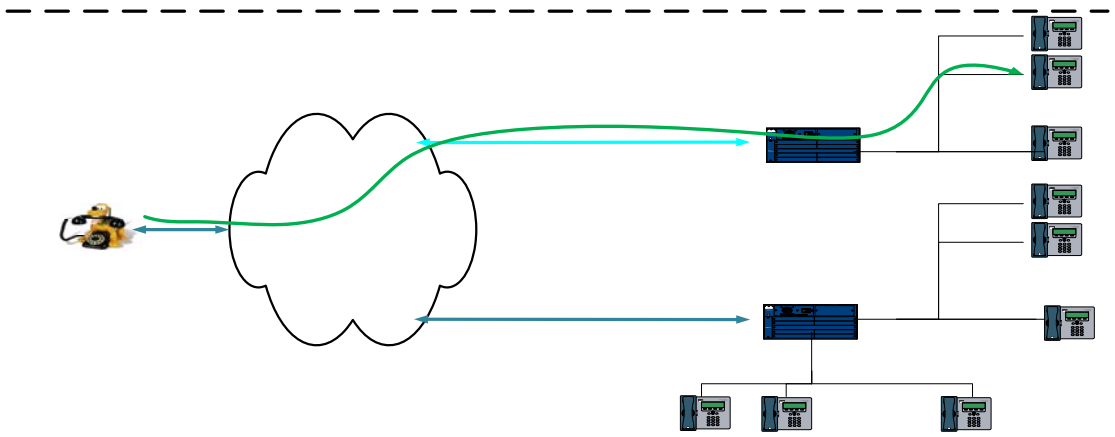
2.2 Telefonia com Tecnologia VoIP em um Ambiente Corporativo

2.2.1 A Tecnologia VoIP.

Com a Convergência de Voz e Dados, a tecnologia VoIp vem de despontando como uma ferramenta eficaz para atender a demanda de telefonia nas grandes corporações.
VoIP é a sigla para Voice over Internet Protocol, o qual transforma o sinal analógico da voz (300 a 3000HhZ) em sinal digital e consequentemente permitindo ser transportado como dados. Seria o mesmo que utilizarmos aplicativos freeware da internet, como Skype ou Oovoo.
Para o ambiente comercial, temos vários produtos e fornecedores que fazem da tecnológica VoIP o seu core business. Estes equipamentos não perdem em nada para a sua tecnológica predecessora, como por exemplo, a tecnologia TDM. Alias, como uma das principais frentes de migração para esta tecnologia, temos as vantagens de redução de custos, otimização dos recursos (cabeamento, servidores e recursos de comunicação de dados), mobilidade, baixo custo de implementação, pois agrega valores no ambiente de dados já existente, qualidade nas chamadas telefônicas, contingência de recursos (base de dados, servidores) e de site, etc.
Em um ambiente Corporativo, além da redução de custos temos a facilidade de redirecionamento das ligações telefônicas de um site para outro, obviamente que para isto o

ambiente contingente e a ser contingenciado devem conter links de comunicação de dados que suporte todo o trafego de voz (IP).
Para apresentar a topologia de um ambiente de Voz, sob a óptica da tecnologia VoIP, na Figura 2, apresentamos o encaminhamento das ligações telefônicas oriundas de um ambiente externo ao site.

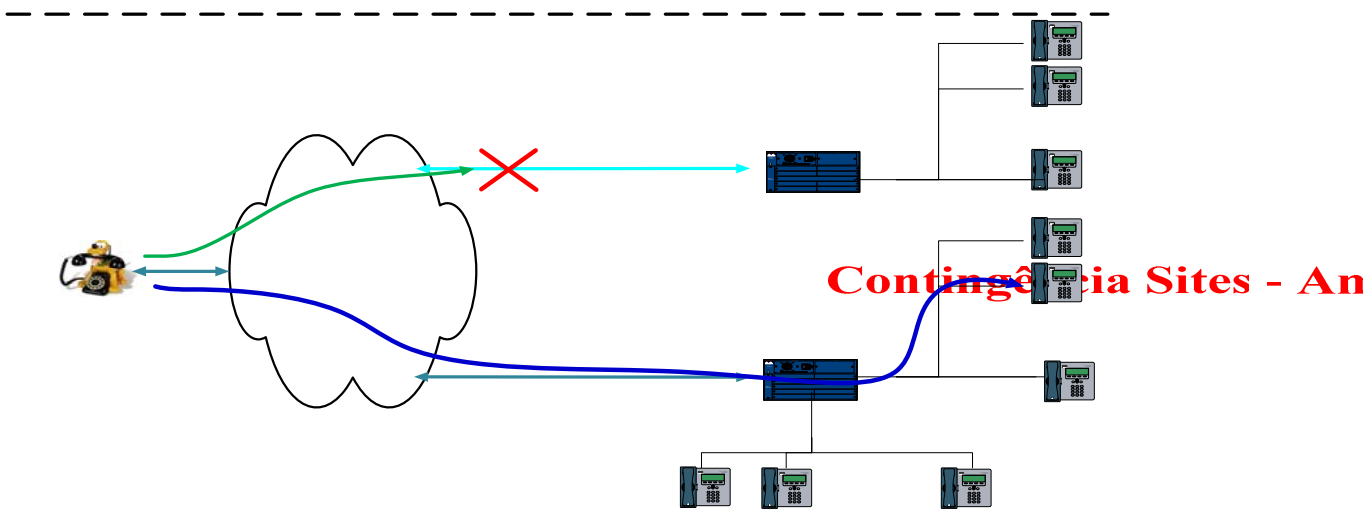
Figura 2 - Ambiente Corporativo.



