FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
CURSO DE ADMINISTRAÇÃO DE EMPRESAS
ÊNFASE EM ANÁLISE DE SISTEMAS DE INFORMAÇÃO

PATRÍCIA MARQUES DA SILVEIRA

PLANO DE CONTINUIDADE DE NEGÓCIOS PARA A EMPRESA ALFA: UMA PROPOSTA COM BASE NA NBR 15999, NO ITIL E NO COBIT

Porto Alegre,
junho de 2009

PATRÍCIA MARQUES DA SILVEIRA

PLANO DE CONTINUIDADE DE NEGÓCIOS PARA A EMPRESA ALFA: UMA PROPOSTA COM BASE NA NBR 15999, NO ITIL E NO COBIT

Trabalho de conclusão de curso apresentado como requisito à obtenção do grau de Bacharel em Administração de Empresas com ênfase em Análise de Sistemas de Informação, na Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Professora Orientadora: Dr. Edimara Mezzomo Luciano

Porto Alegre

junho de 2009

AGRADECIMENTOS

Primeiramente agradeço a Deus pela saúde e determinação.

Deixo meu especial agradecimento a Professora Edimara, pela excelente orientação, auxiliando-me com dedicação, compartilhando seus conhecimentos, bem como pelos momentos de incentivo.

Agradeço aos meus colegas e amigos Luciana Soller e Luciano Oyarzabal, que sempre estiveram juntos nesta caminhada, compartilhando momentos de estudo e descontração. Também aos demais professores e colegas do curso de Administração, pelos momentos compartilhados.

Agradeço a empresa em que ocorreu o estudo, pela oportunidade e incentivo na realização da pesquisa. Aos colegas de trabalho pela compreensão nos momentos de ausência e em especial aqueles que de alguma forma contribuíram para meu trabalho com palavras de incentivo, mostrando interesse e auxiliando nos ajustes finais.

Agradeço aos entrevistados pela contribuição com seus conhecimentos e pela disponibilidade de tempo, mesmo quando estavam ocupados com seus trabalhos.

Dedico especial agradecimento ao meu tio Luiz Carlos Silveira Marques, que sempre se preocupou e incentivou os meus estudos.

Agradeço aos meus padrinhos Márcia e Wanderlei, que sempre se mostraram presentes quando precisei.

Agradeço a minha mãe Marilê pela sua infinita dedicação, amor e compreensão durante todos os momentos da minha vida. Também agradeço aos meus irmãos Sabrina e Diogo por serem pessoas que sempre estão dispostas a ajudar e pelo amor que nos une. Agradeço a todos que amo pela compreensão nos momentos em que não pude estar presente.

Agradeço a lembrança que meu gato Guri deixou antes de ausentar-se no início deste trabalho, onde foi difícil suportar a dor. No entanto, fui presenteada com um novo gatinho, o Gabiru, que me trouxe alegria e companhia durante a elaboração e conslusão deste trabalho. Presente este que nunca vou esquecer, pois foi a maior demonstração de amor que já recebi.

A todos, muito obrigada!

RESUMO

A cada dia que passa, o mercado de TI tem se tornado cada vez mais competitivo e exigente. Para acompanhar este mercado e atender as exigências e requisitos de clientes, as organizações se veem obrigadas a manter-se atualizadas quanto à tecnologia e aos modelos de melhores práticas que têm sido utilizadas pelas organizações. A empresa ALFA possui o seu negócio na área de TI, onde oferece e presta serviço de testes de *software* para diversas empresas, onde cada uma delas possui um tipo de *software* com uma determinada tecnologia e com diferentes requisitos e exigências com relação à entrega dos serviços. Devido à empresa possui uma grande diversidade de clientes, pertencendo eles aos variados setores do mercado, a empresa procura atender a todos os setores oferecendo garantia e qualidade nos serviços. Desta forma, para atender os requisitos do setor bancário, que é um setor do mercado que a ALFA pretende explorar, a empresa verifica a necessidade de um Plano de Continuidade de Negócio (PCN), baseado em práticas e controles de reconhecimento internacional, pois este é um dos requisitos exigidos por este setor. A justificativa deste trabalho é garantir a continuidade do negócio da empresa ALFA com a elaboração de um PCN, fazendo com que a empresa atenda as expectativas de clientes internos e externos, no menor espaço de tempo, em caso de incidente que afete instalações, informações ou pessoas. Desta forma, a empresa mantém-se competitiva e com capacidade de explorar novos setores no mercado de TI, agregando confiabilidade à imagem da organização. Portanto, o objetivo deste trabalho é definir um PCN baseado nas práticas mais utilizadas pelas empresas atualmente, como a metodologia COBIT, as melhores práticas do ITIL e a ISO15999. De forma a atender o objetivo proposto para o trabalho, o método utilizado para orientação da pesquisa foi o estudo de caso, com pesquisa qualitativa. Para a coleta de dados, foi realizada entrevista semiestruturada, observação participante e análise de documentos. As entrevistas ocorreram com quatro funcionários da alta gerência da empresa ALFA e com quatro especialistas em segurança da informação que atuam no mercado de TI. Desta forma, após a análise das entrevistas, observação e análise de documento, foram levantados os requisitos para elaboração da proposta. Entre estes requisitos, foram identificados os recursos das atividades críticas da empresa e para estes recursos foram definidas estratégias de contingência. Como resultados dos estudos, este trabalho propõem dois documentos como forma de gerenciar os incidentes que venham a ocorrer com os recursos da organização. Os documentos foram elaborados conforme o objetivo proposto, sendo utilizadas as informações do ITIL COBIT e

ISO15999. Um dos documentos é o Plano de Gerenciamento de Incidentes (PGI) e o outro é o Plano de Continuidade de Negócio (PCN). Com a elaboração destes planos para empresa ALFA, pretende-se que a empresa mantenha-se competitiva no mercado de TI, conquistando novos setores, agregando confiabilidade a imagem da empresa e que continue atendendo as expectativas dos clientes internos e externos com maior confiabilidade.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A cada dia que passa a Tecnologia da Informação tem se tornado fator de competitividade entre as organizações, pois é através da TI que as empresas organizam os dados e geram informações para as tomadas de decisões. Pelo valor que a TI tem hoje no ambiente organizacional e pelos impactos que poderiam ser ocasionados pela parada dos negócios devido a algum tipo de catástrofe, torna-se fundamental a importância de um Plano de Continuidade de Negócio (PCN) que garanta a continuidade dos serviços no menor espaço de tempo possível.

Desta forma, o presente trabalho tem por objetivo a elaboração de um PCN para a empresa ALFA, pois a empresa possui uma cadeia de clientes de grande valor e com alto nível de criticidade nos projetos trabalhados e deseja manter a qualidade e garantia dos serviços prestados. A proposta para o PCN é que o mesmo esteja inserido dentro de padrões de melhores práticas de reconhecimento internacional.

No capítulo 2 são apresentadas as características da organização e seu ambiente, onde é descrito um breve histórico da empresa.

O capítulo 3 descreve a situação problemática e o capítulo 4 a justificativa da escolha do tema proposto. Os objetivos gerais e específicos estão descritos no capítulo 5.

O referencial teórico utilizado como base para elaboração do trabalho está inserido no capítulo 6.

No capítulo 7 é realizada a apresentação do método de pesquisa a ser utilizado para o trabalho.

No capítulo 8 são apresentados os resultados obtidos através das entrevistas, assim como o plano de ação para elaboração da proposta.

No capítulo 9 são apresentadas as considerações finais do trabalho.

2 CARACTERIZAÇÃO DA ORGANIZAÇÃO E DO SEU AMBIENTE

O objetivo deste capítulo é apresentar a caracterização da empresa em que foi realizado o trabalho, assim como uma breve descrição do histórico, visão e missão.

2.1 HISTÓRICO

Fundada em março de 2004, a empresa ALFA teve seu início devido à ação empreendedora de um estudante de Análise de Sistemas, que identificou a oportunidade do negócio quando participava de um evento referente à qualidade de *software,* que ocorreu na própria universidade em que estudava (PUCRS).

Após a identificação da oportunidade na área de teste de software, a empresa ALFA iniciou seu negócio dentro da incubadora Raiar, localizada no TECNOPUC. No período que permaneceu incubada, a empresa adquiriu conhecimentos e técnicas especializadas na área de atuação. Esta especialização adquirida pela ALFA, fez com que o número de clientes aumentasse, ocasionando a sua graduação da incubadora em 2005.

Desde então, a empresa vem aumentando o número de clientes e procurando adaptar o seu trabalho às melhores práticas utilizadas atualmente e reconhecidas no mercado. Com uma carteira de clientes sólida e de grande importância, para continuar atendendo com alto nível de qualidade, foi necessário realizar modificações internas para atender as diversificações de projetos e suas exigências. A ALFA criou áreas de especialização, onde equipes especializadas são responsáveis pela qualidade dos projetos que envolvem a sua área de conhecimento. A empresa também possui especialistas que são capacitados para atender determinadas exigências de projetos e que trabalham juntamente com as equipes de áreas conforme as necessidades verificadas para cada projeto. Esta hierarquia é apresentada claramente através do organograma ilustrado e comentado na seção 2.6.

2.2 MISSÃO, VISÃO E VALORES

A empresa ALFA tem por missão: “Satisfazer o cliente provendo a melhor solução e estratégia em qualidade de *software*”. Esta missão refere-se à qualidade de entrega dos serviços oferecidos pela empresa, onde a empresa tem como premissa a entrega dos projetos dentro dos prazos contratados pelo cliente e com a qualidade esperada.

A visão projetada pela empresa é: “Ser a líder no Rio Grande do Sul em testes de *software*, ter uma representação no centro do país e atuar solidamente usando o modelo de *offshoring*”.

A ALFA ainda estabelece como princípios de valores para a sua organização as seguintes características:

- Honra;
- Competência;
- Qualidade na prestação de serviços;
- Comprometimento;
- Trabalho em equipe.

Com estes valores, a empresa consegue manter a qualidade dos serviços e um bom relacionamento entre os colaboradores e suas equipes de trabalho.

2.3 OBJETIVOS

O objetivo da ALFA é garantir a qualidade dos produtos desenvolvidos pelos clientes através de testes de *software*. Esta garantia de qualidade é efetivada através de processos de testes inseridos no processo de desenvolvimento do cliente, além da simulação de situações reais encontradas por usuário do *software*.

A empresa também oferece consultoria QA (*Quality Assurance*), que busca auxiliar na melhoria de processos dos clientes com o objetivo de garantir a qualidade dos produtos.

2.4 FORNECEDORES E CLIENTES

Os fornecedores que a ALFA trabalha atualmente são empresas que prestam serviços de internet, telefone, email, consultoria em marketing, assessoria em RH, contabilidade e fornecedores de *hardware* e *software*.

Os clientes são empresas de desenvolvimento de *software*, empresas de TI e empresas particulares que já possuem um *software* implantado e necessitam de avaliação da qualidade do produto.

2.5 CONCORRENTES

A ALFA não possui concorrentes diretos na região sul, atualmente os concorrentes estão localizados na região sudeste. Após o estabelecimento da ALFA no TECNOPUC, algumas empresas de desenvolvimento, que também estavam incubadas, passaram a oferecer o serviço de testes de *software*. Mesmo que estas empresas tenham incluído este serviço para diversificação do negócio, elas não possuem o *know-how* que a ALFA possui, visto que a empresa inicialmente foi composta por bolsistas de iniciação científica e que faziam parte do laboratório da Hewlett-Packard (HP), também localizada no TECNOPUC. Após dois anos de estudos sobre metodologia de testes no laboratório da HP a empresa hoje possui o *know-how* de como implantar as metodologias de testes.

A maioria dos concorrentes da ALFA está localizada em São Paulo, onde existem concorrentes com o mesmo foco da empresa em estudo. No entanto, no mercado internacional, observa-se um grande número de empresas que são especializadas na área de qualificação de software.

2.6 ESTRUTURA ORGANIZACIONAL

Atualmente a estrutura da ALFA está representada conforme o organograma ilustrado na Figura 1.

A Diretoria Administrativa (DADM) é responsável por toda administração da organização, que inclui processo de prospecção, venda, marketing e planejamento estratégico. A pessoa responsável pela diretoria administrativa, também administra e gerencia os *backups* dos servidores. A Gerência Financeira, responsável pelas finanças da empresa, está diretamente ligada a DADM e responde a esta administração.

A Diretoria de Projetos (DPJ) também responde para DADM e é responsável pela gerência dos projetos, realizando a elaboração e controle de cronogramas. Este setor comunica-se diretamente com os clientes pra alinhar questões referentes aos projetos, escopo e prazos. O DPJ trabalha juntamente com o setor de Recursos Humanos (RH), pois as solicitações de recursos e o conhecimento necessário são definidos pelo DPJ. O processo de seleção é realizado pelo setor de RH que possui todas as técnicas e conhecimentos necessários para um qualificado processo de seleção, que tem por objetivo atender as necessidades e solicitação do DPJ.

A Diretoria de Tecnologia da Informação (DTI) possui sob sua responsabilidade a gerência dos recursos de TI utilizada pela empresa, este setor trabalha diretamente com o setor de SQA *(Software Quality Assurance*), que é responsável pelos processos e melhores práticas utilizadas pela empresa, controle e auditoria e revisão dos processos implantados. O SQA também tem sob suas responsabilidades a garantia da qualidade na entrega dos serviços aos clientes.

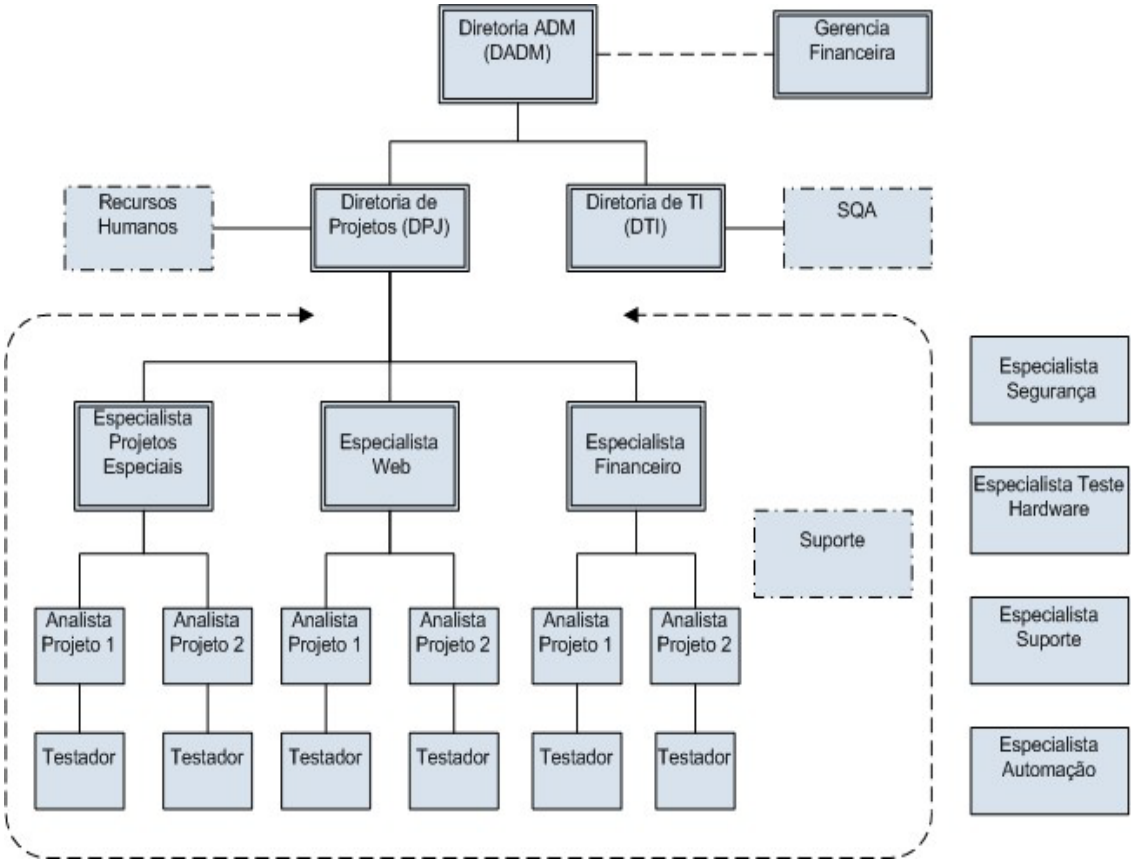

Figura 1: Organograma da empresa ALFA

Abaixo da DPJ estão os Especialistas de áreas que possuem conhecimentos específicos para a área que atendem e estão em constante aprendizado para atender as demandas e os diferentes projetos que são trabalhados frequentemente. São responsáveis por atender as solicitações do cliente e mantêm contato mais frequente com o cliente. Também tem sob responsabilidade o andamento e qualidade dos projetos que correspondem a sua área de atuação.

Os Analistas de Projetos respondem diretamente aos Especialistas de áreas e são alocados nos projetos conforme o conhecimento adquirido em projetos já trabalhados. Possuem como função a elaboração dos casos de testes a serem testados juntamente com os Testadores. Estes executam os casos de testes e reportam aos Analistas de Projetos.

O Suporte trabalha juntamente com os Especialistas de área e suas respectivas equipes atendendo as demandas dos projetos, onde sua responsabilidade é atender os requisitos de preparação do ambiente solicitado pelo cliente.

Para atender as demandas específicas de cada área, Especialistas em Segurança, Teste de Hardware, Suporte e Automação, trabalham entre as equipes Especialistas de Projetos para atender as necessidades cada projeto. Estes Especialistas procuram atualizar seus conhecimentos constantemente para que possam atender todos os tipos de projetos com as variadas tecnologias existentes.

3 SITUAÇÃO PROBLEMÁTICA

Nos últimos anos, a Tecnologia da Informação (TI) passou a ser ferramenta de competitividade e destaque entre as empresas, principalmente para as empresas que tem no seu negócio o foco em serviços de TI. Para as empresas prestadoras de serviços, torna-se fundamental o desenvolvimento de aplicações com base nas necessidades do negócio. Oferecer garantia de serviços compatíveis com a exigência do negócio, agregando controle e minimizando os riscos são objetivos da ALFA. Para Weill e Ross (2006), negócios requerem mudanças constantes, onde implementação de TI envolvem investimentos imediatos e continuados em busca de resultados.

A ALFA faz parte de uma destas empresas, pois o seu negócio é especializado em Testes de Software e Consultoria QA *(Quality Assurance)*, onde o *offshoring* é uma especialização deste tipo de negócio voltada para o modelo internacional. Como prestadora de serviços há mais de cinco anos no mercado, verifica-se esta competitividade pelo fato de os clientes exigirem fornecedores cada vez mais capacitados e adequados a modelos como ITIL, COBIT, CMMi entre outros.

Devido ao rápido crescimento da empresa e frente às necessidades do negócio, a administração da empresa vem trabalhando constantemente para que a infraestrutura de TI supra as necessidades encontradas no padrão de trabalho de clientes mais estruturados. Desta forma, a empresa procura alinhar as exigências de mercado ao modo de trabalho já existente, fazendo uma gestão eficaz e eficiente.

A empresa ALFA já é aderente ao modelo de CMMi e mantém um processo ativo de melhorias contínuas e estudo de metodologias para adequação ao processo de trabalho, visando à garantia de serviços aos clientes. As melhorias baseadas em metodologias estão fazendo com que a empresa construa uma estrutura sólida e confiável, fazendo com que os clientes após o contrato de um projeto voltem a contratar os serviços. Com isto, a confiabilidade da empresa no mercado vem aumentando, fazendo com que novos clientes procurem os serviços da empresa.

Com o objetivo de dar continuidade ao processo de melhor adequação da TI aos requisitos do negócio, a empresa verifica a necessidade de estruturação de um Plano de Continuidade de Negócio (PCN) com base em conceitos teóricos, melhores práticas e controle. Hoje a empresa possui um PCN, mas sem embasamentos teóricos, práticas e controle com nível de reconhecimento. A necessidade de aplicação ao negócio foi identificada

junto à exigência encontrada frente a uma RFI (*Request for Information*) de um grande banco com base no Brasil.

Segundo Sêmola (2003, p.98), o objetivo do Plano de Continuidade de Negócios é "Garantir a continuidade de processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre.". O referido autor ainda cita que o Plano de Contingência deve ser desenvolvido para cada ameaça considerada em cada um dos processos do negócio, onde devem ser definidos em detalhes os procedimentos a serem executados em estado de contingência.

Utilizando como base os principais modelos de administração de TI que tem sido utilizado pelas empresas, como COBIT (*Control Objectives for Information and Related Technology*), ITIL (*Information Technology Infrastructure Library*) e a NBR 15999:2007, que é a norma específica para Gestão de continuidade de negócios. Este trabalho propõe a responder a seguinte questão: como deve ser um Plano de Continuidade de Negócio de modo a minimizar os riscos, garantir a continuidade dos serviços em caso de desastres e satisfazer as expectativas dos clientes (internos e externos)?

4 JUSTIFICATIVA DA ESCOLHA DO TEMA

Com a alta competitividade e lucratividade que gira em torno de negócios bem sucedidos de TI, verifica-se que a interrupção nos negócios pode gerar enormes transtornos e custos para as organizações e seus clientes. Além do transtorno de paradas não planejadas, as empresas correm o risco de perder clientes, projetos e ter a imagem prejudicada perante o mercado.

Este trabalho é importante diante da alta competitividade que gira em torno do mercado de TI, fazendo com clientes bem estruturados exijam garantia na prestação e continuidade dos serviços. É essencial que as organizações se preocupem em definir um Plano de Continuidade de Negócio (PCN) para que, em caso de algum tipo de incidente, o planejamento possa minimizar a perda e perturbação que venha a ser causado para seus clientes e colaboradores.

A administração da empresa ALFA tem observado que com o crescimento da organização também surgem novos requisitos para o negócio, devido ao alto nível de criticidade de negócio de alguns clientes, perante a segurança de suas informações e a importância da não parada de seus negócios. Tendo em vista que o teste de *software* é a última revisão antes de o produto ser lançado ao mercado e que em caso de uma parada crítica da ALFA, não somente os seus clientes serão afetados, mas toda a rede que depende da disponibilidade do *software* testado, aprovado para utilização. A parada do serviço estaria afetando e colocando em risco uma cadeia de fornecimento, onde ocorreriam prejuízos e transtornos incalculáveis, afetando a imagem da ALFA, lucro da empresa cliente que deixa de colocar o *software* em produção e que por sua vez afeta os acionistas. Desta forma a empresa ALFA vem trabalhando para satisfazer as exigências do mercado, fazendo com que a empresa busque a melhor alternativa para adoção e implantação destes requisitos que são considerados estratégicos para a empresa.

Para atender a exigências de clientes críticos e manter a boa imagem da empresa, em caso de algum tipo de desastre, evitando que a ALFA seja responsável por afetar a cadeia de valores de todas as empresas envolvidas no projeto e seus *stakeholders*, torna-se viável para a empresa ALFA um PCN que venha a garantir a segurança nos serviços prestado, diferenciando a oferta de prestação de serviços e garantindo maior qualidade e credibilidade perante os de clientes.

Este estudo é oportuno para garantir a continuidade dos serviços e do negócio da empresa ALFA através de um PCN baseado em práticas como a NBR 15999, ITIL e COBIT, fazendo com que a empresa atenda expectativas de clientes internos e externos, no menor espaço de tempo em caso de incidente maior que afete instalações, informações ou pessoas. Segundo Fernandes e Abreu (2008), o objetivo das práticas do COBIT é contribuir com o sucesso na entrega de serviços e produtos de TI a partir das necessidades do negócio, mantendo o foco no controle. O objetivo do ITIL é prover um conjunto de práticas de gerenciamento de serviços em TI com foco no alinhamento e integração com a necessidade dos clientes e usuários.

Segundo a NBR 15999-1 (2007, pg. 31), o propósito no PCN é “permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais do negócio”. Desta forma, utilizando como base as necessidades encontradas junto à empresa, seria elaborado um plano de continuidade de negócio de forma a contingenciar os recursos que afetam diretamente as atividades identificadas como críticas na empresa.

5 OBJETIVOS

Neste capítulo são apresentados o objetivo geral e os objetivos específicos do trabalho.

5.1 OBJETIVO GERAL

Definir um Plano de Continuidade de Negócio baseado nas práticas mais utilizadas pelas organizações, que permita à empresa qualificar as suas operações e atender as expectativas dos clientes internos e externos.

5.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos a serem alcançados são:

a) Identificar os elementos componentes de um PCN;
b) Avaliar pontos críticos e vulneráveis a riscos;
c) Elaborar um PCN de acordo com a NRB 15999:2007, a metodologia COBIT e as melhores práticas do ITIL.

6 REFERENCIAL TEÓRICO

Este capítulo abordará o referencial teórico utilizado para estudo e argumentação do trabalho.

6.1 TI NAS ORGANIZAÇÕES

Atualmente a TI tem sido considerada como um dos componentes mais importantes nas organizações, sendo que empresas brasileiras intensificaram o uso da TI tanto no nível estratégico como no operacional. Este nível de utilização oferece grandes oportunidades para as empresas quando há sucesso na utilização e aproveitamento dos benefícios oferecidos pelo uso. A oferta de TI e seu aproveitamento amplo e intenso pelos diversos setores das organizações têm sido considerados condições básicas para a competitividade e sobrevivência das organizações. (ALBERTIN e ALBERTIN, 2005a).

Luciano e Freitas (2005) afirmam que a Tecnologia da Informação tem contribuído para a busca de vantagens competitivas entre as empresas como ferramenta capaz não só de reduzir custos e conferir qualidade a produtos e serviços, mas como forma de agregar valor ao negócio através de melhor conhecimento e atendimento às expectativas dos clientes, assim como a criação de novos produtos e serviços. Para Borges (1995) a TI, como ferramenta gerencial, é utilizada para análise dos dados, transformando-os em informações úteis ao negócio da empresa. Conforme as empresas convertem dados em informações, modificam seu processo de decisão, sua estrutura administrativa e sua maneira de trabalhar, fazendo com que decisões oportunistas transformem-se em diretrizes e estratégias.

Laurindo (2002) afirma que nenhuma aplicação de TI, considerada isoladamente, pode manter uma vantagem competitiva, sendo que a competitividade somente poderá ser obtida com a capacidade que a empresa tem de explorar de forma contínua o uso da TI. O autor afirma ainda que o uso eficaz da TI e a integração da estratégia de TI à do negócio são fatores de sucesso para as organizações.

O uso da TI deve ser avaliado por meio de suas dimensões, direcionadores, tipos de uso de TI, desempenho empresarial, administração de TI e executivos de negócio, assim como as relações existentes entre elas. A partir desta identificação foi sugerido pelos autores o Modelo das Dimensões do Uso de TI em Benefício aos Negócios, conforme Figura 2. (ALBERTIN e ALBERTIN, 2005a).

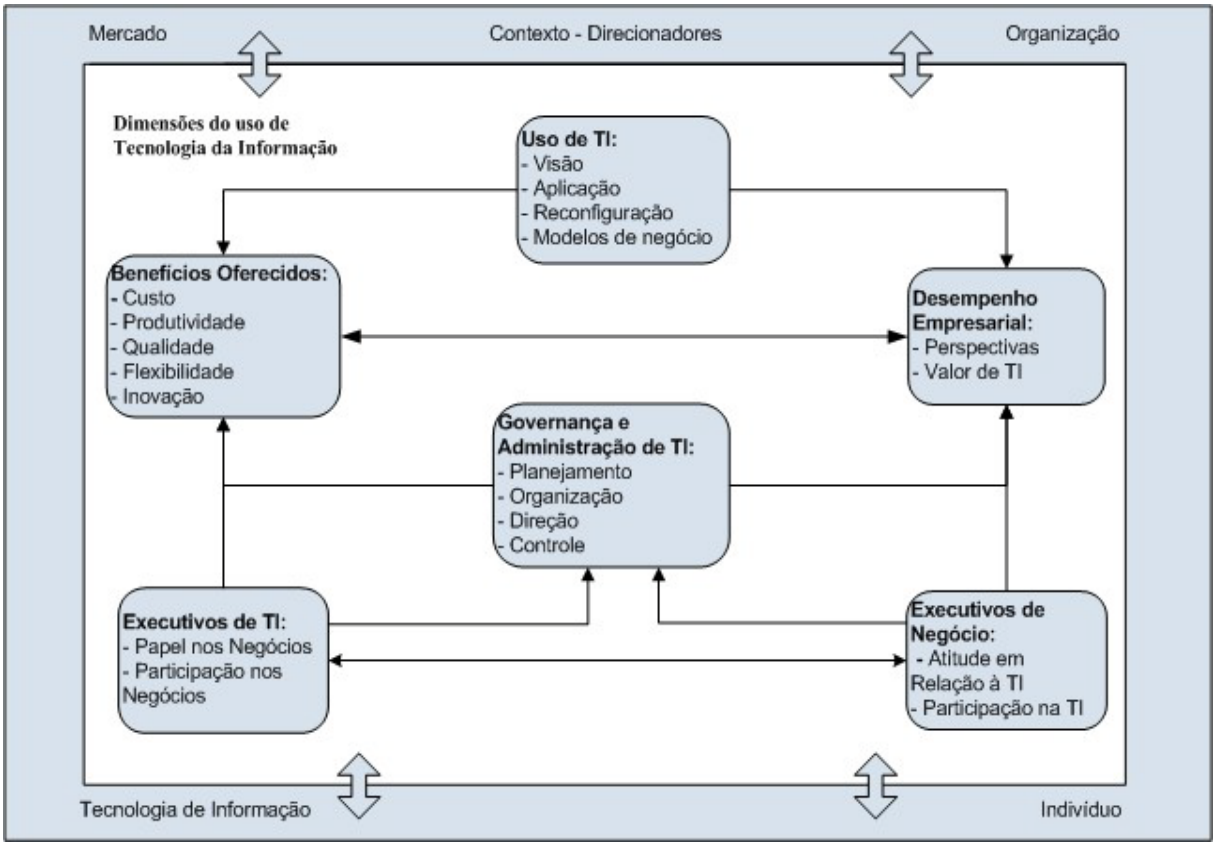

Figura 2: Modelo das dimensões do uso de TI em benefício dos negócios
Fonte: Albertin e Albertin (2005b)

Segundo Albertin e Albertin (2005a), para as organizações o uso da TI é muito importante, pois orienta as ações internas e externas conforme os objetivos, estratégias e operação. O valor que a TI oferece está relacionado com os direcionadores de respostas organizacionais e a qualidade dos estudos destes direcionadores, assim como as diversas aplicações de TI disponíveis para as organizações que possuem níveis diferentes de necessidades, onde ela pode contribuir inclusive para elaboração de novos modelos de negócio.

O aproveitamento dos benefícios ocasionados pelo uso da TI nas organizações, tanto na infraestrutura, como sua aplicação nos processos organizacionais oferece benefícios como custo, produtividade, qualidade, flexibilidade e inovação que deverão ser mensurados nos negócios (ALBETIN, ALBERTIN, 2005a).

Para Foina (2006), a Tecnologia da Informação se propõem a garantir a qualidade e pontualidade das informações dentro das organizações através do uso adequado da tecnologia. Desta forma, assim como outras áreas da empresa, a área de TI também exige um Planejamento Estratégico. O PETI - Planejamento Estratégico de Tecnologia da Informação requer alterações e atualizações conforme as mudanças tecnológicas do ambiente (interno ou

externo). Para o autor o Planejamento Estratégico de TI pode ser dividido da seguinte maneira:

- diagnóstico da situação atual da empresa;
- estabelecimento da situação desejada para o período de planejamento;
- definição das políticas e diretrizes básicas;
- estabelecimento dos Planos de Ação (Táticos).

Devido à crescente utilização tecnológica, além da complexidade e mudança que ocorrem no ambiente externo e interno das organizações e mercado, os desafios da administração de TI têm aumentado. A administração de TI, por ser responsável pelas definições e ações decorrentes do uso da TI, deve ser decorrente do modelo de governança de TI (ALBERTIN, 2005, p.29).

Weill e Ross (2006) afirmam que a unidade de TI não pode ser a única, nem a principal, responsável pelo sucesso do uso da informação e da Tecnologia da Informação, e que é de competência dos líderes organizacionais a capacidade de extrair o maior valor da TI. Empresas com melhor desempenho são aquelas que implantam uma Governança de TI eficiente para sustentar sua estratégia e que “uma governança de TI eficaz é o indicador mais importante do valor que a organização aufere com a Tecnologia da Informação”.

6.2 GOVERNANÇA DE TI

A Governança Corporativa teve sua importância destacada nos negócios devido à gravidade dos impactos causados pelos escândalos corporativos em meados de 2002, em algumas organizações como Enron, Worldcom e Tyco. A governança corporativa não era nova, mas os impactos financeiros causados pelos escândalos fizeram com a confiança de investidores (institucionais e individuais) fosse abalada e que empresas privadas viessem a ter um aumento significativo na preocupação em proteger as pessoas envolvidas nos negócios das organizações. Devido aos impactos ocasionados mundialmente, houve intervenção do governo dos EUA e uma nova legislação passou a exigir mais rigor e exatidão, aumentando o nível de autorregulamentação (WEILL e ROSS, 2006).

Para Fernandes e Abreu (2008), vários fatores motivam a Governança de TI, embora o senso comum considere que a transparência da administração seja o principal motivador desse movimento no ambiente de TI das organizações, conforme apresentado na Figura abaixo.

Figura 3: Motivadores da Governança de TI
Fonte: Fernandes e Abreu (2008, pg. 9)

Ainda, segundo o autor, a implantação de um Programa de Governança de TI justifica-se pela necessidade de sucesso e funcionamento adequado de centros de serviços compartilhados, desta forma se faz necessários processos de TI, eficaz e eficiente.

Segundo Weill e Ross (2006, p. 8), Governança de TI pode ser entendida como "a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI". A definição de Governança de TI inserida pelos autores, apresenta que a governança determina quem tem os direitos decisórios e quem toma as decisões através de mecanismos e procedimentos operacionais que assegurem que os objetivos sejam atingidos.

Fernandes e Abreu (2008) ainda concluem que a Governança de TI objetiva o compartilhamento de decisões de TI com os demais dirigentes da organização, assim como estabelecer as regras, a organização e os processos que envolverão o uso da tecnologia da informação pelos setores e usuários da organização, assim como os clientes e fornecedores, desta forma a Governança de TI determina como a TI deve prover os serviços para a empresa.

A visão de Governança de TI apresentada por Fernandes e Abreu (2008), é representado pelo que chamam de "Ciclo de Governança de TI". Este ciclo é composto por

quatro etapas: (1) alinhamento estratégico e *compliance*, (2) decisão, (3) estrutura e processo e (4) medição do desempenho da TI, conforme representado pela Figura 4.

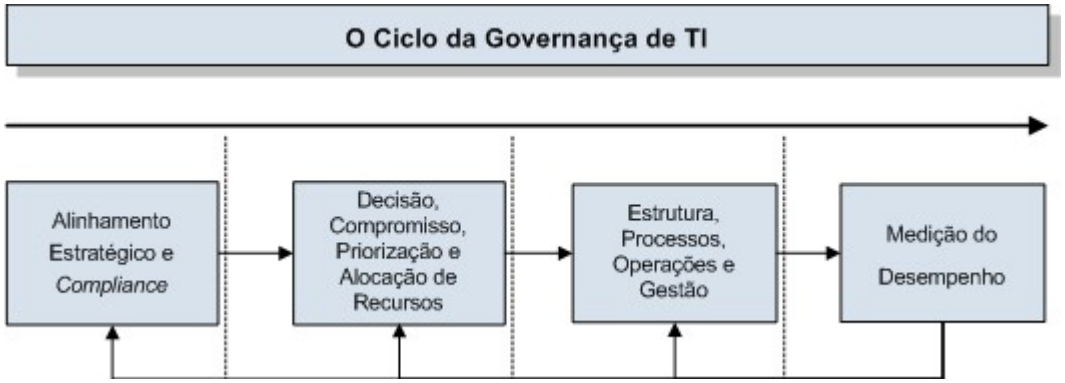

Figura 4: O ciclo da Governança de TI
Fonte: Fernandes e Abreu (2008, p.14)

No Ciclo de Governança de TI apresentando pelo referido autor, cada etapa refere-se a uma situação, conforme apresentado:

A etapa (1), Alinhamento Estratégico e *compliance*, referem-se ao Planejamento Estratégico de TI alinhado com o Planejamento Estratégico de outras áreas da empresa, assim como os requisitos de *compliance* externos.

Etapa (2) decisão, compromisso, priorização e alocação de recursos, definem o processo de tomada de decisões, em que ocasião serão realizadas as decisões relativas a TI, como a arquitetura de TI, serviços de infraestrutura, investimentos, necessidade de aplicação e outros.

A etapa (3) que inclui estrutura, processos, operações e gestão, refere-se à estrutura organizacional e funcional da TI, assim como os processos de gestão e operações dos serviços e produtos de TI. Nesta fase, alinhados com as necessidades estratégicas da empresa, são definidos ou redefinidos operações da empresa, suporte técnico, infraestrutura de TI, segurança da informação, etc.

Por último a etapa (4), medição do desempenho, que abrange coleta de dados e conclusão dos indicadores de resultados referentes ao processo, produtos e serviços de TI e sua contribuição para os objetivos da empresa.

Conforme Albertin e Albertin (2005a), a Governança de TI encontra desafios em suas próprias funções como o alinhamento aos objetivos do negócio, a busca de benefícios (inovação), o melhor aproveitamento dos gastos e aumento da eficiência pela TI e o gerenciamento de riscos de investimentos de TI.

6.2.1 Componentes da Governança de TI

Weill e Ross (2006) afirmam que uma boa governança de TI deve harmonizar decisões da administração e a utilização de TI com os objetivos do negócio. Os autores relacionam cinco decisões de TI que, inter-relacionadas, objetivam uma governança eficaz, onde uma decisão motiva e influencia a outra. Estas decisões são:

- Princípios de TI – inclui um conjunto de declarações de alto nível sobre com a tecnologia da informação é utilizada no negócio. Este conjunto de declarações referentes aos princípios de TI, também ajudam os administradores na tomada de decisões sobre as estratégias tecnológicas e sobre os investimentos em tecnologia que devem ser realizados. Como os princípios orientam todas as decisões de TI, qualquer equívoco atinge as outras quatro decisões comprometendo a eficácia das mesmas;
- Arquitetura de TI – define os requisitos de integração e padronização dos processos do negócio, estabelecendo uma organização lógica para os dados e provendo o direcionamento para a infraestrutura e aplicações;
- Infraestrutura de TI – determina a base do planejamento de TI, tanto técnica quanto humana, que está disponível em todo negócio como forma de serviços compartilhados e de suporte. É de decisão essencial da infraestrutura determinar os locais em que a infraestrutura deve ser posicionada, como devem ser avaliados e quando devem ser atualizados ou terceirizados. Mantendo uma infraestrutura correta faz com que a empresa tenha capacidade de adotar rapidamente novas aplicações de negócio;
- Necessidades de Aplicação de negócio – é considerada a menos madura das cinco decisões, pois requer criatividade e disciplina por parte dos gerentes. Esta decisão especifica a necessidade comercial de TI comprada ou desenvolvida internamente.
- Investimentos e priorização de TI – é a decisão que frequentemente é observada como sendo a mais controversa das cinco, pois envolve escolher quais projetos financiar e quanto gastar.

Fernandes e Abreu (2008, p.15) afirmam que “o principal objetivo da Governança de TI é alinhar a TI aos requisitos do negócio”. O alinhamento tem o objetivo de garantir a continuidade do negócio, atendo as estratégias e compliance. O autor apresenta as etapas da

Governança de TI da seguinte forma:

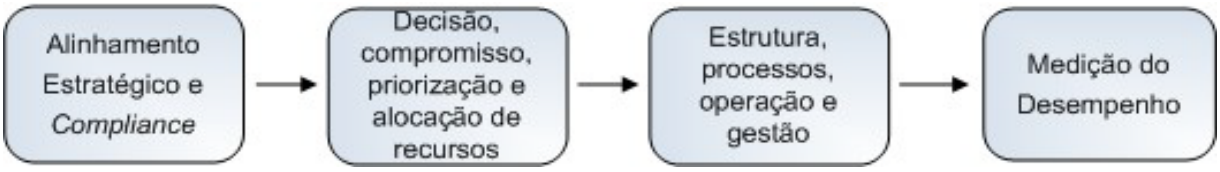

Figura 5: Os domínios e competences da Governança de TI
Fonte: Fernandes e Abreu (2008, p. 17)

Entre os componentes da etapa Estrutura, Processos, Operação e Gestão, está o componente Operações de Segurança da Informação, que contempla atividades relacionadas à segurança da infraestrutura de TI, como aplicativos, monitoramento da segurança, conscientização da segurança da informação, gestão de problemas de segurança de informação, elaboração de plano de continuidade do negócio, análise de vulnerabilidade de segurança da informação, assim como outras atividades relacionadas à segurança da informação.

6.3 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Segundo Caruso e Steffen (1999), o bem mais valioso que uma organização possui é a informação. Devido ao alto grau de relevância que a informação possui para a organização, muitas empresas não sobrevivem mais que poucos dias a um colapso do fluxo de informações, não importando o meio de armazenagem das informações. É importante que as organizações integrem ao ambiente de informação medidas de segurança efetiva a um custo aceitável.

Conforme Sêmola (2003) a Segurança da Informação tem o objetivo de proteger os ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. A segurança da informação pode ser considerada como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três princípios básicos da segurança da informação:

- Confidencialidade – a informação deve ser protegida conforme o seu grau de confidencialidade, limitando o acesso e uso destas informações por pessoas não autorizadas;
- Integridade – a informação deve ser protegida contra alterações indevidas, acidentais ou intencionais, visando manter sua originalidade;

- Disponibilidade – toda informação gerada ou adquirida deve estar disponível aos seus usuários no momento em que ela for necessária.

Segundo Silva et al. (2008) a segurança da informação formaliza seis serviços de segurança:

- Autenticação - prevê a garantia da identidade de um usuário;
- Autorização – realiza o controle de acesso, protegendo contra acesso não autorizado;
- Privacidade – assegura que dados sigilosos não serão revelados a pessoas não autorizadas;
- Integridade – protege contra alterações de dados, inserção ou remoção imprópria;
- Não-repúdio - garante as evidências durante a comunicação impedindo que partes envolvidas neguem sua participação;
- Disponibilidade – garante que os sistemas, dados e recursos estejam disponíveis para uso sem qualquer impedimento. Também garante a rápida disponibilidade no caso de incidentes.

Estes serviços tornam os ativos protegidos contra ameaças à segurança da informação e quando utilizados em conjunto com outras metodologias de segurança, tem com o objetivo de assegurar a garantia total do sistema.

6.4 GESTÃO DA CONTINUIDADE DO NEGÓCIO

Conforme declaração do presidente e diretor da DRI – *Disaster Recovery International*, Johon Copenhaver, a importância do Plano de Continuidade dos Negócios é hoje reconhecida mundialmente. Não importa onde a empresa está localizada, ela deve ser preparada para contingenciar incidentes (COPENHAVER, 2007). Este reconhecimento se deu recentemente, após grandes desastres ocorridos, como o poderoso tsunami no Pacífico, furacão Katrina, o ataque terrorista de 11 de setembro em 2001 nos EUA. Estes são alguns exemplos que causaram impactos significativos em pessoas e organizações do mundo, fazendo com que grandes empresas viessem a se preocupar com o planejamento da continuidade dos seus negócios, pois atualmente é difícil encontrar empresas que não possuem tecnologia de informação e que se preocupem com a segurança destas informações. Mesmo com o reconhecimento desta importância, ainda hoje muitas companhias não possuem um plano de continuidade (SNEDAKER, 2007).