Contingência Sites -

Obviamente, apresentamos a figura acima somente os recursos dispostos no próprio site, mas temos outros recursos de Voz que atendem a todos os sites e normalmente estão instalados em um Data Center, com todos os recursos de infraestrutura necessários – equipamentos redundantes, base de dados duplicados, alimentação elétrica contingenciada, etc. Garantindo a operacionalidade de toda s rede de Telefonia, pois o risco de inoperância dos equipamentos é extremamente comprometedor ao core business da Empresa.
Retomando na Figura 2, temos como exemplo dois sites distinto e em ambiente distintos, podendo ser na mesma cidade ou não. Onde temos a interligação com a rede telefônica publica (PSTN) e em operação normal, tanto no site “A” como no site “B”.
Em caso de Contingencia ou em aplicação do Business Continuity Plan, seja necessário o remanejamento dos recursos do site “A” para o site “B”, desencadeia-se uma sequência de ações técnicas, em termos de programação, para que todas as ligações telefônicas destinadas anteriormente para o site “A” seja encaminhada para o site “B”. O qual é realizado pelos parceiros da Empresa – Operadora de Telefonia Fixa e a Operação Assistida, este responsável pelo ambiente de telefonia da Empresa. Tudo isto sob a supervisão do Staff de Telecomunicação da Empresa.

Figura 3 - Situação de Contingencia



Conforme a Figura 3, o atendimento telefônico é realizado no site “B”, sendo transparente para o Cliente que ligou para originalmente para o site “A”.

III METODOLOGIA DE PESQUISA

Estaremos utilizando, neste trabalho, a metodologia de estudo de caso, tendo como recurso à apresentação de um caso real no ambiente de uma Empresa cujo meio de comunicação de Voz está baseada na tecnologia VoIP, permitindo analisar e apresentar sugestões de viabilidade operacional para a Continuidade do Negócio.
Esta pesquisa esta baseada na analise documentar, analise bibliográfica e na pesquisa de campo. Balizando os recursos teóricos e práticos para a otimização deste trabalho.

3.1 Designação de um Plano de Continuidade do Negócio

A seguir apresentamos a sequencia para a geração de um guia de procedimentos voltado à criação de um Plano de Contingencia de Voz em uma Empresa Corporativa.

Com isto poderemos auxilio o gestor a elaborar um modelo de Plano de Gerenciamento de Risco, Analise de Impacto do Negócio e a um Plano de Recuperação para o ambiente de Telecomunicações, no tocante a Sistema de Telefonia em IP.

3.1.1 Lista de Notificação de Contatos

A tabela a seguir deve conter a relação de todos os envolvidos na atividade de Contingenciamento dos Sites, inclusive os contatos de outros sites.

Tabela 1 - Relação dos Envolvidos Atualizada

Nome	Endereço	Fone	Celular

3.1.2 Revisão Documento

Já na Tabela 2 temos as atualizações realizadas, desde a sua criação, visando dar um brief do conteúdo.

Tabela 2 - Atualizações do Plano de Contingencia do Site.

Data	Sumario Atualização	Autor atualização

3.1.3 Escopo

O escopo deste trabalho é garantir que todos os itens com relação á contingência de Voz em um site tenha sido analisado para garantir a Continuidade do Negócio em caso de eventos mapeados e identificados.

3.1.4 Delimitação do levantamento

As pré-condições para a aplicação deste documento estão listadas abaixo:

- Ambientes voltados á Condomínios;
- Sistema de comunicação de Voz baseado na Tecnologia VoIP;
- Negociação com a Operadora de Telefonia envolvida validada, aprovada e testada;
- Negociação com os Departamentos dos condomínios envolvidos validados, aprovados e testados;
- Departamento de Telecomunicações da Empresa ciente do Plano de contingência;
- Negociação com os Departamentos envolvendo o quantitativo mínimo de operação, garantindo a Operacionalidade do Ambiente.

3.1.5 Sites Envolvidos

Na Tabela 3 apresentamos os sites envolvidos onde este Plano de Contingência encontra aplicabilidade, pois preenche os requisitos descritos.

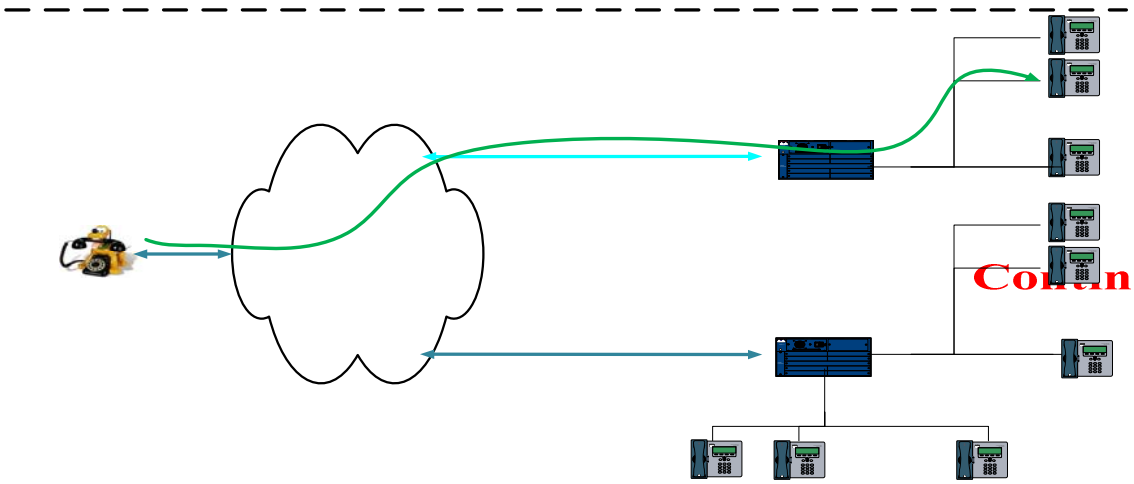
Tabela 3 - Sites Envolvidos

SEQ	Site
1	Centro Administrativo Belém
2	Centro Administrativo Belo Horizonte

3	Centro Administrativo Brasilia
4	Centro Administrativo Campinas
5	Centro Administrativo Campo Grande
6	Centro Administrativo Centro Salvador
7	Centro Administrativo Curitiba 1
8	Centro Administrativo Curitiba 2
9	Centro Administrativo Curitiba 3
10	Centro Administrativo Curitiba 3
11	Centro Administrativo Curitiba 3
12	Centro Administrativo Curitiba 3
13	Centro Administrativo Curitiba 4
14	Centro Administrativo Curitiba 5
15	Centro Administrativo Curitiba 6
16	Centro Administrativo Curitiba 7
17	Centro Administrativo Curitiba 8
18	Centro Administrativo Curitiba 9
19	Centro Administrativo Florianópolis
20	Centro Administrativo Goiania
21	Centro Administrativo Joinville
22	Centro Administrativo Londrina 1
23	Centro Administrativo Maringá
24	Centro Administrativo Porto Alegre
25	Centro Administrativo Recife
26	Centro Administrativo Ribeirão Preto
27	Centro Administrativo Suarez Salvador
28	Centro Administrativo São Paulo 1
29	Centro Administrativo São Paulo 2
30	Centro Administrativo São Paulo 3

A topologia do Ambiente se encontra descrita na Figura 4, onde temos os departamentos envolvidos bem como a faixa DDR do referido site.
Em operação normal, o contato com os diversos departamentos do site é realizado através de ligações telefônicas externas (PSTN) ou pelos canais de voz da Empresa, onde a estrutura do Condomínio permite ligações internas entre os vários sites.

IV Figura 4 - Topologia do Site Original

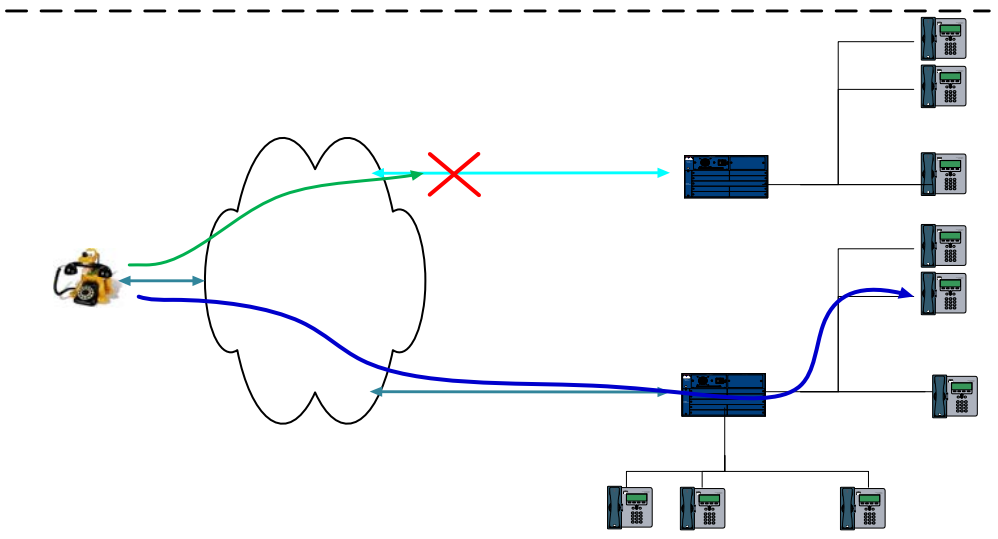


V

Já na apresentamos o encaminhamento das ligações telefônicas para o mesmo numero telefônico, somente que esta sendo atendido no site de contingência, por alguma inconformidade no site Original.

Figura 5 - Site de contingência

PSNT



3.1.6 Prós-condições

Após cada evento, onde o Disaster Recovery foi exercitado ou praticado, deve-se gerar um documento com a finalização da contingência, finalizando e validando a normalidade do Ambiente Original.

3.1.7 Grupo de Recuperação e suas Responsabilidades

Na Tabela 4temos os envolvidos, dentro da Empresa, dentro dos vários grupos de atuação diante de um evento catastrófico.

Tabela 4 - Grupo de recuperação

	Envolvidos	Responsável Empresa
Emergency Management Team (EMT)	Gerentes sênior, RH, Relações Publicas da Empresa, Setor Jurídico, Gerente de Risco e operações e Gestor de TI.	*Incident Manager; *Coordenador RH; *Coordenador Jurídico; * Gestor IT * Coordenador Produção; * (PAM)
Location Response Coordinator (LRC)	Gestor Técnico Regional	* Coordenador Suporte IT Regional; * (PAM).
Local Restoration Team (LRT)	Equipe Técnica Local e staff treinada	* responsável IT site Origem Evento; *responsável IT site contingência; * responsável BCP de cada Área.
Incident Response Team (IRT)	Equipe Supervisora e staff treinado	* responsável IT site Origem Evento; * responsável IT site contingência; * responsável BCP de cada área.
Technical Services Engineering (TSE)	Equipe de Suporte IT	* Coordenador operação Assistida

Estes grupos são responsáveis por:
Cada membro do grupo deverá designar um backup alternativo;
Lista de contatos (nome, endereço, fones, celular, etc.) atualizados;
Todo o grupo deve ter uma copia do Plano de contingência em ambiente particular de fácil acesso e atualizado;

3.1.8 Lista de Atualizações do Plano de Contingência

Para controle e responsabilidade das atualizações.

Tabela 5 - Atualizações do Documento

Revisões	Nome	Setor
1		
2		
3		

4		
5		
6		

3.1.9 Instruções para Uso deste Plano.

3.1.9.1 Acionamento do Plano.

Este plano se torna efetivo quando um da ocorrência de um desastre. Os procedimentos de gestão do problema deste grupo de Disaster Recovery terão inicio e somente após o restabelecimento ao ambiente original, local definitivo ou até a conclusão/ finalização da ameaça, as atividades retornaram a ser geridas pelos responsáveis titulares. Até lá a responsabilidade se mantêm com este grupo de Disaster Recovery.

3.1.9.2 Declaração do Desastre

Os grupos Emergency Management Team e Location Response Coordinator são responsáveis pela declaração do desastre aos demais grupos de recuperação conforme descrito neste plano.

3.1.9.3 Notificação

É importante repassar a toda comunidade dos diversos sites a existência deste grupo de Disaster Recovery, informando os contatos e responsáveis para que, caso ocorra algum problema o grupo Emergency Management Team seja acionado.
Caso tenhamos dois ou mais sistemas inativos por mais de 5 horas, ou algum evento que comprometa o ambiente, seja ela no tocante á rede de comunicação, acessos físico ou aos equipamentos, estes devem ser acionado o grupo Emergency Management Team.

3.1.9.4 Comunicação Externa

A comunicação com a mídia (radio, televisão, jornal e internet) será realizada por uma pessoa responsável pela Relação Publica da Empresa. Inclusive informando às agencias reguladoras, governamentais e demais órgãos externos sobre a declaração do desastre.