O plano de continuidade dos negócios tem o objetivo de garantir a continuidade dos processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível com o objetivo de reduzir os impactos de incidentes. O plano tem alto nível de complexidade, pois pode assumir diversas formas devido à abrangência de sua atuação, sendo formado por diversos planos integrados e focados em diferentes meios, como físicos, tecnológicos ou humanos (SÊMOLA, 2003).

Conforme declaração de Stanton (2007) à revista InfoSecurity uma boa estratégia de continuidade de negócios começa com a idéia de que falhas podem acontecer, onde se deve observar o risco em cada ambiente para avaliar se o planejamento da continuidade é necessário. Para Smitth e Sherwood (1995) a primeira etapa do processo de planejamento é a análise de risco e do impacto do negócio, pois o planejamento da continuidade deve preservar os serviços e assistências essenciais aos clientes, confiança do cliente (interno e externo) e a imagem pública da organização. O processo de planejamento da continuidade do negócio deve determinar os impactos que seriam sofridos pelo desastre, identificando as funções críticas e os recursos críticos dependentes das funções, assim como determinar prazos para a recuperação das funções conforme sua ordem de prioridades. Os autores apresentam um esboço para o processo de planejamento, conforme apresentado na Figura 6 abaixo.

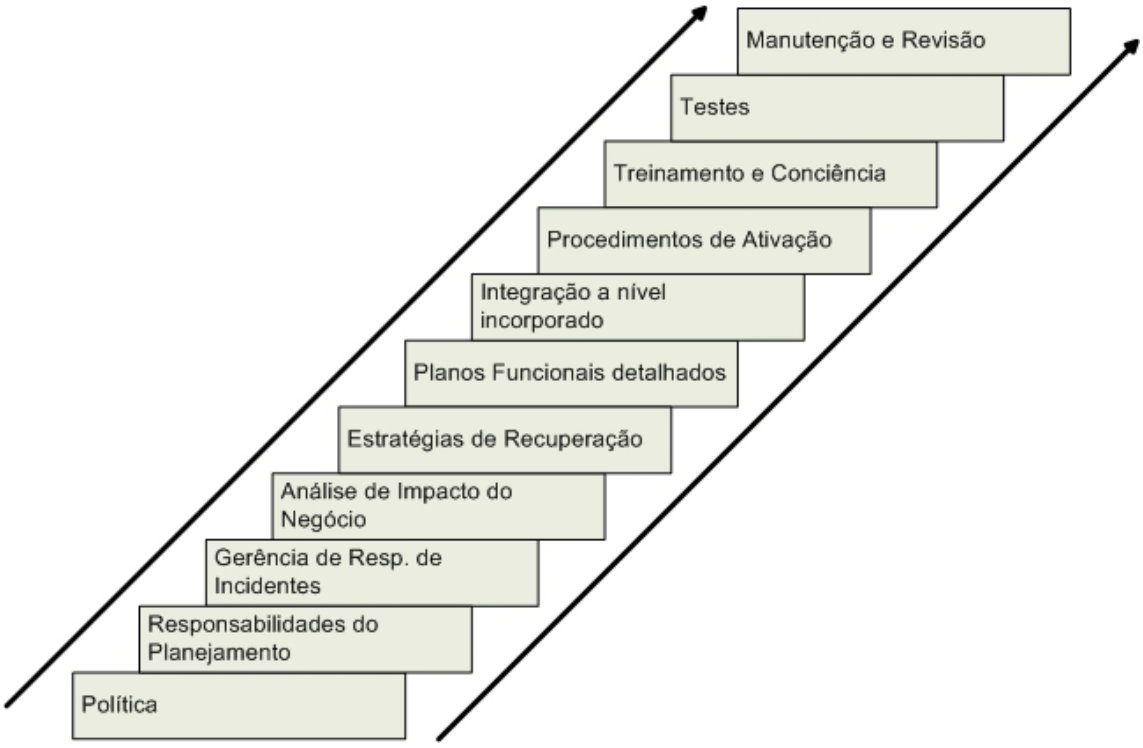

Figura 6: Plano de Continuidade dos Negócios – Etapas a seguir
Fonte: Smitth e Sherwood (1995, p. 17)

A NBR ISO/IEC 17799 (2005, p.103) propõem que o objetivo da gestão da continuidade do negócio é “não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas e desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.”. Ainda segundo a mesma norma, o processo de gestão da continuidade do negócio deve agregar os seguintes elementos:

a) Identificação dos riscos ao qual a organização está exposta, probabilidade do risco ocorrer e o impacto no tempo, assim como a identificação e priorização dos processos críticos do negócio;
b) Levantamento de todos ativos envolvidos nestes processos críticos;
c) Entendimento do impacto que incidente de segurança da informação possam ocasionar sobre o negócio;
d) Consideração quanto à contratação de seguro para continuidade do negócio;
e) Controles preventivos e mitigação;
f) Identificação dos recursos da organização (financeiros, organizacionais, técnicos e ambientais) de forma a identificar os requisitos de segurança;
g) Garantia da segurança de pessoal e proteção das informações e dos bens da organização;
h) Elaboração detalhada dos planos de continuidade do negócio contemplando os requisitos de segurança;
i) Testes e manutenções dos planos e processos;
j) Garantia de que a gestão da continuidade está incorporada aos processos da organização e gerenciamento dos processos de gestão da continuidade pela alta gerência da organização.

6.4.1 Etapas que envolvem o Plano de Continuidade dos Negócios

Nesta subseção será apresentada a visão de diferentes autores sobre algumas etapas que são requisitos para elaboração do PCN, sendo que outras etapas, como treinamentos, testes e manutenção, servem para posterior elaboração, onde o plano é avaliado e ajustado.

a) Política de Segurança da Informação

Segundo Caruso e Steffen (1999) é de grande importância que as organizações cerquem o ambiente de informação com medidas de segurança efetiva a um custo aceitável.

Para isto, uma política de segurança deve ser elaborada, implantada e deve permanecer em contínuo processo de revisão.

A política de segurança deve conter regras claras e simples, deve contemplar aspectos dos ativos de informações quanto à proteção contra acessos não autorizados e prevenção contra incidentes. Além da proteção física e lógica, a política de segurança deve contemplar a recuperação das operações em caso de destruição total ou parcial das atividades. Para Carvalho (2003), a elaboração de uma política de segurança tem o propósito de definir diretrizes, normas, procedimentos e descarte de informação, ela deve formalizar parâmetros e oficializar um código de conduta no trato de informações.

Conforme a NBR ISO/IEC 17799 (2005p. 103) “Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.”.

b) Responsabilidades do Planejamento

Entre outras coisas, a política deve definir as responsabilidades da gerência para o planejamento da continuidade do negócio. É essencial que estas responsabilidades sejam delegadas ao nível superior dentro da estrutura de gerência, encarregando pessoas capacitadas e responsáveis. As responsabilidades de planejamento são da gerência em geral, pois devem administrar o cumprimento do plano caso seja necessário. Para as organizações, o critério principal de sucesso é a habilidade da gerência em estruturar e suportar o agravamento no menos espaço de tempo possível, com eficiente de respostas do problema, delegação das ações e agilidade da tomada de decisão (SMITH e SHERWOOD, 1995).

c) Análise de Riscos

A análise de riscos e vulnerabilidades objetiva diagnosticar a situação atual da segurança da empresa, através do mapeamento dos processos do negócio e o relacionamento deles com os ativos físicos, tecnológicos e humanos que tendem a falhas de segurança. (SÊMOLA, 2003). O autor ainda apresenta a relação de dependência entre os ativos, conforme Figura 7.

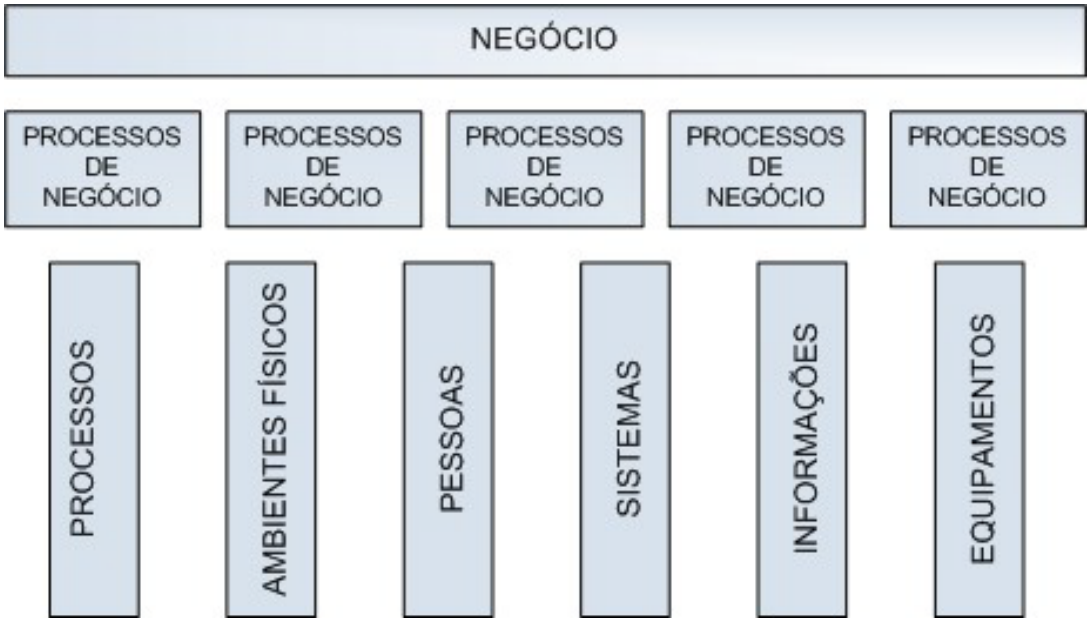

Figura 7: Relação de dependência entre ativos, processos e o próprio negócio
Fonte: Sêmola (2003, p. 109)

Para a análise de riscos existem duas linhas metodológicas para orientação. A quantitativa, que mensura os impactos financeiros provocados por incidentes, e a qualitativa, que permite estimar os impactos ao negócio provocados pela vulnerabilidade de ameaças. Ainda segundo o autor, devem ser considerados os seguintes aspectos para Análise dos Riscos:

a) Identificação da relevância que o processo do negócio tem para organização;
b) Identificação da dependência dos processos de negócio com o ativo;
c) Entendimento do impacto resultante, no caso de ocorrência de uma ameaça;
d) Probabilidade da ameaça ocorrer;
e) Severidade potencial na exploração no ativo;
f) Qualificação das vulnerabilidades presentes no ativo;
g) Qualificação das ameaças potenciais.

Após identificação da probabilidade e severidade de uma ameaça atingir cada vulnerabilidade encontrada para o ativo, deve-se projetar o nível do risco de cada processo do negócio considerando o risco de cada ativo. A Figura 8 representa o risco medido pela relação de probabilidade e impacto.

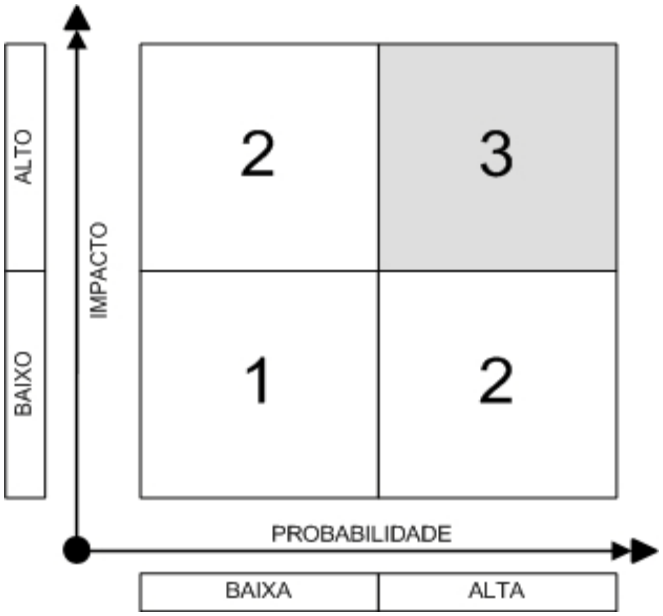

Figura 8: Quadrante do Risco medido pela relação de Probabilidade e Impacto
Fonte: Sêmola (2003, p. 112)

Caruso e Steffen (1999) consideram a relação da segurança de ativos de informação com custo/benefício, onde não se deve gastar mais dinheiro em segurança do que o valor do ativo protegido. Os autores ainda apresentam como forma mais eficiente de se obter a análise de custo/benefício, fazer com que os próprios usuários de cada sistema avaliem o valor para a organização, pois afirmam que quem trabalha com as informações é o mais indicado para fazer a análise do risco. Os autores apresentam o fluxo de análise das ameaças conforme a Figura 9.

Figura 9: Fluxo de análise das ameaças
Fonte: Caruso e Steffen (1999, p.67)

Segundo a NBR ISO/IEC 17799 (2005, p. 104) “convém identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as consequências para a segurança da informação.”

d) Análise de Impacto nos Negócios

A análise de impacto do negócio envolve a identificação de funções críticas do negócio dentro da organização, determinando o impacto de não executar a função do negócio e de não verificar as implicações do custo. As finalidades de uma análise de impacto são:

- Identificar os riscos potenciais;
- Estimar os efeitos de um desastre no conjunto da organização;
- Definir as exigências para uma estratégia de recuperação, incluindo os recursos necessários para a recuperação;
- Fornecer recursos financeiros para a preparação e recuperação do desastre;
- Determinar a criticidade de cada função do negócio baseado no impacto total da organização e estabelecer prioridade de recuperação;
- Avaliar os impactos financeiros e operacionais, determinando os efeitos quando possível, como estimativa de rendimentos perdidos e produtividade;
- Determinar prazos para a recuperação das funções.

Desta forma pode-se identificar o que é critico para manter a organização em operação e determinar a abrangência do plano de continuidade (DEVARGAS, 1999).

e) Estratégias de Contingências

Ao avaliar as opções para recuperação da função do negócio, devem-se utilizar critérios que assegurem que a estratégia esteja disponível e seja útil para a recuperação. A habilidade de contatar os recursos responsáveis pela recuperação é muito importante, portanto deve-se manter uma lista de contatos, equipamentos, telefones, softwares e outras informações necessárias e fundamentais para colocar o PCN em funcionalidade (TEXAS DEPARTMENT OF INFORMATION RESOURCES, 2004). Segundo Sêmola (2003), as estratégias de contingência são agrupadas normalmente nas seguintes categorias:

a) Hot-site: refere-se a uma estratégia pronta para entrar em operação assim que uma situação de risco ocorrer, onde o tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falhas;
b) *Warm-sites*: se aplica a funções que possuem maior tolerância à paralisação, podendo permanecer indisponível por mais tempo até o retorno operacional da atividade. Um exemplo é o serviço de e-mail;
c) Realocação de Operações: esta estratégia tem a função de desviar a atividade

atingida para outro ambiente físico, equipamento ou *link*, pertencente a mesma empresa. Esta estratégia se torna possível quando há recursos disponíveis para alocação em situações de crise;

d) Bureau de serviços: esta estratégia tem o objetivo de transferir as funções atingidas para um ambiente terceirizado, fora dos domínios da empresa. Esta estratégia torna-se restrita a algumas operações pelo tempo de tolerância maior em função da reativação operacional da atividade;

e) Acordo de reciprocidade: esta estratégia é conveniente para contingências que demandariam investimentos altos, pois propõem um acordo formal com empresa semelhante que também esteja disposta a possuir uma alternativa de continuidade operacional. As empresas estabelecem as situações de contingência e definem os procedimentos de compartilhamento de recursos para alocação das atividades atingidas no ambiente da outra empresa;

f) *Cold-site*: este modelo propõe uma alternativa de contingência aplicável em situações com tolerância de indisponibilidade ainda maior, pois propõem um ambiente com recursos mínimos de infraestrutura e telecomunicações, desprovidos de recurso de processamento de dados;

g) Autosuficiência: esta estratégia é aplicada quando não há outra possibilidade de estratégia para determinada atividade. Geralmente ocorre quando nenhuma outra estratégia se aplica à atividade, quando os impactos não são significativos ou quando se torna inviável financeiramente, tecnicamente ou estrategicamente.

f) Planos Funcionais Detalhados

Conforme as estratégias de contingência definidas, os planos detalhados devem ser elaborados para mostrar como a resposta e a recuperação será efetuada. O planejamento detalhado do plano deve ser efetuado necessariamente pelas pessoas responsáveis pelo conhecimento técnico específico do negócio (SMITH e SHERWOOD, 1995).

Sêmola (2003) apresenta a divisão dos planos em três módulos distintos e complementares que tratam cada situação da empresa:

a) Plano de administração de crise – tem o objetivo de descrever o passo a passo do funcionamento das equipes envolvidas no plano de contingência antes, durante e depois da ocorrência do incidente;

b) Plano de continuidade operacional – descreve os procedimentos de contingência

para os ativos que suportam cada processo de negócio, com o objetivo de diminuir o tempo de indisponibilidade e impactos ao negócio;

c) Plano de recuperação de desastres – objetiva definir um plano de recuperação e restauração das funcionalidades dos ativos afetados pelo incidente, com a finalidade de estabelecer as condições originais.

g) Integração ao nível Incorporado

Nesta etapa, conforme Smitth e Sherwood (1995), cada unidade de negócio deve desenvolver seus próprios planos, após o desenvolvimento do plano por cada unidade, deve-se integrar e coordenar os planos, assegurando que os objetivos sejam alcançados.

h) Procedimentos de Ativação

Para cada plano deve haver um procedimento claro e definido, apresentando porque o incidente é relatado, escalado, confirmado e então selecionado para ser ativado em resposta ao incidente. Estes procedimentos devem ser definidos para todos os planos (SMITH e SHERWOOD, 1995).

i) Treinamento e Consciência

Conforme Herbane, Elliott e Swartz (2004) as organizações que procuram inserir a continuidade dos negócios ao processo de trabalho podem utilizar uma combinação de meios para comunicar sua relevância, onde podem ser realizados treinamentos, exercícios do levantamento de consciência e reuniões para levantar as necessidades. Estas medidas refletem a importância da continuidade dos negócios para a organização

j) Testes

As etapas de análise e desenvolvimento do PCN são apenas o começo. O teste e a manutenção objetivam a validação e a atualização da documentação já elaborada. Os testes, também chamados de exercícios, têm a finalidade de expor as áreas do plano que necessitam ser revisadas, demonstram as ações de proteção a serem tomadas antes de um evento ocorrer, pois a execução do teste demonstra como o plano trabalhará, caracterizando se a recuperação será bem sucedida ou não.

A execução dos testes deve se concentrar nas funções prioritárias do negócio, conforme a determinação da análise se impacto. Sendo que cada vez que forem executados os

testes e realizada atualização ou alteração do plano, é necessário que sejam executados novos testes para validação da manutenção do plano (TEXAS DEPARTAMENT OF INFORMATION RESOURCES, 2004).

k) Manutenção e Revisão

O plano de continuidade exige esforços que devem ser realizados para mantê-lo dentro das mudanças tecnológicas e exigências de segurança. O plano de continuidade deve ser freqüentemente avaliado para medir a eficácia do programa e a consciência da organização perante a sua importância, onde deve ser verificada a necessidade de treinamentos. Deve-se avaliar se os procedimentos estão sendo seguidos para a segurança e os resultados devem ajudar a identificar e corrigir problemas (DEVARGAS, 1999).

6.4.2 Gestão de Continuidade do Negócio segundo NBR 15999-1:2007

A criação da NBR 15999-1: 2007 ocorreu através do conhecimento e experiências de especialistas da comunidade de continuidade de negócios. A norma tem por objetivo apresentar melhores práticas para a gestão da continuidade de negócios, servindo como referência para as organizações e aos setores interessado (NBR 15999-1, 2007).

A norma sugere que se estabeleça uma Gestão da Continuidade dos Negócios (GCN), onde a alta direção seja responsável pelos processos de gestão e governança, mantendo as estratégias e os planos de recuperação de forma a garantir a continuidade do negócio, sendo que para a garantia da continuidade do negócio, devem-se realizar treinamentos, testes, manutenção e análise crítica dos planos. Para a norma 15999-1, o GCN é um processo da organização que deve estabelecer uma estrutura estratégica e operacional adequada para preparar a organização contra possíveis paradas não planejadas, retomada dos serviços dentro de um prazo predeterminado e capacidade de gerenciar uma parada de forma a proteger e manter a imagem da organização.

A norma ainda segue o modelo *Plan-Do-Check-Act* (PDCA) que se aplica a todas as partes do ciclo de vida da gestão da continuidade de negócio, de forma a garantir que a continuidade do negócio esteja devidamente gerenciada (NBR 15999-2, 2007).

O ciclo de vida da gestão da continuidade de negócio, apresentado a NBR 15999-1: 2007, apresenta seis elementos, sendo que estes elementos podem ser implementados em

organizações de diversos setores. A seguir, a Figura 10 ilustra o ciclo de vida da gestão da continuidade de negócios proposto pela norma 15999-1.

Figura 10: Ciclo de vida da gestão da continuidade de negócios
Fonte: ABNT NBR 15999-1 (2007, p. 8)

O ciclo de vida da gestão da continuidade, apresentado pela norma, é composto por seis elementos, onde são apresentadas algumas diretrizes conforme descrição abaixo:

a) Gestão do Programa de GCN

- Atribuição de responsabilidades, onde se deve determinar as pessoas responsáveis por implementar e manter o programa de GCN;
- Implementação da continuidade do negócio na organização, nesta etapa deve-se realizar a comunicação do programa aos interessados, treinamentos e testes para validação do PCN;
- Gestão contínua da continuidade do negócio, onde se deve realizar analise crítica dos planos e soluções de continuidade do negócio, manutenção nos processos, documentos e estratégias de continuidade. Nesta etapa também ocorre elaboração dos documentos de continuidade.

b) Entendendo a Organização

- Identificar os objetivos da organização, as atividades, os ativos, os recursos (externos e internos);
- Realizar a Análise de Impacto, avaliando o impacto e consequências sobre o tempo de falha das atividades, podendo estabelecer períodos como tempo máximo de parada de uma atividade, nível mínimo de desempenho da atividade após seu reinício e tempo máximo de retomata dos níveis normais.
- Identificação das Atividades críticas;
- Determinação dos requisitos de continuidade, determinando os recursos necessários para cada atividade durante a recuperação. Os requisitos devem ser aprovados pela alta direção;
- Avaliação dos riscos, para entendimento dos riscos, critérios de aceitação, níveis de aceitação e estratégias de avaliação dos riscos para as atividades críticas da organização.

c) Determinando as estratégias de continuidade de negócios, onde se devem estabelecer soluções adequadas de forma a minimizar os efeitos de um incidente, fornecendo continuidade às atividades críticas durante e após o incidente. A norma ainda menciona que é importante que a organização possua estratégias para as atividades críticas e paras os recursos que serão utilizados nestas atividades durante a restauração. As estratégias dependem de fatores como o período máximo de interrupção, custo de implementação e as consequências causadas pela não execução da estratégia. Ainda segundo a ISO, as estratégias são necessárias para os seguintes recursos pessoas, instalações, tecnologia, informação, suprimentos e partes interessadas, conforme as necessidades da empresa. As estratégias também devem passar pela aprovação da alta direção;

d) Desenvolvendo e implementando uma resposta de GCN, neste elemento deve-se elaborar e implementar os planos detalhados de continuidade conforme a análise e identificação dos riscos. O conteúdo dos planos deve conter:

- Objetivo e Escopo, onde se deve detalhar o objetivo do plano e o escopo das atividades críticas que necessitem de recuperação, assim como o tempo e nível de recuperação;

- Papéis e responsabilidades, onde deve definir as pessoas envolvidas durante e após o incidente, assim como os seus papéis;
- Ativação de planos, onde ocorre o detalhamento das informações sobre o critério para ativação dos planos, forma de comunicação com a equipe e locais de encontro;
- Proprietário, indicação do principal responsável pelo plano;
- Detalhes de contado, onde se devem incluir no plano as informações dos contatos interessados.

Além do conteúdo dos planos conforme descritos acima, a elaboração do plano ainda deve ser realizada em duas etapas:

- Plano de Gerenciamento de Incidentes (PGI) – tem por objetivo gerenciar a fase inicial de um incidente, de forma a cobrir os principais recursos necessários para o gerenciamento do incidente.
- Plano de Continuidade de Negócios (PCN) – tem por objetivo recuperar e manter os serviços e atividades da organização em caso de interrupção.

A norma ainda menciona que, para empresas pequenas, pode-se incluir em um único documento todos os planos de continuidade elaborados para os recursos da organização, não sendo necessária a elaboração de um documento para cada risco. Quanto ao Plano de Retorno, a norma diz que este pode ser planejado enquanto a empresa está operando com o PCN.

e) Testando, mantendo e analisando criticamente os preparativos de GCN

- Elaborar um programa de testes de forma a garantir e validar os preparativos de gerenciamento e continuidade de negócio.
- Analisar criticamente todos os procedimentos de continuidade.

f) Incluindo a GCN na cultura da organização

- Elaborar um programa que mantenha e aumente a consciência da organização quanto a GCN.
- Treinamento envolvendo as pessoas relacionadas diretamente à GCN.

Na próxima subseção será apresentado o gerenciamento da continuidade segundo o ITIL.

6.4.3 Gerenciamento da Continuidade Segundo ITIL

O desenvolvimento das melhores práticas do ITIL ocorreu no final dos anos 80 pelo CCTA (*Central Computer and Telecommunications Agency*) para atender a solicitação do governo britânico que estava insatisfeito com o nível de qualidade dos serviços de TI. Desta forma, foi solicitado o desenvolvimento de melhores práticas para o gerenciamento de TI, objetivando a utilização eficiente e responsável dos recursos de TI. Em abril de 2001, após a incorporação do CCTA ao OGC (*Office of Government Commerce*) - que corresponde a um órgão responsável pelas melhorias dos processos de contratação e gestão de serviços – este passou a ser o órgão responsável pela evolução e divulgação da ITIL (FERNANDES e ABREU, 2008).

Pasqualetto e Luciano (2006) definem ITIL como um "grupo de práticas que apresentaram resultados positivos e orientam as organizações pelo melhor caminho dentro da TI". O ITIL possui uma abordagem de Gerenciamento de Serviços de TI mais aceito no mundo, fornecendo um conjunto de melhores práticas, provenientes de setores públicos e privados em nível internacional (OGC, 2005a).

A estrutura do ITIL é composta por sete módulos. Na Figura 11 está representada a estrutura do ITIL e um resumo de como os seus módulos se relacionam com a tecnologia e o negócio.

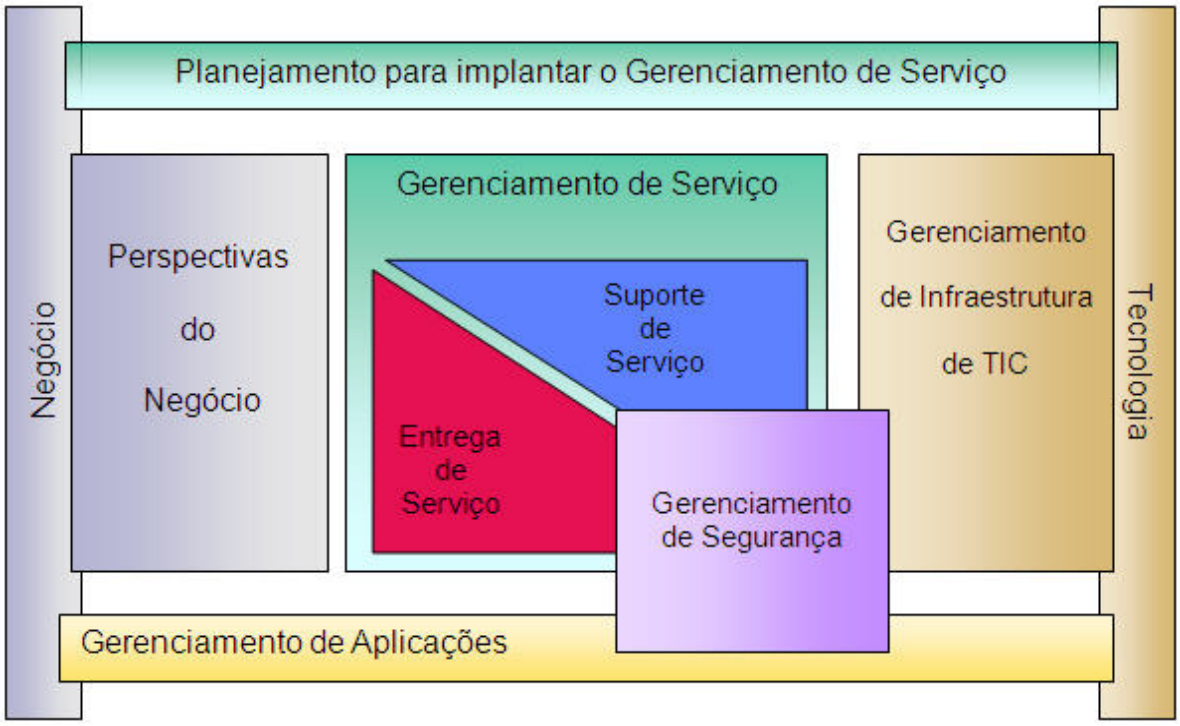

Figura 11: ITIL (*Framework)*
Fonte: OGC (2005a)

a) Perspectiva do Negócio

A perspectiva do negócio tem o objetivo de alinhar a gestão empresarial com os componentes da Tecnologia da Informação e Comunicação (TIC), visando uma infraestrutura que suporte os processos de negócio e um melhor gerenciamento de padrões e melhores práticas.

b) Gerenciamento de Infraestrutura de TIC

Este módulo cobre todos os aspectos da gerência de infraestrutura da TIC no aspecto da identificação das necessidades do negócio através de processos, testes, distribuição das instalações, suporte contínuo e manutenção dos componentes TIC e serviços de TI.

c) Gerenciamento de Aplicações

A gerência de aplicações abrange o ciclo de vida de desenvolvimento do software e se estende para sustentação do ciclo de vida do software e de teste de serviço. A gerência de aplicações possui influência nas mudanças organizacionais conforme as exigências encontradas nas necessidades do negócio.

d) Planejamento para Implantar o Gerenciamento de Serviços

Possui a finalidade de analisar questões e tarefas envolvidas no planejamento, execução e melhoria dos serviços e processos dentro das organizações. Este módulo também abrange questões culturais e mudança organizacional.

e) Suporte de Serviços

O objetivo é garantir que os serviços de TI estejam alinhados com as necessidades do negócio. É fundamental que os serviços de TI acompanhem e sustentem os processos do negócio, e que seja um facilitador de mudanças perante as transformações da organização. Os componentes que estão incluídos para o suporte de serviços são:

- Gerenciamento de Incidentes;
- Gerenciamento de Problemas;
- Gerenciamento de Mudanças;
- Gerenciamento de Liberações;
- Gerenciamento de Configurações.

f) Entrega de Serviços

Abrange os processos necessários para o planejamento e entrega de serviços, assegurando a qualidade aos serviços entregues. Os componentes para entrega de serviços são:

- Gerenciamento de Nível de Serviço;
- Gerenciamento da Capacidade;
- Gerenciamento da Disponibilidade;
- Gerenciamento Financeiro;
- Gerenciamento da Continuidade dos Serviços.

Para uma eficiente prestação de serviço de TI nas organizações, é essencial o acompanhamento da evolução e exigências do negócio, desta forma obtêm-se melhoramento contínuo na qualidade dos serviços alinhado com os requisitos do negócio, e de forma rentável. Para atingir os objetivos, é necessário considerar três aspectos: as pessoas, com suas competências; processos eficazes e eficientes; Infraestrutura de TI. Estes três componentes, aplicados de forma adequada dentro de um objetivo, são um facilitador para realização e concretização dos objetivos planejados (OGC, 2005a).

g) Segurança de Serviços

Este módulo refere-se aos processos de planejamento e gestão de segurança da informação e serviços de TI, incluindo a gestão de incidentes, sendo que o ITIL serve como o alicerce para a gestão da segurança. Os processos do ITIL que possuem relação com a gestão da segurança são pertencentes ao módulo Suporte de Serviços e Entrega de Serviços (OGC, 2005b).

Os incidentes de segurança da informação correspondem a eventos que podem causar dano à confidencialidade, integridade e disponibilidade da informação ou processamento da informação. A falta de segurança e da continuidade dos negócios custa dinheiro por parada dos serviços, ocasionando uma publicidade negativa para a organização e conseqüentemente a perda da confiança do cliente. É de grande importância uma correta segurança da informação que venha a garantir a continuidade dos serviços, para isto é essencial uma rigorosa análise de riscos, para o conhecimento do impacto e um planejamento para evitar (OGC, 2005b).

Para Mansur (2007) o objetivo do Gerenciamento de Continuidade de TI é proteger os serviços de qualquer eventualidade que venha a ocorrer, reduzindo possíveis erros e falhas,

restaurando os serviços conforme o tempo estipulado no plano de prevenção. O autor ainda cita algumas necessidades do negócio que justificam o gerenciamento da continuidade:

- Aumentar da credibilidade no mercado;
- Reduzir a dependência do negócio em relação a TI;
- Reduzir o custo e tempo de recuperação dos serviços de TI;
- Eliminar ou reduzir multas contratuais provocadas por falhas nos serviços de TI;
- Manter-se em operação em caso de grandes desastres.

Segundo Magalhães e Pinheiro (2007, p. 399) “toda grande organização tem seus negócios de algum modo dependentes de TI, tornando assim os serviços de TI críticos para a continuidade do negócio da organização”. Os autores ainda reforçam que além da tecnologia existente nas organizações, existem outros dois elementos – pessoas e processos – e que os três elementos devem estar sempre sincronizados.

O processo de Gerenciamento da Continuidade dos Negócios (GCN) é base de suporte para um processo de Gerenciamento da Continuidade dos Serviços de TI (GCS), pois o PCN determina os processos e sistemas críticos da área de TI que suportam o negócio da organização, orientando da melhor forma para evitar a indisponibilidade dos serviços de TI.

A Figura 12 está representada a associação entre os processos de GCN e GCS.

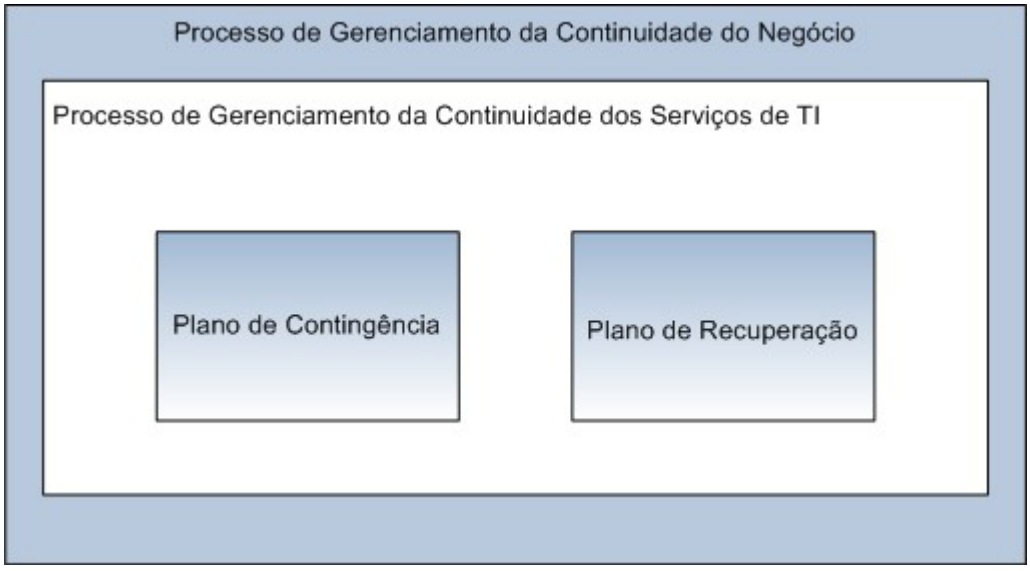

Figura 12: Associação entre processos
Fonte: Magalhães e Pinheiro (2007, p. 400)

O Plano de Continuidade dos Negócios deve orientar de forma clara quando o plano deve ser ativado e possuir a capacidade de recuperação com sucesso, de modo a garantir a continuidade dos serviços caso ocorra uma catástrofe. Desta forma, o plano garante a qualidade dos serviços acordados com os clientes fazendo com que os mesmos continuem

com suas atividades normalmente não sendo afetados pela falta ou atraso na entrega do serviço (OGC, 2005b).

Para Magalhães e Pinhero (2007), a estrutura de um PCN deve ser composta pelo menos pelos seguintes tópicos:

a) Sumário executivo, contendo:
   - Propósito do plano;
   - Autoridade e responsabilidades das pessoas-chave;
   - Tipos de emergência que podem ocorrer;
   - Local e gerenciamento da operação.

b) Gerenciamento dos elementos de emergência, contendo:
   - Direção e controle;
   - Comunicação;
   - Recuperação e restauração;
   - Administração e logística.

c) Procedimentos de resposta à emergência, onde deve conter uma lista com ações a serem tomadas pelo menos durante os três primeiros dias:
   - Alertas, no caso de aviso de catástrofes naturais;
   - Condução da evacuação;
   - Desligamento das operações;
   - Restauração das operações.

d) Documentos de suporte:
   - Lista de emergência – lista contendo o nome e telefone 24 horas das pessoas envolvidas no processo, assim como suas responsabilidades.
   - Planta das instalações físicas – planta com as informações de localização dos hidrantes, extintores, caixa de energia, saídas e escadas.
   - Guias para disponibilidade – desenho contendo as informações da infraestrutura de TI alinhada aos fornecedores externos e internos.
   - Procedimentos para recuperação – documento contendo a descrição dos processos para que, em caso de incidente, os serviços possam ser restaurados no menor espaço de tempo possível.

e) Identificar desafios e priorizar atividades:
   - Elaborar uma lista de ações a serem executadas e determinar quem e quando.
   - Determinar para quem serão encaminhados os problemas identificados na fase de levantamento das vulnerabilidades.

6.4.5 Gerenciamento de Continuidade Segundo COBIT

O COBIT é um guia de melhores práticas criado em 1994 pela ISAFA (Information Systems Audit and Control Fundation). Seu desenvolvimento ocorreu através do consenso de especialistas com o objetivo de estabelecer melhores práticas para a gestão de TI. Desde a sua criação o COBIT vem evoluindo através da incorporação de padrões internacionais e específicos para processos de TI. Em 1998 foi publicada e 2ª edição e no ano de 2000 foi publicada a 3ª edição pelo IT Governance Institute (ITGI), órgão criado pela ISACA. No ano de 2005 o modelo evoluiu com o alinhamento a modelos como COSO, ITIL e ISO/IEC 17799 e foi publicada a versão 4.0. Em 2007 o modelo passou por nova atualização e foi publicada a versão 4.1, cujo foco é a eficácia no controle e nos processos de avaliação e divulgação dos resultados (FERNANDES e ABREU, 2008)

O objetivo do COBIT é proporcionar boas práticas para o gerenciamento de TI, a partir das necessidades do negócio, através de uma estrutura com foco no controle e menos na execução. A adoção das práticas ajuda a melhorar os investimentos de TI, assegura a entrega dos serviços e fornece uma visão de quando de algo vai mal. O controle do COBIT contribui para as necessidades organizacionais através de:

a) Estabelece uma ligação com os requisitos do negócio;
b) Organiza as atividades de TI em um modelo de processos geralmente aceitos;
c) Identifica os principais recursos de TI para um melhor aproveitamento;
d) Defini os objetivos de controle de gestão que devem ser considerados.
e) As melhores práticas do COBIT orientam as organizações alinhando as metas da organização às metas de TI, fornecendo métricas e identificando responsabilidades associadas ao processo do negócio e TI (IT GOVERNANCE INSTITUTE, 2007).

Para Mansur (2007) a utilização do COBIT “aumenta a aceitação e reduz o tempo para efetivar o programa de governança de TI, pois permite o uso dos resultados das auditorias como uma oportunidade para melhorar os serviços de TI”.

Segundo IT Governance Institute (2007) a base de sustentação da Governança de TI pode ser representadas por cinco áreas e seus respectivos focos, conforme Figura 13.

Figura 13: Foco da Governança
Fonte: IT Governance Institute (2007, p.5)

Abaixo é apresentado o objetivo de cada foco:

a) Alinhamento Estratégico – tem o objetivo de garantir o alinhamento entre o plano de negócio e o de TI, definindo manutenção e validação da preposição de valor de TI, e alinhar a TI com as operações da empresa;
b) Agregação de Valor – deve executar a proposição de valor, assegurando que a TI proporcione os serviços prometidos conforme a estratégia;
c) Gerenciamento de Recursos – otimização dos investimentos e adequada gestão dos recursos críticos de TI (aplicações, informações, infraestrutura e pessoas);
d) Gerenciamento de Riscos – requer conhecimento dos riscos da organização por parte da gerência, compreensão dos requisitos, transparência sobre os riscos significativos para a organização e incorporação de responsabilidades para gestão de riscos;
e) Medição de Desempenho – acompanhamento e monitoramento da execução da estratégia, conclusão dos projetos, uso dos recursos, execução dos processos e prestação de serviços.

Conforme Fernandes e Abreu (2008), “o COBIT fornece um modelo padrão de referência e uma linguagem comum, permitindo que todos de uma organização sejam capazes de distinguir e gerenciar atividades no âmbito da TI”. O modelo utiliza o ciclo de melhoria

contínua que inclui: planejar, construir, executar e monitorar. A Figura 14 ilustra a integração entre os domínios na estrutura.

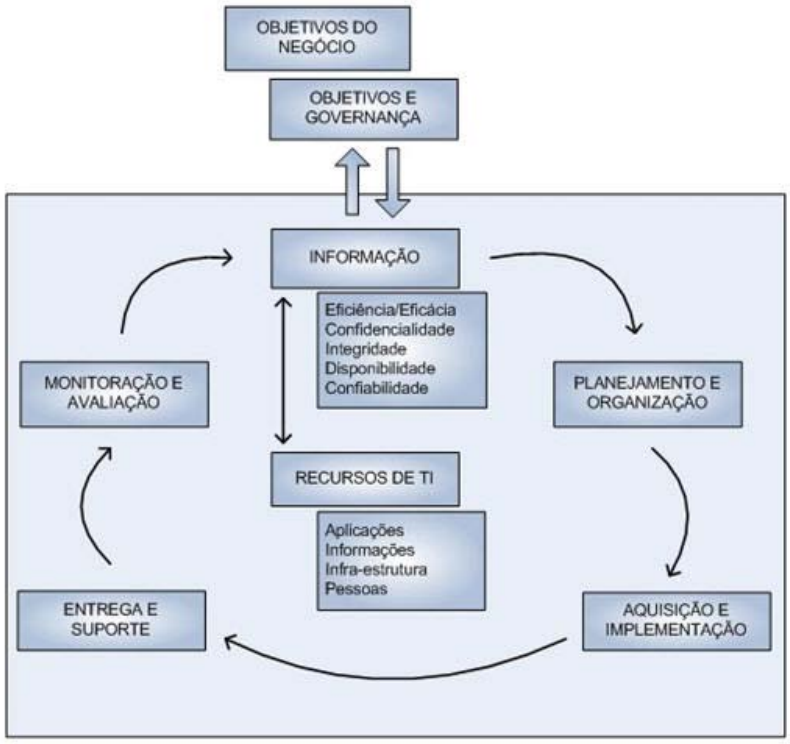

Figura 14: Domínios do COBIT (*Framework*)
Fonte: IT Governance Institute (2007, p. 26)

O COBIT possui 34 processos de TI, sendo que estes processos estão divididos entre os quatro domínios relacionados ao negócio: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, e por último Monitoração e Avaliação. O Quadro 1 apresenta os domínios e os processos de TI identificados pelo COBIT.

a) Planejamento e Organização	• Definir um plano estratégico de TI; • Definir a arquitetura da informação; • Determinar a direção tecnológica; • Definir a organização de TI, processos e relacionamentos; • Gerenciar os investimentos em TI; • Comunicar objetivos e direcionamentos gerenciais; • Gerenciar recursos humanos; • Gerenciar a qualidade; • Avaliar e gerenciar os riscos de TI; • Gerenciar projetos.

b) Aquisição e Implementação	• Identificar soluções automatizadas; • Adquirir e manter software; • Adquirir e manter infraestrutura tecnológica; • Viabilizar operação e utilização; • Adquirir recursos de TI; • Gerenciar mudanças; • Instalar e aprovar soluções e mudanças.
c) Entrega e Suporte	• Definir e gerenciar níveis de serviço; • Gerenciar serviços terceirizados; • Gerenciar desempenho e capacidade; • **Garantir a continuidade dos serviços;** • Garantir a segurança dos sistemas; • Identificar e alocar recursos; • Educar e treinar usuários; • Gerenciar central de serviços e incidentes; • Gerenciar configurações; • Gerenciar problemas; • Gerenciar dados; • Gerenciar ambiente físico; • Gerenciar operações.
d) Monitoração e Avaliação	• Monitorar e avaliar o desempenho da TI; • Monitorar e avaliar os controles internos; • Assegurar conformidades com requisitos externos; • Fornecer governança para TI.