3.1.9.5 Política de Backup dos Dados

Todos os sites devem ter a política de backup dos dados consolidas em comum, isto é, os servidores devem ter seus backups garantidos e os usuários dos desktops individuais liberados para acesso remoto (mstsc, por exemplo) padrão do grupo. As mídias de backup devem ser armazenados em segurança, geograficamente distantes e isolados de riscos ambientais.
É necessário realizar um trabalho anterior de negociação de preservação das mídias, em termos de quantidade/volume de armazenamento e prazo deste quantitativo.

3.1.9.6 Política de atualização dos Ramais Telefônicos e suas Facilidades

Os Departamentos dos sites são responsáveis pela legitimidade e atualizações das informações contidas nos documentos de Contingências, onde constam as seguintes informações:

a) Departamentos Contingenciados;
b) Destino do site de contingência;
c) Ramais envolvidos na contingência (ramais do site de origem e ramais do site de destino);
d) Facilidades (facilidades dos ramais do site de origem e facilidades dos ramais do site de destino);
e) Contatos dos responsáveis pela contingência do Departamento afetado.

3.1.9.7 Procedimentos para Gestão das Emergências

Os procedimentos a seguir devem ser rigorosamente executados, pois é fruto de testes e avaliações anteriores para situações de emergências. Quando um evento não for corretamente identificado, os padrões normais de procedimentos devem ser executados até que se tenha uma noção completa do problema.
Vale salientar que qualquer pessoa que não esteja na relação de envolvidos ou do staff do grupo de contingência deve ser descartada, podendo comprometer a operacionalização desta Contingência.
A informação deste procedimento é fornecido pelos gestores do ambiente afetado, portanto devendo ter em mãos uma copia deste documento de contingência em seu ambiente particular. departamento em questão deve ter, previamente, um ambiente determinado para se reunir em caso de impossibilidade de acesso ao ambiente de trabalho. Desta forma, garantindo o contato e ações evasivas para o problema.

3.1.9.8 Impossibilidade de acesso ao Ambiente

A seguir apresentamos as possíveis situações em que este documento se aplica:

Tabela 6 - Eventos para o Redirecionamento das Ligações Telefônicas

SEQ	Risco	Medida
1	Incêndio	Caso de incêndio no ambiente;
2	Falta de Energia Elétrica	Caso os equipamentos da comunicação de dados sejam afetados por falta de energia elétrica e com previsão de retorno maior que período pré-estipulado;
3	Falha nas comunicações	Caso os links de dados, fornecidos pela Operadoras/Concessionárias extrapolem o período pré-estipulado;
4	Inundação na Sala de Equipamentos	Caso tenhamos, tanto nas salas de concentradores como na sala dos equipamentos, algum problema de inundação;
5	Movimentação Sindical	Bloqueio no acesso ao ambiente de trabalho;
6	Problemas de Hardware	Caso os equipamentos sejam afetados por problemas diversos que o tornem inoperantes e com previsão de retorno maior que período pré-estipulado;
7	Falha Humana	Erro de natureza humana que possa comprometer a operação no site;
8	Sabotagens / virus	Caso os equipamentos sejam afetados por problemas diversos que o tornem inoperantes e com previsão de retorno maior que período pré-estipulado

A sequencia de procedimento quando da ocorrência de algum evento se encontra descrito na Tabela 7.

Tabela 7 - Procedimento em Caso de Evento

Passos	Ação
1	Notificar o Gestor Técnico Local
2	Se a indisponibilidade for maior que 01 hora, reencaminhar as ligações telefônicas

	para os sites de Contingências Primários garantindo que o site Receptor das ligações esteja preparado para atender a demanda de ligações, tanto em termos de operadores como em termos de assunto. Caso a indisponibilidade seja maior que 02 horas, endereçar inicialmente as ligações telefônicas para os sites de contingências primários garantindo que o site Receptor das ligações esteja preparado para atender a demanda de ligações, tanto em termos de operadores como em termos de assunto. Encaminhar parte do Contingente de funcionários para o site de contingência Efetivo, o qual estará apto a receber a demanda necessária por um longo período de tempo e com todas as facilidades que o ambiente original.

Sob o ponto de vista do grupo de contingência, o Gestor Técnico Regional realizará:

a) Acompanhamento toda a programação de encaminhamento das ligações telefônicas do site de Origem para o site de Destino;
b) Informe á Operadora de Telefonia local sobre as alterações no encaminhamento das ligações telefônicas;
c) Sincronismo com os Usuários de cada site sobre a Operacionalização do Plano de contingência;
d) Sincronismo com o PAM e a operação Assistida CISCO, conferindo a programação de encaminhamento das ligações telefônicas.

3.1.9.9 Revisão e Manutenção do Plano de Contingência.

Este Plano é um documento “vivo” e, portanto deve ser revisado semestralmente e exercitado anualmente. Este teste/simulação deverá garantir as revisões e atualizações deste Plano de contingência em decorrência de mudanças e atualizações no Ambiente. Tanto em termos de rotatividade de funcionários, modus operante do ambiente como a inserção de novas tecnológica que podem propiciar novos procedimentos.
Este Plano de Contingência devera ser armazenado em local comum, podendo ser visto por toda a Administração Local e a Emergency Management Team (EMT). Cada equipe de Recovery terá seu próprio diretório com a gestão do coordenado do Recovery Plan.
Location Response Coordinator (LRC) será responsável pelo Plano. Um coordenado do Recovery Plan será designado para cada site da Empresa com as responsabilidades descritas abaixo:

a) Atualizar o Plano de contingência trimestralmente ou quando houver alguma alteração nas características do Ambiente - rotatividade de funcionários, modus operante do ambiente como a inserção de novas tecnológica;
b) Fornecer copia do Plano para todos os membros do time - Os membros da equipe devem ter copias em seu ambiente pessoal (casa, carro, laptop, etc.). Garantindo o fácil acesso ao documento;
c) Regularmente rever e atualizar as informações no plano de recuperação de desastres (por exemplo, listas de contato, equipamentos de inventario, procedimentos, etc.). Comunique-se com o Emergency Management Team (EMT). para obter as informações atualizadas periodicamente;
d) Realizar reunião com a equipe garantindo familiarização com o Plano de Contingência.com periodicidade semestral;
e) Manter um registro preciso dos locais de sites alternativos, fornecedores de equipamentos, locais de armazenamento de dados, geradores de energia portáteis e planos de implementação;

3.1.9.10 Alerta / Verificação / Fases da declaração

A seguir apresentamos o checklist para recuperação, as reações ao evento e o plano de diagrama de fluxo, o qual será utilizado pelos membros do Technical Services como um guia rápido.

3.1.9.11 Plano Checklist

Declarada a contingência, baseada no Plano de Continuidade do Negócio , a equipe Emergency Management Team (EMT) acionará o grupo de contingência conforme sequência e responsabilidades apresentadas na Tabela 8.

Tabela 8 - Sequencia Acionamento Contingência

Initials	Task to be completed - Implement	Responsible
1	Acionamento Contingência	Emergency Management Team (EMT)
2	Distribuição as Lista de Contato dos Envolvidos da Equipe de contingência	Location Response Coordinator (LRC)
3	Informe contingência á Operadora Telefonia	Operação Assistida
4	Acionar Prestador de Serviço Externo para possíveis problemas de Cabeamento	Location Response Coordinator (LRC)
5	Conferir Banda dos Circuitos de Dados - Garantia QoS	Operação Assistida
6	Confirmação DDR OK	Operação Assistida
7	Garantir acesso de toda a equipe de contingência nos Sites de contingência	Location Response Coordinator (LRC)
8	Garantir que a Identificação dos ramais do Site de Contingência esteja OK	Technical Services Engineering (TSE)
9	Confirmar Documentação de Contingência - Tabela de Redirecionamento das Ligações	Local Restoration Team (LRT)
10	Informar IRT do Site de Origem sobre atuação	Location Response Coordinator (LRC)
11	Informar IRT do Site de contingência sobre atuação	Location Response Coordinator (LRC)
12	Reconfiguração redirecionamento ligações Telefônica Site Origem	Operação Assistida
13	Reposicionar Aparelhos Telefônicos Backups	Technical Services Engineering (TSE)
14	Teste e Validação Ramais Destinos	Incident Response Team (IRT)
15	Teste e validação Redirecionamento ligações Telefônicas	Incident Response Team (IRT)

Já para o retorno da contingência temos a sequência apresentada na Tabela 9

Tabela 9 - Retorno da Contingência

Initials	Task to be completed - Return	Responsible
1	Acionamento Retorno Contingência	Emergency Management Team (EMT)
2	Distribuição as Lista de Contato dos	Location Response

	Envolvidos da Equipe de contingência	Coordinator (LRC)
3	Informe contingência á Operadora telefônica	Operação Assistida
4	Acionar Prestador de Serviço Externo para possíveis problemas de Cabeamento	Location Response Coordinator (LRC)
5	Conferir Banda dos Circuitos de Dados - Garantia QoS	operação Assistida
6	confirmação DDR OK	operação Assistida
7	Garantir acesso de toda a equipe de contingência nos Sites de contingência	Location Response Coordinator (LRC)
8	Garantir que a identificação dos ramais do Site de Contingência esteja OK	Technical Services Engineering (TSE)
9	Confirmar documentação de Contingência - Tabela de Redirecionamento das ligações	Local Restoration Team (LRT)
10	Informar IRT do Site de Origem sobre atuação	Location Response Coordinator (LRC)
11	Informar IRT do Site de contingência sobre atuação	Location Response Coordinator (LRC)
12	Reconfiguração redirecionamento ligações telefônica Site Origem	operação Assistida
13	Reposicionar Aparelhos telefônicos Backups	Technical Services Engineering (TSE)
14	Teste e validação Ramais Destinos	Incident Response Team (IRT)
15	Teste e validação Redirecionamento ligações telefônicas	Incident Response Team (IRT)

No Anexo 1 temos o fluxograma de ações de cada entidade dentro do Plano de contingência do Sistema de Telefonia VoIP.

3.1.9.12 Notificação do Incidente no Site

A seguir apresentamos como realizar o acionamento dentro e fora do horário Comercial

PERIODO	ACAO
Dentro do horário Comercial	Durante o horário Comercial, deve-se informar aos Local Response Coordinator (LRC), sobre o evento e assegurar que os padrões de emergência estejam sendo praticados.
Fora do horário Comercial	Fora do horário Comercial o staff de Vigilância deve informar o grupo Technical Services que repassará ao Location Response Coordinator (LRC)

3.1.9.13 Prover Status ao EMT.

O Location Response Coordinator (LRC) contatará o Emergency Management Team (EMT) e repassará as informações quando qualquer uma das condições abaixo se apresentarem:

- Cinco ou mais instalações estiver inativas ou com problemas, dentro do site, por mais de 05 horas;
- Qualquer problema de impeça as atividades normais do ambiente.

O LRC providenciará as seguintes informações:

a) Local do desastre;

b) Tipo do desastre (fogo, inundação, movimentação sindical, etc.);
c) Sumarizar os estragos;
d) A localização do Centro de Comando de Emergências, telefones de contatos, localização dos encontros fora do ambiente do Desastre;
e) Quantificas o tempo de restabelecimento;

O EMT contatará os lideres dos demais times reportando o acionamento do Plano de contingência.

3.1.9.14 Tomada de Decisão.
Baseados nas informações recebidas, o EMT, em conjunto com o LRC, decidirão qual será a resposta ao evento, mobilizar o IRT, permanecer e reparar o problema no mesmo site com o staff atual ou migrar para o site de contingência.

3.1.9.15 Repasse aos Membros dos Grupos.
Se o Desastre não for declarado, o grupo de resposta local estará resolvendo o problema com status periódicos ao EMT.
Caso o Desastre for declarado, o Location Response Coordinator desencadeará as ações necessárias, repassando a decisão para os membros do Incident Response Team para ações imediatas em sua implantação.
Plano de contingência é acionada quando um evento não mapeado ocorre e o tempo de recuperação não pode ser mensurado. é importante manter a hierarquia de comandos sobre o Plano de Contingência, prevendo inclusive os contatos alternativos em caso de indisponibilidade do titular.

3.1.9.16 EMT Notifica as Equipes e Clientes
De posse da lista de envolvidos do Plano de Contingência, Os membros do EMT acionarão as equipes e, se for de conhecimento, repassar as ações e operações necessárias para a restauração do ambiente.