Quadro 1: Domínios e Processos do COBIT
Fonte: Fernandes e Abreu (2008)

Segundo IT Governance Institute (2007), os serviços de TI exigem planos de continuidade que garantam a entrega, minimizando a ocorrência e o impacto da interrupção dos serviços relacionados às principais atividades organizacionais. O plano de continuidade dos serviços necessita de contínuo desenvolvimento, manutenção e testes que garantam a sua efetividade.

O controle oferecido pelos processos do COBIT tem o objetivo de garantir a continuidade dos serviços atendendo os requisitos de negócio de TI e garantindo a

organização o mínimo de impacto caso ocorra interrupção dos serviços. O foco concentra-se na elaboração de soluções alternativas e o desenvolvimento de planos de continuidade que envolva manutenção e testes. Estes requisitos podem ser atingidos através de:

a) Desenvolvimento e manutenção da contingência de TI;
b) Treinamento e testes dos planos de contingência;
c) Disponibilização de cópias dos planos de contingências e dados de localização (*offsite*);

Logo abaixo são apresentados os processos para garantia da continuidade dos serviços conforme COBIT:

a) Framework da Continuidade de TI

Desenvolvimento de um framework de apoio a continuidade dos serviços através de um processo consistente. O objetivo do framework é auxiliar a determinar as flexibilidades da infraestrutura e conduzir o desenvolvimento de recuperação pós-catástrofe e planos de contingência de TI. O framework deve abordar a estrutura organizacional para a gerência de responsabilidades, assim como processos de planejamento para elaboração das regras e estruturas de documentação, testes e execução do plano. O plano deve apontar os recursos críticos, monitoração e notificação da indisponibilidade, processos alternativos, assim como princípios de backup e recuperação.

b) Plano de Continuidade de TI

Desenvolvimento do plano de continuidade com base no *framework* de forma a reduzir o impacto de um incidente nas funções e processos críticos para o negócio. Os planos devem ser desenvolvidos com base nos riscos e impactos no negócio, oferecendo recuperação e alternativas para processos críticos dos serviços de TI. O plano também deve fornecer informações orientando na utilização, funções e responsabilidades, abordando procedimentos, processos de comunicação e testes.

c) Recursos Críticos de TI

Garantir a continuidade estabelecendo prioridades de recuperação conforme as prioridades e necessidades da empresa, de forma a manter um nível aceitável e cumprimento das exigências contratuais.

d) Manutenção do Plano de Continuidade de TI

Definir e executar procedimentos de controle de mudanças que assegurem que o plano de continuidade seja mentido atualizado conforme as exigências do negócio. As mudanças devem ser comunicadas em tempo oportuno.

e) Testes do Plano de Continuidade de TI

Testes asseguram que os sistemas de TI possam ser recuperados, apontando deficiências no plano. Os testes devem ser monitorados através de documentação (relatórios) que apontem os resultados.

f) Treinamento do Plano de Continuidade de TI

Desenvolver e executar treinamentos regulares para os envolvidos no processo, apresentando procedimentos, papéis e responsabilidades em caso de desastres. Avaliar as necessidades de treinamentos conforme resultados dos testes de contingência.

g) Distribuição de Plano de Contingência de TI

Determinação de estratégia para garantir que os planos sejam distribuídos, de modo a assegurar que estejam disponíveis aos interessados autorizados, quando e onde for necessário, sendo acessível independente do cenário do desastre.

h) Recuperação e Retomada dos Serviços de TI

Planejar ações para o período de recuperação e recomeço dos serviços de TI, onde deve ser incluído locai alternativo, processo de iniciação, comunicação do cliente e interessados, assim como procedimentos alternativos de reestruturação, assegurando o tempo de recuperação, investimentos e tecnologia necessária para suporte da recuperação.

i) Offsite Backup de armazenamento

Armazenar fora da organização documentação e outros recursos de informação de TI necessários para o plano de continuidade do negócio, determinando o conteúdo de backup entre a empresa e equipe de TI. A gerência deve continuamente avaliar e assegurar as informações armazenadas fora da organização para fins de segurança. Garantir a

compatibilidade de hardware e software para restauração dos dados e arquivos, testando e realizando atualizações dos dados arquivados.

j) Revisão Pós Retomada

Determinar se a gerência estabeleceu procedimentos para avaliar a adequação do plano, referente ao sucesso de restauração pós-catástrofe e atualização do plano.

6.4.6 Resumo dos principais conceitos relacionados à Continuidade de Negócio

Abaixo é apresentado o resumo dos principais conceitos em relação à continuidade de negócio verificados na ISO, no ITIL e no COBIT.

Etapas	Itens	ISO 15999	ITIL	COBIT
Planejamento	1. Programa de Gestão da Continuidade de Negócios (GCN)	X		
	2. GCN x Estratégia organizacional	X		
	3. GCN x Gestão de Riscos	X		
	4. Política de gestão da continuidade de negócios	X		
Analise de Riscos e Impactos	1. Análise de impacto no negócio	X	X	X
	2. Estabelecimento de período máximo de interrupção da atividade	X		X
	3. Estabelecimento de nível mínimo de desempenho da atividade após reinício	X		
	4. Estabelecimento de tempo máximo até retomada dos níveis normais das operações	X		
	5. Identificação das atividades críticas	X	X	X
	6. Determinação dos requisitos de continuidade (pessoas, local, recursos financeiros)	X	X	X
	7. Aprovação dos requisitos pela alta direção	X		
	8. Análise dos riscos	X	X	X
Estratégias de continuidade de negócio	1. Determinação das Estratégias	X	X	X
	2. Registro de medidas de mitigação do risco	X		X
	3. Aprovação das estratégias pela alta direção	X		
Conteúdo do Plano	1. Objetivo e escopo	X	X	X
	2. Papéis e responsabilidades	X	X	X
	3. Instruções de ativação do plano	X	X	X
	4. Definição do responsável do plano (análise crítica, atualização)	X		
	5. Detalhes de Contatos	X	X	

	6. Lista de tarefas/ações	X	X	X
	7. Atividade das pessoas	X	X	X
	8. Contatos emergenciais	X	X	
	9. Comunicação	X	X	X
	10. Plano de gerenciamento de incidentes	X		
	11. Plano de continuidade de negócios	X	X	X
Teste	1. Teste para validação dos processos de restauração	X		X
	2. Relatórios documentando os resultados	X		X
Revisão/ Manutenção	1. Manutenção após execução dos testes	X		X
	2. Análise critica dos componentes da GCN	X		
Conscienti-zação da GCN	1. Treinamentos para os envolvidos no processo	X		X
	2. Conscientização	X		X

Quadro 2: Resumo dos principais conceitos relacionados à continuidade de negócio

No próximo capítulo será apresentado o método de pesquisa utilizado para o trabalho.

7 MÉTODO DE PESQUISA

Neste capítulo será apresentada a metodologia e técnicas utilizadas para orientação no planejamento da pesquisa. Para Fachin (2006), o método é um instrumento de orientação utilizado como facilitador para o pesquisador planejar uma pesquisa, assim como executar, analisar e interpretar os resultados obtidos através do trabalho realizado.

Neste trabalho foi realizada uma pesquisa do tipo exploratória. De acordo com Gil (1999) as pesquisas exploratórias têm como principal finalidade "desenvolver, esclarecer e modificar conceitos, idéias, tendo em vista, a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores". O autor ainda afirma que entre todos os tipos de pesquisa, esta é a que menos apresenta rigidez no planejamento, onde se pode envolver levantamentos bibliográficos, documentos, entrevistas não padronizadas e estudo de caso.

Para Andrade (2003, p.124) "a pesquisa exploratória é o primeiro passo de todo trabalho científico", onde suas finalidades são obter maiores informações sobre determinados assuntos através de bibliografias; facilitar a delimitação de um tema de trabalho; definir os objetivos de uma pesquisa ou formular hipótese ou descobrir um novo enfoque para o trabalho. A autora ainda afirma que é através de pesquisas exploratórias que pode ser avaliada a possibilidade de desenvolvimento de uma boa pesquisa focando um determinado assunto.

A pesquisa exploratória é utilizada quando o pesquisador possui pouca informação a respeito do assunto, tornando-se instrumento de ajuda para identificar a melhor forma de atender as necessidades da empresa para o assunto em estudo. A vantagem da pesquisa exploratória é a revisão de literatura que pode ser utilizada como base de estudo e consulta para obtenção das informações e melhor compreensão da questão. (HAIR et al., 2007).

Pelo fato do trabalho se caracterizar por um estudo e proposta de um Plano de Continuidade dos Negócios para a empresa ALFA, o método a ser utilizado para a pesquisa é o estudo de caso. Segundo Fachin (2006) o estudo de caso é caracterizado por ser um estudo intensivo, onde é levada em consideração a compreensão, como um todo, do assunto investigado. Por ser um estudo intensivo é possível ter uma visão ampla e descobrir relações que de outra forma não seriam descobertas. Conforme Costa e Costa (2001, p.62) o estudo de caso é um estudo limitado a uma ou poucas unidades, que podem ser uma empresa, um setor, uma comunidade ou um país. O autor ainda afirma que "é uma pesquisa detalhista e profunda".

Além da importância de detectar novas relações, o estudo de caso pode ser auxiliado pela formulação de hipóteses, assim como utilizando formulários ou entrevistas. O questionário também pode ser utilizado como instrumento de pesquisa (FACHIN, 2006). A autora ainda salienta que a principal função do estudo de caso é a explicação sistemática dos fatos que ocorrem no contexto social, assim como seus relacionamentos com variáveis.

Para Gil (2009) o estudo de caso é o processo de coleta de dados mais complexo que em outras pesquisas, pois utiliza mais de uma técnica para a coleta dos dados. A obtenção de dados por mais de um meio torna-se fundamental para garantir a qualidade dos resultados, pois garante a validade do estudo evitando as conclusões pessoais do pesquisador.

Costa e Costa (2001, p.62) falam que uma pesquisa pode ter uma abordagem qualitativa e/ou quantitativa. Onde a qualitativa preocupa-se com a realidade e não pode ser qualificada, pois ela trabalha com crenças, valores e atitudes. Também pode trabalhar com dados, mas não deve envolver estatística avançada. Já a abordagem quantitativa possui suporte em medidas e cálculos mensurativos. Os autores ainda concluem que “a abordagem qualitativa busca a compreensão e a quantitativa a explicação”.

O modo de pesquisa utilizado para este trabalho é o modo qualitativo. De acordo com Roesch (2006) a pesquisa qualitativa é apropriada quando o estudo tem o objetivo de melhorar o programa de um plano ou quando trata de propor um novo plano. A pesquisa qualitativa prevê a coleta de dados a partir de interações sociais entre pesquisador e o objeto de estudo, possibilitando que o pesquisador participe e tenha envolvimento nas observações e análise da pesquisa (APPOLINÁRIO, 2006).

Para Hair et al. (2007, p.100) os dados qualitativos “representam descrições de coisas sem a atribuição direta de números. Os dados qualitativos geralmente são coletados utilizando-se algum tipo de entrevista não-estruturada”. O autor ainda fala que as técnicas qualitativas são mais freqüentes em projetos que possui o tipo de pesquisa exploratória e que os pesquisadores têm preferência por dados qualitativos quando os entrevistados são livres para responder os questionamentos durante a entrevista, pois permite a identificação de questões que não seriam identificadas caso a entrevista ocorresse de forma estruturada, permitindo que o pesquisador analise e interprete os dados provenientes da pesquisa realizada.

Abaixo está representado o fluxo de interação que foi elaborado para melhor orientação durante a pesquisa até a elaboração do Plano de Continuidade dos Negócios.

Na Figura 15 é representado o fluxo de interação que terá a pesquisa.

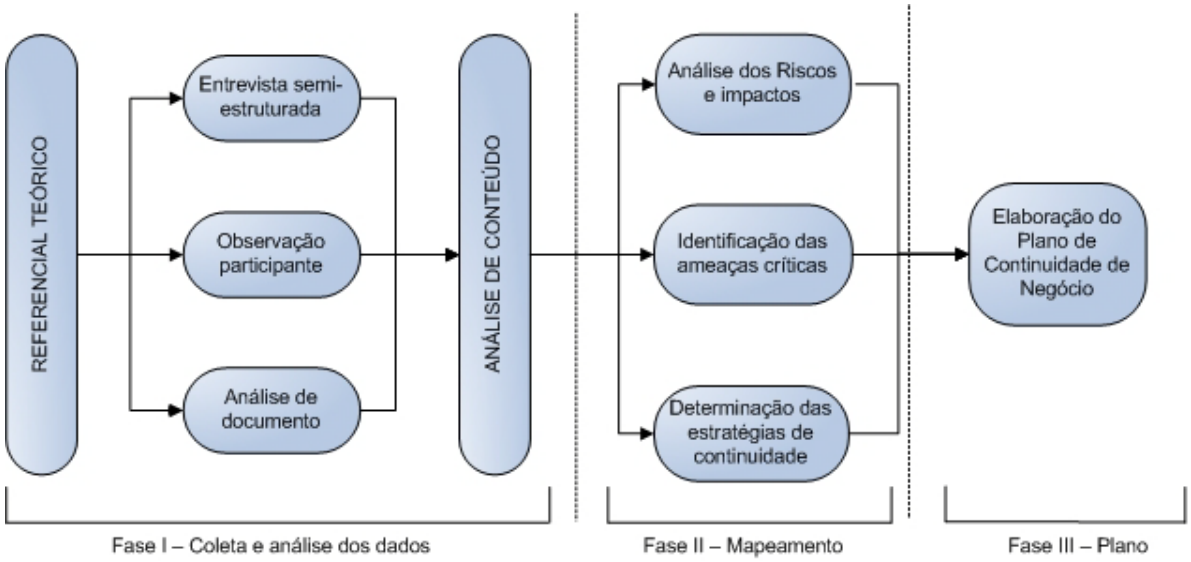

Figura 15: Desenho de Pesquisa
Fonte: Adaptado de Rech e Souza (2008, p.167)

7.1 COLETA DE DADOS

Com o objetivo de coletar informações necessárias para a pesquisa, as técnicas utilizadas para coleta de dados foi a entrevista semiestruturada, observação e análise de documento.

Conforme Roesch (2006, p.159) as entrevistas e observações são as técnicas mais utilizadas quando a pesquisa tem caráter qualitativo. Em “entrevistas semiestruturadas utilizam-se questões abertas, que permite ao entrevistador compreender e captar a perspectiva dos participantes da pesquisa”, possibilitando que o pesquisador direcione as questões de forma a obter uma melhor exploração do assunto.

A entrevista semiestruturada possibilita a obtenção de maiores informações, pois conforme as respostas do entrevistado o entrevistador fica livre para perguntas relacionadas ao assunto e que não foram originalmente incluídas no roteiro previamente definido. Desta forma os resultados das informações se tornam mais detalhistas e esclarecedoras, melhorando o resultado da abordagem (HAIR et al., 2007).

A observação participante foi utilizada no trabalho pelo fato da pesquisadora trabalhar na empresa ao qual ocorreu o estudo proposto. Segundo Gil (1999) a vantagem da observação participante é o pesquisador estar inserido no grupo e poder chegar ao conhecimento requerido. Ainda sobre as vantagens dos dados observacionais, Hair et al. (2007) fala que pelo fato de ser uma abordagem não invasiva, pois os observados não possuem o conhecimento de

estarem participando de um projeto de pesquisa e não receberam nenhum tipo de influência por questionário ou instrução, faz com que o resultado da observação não sofra influências ou tendências. Conforme Yin (2005, p. 122) “para alguns tópicos de pesquisa, pode não haver outro modo de coletar evidências a não ser através da observação participante”, é através dela que o pesquisador possui a capacidade de perceber os fatos conforme o ponto de vista de alguém de dentro da empresa, e não de um ponto de vista externo.

Para Roesch (2006) a observação participante tem sido muito utilizada nas organizações e pode combinar observação com entrevista durante o envolvimento com o grupo. Além da observação participante, será utilizada a análise documental, pois tem como propósito “descrever e explicar as idéias das pessoas sobre determinado assunto” (NEGRINE, 1999, p.79). Testa, Luciano e Rech (2008, p.85) falam que “a pesquisa documental não necessita obrigatoriamente de instrumentos de coleta de dados formalmente estruturado para utilização”. Os autores ainda falam que se deve analisar a pertinência de uso do documento, verificando a qualidade e confiabilidade das informações contidas no documento, assim como sua contribuição para pesquisa.

Segundo Testa, Luciano e Rech (2008, p.71) “a construção dos roteiros de coleta de dados em entrevistas apresenta particularidades dependendo do grau de construção do mesmo. Quando menos estruturada a entrevista, mais flexibilidade existe no roteiro.”. Os autores ainda falam que para estas situações o roteiro deve ser composto de temas genéricos baseados no referencial teórico e na problemática do trabalho, possibilitando ao entrevistado buscar as respostas para solução do problema. Desta forma, os autores sugerem a elaboração do “quadro de dimensões e variáveis”.

A seguir é apresentado o quadro de dimensões e variáveis utilizado como base para as entrevistas.

Dimen-sões	Variáveis	Fonte	Questões
Política de Segurança	Segurança	Caruso e Steffen (1999) Sêmola (2003) Mansur (2007) NBR 17999 (2005)	1. Existe uma política de segurança visando prevenção contra incidentes de segurança da informação?
			2. Ela passa por processos de revisão? Com que periodicidade?
			3. Quem são os envolvidos no processo de revisão?
Gerência da Continuidade dos Negócios	Responsabilidades da Gerência de Incidentes	Smith e Sherwood (1995) Magalhães e Pinheiro (2007) NBR15999-1 (2007)	4. Existem responsáveis pela gerência de incidentes de segurança da informação?
		Smith e Sherwood (1995) NBR15999-1 (2007)	5. Quais os critérios para escolha dos responsáveis pela gerência de incidentes de segurança da informação?
	d e	Sêmola (2003)	6. Como é realizada a análise de riscos aos quais os ativos da

		NBR15999-1 (2007)	empresa estão impostos?
		Caruso e Steffen (1999) Magalhães e Pinheiro (2007) NBR15999-1 (2007)	7. Quais os ativos (processos, pessoas, sistemas, informações, etc.) que possuem maior valor para organização?
	Análise de Impacto nos Negócios	Devargas (1999) ITGI (2007) NBR15999-1 (2007)	8. Como é realizada a análise de impacto nas funções críticas do negócio dentro da organização?
			9. Qual o impacto (financeiro e não financeiro) da perda ocasionada pela não execução das funções críticas para o negócio?
		Devargas (1999) NBR15999-1 (2007)	10. Como é determinada a prioridade e prazos de recuperação para a função atingida?
			11. Como é determinado o valor do recurso financeiro para preparação e recuperação de desastres?
Gerenciamento da Continuidade dos Serviços de TI	Estratégias de Recuperação	Sêmola (2003) ITGI (2007) NBR15999-1 (2007)	12. Quais estratégias de contingência que a empresa adota (Hot-site, warm-sites, realocação de operações, bureau de serviços, acordo de reciprocidade, cold-site, auto-suficiência)? Qual o motivo que a empresa possui para adotar tal estratégia?
			13. A empresa acha conveniente assinar acordos de reciprocidade entre empresa semelhante de forma a garantir alternativa de continuidade para as empresas acordadas?
			14. A empresa armazena fora da empresa documentação e outros recursos de informação de TI necessários para o PCN? Estes recursos são continuamente atualizados?
	Planos Funcionais Detalhados	Sêmola (2003) Mansur (2007) DRI (2007) ITGI (2007) NBR15999-1 (2007)	15. O PCN da empresa foi desenvolvido com base na análise dos riscos e impactos?
		Sêmola (2003) ITGI (2007) NBR15999-1 (2007)	16. A empresa possui planos funcionais detalhados? Quais (plano de administração de crises, plano de continuidade operacional, plano de recuperação de desastres)?
		ITGI (2007) NBR15999-1 (2007)	17. Os planos contêm informações sobre processos de iniciação e comunicação do cliente?
		Smith e Sherwood (1995) NBR15999-1 (2007)	18. Quem são os responsáveis pela elaboração dos planos funcionais?
			19. Os responsáveis pela elaboração dos planos possuem conhecimento técnico e específico do negócio?
		Magalhães e Pinheiro (2007) NBR15999-1 (2007)	20. O PCN possui documentos de suporte como lista de emergência, planta das instalações físicas, guias para disponibilidade e procedimentos de recuperação?
	Procedimen-tos de Ativação	DRI (2004) ITGI (2007) OGC (2005b) NBR15999-1 (2007)	21. A empresa possui procedimentos de ativação para os diferentes planos? Como são definidos estes procedimentos?
	Treinamen-to e Consciência	Herbane, Elliot e Swartz (2004) ITGI (2007) NBR15999-1 (2007)	22. Como e para quem é realizada a comunicação da relevância do PCN?
			23. São realizados treinamentos ou reuniões para disseminação do PCN?