3.1.9.17 Contato Geral com os Parceiros.

Na Tabela 10 temos os contatos dos Parceiros, no tocante a Telefonia, que estão envolvidos no Plano de contingência.

Tabela 10- Relação de Parceiros

Empresa	Contato	Setor	Telefone Fixo / Celular
Embratel	Contato 1	DDR	
Embratel	Contato 2	DDR	
telefônica	Contato 1	DDR	
telefônica	Contato 2	DDR	
CISCO	Contato 1	operação Assistida	
CISCO	Contato 2	operação Assistida	

3.1.9.18 Declaração do Desastre

Uma vez que o Desastre é declarado, o Response Team (IRT) é mobilizado. O time de recuperação iniciará e coordenará as ações para a recuperação. Os membros do IRT devem se deslocar para o Centro de Comando o mais breve possível.

O grupo LRT deve permanecer no site afetado até dando um parecer / avaliação dos estragos até que a chegada do grupo IRT.

3.1.9.19 Avaliação detalhada dos Estragos

Deve-se realizar uma avaliação em conjunta dos prejuízos por parte dos coordenadores locais, LRC e IRT. Também incluir se possível, os parceiros responsáveis pelos equipamentos assegurando-se que sua opinião possa dirimir todas as possíveis variáveis não detectadas sobre a operacionalidade do ambiente.

a) Elaborar um brief sobre os requisitos da avaliação e revisando:

- Procedimentos da avaliação;
- Levantamento dos Requisitos;
- Questões de segurança

b) Avaliação dos Resultados

a. Permissão de Acesso ao Site
   - Realizar uma inspeção in loco das áreas afetadas para avaliar os danos aos registros essenciais (arquivos impressos, manuais, contratos, documentação, etc.) e dados eletrônicos;
   - Obter informações sobre danos à estrutura (por exemplo, condições ambientais, a integridade física da estrutura, móveis e utensílios) pelo LRC / LRT.

c) Criar uma Lista de Prioridade de Restauração, identificando as instalações, arquivos vitais e equipamentos necessários para as atividades que podem ser operacionalizados e recuperados rapidamente;
d) Criar uma Lista de Prioridade de Recursos Salvos, identificando os sites e registros que podem ser salvos eventualmente;
e) Recomendações para os recursos necessários;
f) Entre em contato com a EMT e decida se a situação exige o lançamento de planos de recuperação de empresas (desastres de longo prazo) ou se o trabalho pode voltar ao site primária rapidamente (curto prazo - semana).

3.1.9.20 Contato com EMT - Decide em continuar na fase de Recovery do Negócio

A LRC reúne informações do IRT e de outras fontes para informar sobre detalhes da avaliação do estrago.

Com base na informação obtida a partir da LRC, a EMT decide em continuar com a fase de recuperação de Negócio deste plano. Caso não seja possível a avaliação do recuperação ainda não for conclusiva, deve-se permanecer no local até a conclusão do mesmo e reportando periodicamente EMT sobre seu status.

A fase de recuperação de negócios deste plano será implementada quando as restaurações do suporte forem atingidos, tanto com relação às funcionalidades dos sistemas com das instalações no site de contingência.
Durante a fase de Inicial de Resposta, os serviços devem ser redirecionados para o site de contingência, permitindo a operação e atendimento aos Clientes. Inicialmente de forma reduzida até que tenha sua operação em sua totalidade. Após 05 horas o sistema e as instalações devem estar 100% operacionais.

3.1.9.21 Fase da recuperação do Negócio (05 horas – recuperação Completa)
Esta seção documenta as etapas necessárias para ativar o Plano de recuperação do Negócio com recuperação completa do suporte dos sistemas e das funcionalidades da instalação no site de contingência.

3.1.9.22 Requisitos de operação das Instalações e Sistemas
A configuração das instalações e do sistema de cada site são importantes para o restabelecimento das operações normais. A lista de se encontra no **Erro! Fonte de referência não encontrada.**, onde devemos ter duas listas: 1) relação dos ramais e suas facilidades no site de Origem e; 2) relação dos ramais e suas facilidades no site de Destino.
3.1.9.23 Notificado do Staff de Engenharia Técnica

O acompanhamento do staff técnico é importante de readequações das possíveis distorções referente á configuração do novo ambiente em relação ao site Original.

3.1.9.24 Planejamento Prévio para a Realocação
Faça contatos antecipados com hotéis, fornecedores, restaurantes como suporte de infraestrutura para o caso de emergências.

3.1.9.25 Notificar o EMT e as Unidades de Negócio da Corporação para Inicio da Recuperação
Informar a todos os funcionários envolvidos sobre o Inicio da Recuperação, repassando-lhes todas as alterações nos processos e procedimentos, inclusive com informações de contato e horário de funcionamentos do ambiente, etc.

3.1.9.26 Recuperação das Operações
Após todas as operações relevantes em funcionamento no site de contingência, os funcionários devidamente acomodados e todos os processos e procedimentos em andamento a Corporação pode decretar o sucesso da contingência.

3.1.9.27 Atualização da Documentação
Após todas as etapas concluídas, o ambiente Contingenciado e os reparos do ambiente Antigo, faz-se necessário uma revisão no documento atual, revendo alguns conceitos e valores com o intuito de aprimorar este Plano:
a) Significado e objetivos da política interna;
b) Visão, valores e credos que permeiam a organização;
c) O comprometimento dos gestores na implementação da comunicação;
d) Planos, padrões, procedimentos e sistemas relacionados à implementação e medidas de desempenho;
e) Informações factíveis que contribuam para o envolvimento dos trabalhadores;

f) Sugestões e ideias que contribuam para as melhorias;
g) Relatórios de desempenho e
h) Lições aprendidas com incidentes e acidentes;
i) Report a toda a Comunidade envolvida sobre o Sucesso da Contingência.

IV CONCLUSAO

Conforme apresentado acima, os detalhes abordados visaram apresentar todas as variáveis mensuradas, quando um site original se apresenta inacessível ou impossibilitado de operar.

Anteriormente foi repassado que este Plano de Continuidade do Negócio, voltado a Contingencia de Comunicação de Voz e baseado na tecnologia VoIP, é um documento "VIVO" e como tal necessita de atualizações e aprimoramento. Até mesmo porque temos muitas variáveis que estão constantemente influenciando no dia a dia no ambiente, seja ela tecnológica, mudança de topologia, alterações dos departamentos, restruturação do ambiente, etc. Devendo ser constantemente atualizada. Além do que, o melhor golpe de "Misericórdia" seria a realização de testes periódicos com o intuito de mitigar os possíveis erros ou variáveis não contempladas.

Toda esta estrutura de site de Contingencia é oneroso para a Empesa, em termos de espaço físico, recursos tecnológicos (aparelhos telefônicos de backup, rede de dados que comporte a comunicação de voz), negociações com as Operadoras , etc. Mas é o ônus de ser manter a Continuidade do Negócio, imaginando-se como um seguro para a Empresa, pois a perda do Core Business, Imagem e Reputação da Marca da Empresa não tem preço
A relação custo-benefício para a implementação de um Plano de Continuidade do Negócio em uma organização é extremamente benéfica, pois a baixo custo temos a garantia de continuidade do Negócio frente ao prejuízo humano, material, financeiro, imagem ou ambiental.
Para que se tenha um documento "clean", pratico e atualizado a proposta maior é TESTAR, TESTAR e TESTAR.
Garantimos assim dirimir todos os possíveis problemas o qual o BCP se propõe a sanar.

VI REFERÊNCIAS BIBLIOGRÁFICAS

MARINHO Fernando. Como Proteger e Manter seus Negócios: Um Plano Básico Para Contingências e Continuidade nas Empresas. 1. ed. Editora CIENCIA MODERNA, 2008.

SALDANHA, Fernando. Introdução a Planos de Continuidade e Contingência Operacional, Ed. Papel & Virtual, 1999.

DINIZ, Roberto. Processo Decisório em Tecnologia da Informação. 1ª edição. Ed. Editora CIENCIA MODERNA, 2008.

DISASTER RECOVERY INSTITUTE . O Common Body of Knowledge e Professional Practices for Business Continuity Planners, do Disaster Recovery Institute International – DRI International (www.drii.org);

PMI - PROJECT MANAGEMENT INSTITUTE. (2004). Um Guia do conjunto de conhecimentos em gerenciamento de projetos. 3 ed. Pennsylvania: Project Management Institute.

Business Continuity Management 2000. Australian National Audit Office http://www.anao.gov.au/~/media/Uploads/Documents/business_continuity_management_.pdf

Business Continuity Planning march 2008.Federal Financial Institutions Examination Council (FFIEC). http://www.ffiec.gov/

Congresso Nacional de Excelência em Gestão - 22 e 23 de novembro de 2002 - Niterói, RJ Universidade Federal Fluminense - Centro Tecnológico - Escola de Engenharia - LATEC - Mestrado Profissional em Sistemas de Gestão

Guia de orientação para o gerenciamento de riscos corporativos / Instituto Brasileiro de Governança Corporativa; coordenação: Eduarda La Rocque. São Paulo, SP: IBGC, 2007 (Série de Cadernos de Governança Corporativa, 3). www.ibgc.org.br.

MORGADO, C.R.V. Gerencia de riscos. Rio de Janeiro: SEGRAC – Núcleo de Pesquisa em Engenharia de Segurança, Gerenciamento de Riscos e Acessibilidade na UFRJ, 2000.

SALDANHA, Fernando. Introdução a Planos de Continuidade e Contingencia Operacional. 1ª edição. Papel Virtual Editora ,2000