Controle	Testes	DRI (2004) ITGI (2007) NBR15999-1 (2007)	24. São realizados testes para validação do PCN?
			25. Existe concentração de testes nas funções prioritárias do negócio?
			26. Com que frequência são realizados os testes para validação do PCN?
	Manutenção e Revisão	Devargas (1999) ITGI (2007) NBR15999-1 (2007)	27. Como é realizada a avaliação e manutenção do PCN?
			28. Com que freqüência é realizada a revisão e manutenção do PCN?

Quadro 3: Quadro de dimensões e variáveis

Além das entrevistas semiestrurada aplicada os funcionários de alta gerência da empresa em estudo, foi elaborado um segundo questionário com objetivo de coletar mais informações sobre PCN. As perguntas deste segundo questionário foram realizadas com quatro especialistas em Segurança da Informação.

No Quadro 4 é apresentado o roteiro de entrevistas que foi utilizado com os especialistas em Segurança da Informação.

Qual a importância da segurança da informação nas organizações?
Qual a sua visão em relação ao preparo das organizações para contingenciar grandes desastres?
Qual a tendência do mercado quanto à segurança da informação? (SOC - *security operaition center*, Gestão de Riscos , PCN, Outsourcing, Certificações)
Como as empresas, que se preocupam com a segurança da informação, realizam a Análise dos Riscos ?
Entre os modelos ou melhores práticas atualmente utilizadas pelas empresas brasileiras, quais contribuem para a segurança da informação e continuidade dos negócios? Como ou em que aspecto?
Quais vantagens que uma empresa pode obter externamente quando ela está preparada para dar continuidade aos seus serviços em caso de incidente que afetem as suas instalações?
O fato de uma empresa possuir PCN pode influenciar uma empresa cliente no fechamento de um negócio? Como?
Empresas que possuem um PCN podem ser consideradas como empresas inovadoras ou isso já é *commodity*?
Quais vantagens uma empresa pode obter quando ela possui um PCN bem estruturado?
De que forma a SOX pode contribuir com o PCN?

Quadro 4: Roteiro de entrevistas aplicado aos especialistas em Segurança da Informação

No próximo capítulo será apresentada a análise dos resultados obtidos.

8 RESULTADOS

Na seção 8.1 deste capítulo serão apresentados os resultados obtidos através da análise das entrevistas semi-estruturadas realizadas com os profissionais da empresa em estudo. Os resultados obtidos através da análise de documento e observação participante também serão apresentados nesta seção. Na seção 8.2 serão apresentados os resultados obtidos através das entrevistas realizadas com os especialistas em Segurança da Informação. Na seção 8.3 será apresentado o plano de ação para elaboração da proposta.

8.1 ANÁLISE DE DADOS COLETADOS NA EMPRESA

As entrevistas semiestruturadas foram realizadas com o **Diretor Administrativo, Diretor Financeiro, Diretor de TI (SQA) e Diretor de Projetos** da empresa em estudo, onde os entrevistados responderam as questões apresentadas no Quadro dimensões e variáveis do capítulo 7. Estas entrevistas foram realizadas no próprio horário e local de trabalho, resultando em uma hora e trinta minutos de gravações.

Antes de iniciar as entrevistas, foram apresentados os objetivos do trabalho, também foi informado aos entrevistados sobre a importância das informações obtidas com as perguntas do questionário e que qualquer informação complementar ou observação seria de grande importância para a análise.

Nas subseções abaixo, serão apresentados os resultados das entrevistas conforme a ordem em que foram realizadas e não pelo cargo que o profissional ocupa na empresa, sendo os entrevistados identificados como ENT1, ENT2, ENT3 e ENT4. As questões serão apresentadas conforme a dimensão na qual estão inseridas.

Na subseção seguinte serão analisadas as questões relacionadas à variável da dimensão Política de Segurança.

8.1.1 Política de Segurança

A primeira pergunta realizada na dimensão Política de Segurança, foi se existe uma política de segurança visando à prevenção de incidentes de segurança da informação. Todos os entrevistados afirmaram que não há uma política se segurança da informação institucionalizada, o que a empresa possui é um NDA com os colaboradores onde consta que

as informações internas e as informações obtidas de clientes devem ser mantidas sob sigilo. O entrevistado ENT2 ainda falou que, apesar da empresa possuir um NDA com os colaboradores, hoje a empresa não possui uma infraestrutura que permita o controle de cópias de documentos, assim como a saída destes documentos da empresa. Os entrevistados ENT1 e ENT3 ainda ressaltaram que a empresa possui normas de segurança referente ao controle de acesso às dependências internas da empresa, sendo que estas normas são apresentadas para os colaboradores assim que são contratados.

Em continuidade às entrevistas, perguntou-se aos entrevistados sobre o processo de revisão da política de segurança, periodicidade da revisão e os envolvidos neste processo. Os entrevistados ENT1 e ENT2 responderam que a política de segurança não passa por processos de revisão e que não há responsáveis por este processo. Já ENT3 não soube responder a questão. No entanto, ENT4 reconheceu a importância e informou que deveria existir uma revisão, mas como hoje não existe uma política de segurança, logo também não existe processo de revisão. O entrevistado ainda informou que quando for formalizada uma política de segurança, a revisão deverá ocorrer de seis em seis meses.

Foi observado que a empresa possui um *firewall* onde é realizado o controle e bloqueio de acesso a determinados conteúdos, tentativa de invasão à rede e *downloads* conforme o conteúdo e tipo de arquivo. A empresa também possui controle de acesso a informações e documentos, onde cada usuário possui um perfil de acesso ao repositório, e que as informações e os documentos são disponibilizados aos usuários conforme a necessidade de utilização para cada projeto.

Com base na entrevista com os profissionais da empresa e as observações realizadas, constatou-se que não há documentos que formalize o desenvolvimento de uma Política de Segurança para a organização, onde haja responsáveis pelo seu desenvolvimento, revisão, manutenção e disseminação. Existem algumas regras de seguranças que são comunicadas aos colaboradores da empresa quando contratados, mas não há um controle para verificar se estas regras estão sendo seguidas.

O quadro abaixo apresenta uma síntese referente à dimensão de Política de Segurança.

Variável	**Síntese**
Segurança	Os entrevistados informam que a empresa possui uma política de segurança, mas que ainda não está formalizada. Nota-se que a empresa não possui uma política de segurança adequada e formalizada, pois não

	há responsáveis pela sua manutenção, revisão, divulgação, disseminação e controle.

Quadro 5: Resumo das respostas da dimensão Política de Segurança

Na próxima subseção serão analisadas as questões relacionadas às variáveis da dimensão Gerência da Continuidade dos Negócios.

8.1.2 Gerência da Continuidade dos Negócios

Para esta dimensão a primeira pergunta abordou sobre a existência de responsáveis pela gerência de incidentes de segurança da informação. ENT1 afirmou que há três responsáveis pela Gerência de Incidentes: o Diretor Administrativo, o Diretor Financeiro e o Diretor de Projetos. ENT2 informou somente o Diretor Administrativo e o Diretor de Projetos. Já ENT3 informou que o responsável é a Diretoria Administrativa. ENT4 afirmou que hoje existe um responsável que é o Diretor Administrativo, mas futuramente a idéia é que existam mais pessoas para esta gerência.

Na segunda pergunta abordou-se sobre os critérios para a escolha dos responsáveis pela gerência de incidentes de segurança da informação. O entrevistado ENT1 afirmou que para a escolha dos responsáveis pela gerência de incidentes foi considerado o conhecimento técnico que cada uma das pessoas envolvidas possui na sua respectiva área. Onde o Diretor Administrativo cuidaria da parte técnica de suporte; Diretor Financeiro cuidaria dos custos envolvidos para recuperação; Diretor de Projetos para avaliação das perdas e comunicação com cliente. De acordo com ENT2 e ENT3, o entrevistado ENT4 afirmou que o critério utilizado para escolha das pessoas envolvidas na gerência de incidentes foi o nível de responsabilidade que elas possuem por qualquer evento que ocorra na empresa. ENT4 ainda ressaltou que, além do nível de responsabilidade das pessoas dentro da empresa, foi considerado o conhecimento técnico e do negócio.

A terceira pergunta abordou sobre a realização da Análise de Riscos aos quais os ativos da empresa estão impostos. Concordando com ENT1, o entrevistado ENT2 afirmou que os riscos são avaliados com base em eventos já ocorridos na empresa e que a listagem dos riscos que a empresa possui hoje são em relação a incidentes que já ocorreram em projetos. Como incidentes que viessem a ocasionar grandes perdas nunca ocorreram, para o PCN foi realizado um levantamento dos possíveis riscos que pudessem vir a ocorrer e causar maiores

impactos. ENT3 não soube responder a questão e ENT4 afirma que os riscos são mais estudados em nível de projetos do que de uma maneira global.

Dando continuidade ao mesmo assunto, na quarta pergunta abordou-se sobre os ativos de maior valor para a organização. De acordo com ENT1, ENT2 afirmou que os ativos de maior valor para a organização são as informações, servidores e pessoas. Já ENT3 e ENT4 concordam com os outros respondentes afirmando que a informação é o maior ativo.

Na quinta e sexta pergunta, abordou-se sobre a análise de impacto nas funções críticas do negócio dentro da organização e os impactos causados pela não execução destas funções. De acordo com a resposta do ENT1, ENT2 falou que a análise do impacto é realizada conforme a ocorrência do risco, podendo ser classificado como baixo, médio ou alto. Segundo os entrevistados, os riscos que possuem impacto alto são os que mais preocupam a empresa, pois são os que não atendem as expectativas do cliente e que podem ocasionar grandes perdas financeiras e até mesmo a perda do cliente, prejudicando a confiabilidade e imagem da empresa. Os entrevistados ainda ressaltaram que o impacto também depende do acordo que é realizado com o cliente, pois os SLA's determinam o valor da multa no caso de atraso nos serviços. Já ENT3 não soube responder a questão e ENT4 afirmou que hoje não existe um indicador de análise que informe corretamente o valor da perda. Sabe-se, através da experiência do dia a dia, que a perda de informações de um servidor ocasionaria um impacto muito alto, pois impactaria diretamente no cliente, podendo ocasionar perdas financeiras ou até mesmo a perda do cliente.

Na sétima pergunta abordou-se sobre a prioridade e prazos de recuperação para as funções atingidas por incidentes. ENT1 afirmou que o prazo máximo de recuperação é de quatro dias para deixar a empresa operante para continuidade dos serviços. Os entrevistados ENT2 e ENT4 não souberam responder exatamente os prazos de recuperação, mas afirmaram que qualquer função atingida possui alta prioridade para recuperação, devendo possuir o menor prazo possível. Já ENT3 afirmou que os serviços prestados pela empresa são de grande importância e alta criticidade, não podendo ocorrer atrasos que causem grandes impactos para os clientes. Então, qualquer evento que ocorra e que venham a prejudicar os clientes, deve ser tratado com a maior prioridade.

A oitava pergunta abordou se a empresa possui recursos financeiros para a preparação e recuperação do desastre. Os entrevistados ENT1 e ENT3 afirmaram que a empresa possui hoje um seguro Bancário que cobre a perda dos ativos físicos da empresa, como máquinas e servidores. Já ENT2 e ENT4 não souberam responder a questão.

Em análise realizada em documento, verificou-se que existem responsáveis pela gerência de incidentes e que cada área possui um responsável direto. Foram listadas sete áreas e sete responsáveis, sendo que alguns responsáveis nomeados não possuem responsabilidades de gerencia dentro da organização. Verificou-se também que algumas pessoas que fazem parte desta listagem não prestam mais serviços para a empresa.

Ainda em análise de documento, foi verificado que no atual PCN da empresa, são listados todos os riscos identificados e não apenas os riscos que vão ser contingenciados e os detalhes de recuperação para estes. No PCN atual, também não foram verificadas informações referente ao valor do recurso financeiro disponível para recuperação, assim como não foram verificadas informações de telefone ou endereço do local secundário. Já em relação aos prazos para recuperação das funções atingidas, verificou-se que nem todas as contingências listadas no documento possuem informações de prazo de resolução.

No dia a dia da empresa foi observado que eventos que venham a ocasionar qualquer tipo de atraso na entrega dos serviços ao cliente possuem tratamento com alta prioridade, pois o objetivo é a entrega dos serviços com qualidade e no prazo previsto e informado ao cliente.

Conforme os resultados obtidos através das entrevistas, análise de documento e observação verificou-se que nem todos os responsáveis pela gerência de incidentes listados no PCN atual sabem que são responsáveis pelo gerenciamento de incidentes, demonstrando desconhecimento sobre suas atividades e ações quando ao gerenciamento do plano.

O quadro abaixo apresenta uma síntese referente à dimensão da Gerência da Continuidade dos Negócios.

Variável	**Síntese**
Responsabilidades da Gerência de Incidentes	A empresa possui responsáveis de nível gerencial para a Gerência de Incidentes, no entanto nem todos os gerentes sabem que estão envolvidos no processo de continuidade, apresentando desconhecer suas atividades ou ações quanto ao gerenciamento do plano.
Análise de Riscos	Os entrevistados informaram que para o PCN foi realizado um levantamento dos possíveis riscos que pudessem vir a ocorrer e causar maiores impactos. Todos os entrevistados apresentaram concordância ao afirmar que as informações armazenadas nos servidores são o maior ativo que a empresa possui.
Análise de	Foi informado pelos entrevistados que a análise do impacto ocorre

Impacto nos Negócios	conforme a ocorrência do risco, sendo que a empresa classifica os riscos em três níveis: baixo, médio e alto. O impacto alto é o que mais preocupa a empresa, pois estes impactam no cliente deixando de atender suas expectativas, podendo ocasionar perdas financeira, perda do cliente e prejudicando a imagem da empresa. Os entrevistados ainda afirmam que a empresa determina sempre o menor prazo de recuperação dos serviços quando o cliente é atingido. Alguns entrevistados apresentaram concordância ao afirmar que a empresa possui recursos financeiros que cobre perdas materiais, no entanto outros entrevistados mostraram desconhecer esta informação.

Quadro 6: Resumo das respostas da dimensão Gerência da Continuidade dos Negócios

Na subseção seguinte serão analisadas as questões relacionadas às variáveis da dimensão Gerenciamento da Continuidade de Serviço.

8.1.3Gerenciamento da Continuidade dos Serviços de TI

A primeira pergunta abordou sobre as estratégias de contingência que a empresa adota, como *hot-site*, realocação de operações, entre outros. ENT1 afirmou que hoje, na falta de um recurso humano, a empresa utiliza a realocação de recursos. Não há outra estratégia imediata, a empresa considera-se auto-suficiente, pois outras estratégias teriam um custo muito alto Já ENT2 afirmou que a empresa não possui estratégias de contingência, mas considera importante estratégia como *hot-site*, principalmente para área técnica da empresa. ENT4 apresentou concordância com ENT2 ao afirmar afirma que a empresa não possui nenhuma estratégia de contingência, a não ser o *webmail*, pois o fornecedor de email possui o próprio plano de contingência. Já ENT3 afirmou não possuir o conhecimento sobre estratégias de contingência adotadas pela empresa.

A segunda pergunta, também abordou sobre estratégias de contingência, onde foi perguntado se a empresa acha conveniente assinar acordo de reciprocidade com empresa semelhante de forma a garantir alternativa de continuidade para as empresas acordadas. Todos os entrevistados afirmam que hoje a empresa não possui este tipo de estratégia, mas deve ser avaliada, pois parece ser muito interessante e viável.

Na terceira pergunta questionou-se sobre o armazenamento das informações e documentos necessários para o PCN e se estes recursos são continuamente atualizados. Todos os entrevistados afirmam que a empresa possui *backup* das informações armazenadas em servidor fora da empresa e estas informações são atualizadas periodicamente, inclusive um dos servidores possui *backup* automático de uma em uma hora. Durante a entrevista com ENT1, foi realizado o questionamento sobre o *backup* de um determinado servidor, que é novo na empresa. O entrevistado informou que ainda estava sendo providenciado o seu *backup*, mas o servidor ainda não possuía uma forma segura de proteger as informações ali armazenadas.

Dando continuidade as perguntas sobre elaboração do PCN, na quinta pergunta foi abordado se o PCN foi desenvolvido com base na análise dos riscos e impactos. ENT1 informou que o PCN foi elaborado com base nos riscos e impactos identificados pela empresa. Já os respondentes ENT2 e ENT3 não souberam responder a pergunta. No entanto, ENT4 apresentou concordância com RESP1 e afirmou que o PCN foi desenvolvido com base na análise dos riscos e impactos, onde foram levantados os possíveis riscos e analisados os impactos que poderiam ocasionar para o cliente.

Na sexta pergunta questionou-se sobre os tipos de planos que a empresa possui, como plano de administração de crise, plano de continuidade operacional e plano de recuperção de desastres. ENT1 afirmou que atualmente existe apenas um único plano, que é o PCN, e que este possui informações macro. Os outros entrevistados não souberam informar se a empresa possui diferentes planos.

Na sétima pergunta abordou-se sobre o detalhamento dos planos, se estes contêm informações sobre o processo de iniciação e comunicação com o cliente. ENT1 afirmou que o PCN não possui informações detalhadas, com um passo a passo do que fazer, quem comunicar e quando comunicar. Já ENT2 e ENT3 não souberam responder a pergunta. No entanto, ENT4 afirmou que a empresa não possui planos detalhados, mas reconheceu que deveria ter.

Na oitava e nona pergunta abordou-se sobre os conhecimentos dos responsáveis pela elaboração do PCN, se os envolvidos possuem conhecimento técnico e específico do negócio. ENT1 afirmou que contou com a ajuda de uma pessoa que também trabalha na empresa para a elaboração do PCN e que eles possuem conhecimento técnico e do negócio, mas não conhecimentos específicos em segurança ou em formas de contingência. Já os outros entrevistados não souberam responder a pergunta, sendo que ENT4 ainda completou a

resposta informando que os responsáveis deveriam ser o Suporte e o Diretor de TI, que são os responsáveis pela tecnologia da empresa e que apesar deles possuírem o conhecimento do negócio, deveriam aprimorar os conhecimentos relativos ao plano de continuidade e melhores estratégias de continuidade.

Na décima pergunta ainda na dimensão Gerenciamento da Continuidade dos Serviços de TI, questionou-se sobre documentos de suporte, como lista de emergência, planta das instalações físicas, guia para disponibilidade e procedimentos de recuperação. Os entrevistados ENT1 e ENT4 informaram que o PCN não possui estas informações. Já os respondentes ENT2 e ENT3 não souberam responder a pergunta.

Sobre os procedimentos de ativação do PCN, na décima primeira pergunta foi abordado se a empresa possui procedimentos de ativação para os diferentes planos e como são definidos estes procedimentos. ENT1 afirmou que o plano não possui procedimentos de ativação e os outros entrevistados não souberam responder a pergunta.

Nas últimas perguntas questionou-se como é realizada a comunicação da relevância do PCN e se são realizados treinamentos ou reuniões para disseminação do PCN. Todos os entrevistados afirmam que não foi realizada a comunicação do PCN para os colaboradores da empresa e também não são realizados treinamentos para disseminação do PCN.

Conforme análise de documento verificou-se que a empresa possui estratégias de contingência, como realocação de recurso, local secundário para realocação das operações e *backup*. O PCN além de ser único, contém informações macro, não possuindo informações detalhadas de quando deve ser ativado, quem deve ativar o plano, quem deve realizar a comunicação e quem deve ser comunicado. O plano também não contém uma lista de emergência, telefones de contato dos colaboradores, telefone do local secundário e seguradora. No entanto verificou-se que o documento foi elaborado com base na análise dos riscos e impactos.

Em observação dentro da empresa, verifica-se que nenhum dos colaboradores da empresa possui conhecimento sobre a existência do plano de continuidade, constatando-se uma deficiência na parte de comunicação da relevância do plano. Durante as entrevistas também foi observado a falta de conhecimento por parte dos envolvidos no gerenciamento de continuidade no que se refere às informações contidas no PCN.

Segundo análise das entrevistas, documentação e observação, verificou-se que muitas das questões os entrevistados não souberam responder, pois nem todos os responsáveis pela gerência de incidentes possuem o conhecimento das informações contidas no PCN,

constatando-se uma deficiência na comunicação entre os responsáveis pela ativação e gerenciamento do PCN. Observa-se também uma falta de conhecimento sobre o processo de gestão de continuidade do negócio (GCN), visto que não são realizados treinamentos explicando procedimentos do plano para os próprios integrantes e participantes do gerenciamento PCN.

O quadro abaixo apresenta uma síntese referente à dimensão do Gerenciamento da Continuidade dos Serviços de TI.

Variável	Síntese
Estratégias de Recuperação	Um dos entrevistados informou que a empresa utiliza-se da estratégia de realocação de recursos e afirma ser autosuficiente em outros requisitos de estratégia de recuperação por motivos de custos. Os entrevistados afirmam que a empresa não possui acordos de reciprocidade com outra empresa, mas apresentaram interesse nesta estratégia. Os entrevistados afirmam que frequentemente são realizados *backup* das informações internas da empresa e que estas informações são armazenadas em servidor externo.
Planos Funcionais Detalhados	O plano foi desenvolvido com base na análise dos riscos e impactos realizados pelos responsáveis pela elaboração do documento. No entanto, o PCN atual não possui planos funcionais detalhados, possui tarefas macros do que deve ser feito e estas informações estão contidas em um único documento. O PCN também não possui informações sobre o processo de iniciação e comunicação do cliente interno e externo. Os responsáveis pela elaboração do plano possuem conhecimento técnico e do negócio, mas não possuem conhecimento específico sobre gestão de continuidade de negócios.
Procedimentos de Ativação	Um dos entrevistados afirmou que não há procedimentos ativação detalhando quando o PCN deve ser ativado Os outros respondentes não souberam responder a questão.
Treinamento e Consciência	Todos os entrevistados afirmaram que não há procedimentos de treinamento.