ANEXOS

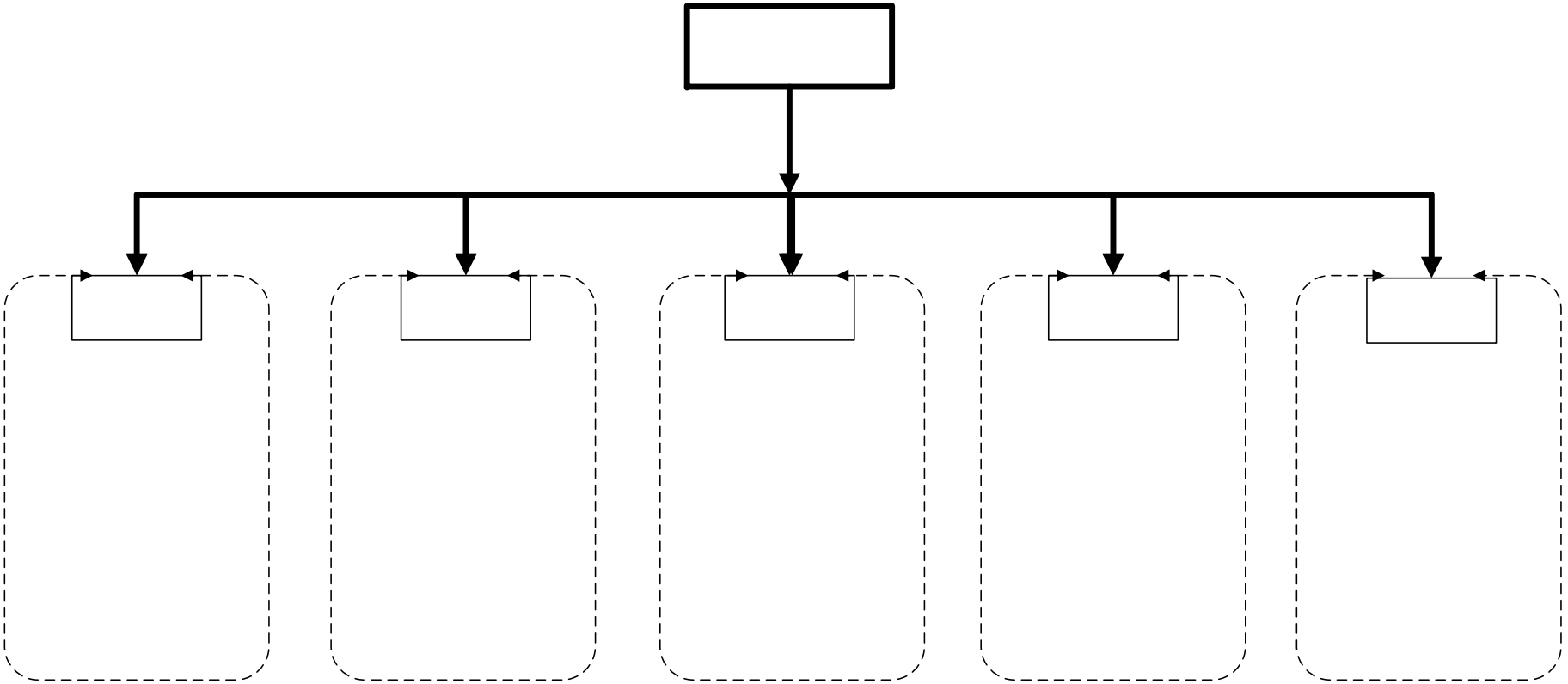
Anexo 1 - Grupos e Responsabilidades

Componentes	Envolvidos	Responsabilidade	Ações
Emergency Management Team (EMT)	Gerentes Seniors, RH, Relações Publicas da Empresa, Setor Jurídico, Gerente de Risco e Operações e Gestor de TI.	Responsável pela coordenação de todos os esforços de Disaster Recovery, evolução e determinação da Declaração do Desastre e comunicação com os Gestores Sênior.	* Avaliar como as ações de Recuperação devem tomadas e quais equipes devem ser acionadas; * Avaliar e analisar os resultados da Avaliação de Danos; *Priorizar as restaurações necessárias baseadas nos relatórios de Danos; * Atuar como um Canal de comunicação entre as equipes da Empresa e Grandes Clientes; * Trabalhar com os Fornecedores e a equipe Interna para desenvolver um cronograma de restabelecimento/reparo.
Location Response Coordinator (LRC)	Gestor Técnico Regional	Responsável pela coordenação de todos os esforços de Disaster Recovery, em sua região. Estabelecendo uma Central de Comando e comunicação com o Emergency Management Team	* Notificar a Incident Recovery Team; * Reunir informações e avaliações de danos e relatá-lo a EMT; * Determinar as necessidades de recuperação; * Estabelecer um Centro de comando e operações onde os membros das equipes EMT / LRT / IRT se reúnem para coordenar a avaliação dos danos e tarefas de recuperação de negócios para as operações afetadas; * Notificar todos os Chefes de Equipe e aconselhá-los a ativar seus planos se for o caso, com base na situação de desastre; * Se nenhum desastre for declarado, tomar as medidas necessárias para retornar à operação normal; * Determinar se os Fornecedores ou de outras equipes são necessários para auxiliar na avaliação nos detalhes dos danos; * Preparar um relatório pós-desastre; * Coordenar o desenvolvimento de planos específicos de recuperação do local e garantir que eles são atualizados semestralmente.

Local Response Team(LRT)	Equipe Técnica Local e staff treinado	Responsável pelo alerta/notificação do problema durante Horário Comercial. Fora do horário Comercial, esta equipe fará parte da equipe Incident Response Team durante um evento de declaração de Desastre.	* Fornecer as seguintes informações ao LRC sobre o evento a interrupção: a) Tipo de Evento; b) Local de ocorrência; c) Tempo de ocorrência. * Coordenar o retorno da comunicação de Voz e Dados a) Trabalhar com o roteamento alternativo de Voz e Dados para os sites alternativos; b) Recuperação de Correio de Voz e E-mails quando solicitado pelo EMT; c) Validação do Correio de Voz e E-mails no site alternativo; d) Validar o checklist dos Requisitos Mínimos Aceitáveis de Operação; * Coordenar o restabelecimento das Operações dos Sistemas de informações: a) Trabalhar com os gestores para recuperação dos sistemas críticos, aplicações e infraestrutura no site de Contingência; b) recuperação de arquivos críticos e informações relacionadas quando requisitadas pelo EMT; c) Assegurar que a rede de dados e a segurança do local sejam atuantes no site de contingência; d) Validar o checklist dos Requisitos mínimos aceitáveis de operação, determinando os recursos necessários para operação.

Incident Response Team (IRT)	Equipe Supervisora e staff treinado	Responsável pelo alerta/notificação do problema durante horário Comercial. Fora do horário Comercial, esta equipe fará parte da equipe Incident Response Team durante um evento de declaração de Desastre.	* Fornecer as seguintes informações ao LRC sobre o evento a interrupção: a) Tipo de Evento; b) Local de ocorrência; c) Tempo de ocorrência. * Coordenar o retorno da comunicação de Voz e Dados a) Trabalhar com o roteamento alternativo de Voz e Dados para os sites alternativos; b) recuperação de Correio de Voz e E-mails quando solicitado pelo EMT; c) validação do Correio de Voz e E-mails no site alternativo; d) Validar o checklist dos Requisitos mínimos aceitáveis de operação; Coordenar o restabelecimento das operações dos Sistemas de informações: a) Trabalhar com os gestores para recuperação dos sistemas críticos, aplicações e infraestrutura no site de contingência; b) recuperação de arquivos críticos e informações relacionadas quando requisitadas pelo EMT; c) Assegurar que a rede de dados e a segurança do local sejam atuantes no site de Contingência; d) Validar o checklist dos Requisitos mínimos aceitáveis de operação, determinando os recursos necessários para operação.
Technical Services Engineering (TSE)	Equipe de Suporte IT	Responsável por suporte às atividades de recuperação das atividades tecnológicas.	* Apos notificação da Declaração do Desastre, revisar e dar suporte: a) Facilitar a recuperação tecnológica e atividades de recuperação, fornecendo orientações sobre equipamentos e sistemas substituídos; b) Coordenar a remoção de equipamentos e recursos para a operação do site de contingência.

Anexo 2- Ativação do Plano de contingência do Sistema de Telefônica VoIP



PUBLIC

Emergency Management

Location Response

Anexo 3 - Configuração do Ramal

RAMAL	ANDAR	PLANTA	TELEFONE	MODELO	NOME USUARIO	MATRÍCULA	DEPARTAMENTO (premier, private, agencia, hsbc, losango)	BDU	Line CSS 1	Grupo de Captura	Voice Mail	CADEADO	GRAVADO	FAX	MODEM	SEM FIO	AUDIO CONF	EXTENSAO	COMPARTILHADO	HEADSET ? MODELO ?	FUNÇÃO DO RAMAL (guarita, copa, sala de reuniao, manutenção, restaurante, head, alarme, FET)	GERENTE	OBS