Quadro 7: Resumo das respostas da dimensão Gerenciamento da Continuidade dos Serviços de TI

Na próxima subseção serão analisadas as questões relacionadas às variáveis da dimensão Controle.

8.1.4 Controle

Na a dimensão controle foram realizadas cinco perguntas. Nas três primeiras perguntas, questionou-se sobre a realização de testes para validação do PCN, se há concentração de testes nas funções críticas e a periodicidade em que ocorrem. Todos os entrevistados afirmaram que não foram realizados testes para validação do PCN.

Nas duas últimas perguntas abordou-se sobre a manutenção no PCN e a periodicidade desta manutenção. Os entrevistados ENT1, ENT2 e ENT4 informaram que ainda não foram realizadas manutenções no PCN e o ENT3 não soube responder a questão.

Conforme análise de documento, verificou-se que no PCN não há informações sobre manutenções ocorridas ou alterações realizadas devido a resultados de testes realizados.

Segundo análise das perguntas realizadas na dimensão controle, verificou-se novamente a falta de conhecimento sobre uma gestão de continuidade de negócios, visto que não foram realizados testes para validação do plano, sendo que o teste é um instrumento de avaliação do funcionamento das estratégias e dos tempos de respostas determinados durante a elaboração do plano.

O quadro abaixo apresenta uma síntese referente à dimensão Controle.

Variável	Síntese
Testes	Todos os entrevistados afirmaram que não há processos de testes para o PCN.
Manutenção e Revisão	Três entrevistados afirmaram que ainda não houve manutenção no PCN, sendo que um dos entrevistados não soube responder a questão.

Quadro 8: Resumo das respostas da dimensão Controle

Na próxima subseção será apresentada a análise das entrevistas realizadas com especialistas em segurança da informação.

8.2 ANÁLISE DE DADOS COLETADOS NA ENTREVISTA COM ESPECIALISTAS

As entrevistas foram realizadas com quatro especialistas em segurança da informação e os entrevistados responderam as questões apresentadas no Quadro 4 do capítulo 7. Estas entrevistas foram realizadas em locais e horários diferentes, conforme a disponibilidade do entrevistado, resultando em uma hora e trinta minutos de gravação das entrevistas.

Em todos os encontros realizados com os diferentes entrevistados, foram apresentados os objetivos do trabalho. Foi informado aos entrevistados sobre a importância das informações obtidas com as perguntas realizadas durante a entrevista e que qualquer informação complementar ou observação seria de grande importância para a conclusão da análise. Os entrevistados serão identificados através das siglas ESP1, ESP2, ESP3 e ESP4, sendo apresentada somente a sua formação e área de atuação.

O primeiro entrevistado foi o ESP1, que possui graduação em Segurança da Informação na UNISINOS e Mestrado em Computação Aplicada na mesma universidade, já trabalhou com consultorias em segurança da informação para empresas de TI. O segundo entrevistado foi ESP2, este possui graduação em Administração de Empresas com ênfase em Análise de Sistemas na PUCRS e atualmente trabalha na área de segurança da informação. O terceiro entrevistado foi ESP3, que também possui formação em Administração de Empresas com ênfase em Análise de Sistemas na PUCRS, atualmente faz pós-graduação em Gestão Estratégica da Tecnologia da Informação na mesma universidade. Atualmente trabalha com Governança e Segurança da Tecnologia da Informação, sendo que já trabalhou como Gerente de Riscos Operacional e Segurança, Gerente de Desenvolvimento de Sistemas e Programador. O quarto e último entrevistado foi ESP4, bacharel em Sistemas de Informação pela ULBRA, atualmente trabalha na área de Risco Operacional e Segurança, sendo sua especialidade em Continuidade do Negócio. Abaixo serão apresentados os resultados das entrevistas na ordem em que ocorreram.

Na primeira pergunta abordou-se sobre a importância da segurança da informação nas organizações.

O especialista ESP1 falou que desde que entramos na era da informação, no começo do século, a informação tem ganhado muita importância. O entrevistado falou que a segurança da informação está relacionada ao valor que ela representa para a organização, ou seja, quanto mais importante a informação for para o negócio da organização, mais importância tem a segurança da informação no contexto da organização. Seguindo a mesma idéia, o especialista

ESP2 afirmou que hoje a segurança da informação é primordial para as organizações, pois tudo depende da tecnologia, o negócio depende da tecnologia. Um exemplo que o entrevistado comentou é que se uma empresa disponibiliza suas informações através de um acesso externo (internet), então a primeira tarefa a fazer é pensar na segurança da informação. O respondente também colocou que dependendo do tamanho da organização, deve-se pensar no quanto se vai investir em segurança da informação, sendo que dependendo do tamanho da organização o investimento pode ser maior ou menor. Em grandes empresas, onde as informações requerem maior sigilo, é fundamental que exista dentro das organizações uma área que trate somente das questões de segurança da informação. Alguns bancos já exigem a existência de áreas que tratem somente desta questão de segurança da informação.

Em resposta a primeira pergunta, o especialista ESP3 falou que a segurança da informação cada vez mais tem conquistado seu espaço nas organizações. Infelizmente este espaço tem sido conquistado no momento em que as empresas começam a ter problemas com a segurança da informação, só então este assunto começa a ser fator de preocupação dentro as organizações. Na visão do respondente ESP3 e seguindo os conceitos da ISO, a segurança da informação visa à proteção das informações em relação à confidencialidade, pois deve haver a preocupação em proteger os ativos de informações da empresa, visto que o trabalho das pessoas da organização é transformado em informação e pode ser uma vantagem competitiva que a empresa possui; disponibilidade, onde a informação deve estar disponível para seu público alvo; integridade, pois a informação precisa estar disponível no tempo necessário e com qualidade.

O especialista ESP4 afirmou que hoje a informação é o maior ativo de uma organização. O entrevistado ESP4 apresentou concordância com as informações do ESP3, quando também mencionou que fazem parte deste ativo todas as informações que as pessoas trazem para dentro da organização através dos seus conhecimentos, logo se o ativo da informação é o mais importante, então se devem zelar estas informações e proteger este ativo.

O quadro abaixo apresenta uma síntese referente à primeira pergunta.

Pergunta	**Síntese**
Abordou sobre a importância da segurança	Todos os especialistas, de comum acordo, afirmaram que a segurança da informação é importante para as organizações. O ESP1 afirmou que quanto mais importante a informação for para o negócio da organização, mais importância tem a segurança da informação, já o ESP2 complementou

da informação nas organizações.	afirmando que dependendo do tamanho da organização, deve-se avaliar os investimentos em segurança, sendo que dependendo do tamanho da organização o investimento pode ser maior ou menor. O ESP3 falou que a informação é o principal ativo de uma organização. Apresentando a mesma opinião que o ESP3, ESP4 falou que faz parte do ativo de informação o conhecimento que as pessoas trazem para dentro da organização, por isto a importância de proteger este ativo.

Quadro 9: Resumo das respostas sobre a importância da segurança da informação nas organizações

Na segunda pergunta abordou-se sobre a visão dos entrevistados em relação ao preparo das organizações para contingenciar grandes desastres.

O especialista ESP1 falou que, em relação ao preparo das organizações para contingenciar grandes desastres, atualmente as empresas tem a parte técnica bem evoluída. A parte de gestão, que seria os planos (a documentação), fica difícil de analisar, pois geralmente as empresas não abrem estas informações, pois abordam dados estratégicos e muito importantes. Nesta mesma questão, ainda foi questionado ao entrevistado a sua visão sobre a elaboração dos planos por diferentes áreas. O entrevistado falou que quando se elabora um plano de gestão de continuidade do negócio, devem-se definir os processos. Não se faz um plano de continuidade para uma organização inteira, o que se deve fazer é pegar um determinado processo e verificar quais áreas estão relacionadas ao processo para ser mapeado. Para cada área deve-se designar um responsável, que vai responder por aquela pequena parte do plano de continuidade, sendo este também responsável por designar subtarefas dentro da sua área e isto vai se ramificando até a parte operacional. Então, na parte estratégica se tem um profissional cuidando da gestão como um todo, na parte administrativa os responsáveis cuidando das áreas e na parte operacional os funcionários que vão operar na continuidade. O entrevistado ainda conclui que quem está no “topo” deve ter uma visão geral do todo, por isto a documentação é importante.

O especialista ESP2 informou ter como conhecimento as informações da empresa em que trabalha atualmente, onde existe um PCN. Para este plano é exigido que sejam realizados testes de recuperação de desastres uma vez por ano, onde existe um site *backup* com os principais serviços e uma vez por ano deve-se que testar para verificar o seu funcionamento. O entrevistado falou que é muito caro manter uma contingência para desastres, então depende de quanto a empresa está disposta a gastar ou qual a importância que ela dá para os serviços

dela. O entrevistado concluiu dizendo que o preparo está muito relacionado ao que a empresa está sendo cobrada e as exigências.

Para a segunda pergunta o especialista ESP3 afirmou que o tema de segurança da informação é relativamente novo e vem ganhando espaço nas organizações, sendo que recuperação de desastres e PCN são assuntos mais novos ainda. Na opinião do entrevistado, o preparo das organizações pode ser classificado em dois grupos. Um deles seriam Instituições Financeiras e empresas de Telecom, que por possuírem uma série de órgãos regulatórios que acabam tornando estes requisitos como obrigatórios para estas organizações, este assunto já tem uma importância e uma estrutura de custo direcionada para o desenvolvimento deste tema. Estas organizações já possuem este assunto difundido, possuem uma área de segurança e uma equipe ou uma área de continuidade do negócio que abordam a recuperação de desastres. No outro grupo estão outras organizações que não tratam este assunto com tanta maturidade, pois sabem da importância, conhecem os impactos, mas não tratam o problema. Estas empresas não investem na capacitação da equipe, na elaboração de um programa de gestão de continuidade do negócio desde a elaboração de uma política até o estabelecimento de processos, testes de recuperação de desastres e atualização dos planos de continuidade. O especialista concluiu dizendo que hoje, no Brasil, Instituições Financeiras, empresas de Telecomunicações e empresas que de alguma forma estão submetidas à Sarbanes Oxley, seja por relacionamento com empresa no exterior ou por possuir um capital aberto, já enxergam o tema com bastante maturidade, sendo que outras empresas ainda estão imaturas com relação a este assunto.

Respondendo a segunda pergunta, o especialista ESP4 afirmou que quando se trata de questões de grandes desastres, como as recentes enchentes de Santa Catarina, enchentes do Nordeste, pandemias como gripe aviária e gripe suína, verifica-se que o exterior está mais preparado para lidar e tratar destas situações do que o Brasil. No Brasil a cultura continuidade do negócio ainda é muito recente e está cultura está sendo utilizada muito mais para cumprir legislação do para a própria continuidade do negócio das organizações.

O quadro abaixo apresenta uma síntese referente à segunda pergunta.

Pergunta	**Síntese**
Abordou sobre a visão dos	ESP1 falou que quando se trata da parte técnica (infraestrutura) verifica-se que as empresas estão bem preparadas, mas em relação a gestão e documentação fica difícil avaliar, pois as documentações contêm

especialistas em relação ao preparo das organizações para contingenciar grandes desastres.	informações confidenciais e geralmente as empresas não divulgam ou apresentam estas informações. De comum acordo, os especialistas ESP2 e ESP3 afirmam que o preparo das organizações está relacionado às exigências ou regulamentações impostas a ela. O ESP3 ainda informa que para Instituições Financeiras e empresas que possuem contratos com o exterior, esta questão já é tratada com bastante maturidade, sendo que outras empresas ainda estão imaturas com relação a este assunto. Já ESP4 afirmou que o exterior está mais preparado para lidar e tratar grandes desastres do que o Brasil, pois a cultura de continuidade dos negócios ainda é muito recente no Brasil, sendo que a maioria das empresas que possuem um PCN é por que estão cumprindo legislação.

Quadro 10: Resumo das respostas sobre o preparo das organizações para contingenciar grandes desastres

Para a terceira pergunta abordou-se sobre a tendência do mercado quanto à segurança da informação.

O especialista ESP1 falou que a informação ganhada mais importância a cada dia e que a competitividade de uma empresa está relacionada ao número de informações que ela possui do mercado e do negócio na qual ela atua, logo a segurança tem como tendência crescer muito ainda. O entrevistado ainda complementou que hoje, por falta de conhecimento em segurança da informação de uma forma geral e principalmente na parte de gestão da segurança da informação, a terceirização tem sido muito procurada pelas empresas, pois as organizações têm dificuldades de encontrar no mercado profissionais qualificados, então elas procuram terceirizar estes serviços.

O especialista ESP2 falou pela sua experiência nas empresas em que trabalhou, afirmando que as empresas estão investindo cada vez mais na segurança, sendo utilizado PCN, Gestão de Ricos, Certificações, entre outras alternativas. O entrevistado ressalta que depende do quanto é crítico a questão de segurança para a empresa, quanto mais crítico for, mais as empresas vão investir. Discordando de ESP1, ESP2 afirmou que segurança da informação normalmente não é terceirizada, que desconhece empresas que terceirizem a parte de segurança.

Em resposta a terceira pergunta, o especialista ESP3 afirmou que hoje as principais preocupações quanto à segurança da informação estão relacionados à Gestão de Acessos, Gerenciamento de Riscos referente à tecnologia da informação e Continuidade dos Negócios

que são temas importantes e bem discutidos atualmente. Em relação à infraestrutura tecnológica, a questão da segurança já está madura e desenvolvida há bastante tempo, sendo que as empresas já possuem um antivirus, um *firewall* e proteções contra ameaças internas e externas. Com relação ao o*utsourcing*, o que tem se praticado no mercado e o que se procura fazer é um mix, onde se deve manter na empresa uma estrutura de segurança enxuta, que conheça muito bem a cultura e o negócio da organização, já que a questão de segurança é um aspecto cultural, e utilizar uma consultoria externa de apoio para verificar as atualizações do mercado, as tendências e as novidades em relação às ameaças. Quando se trata de infraestrutura de segurança da informação, alguns paradigmas já foram quebrados, sendo que algumas empresas já realizam a terceirização por completo da infraestrutura, com administração de *firewall*, administração de IBS, IDS, monitoramento do ambiente, identificação de ameaças, resposta a ameaças, sendo que quem contrata estes serviços recebe relatórios com o diagnóstico do monitoramento, além de ter a garantia dos serviços através de contratos e SLA'S. O entrevistado ainda reforça que para Gestão da Segurança deve-se manter uma equipe interna.

Respondendo a terceira pergunta, o especialista ESP4 falou que a principal tendência do mercado está voltada para Gestão de Risco, pois este assunto é abordado desde modelos como ITIL (que fala sobre Gestão de Mudanças, Continuidade do Negócio e que usam a Análise Riscos) até os regulatórios de empresas Financeiras que utilizam Análise de Risco Operacional, Risco de Mercado, Risco de Crédito que são obrigatórios nestas instituições.

O quadro abaixo apresenta uma síntese referente à terceira pergunta.

Pergunta	**Síntese**
Abordou sobre a tendência do mercado quanto à segurança da informação.	O ESP1 falou que devido a falta de pessoas qualificadas no mercado e com conhecimento em segurança da informação, principalmente da gestão de segurança, a terceirização tem sido uma alternativa adotada pelas organizações. Em contrapartida, ESP2 afirma que desconhece empresas que terceirizem a parte de segurança. O entrevistado completou a resposta falando que as empresas estão investindo cada vez mais em segurança, sendo que PCN, Gestão de Riscos e Certificações estão sendo mais utilizados. Já o entrevistado ESP3 falou que a tendência é Gestão de Acessos, Gerenciamento de Riscos e Continuidade dos Negócios. O entrevistado ainda falou que a contratação de consultoria externa de segurança é uma prática que vem sendo

	utilizada no mercado como apoio. O especialista ainda comentou que algumas empresas já terceirizam por completo a segurança de infraestrutura. Concordando com algumas tendências já apontadas por ESP2 e ESP3, ESP4 apontou como tendência a Gestão de Riscos.

Quadro 11: Resumo das respostas sobre a tendência do mercado quanto a segurança da informação

A quarta pergunta abordou como as empresas, que se preocupam com a segurança da informação, realizam a análise de riscos.

O especialista ESP1 informou que até pouco tempo não existia nenhum guia que determinasse exatamente como ela deveria ser feita, e hoje também não existe, o que existe é a ISO 27005 que possui as diretrizes básicas que devem conter uma metodologia de gestão de risco de uma organização. Então, as empresa adotam, em alguns casos, metodologias já conhecidas como Octave ou adaptam as metodologias já existentes e geram suas próprias metodologias, pegando as informações mais importantes para gerar o seu cálculo como a probabilidade, o impacto, a severidade entre outros. Em continuidade a esta mesma questão, o entrevistado completou falando que quando é definido um processo de negócio para fazer gestão de risco, deve-se mapear tudo que está relacionado e é esta a maior dificuldade para se fazer um plano. O entrevistado ainda afirmou que a gestão de riscos nunca acaba, é como o processo evolutivo do PDCA, pois vai estar sempre localizando novos riscos, calculando os novos riscos e relacionando novos ativos à gestão de risco. A análise do risco fornece o fator de risco que é um número de acordo com a forma de cálculo, mas para o plano de continuidade, além da análise do risco é considerada a análise de impacto do negócio e a gestão do risco. Para a gestão de riscos devem-se identificar todos os riscos que o processo está exposto, assumir o risco, mitigar e tratar. O entrevistado ainda conclui que o plano de continuidade dos negócios deve abordar o inesperado.

O especialista ESP2 comentou que existe um cálculo padrão que envolve a probabilidade do problema, impacto e mitigação do controle. Sendo que quanto maior o controle, menor vai ser o risco e quanto menor o controle maior o risco.

Como resposta para quarta pergunta, o especialista ESP3 falou que a Análise dos Riscos funciona como o PDCA da administração, onde se deve entender os processos da organização, para os processos deve-se identificar os principais fatores de risco (que conforme a Basiléia seriam pessoas, processos, tecnologia e fatores externos). Devem-se analisar os processos da organização sobre estes quatro fatores de forma a identificar os fatores riscos.

Após a identificação dos fatores, deve-se analisar a probabilidade do risco ocorrer e os impactos causados pelo risco. Depois da avaliação dos riscos, deve-se fazer o mapeamento dos controles. ESP3 ainda falou que a melhor prática para avaliação dos riscos seria é através de um Comitê de Avaliação dos Riscos, composto pelos principais executivos da organização, que avaliam sobre a ótica dos impactos se o risco é aceitável ou não para a organização, o quanto é ofensor ou não. Sendo que para os riscos deve-se determinar um nível de aceitação, neste caso o entrevistado exemplificou a analogia do 80-20, onde "20% dos fatores de riscos que podem gerar 80% das perdas". Após a aceitação dos riscos e identificação dos mais ofensores, deve-se direcionar o esforço quanto ao gerenciamento do risco, onde vai se criar os planos de ação para o tratamento dos riscos. Então, depois de identificar os riscos, avaliar os riscos, controles e identificar os riscos mais ofensores, deve-se fazer o tratamento do risco e monitorar os planos de ação. Também se é recomendado manter em constante monitoramento os riscos identificados como aceitáveis para avaliar se não passaram a ser ofensores, pois no momento em que estes outros riscos são identificados como ofensores, devem ser tratados e elaborados planos de ação.

Respondendo a quarta pergunta, o especialista ESP4 falou que as Análises de Riscos são feitas através da adaptação de modelos de *frameworks* existentes. O entrevistado afirmou que hoje este assunto ainda está muito empírico e muito no começo, pois hoje as Análises de Riscos são realizadas através de uma matriz simples e qualitativa onde se trabalha com vulnerabilidades versos ameaças, probabilidade, mas sempre em uma visão qualitativa indicando se é baixa, média ou alta. As análises não são baseadas em números, em cima de uma visão quantitativa, onde exista um histórico.

O quadro abaixo apresenta uma síntese referente à quarta pergunta.

Pergunta	**Síntese**
Abordou como as empresas, que se preocupam com a segurança da informação, realizam a análise de riscos.	ESP1 e ESP4 falaram que para análise dos riscos normalmente as empresas adaptam metodologias já existentes e criam suas próprias metodologias. ESP4 ainda comentou que a análise tem uma visão qualitativa. ESP2 comentou que para o cálculo envolve probabilidade do problema, impacto, mitigação e controle. ESP1 e ESP3 falaram que a análise de riscos funciona como o PDCA, onde ESP3 completou a resposta falando que se deve entender os

	processos da organização, identificar os principais fatores de riscos (pessoas, processos, tecnologia e fatores externos), analisar a probabilidade de o risco ocorrer e os impactos causados, mapear os controles e monitorar o plano de ação. O especialista ressalta que a melhor prática para obtenção dos riscos é um Comitê de Avaliação dos Riscos composto pela gerência da organização.

Quadro 12: Resumo das respostas sobre análise de riscos

Na quinta pergunta questionou-se, entre os modelos de melhores práticas atualmente utilizados pelas empresas brasileiras, quais deles contribuem para a segurança da informação e continuidade dos negócios.

Entre os modelos e melhores práticas identificadas como os mais utilizados atualmente pelas empresas, o especialista ESP1 apontou a ISO 27002 que, conforme informações do entrevistado contêm todos os controles necessários para se ter um nível aceitável de segurança da informação dentro de uma organização; guias como COBIT e ITIL que também estão relacionadas com a segurança, pois fazem a comunicação entre a parte mais estratégica e administrativa da empresa com a parte técnica, no caso a TI; ISO 27005 para gestão de riscos, que está dentro do plano de continuidade dos negócios; DRI como principal referência para continuidade dos negócios, pois este guia existe há bastante tempo; SOX, que apesar de não ser um guia é uma lei que determina alguns controles necessários e serve como incentivo para implementação de outros guias. No final da entrevista, ESP1 complementou sua resposta falando que a ISO 15999 é nova e é específica para PCN.

O especialista ESP2 informou que a ISO 27001 possui um foco maior na segurança da informação, pois é específica para este assunto, tratando sobre a gestão de incidentes, monitoria patrimonial, entre outros. O entrevistado não soube informar em que aspectos ou como ela poderia contribuir. O entrevistado ainda informou que o ITIL não tem muito foco na segurança da informação.

Para a quinta pergunta, o especialista ESP3 falou que basicamente a ISO 17799 e a família de ISO originárias a ela, possuem as informações referente a estrutura, políticas, controle e o processo de gerenciamento de segurança da informação; o ITIL também ajuda no gerenciamento de segurança da informação; o COBIT é um framework importante para começar o processo de Governança de TI e também em relação a segurança, onde tem uma série de objetivos de controle ligados a tecnologia da informação e gerenciamento de riscos; a BS25999 ligada a continuidade dos negócios, também é um padrão a ser utilizado, sendo que

no Brasil somente uma organização é certificada até o momento, que é a CAIXA; o DRI também é considerado como fonte de referência principalmente para recuperação de desastres.

Em resposta a quinta pergunta, o especialista ESP4 citou a BS25999/1 e BS25999/2 como modelo que vem sendo utilizado como melhores práticas para implementação da continuidade dos negócios. Também são utilizados como base normas ISO como a 27000, modelos como ITIL e COBIT para continuidade do negócio, gestão do serviço e gestão da informação.

O quadro abaixo apresenta uma síntese referente à quinta pergunta.

Pergunta	**Síntese**
Abordou os modelos de melhores práticas atualmente utilizados pelas empresas brasileiras e quais contribuem para segurança da informação e continuidade dos negócios.	Em concordância os especialistas ESP1, ESP2 e ESP3 citaram a norma BS25999 (ISO15999) e os modelos ITIL e COBIT. ESP1 e ESP2 ainda apresentaram concordância ao citar o DRI como um modelo a ser utilizado e todos os especialistas citaram normas relacionadas à segurança da informação sendo citada a norma ISO17799 e a família da ISO 27000. ESP1 ainda mencionou a lei SOX.

Quadro 13: Resumo das respostas sobre modelos de melhores práticas utilizados pelas empresas

A sexta pergunta abordou quais vantagens que uma empresa pode obter externamente quando ela está preparada para dar continuidade aos seus serviços em caso de incidentes que afetem as suas instalações.

O especialista ESP1 comentou que a maior vantagem que uma empresa procura é a financeira, pois as organizações têm como premissa básica a obtenção do lucro. Então, todos os controles, como segurança da informação, gestão de riscos ou PCN, tem como objetivo dar lucro a empresa reduzindo os custos de retrabalho, falhas e outras questões relacionadas à segurança da informação. O *marketing* também foi identificado pelo entrevistado como uma vantagem, pois pode trazer algumas facilidades. Um dos exemplos de lucro citados pelo entrevistado foi o de um banco do estado do Rio Grande do Sul, que obteve um grande lucro por ser uma das primeiras empresas certificadas na ISO 17799, o que levou o banco a conseguir um financiamento na Europa com uma taxa de juro bem mais baixa por ser

certificado. Outro exemplo que ESP1 colocou é relacionado à governança corporativa, onde "uma empresa que tem seus processos mapeados, que demonstra e evidencia maturidade nestes aspectos, ela consequentemente tem suas ações valorizadas e em algum momento ela vai vender as suas ações com um ganho de até 15% acima por implementar estes controles, então tudo acaba lucro financeiro".

O especialista ESP2 falou que um PCN passa credibilidade e isso influencia positivamente na imagem da empresa e consequentemente pode trazer mais lucros para a empresa.

Em resposta a sexta pergunta o especialista ESP3 falou que a principal vantagem é a perpetuidade do negócio, pois no caso de indisponibilidade de algum serviço ou algum desastre que impeça a continuidade do negócio, a empresa está sujeita a perdas, podendo ser por multas contratuais ou até mesmo a perda do cliente. O entrevistado ESP3 também falou do PCN como diferencial competitivo, onde empresas que possuem estratégias de continuidade, também têm recuperação rápida, fazendo com que eventos adversos não prejudiquem o serviço que está sendo entregue ao cliente final.

Respondendo a sexta pergunta, o especialista ESP4 informou que em Instituições Financeira a continuidade do negócio já é obrigatória através da resolução 3380, onde os parceiros devem ter continuidade do negócio. Então, empresas que queiram ser parceiras de Instituições Financeiras e também parceiras de empresas que já fornecer trabalho ou serviços para estas Instituições vão ser obrigadas a ter um PCN. O entrevistado conclui falando que esta questão do PCN vai acabar se tornar uma cadeia entre clientes e fornecedores, onde a continuidade dos negócios tende a ser tornar natural para todas as empresas.

O quadro abaixo apresenta uma síntese referente à sexta pergunta.

Pergunta	**Síntese**
Abordou quais vantagens que uma empresa pode obter externamente quando ela está preparada para dar continuidade aos seus serviços em	ESP1 falou que a maior vantagem é o lucro, pois reduz o custo de retrabalho e contribui positivamente com o marketing da empresa. Apresentando o mesmo pensamento que ESP1, o ESP2 falou que um PCN passa credibilidade e isso influencia positivamente na imagem da empresa e consequentemente traz lucros. Já ESP3 falou que a principal vantagem é a perpetuidade do negócio, evitando multas contratuais e perda do cliente. O especialista também falou da vantagem como um diferencial competitivo.

caso de incidentes que afetem as suas instalações.	ESP4 falou que para Instituições Financeiras a continuidade dos negócios é obrigatório, então empresas que querem ser fornecedoras destas Instituições, obrigatoriamente vão ter um PCN.

Quadro 14: Resumo das respostas sobre vantagens que uma empresa pode obter quando está preparada para dar continuidade aos seus serviços

Na sétima pergunta foi abordado se o fato de uma empresa possuir um PCN pode influenciar uma empresa cliente no fechamento de um negócio.

O especialista ESP1 afirmou que pode influenciar sim, mas também depende da área de atuação da empresa. Outro ponto apresentado pelo entrevistado é custo de implementação do controle de continuidade do negócio e o valor real do negócio, pois se o custo de implementação for superior ao valor do negócio, então não vale a pena ser implementada a continuidade. A empresa antes de implantar um controle de continuidade, deve analisar o quanto ela está disposta a pagar pela estratégia de contingência a ser adotada. Outro exemplo apresentado pelo entrevistado é o de uma grande empresa que faz hospedagem em servidor dedicado de diversos serviços de diferentes clientes, esta empresa pegou fogo no final de 2008 e foram perdidos todos os servidores da empresa. Esta empresa fez deste desastre uma estratégia de *marketing*, pois iniciaram um processo de restauração do site e em dois dias foram restaurados milhares de sites que estavam hospedados nos servidores dedicados da empresa. Com este exemplo, o entrevistado conclui que este tipo de contingência tem um custo bem elevado, então a empresa deve verificar até quanto está disposta a pagar pelo serviço que garanta a restauração e continuidade em pouco tempo. Logo, a decisão de investimento e o valor a ser investido, estão relacionados com a área de atuação da empresa. O especialista também colocou que o PCN não deve ser relacionado com grandes negócios, pois empresas pequenas também podem ter PCN com um valor baixo, basta ter isto documentado.

O especialista ESP2 afirma que pelo fato do PCN passar mais credibilidade para uma empresa que está contratando ou utilizando os serviços, ela pode sim ser um requisito e um fator de decisão para o fechamento de um negócio.

Em resposta a sétima pergunta, e apresentando a mesma opinião que o entrevistado ESP2, o especialista ESP3 afirmou que um PCN pode ser fator de diferencial e decisão para ganhar uma concorrência, tornando-se vantagem competitiva. O entrevistado ainda informa que se a questão de continuidade estiver difundida na cultura da empresa contratante, sem

dúvida ela vai exigir o mesmo da contratada, inclusive empresas que exigem este requisito normalmente possuem uma equipe de auditoria para auditar o PCN da empresa a ser contratada. O entrevistado também afirma que empresas que não possuem esta cultura, não vão exigir da empresa contratada um PCN, sendo analisadas outras variáveis como custo, SLA'S de disponibilidade, entre outros.

Respondendo a sétima questão e apresentando o mesmo pensamento que os outros especialistas, o especialista ESP4 informou que um PCN pode sim influenciar no fechamento do negócio. ESP4 ainda completou a informação falando que se a empresa tem como regulamentação a obrigatoriedade de contratar somente parceiros que possuam PCN, esta empresa não vai fugir da regra. Em outros casos, o PCN pode ser visto como um diferencial quando é informado que se tem um site secundário ou que em caso de eventualidades o trabalho pode ser continuado sem prejuízos ou impacto para o cliente.

O quadro abaixo apresenta uma síntese referente à sétima pergunta.

Pergunta	**Síntese**
Perguntou se o fato de uma empresa possuir um PCN pode influenciar uma empresa cliente no fechamento de um negócio	ESP1 falou que dependendo da área de atuação da empresa um PCN pode influencia no fechamento de um negócio. O especialista também falou deve-se analisar o valor real do negócio com a estratégia de continuidade a ser adotada. Todos os especialistas apresentaram a mesma opinião quando afirmaram que um PCN pode ser fator de decisão para o fechamento de um negócio. Os especialistas ainda afirmaram que o PCN passa maior credibilidade para o cliente, pode ser visto como vantagem competitiva e diferencial.

Quadro 15: Resumo das respostas sobre a influência do PCN no fechamento de um negócio

A oitava pergunta abordou se empresas que possuem um PCN podem ser consideradas como empresas inovadoras ou isso já *commodity*.

Na opinião do especialista ESP1, o PCN não é considerado como questão inovadora para uma empresa. O entrevistado considera que empresas que possuem um PCN são empresas conscientes. Um exemplo que o entrevistado colocou, foi o de uma empresa desenvolvera de *software*, que não possui um plano de continuidade. Esta empresa pode não ter um PCN, por que os gestores desta empresa não se preocuparam com este ponto, mas é considerada inovadora por gerar novas tecnologias.

O especialista ESP2 informou que uma coisa é a empresa possuir um PCN e outra é possuir requisitos de infraestrutura para dar segurança. ESP2 concluiu a informação falando que o PCN não é *commodity*, é um diferencial. Hoje, muitas empresas fazem ações isoladas para dar continuidade aos serviços, como um *firewall*, servidor de *backup* e outros equipamentos. Outra coisa é manter um PCN com realização de testes que dê garantia da continuidade do negócio e não somente dos serviços.

Para oitava pergunta o especialista ESP3 afirmou que esta questão depende do mercado de atuação. No mercado Financeiro já é *commodity*, devido às exigências impostas a este setor, tornando o PCN uma obrigatoriedade. Para outros mercados pode ser uma questão de inovação e de diferencial competitivo diante de uma concorrência.

Em resposta a oitava questão, o especialista ESP4 informou que PCN está longe de ser *commodity* e afirma que o fato de uma empresa possuir um PCN é considerada como inovadora. O entrevistado ainda completou a informação falando que as estratégias de continuidade mudaram muito nos dois últimos anos, pois antes não se pensava em estratégia como se pensa hoje. Atualmente esta questão está madura em comparação há dois anos e tende a amadurecer cada vez mais.

O quadro abaixo apresenta uma síntese referente à oitava pergunta.

Pergunta	**Síntese**
Abordou se empresas que possuem um PCN podem ser consideradas como empresas inovadoras ou isso já uma *commodity*.	Na opinião de ESP1, o PCN não é considerado questão inovadora, o especialista fala que empresas que possuem um PCN são empresas conscientes. Já ESP2 afirmou que PCN não é *commodity*, é um diferencial. O especialista ainda falou que hoje muitas empresas fazem ações isoladas para dar continuidade aos serviços, mas um PCN requer mais que ações isoladas, são necessários testes para validação do plano. Na opinião de ESP3, o PCN está ligado ao mercado de atuação, onde no mercado Financeiro pode ser considerado *commodity* e em outros mercados uma questão de inovação e diferencial competitivo. Em contrapartida, ESP4 afirma que PCN está longe de ser *commodity*, e afirma que empresas que possuem PCN são consideradas inovadoras.

Quadro 16: Resumo das respostas sobre a consideração de empresas que possuem PCN

A nona pergunta abordou sobre as vantagens que uma empresa pode obter quando possui um PCN bem estruturado.

O especialista ESP1 indicou como vantagem o que o próprio plano de continuidade propõem, pois em caso de um incidente ou desastre a empresa tem a garantia de que vai conseguir retornar. Nesta questão o entrevistado também ressaltou a importância dos testes, pois a garantia da restauração dos serviços depende dos testes realizados no PCN. Desta forma, segundo o entrevistado “o plano não tem chance de errar, ele vai funcionar”. Para complementar a resposta, ESP1 ainda falou que uma vantagem de se ter um PCN seria a minimizar os prejuízos de um incidente ou desastre caso venha a ocorrer.

Em resposta a nona pergunta, o especialista ESP2 informou que a vantagem é obter um menor impacto para o negócio diante de um desastre e manter a disponibilidade dos serviços.

Para nona pergunta o especialista ESP3 afirmou que a principal vantagem é a garantia de que eventos adversos não vão comprometer o negócio, tanto no caso de um desastre até as pequenas interrupções do dia a dia que podem acontecer. Fazendo com que a operação continue operando e volte a se restabelecer no menor espaço de tempo possível.

Respondendo a nona questão, o entrevistado LAB afirmou que a maior vantagem é a certeza de que o negócio não vai parar, este é o objetivo do PCN. Quando se tem um PCN bem estruturado também deve-se ter um processo de Gestão de Continuidade que vai controlar a execução dos testes, as atualizações e a equipe de continuidade nas áreas. No momento em que é realizada uma mudança dentro da organização, o PCN também pode sofrer alterações, por isto a importância da Gestão da Continuidade manter este controle. O entrevistado completou a resposta informando que quanto mais atualizado estiver o PCN melhor é, pois nunca se sabe quando vai ocorrer um desastre. O entrevistado ainda completou a informação falando da importância de teste real, avisados ou não, para verificar a efetividade do PCN.

O quadro abaixo apresenta uma síntese referente à nona pergunta.

Pergunta	**Síntese**
Abordou sobre as vantagens que uma empresa pode obter quando possui um PCN bem	Todos os entrevistados apontam como vantagem a garantia de continuidade do negócio e a minimização dos impactos. ESP1 falou que a vantagem é o que o próprio PCN propõem, pois em caso de incidente ou desastre a empresa tem a garantia que vai conseguir retornar. Outra vantagem citada é minimizar os prejuízos de um incidente. Já ESP2 apresenta como vantagem obter o menor impacto

estruturado.	para o negócio diante de um desastre e manter a disponibilidade dos serviços. ESP3 falou que a vantagem é a garantia de que eventos adversos não vão comprometer o negócio, fazendo com que o negócio continue operando no menor espaço de tempo. ESP4 afirmam que a maior vantagem é a garantia de que o negócio não vai parar. O especialista ainda fala da importância do controle da Gestão da Continuidade quanto a testes, manutenções e atualizações.

Quadro 17: Resumo das respostas sobre as vantagens que o PCN pode trazer para empresa

Na décima e última pergunta foi abordado aos especialistas sobre a contribuição da SOX com o PCN.

O especialista ESP1 falou que a contribuição seria nas questões de auditoria e da responsabilidade social. O exemplo citado pelo entrevistado nesta questão foi “uma grande fábrica em uma pequena cidade, sendo que uma grande parte da população trabalha nesta fábrica que pega fogo, logo grande número de habitantes desta cidade vai estar desempregado”. Neste caso, continuar o negócio seria a responsabilidade social considerada pela SOX, logo “o plano de continuidade dos negócios está apoiado por uma das diretrizes básicas do SOX”.

Apresentando a mesma opinião que ESP1, o especialista ESP2 afirmou que a SOX está voltada a auditoria, então ela vai dar a garantia de que o PCN está adequado e apontar as questões que devem ser melhoradas no PCN.

O especialista ESP3 optou por não responder esta questão informando não possuir maiores conhecimentos neste assunto.

Em resposta a última questão, o especialista ESP4 informou que a SOX contribui muito com a parte de Segurança da empresa. A SOX garante a não ocorrência de falhas dentro de uma organização, desta forma ela contribui para continuidade dos negócios.

O quadro abaixo apresenta uma síntese referente à décima pergunta.

Pergunta	**Síntese**
Foi abordado aos especialistas sobre a contribuição da	Todos os especialistas que responderam a pergunta apresentaram a mesma opinião informando que a SOX contribui com a auditoria garantindo a não ocorrência de falhas no PCN.

SOX com o PCN.	ESP1 ainda aponta a responsabilidade social considerada pela SOX, pois a continuidade do negócio também está ligada a responsabilidade social.

Quadro 18: Resumo das respostas sobre a contribuição da SOX com o PCN

Na subseção seguinte serão apresentadas as ações para elaboração da proposta.

8.3 PROPOSTA PARA PGI E PCN

O plano de ação para elaboração da proposta foi desenvolvido a partir das informações obtidas através da análise dos dados e do referencial teórico. Sendo utilizado como principal fonte as informações da NBR 15999, ITIL e COBIT. Abaixo são apresentadas as ações e os requisitos iniciais para elaboração do PGI e PCN.

Conforme o elemento “Entendendo a Organização” da norma 15999-1, primeiramente foi realizado o entendimento da organização, conforme as ações apresentadas no Quadro 19. As ações realizadas abaixo, também referem-se às consultas realizadas no COBIT e as melhores práticas do ITIL.

Ação	**Resultado**
Identificar os objetivos da organização	- manter o nível dos serviços de forma a cumprir as SLA’S dos projetos; - manter imagem confiável; - atender as expectativas dos clientes quanto à qualidade e prazos de entrega.
Identificar as atividades críticas que necessitem recuperação	- serviço de internet - serviço de email - execução dos projetos - entrega dos projetos - contato com cliente - acesso as informações dos projetos e administrativas
Identificar os ativos	- informação - servidores - recursos humanos - equipamentos
Identificar os principais responsáveis	- Diretor Administrativo (nome) - Diretor de Projetos (nome) - Diretor de TI (nome) - Gerente Financeiro (nome)

Identificar e avaliar as ameaças - Análise de Impacto no negócio	A análise de impacto para as possíveis ameaças foi realizada através da relação da probabilidade e impacto causado nas atividades, sendo assim determinada a prioridade do risco. Para determinação da probabilidade e do impacto, foram utilizados os seguintes valores para as qualificações: baixo = 1, médio = 2 e alto = 3. Ver Quadro 20: Análise de impacto das possíveis ameaças.
Identificar o tempo máximo de interrupção de cada atividade.	Para cada uma das atividades identificadas como críticas foram estabelecidos tempos de recuperação. Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação. Obs.: Para os riscos em que ocorre apenas a queda do nível de serviço, não são identificados os tempos de interrupção e retomada, pois o serviço continuou operando. Ver Quadro 20: Análise de impacto das possíveis ameaças.
Identificação das ameaças críticas	As ameaças críticas foram determinadas após a análise dos riscos e impactos causados nas atividades da organização. Sendo considerado como crítica aquelas que ocasionam grandes perdas nas atividades do negócio. A coluna "AC" do Quadro 20 apresenta quais ameaças foram consideradas críticas.

Quadro 19: Ações para elaboração da proposta do PCN e PGI

Abaixo é apresentado o Quadro 20, este quadro contém os resultados obtidos através das ações executadas do Quadro 19.

Recursos da Organização	Risco	Probabili-dade	Impacto	Priori-dade	Período de interrupção*	AC**
Pessoas	Falta de colaborados chave por motivo de doença.	Baixa	Alto	4	TMP= 2d NM= 70% TMR= 3d	C
	Perda de colaborador chave por desligamento	Baixa	Alto	4	TMP= 3d NM= 60% TMR= 4d	C
	Perda de colaborador chave por pedido de demissão.	Baixa	Alto	4	TMP= 3d NM= 60% TMR= 4d	C
	Compartilhamento de recurso com outros projetos	Alta	Alto	6	----------	
	Superalocação de recurso	Média	Média	4	----------	
	Troca de recurso durante o projeto	Baixa	Alto	4	----------	
	Falta de conhecimento técnico da equipe de testes	Média	Média	4	----------	
	Troca de equipe do projeto durante a execução do projeto	Baixa	Alta	4	----------	
Instalações	Alagamento na parte interna da empresa por estouro de cano de água	Baixa	Alta	4	TMP= 4d NM= 80% TMR= 5d	C
	Incêndio total/parcial da empresa	Baixa	Alta	4	TMP= 4d	C

					NM= 80% TMR= 5d	
	Desabamento do prédio por catástrofe natural ou intencional	Baixa	Alta	4	TMP= 4d NM= 80% TMR= 5d	C
Equipamentos de Tecnologia	Falha de equipamento	Média	Baixa	3	TMP= 0,5h NM= 100% TMR= 0,5h	
	Avaria no equipamento (computadores em geral)	Média	Média	4	TMP= 0,5h NM= 100% TMR= 0,5h	
	Avaria nos servidores	Média	Alta	5	TMP= 1d NM= 90% TMR= 2d	C
	Uso não autorizado de equipamentos	Média	Média	4	———	
	Uso não adequado dos meios de comunicação	Média	Alta	5	———	
	Falha na rede interna da empresa	Média	Alta	5	TMP=1h NM=100% TMR=1h	
	Roubo de equipamento	Baixa	Alta	4	TMP= 0,5h NM= 100% TMR= 0,5h	
	Restrição tecnológica proveniente do cliente	Baixa	Média	3	———	
Informação	Acesso não autorizado a documentos/ informações confidenciais da empresa (por meio externo)	Baixa	Alta	4	———	
	Acesso não autorizado a documentos/ informações confidenciais da empresa (por meio interno)	Baixa	Alta	4	———	
	Alteração não autorizada de documentos	Baixa	Alto	4	———	
	Roubo de informações/documentos confidenciais	Baixo	Alto	4	———	
	Perda de dados/informações dos servidores	Média	Alta	5	TMP= 1d NM= 90% TMR= 1d	C
	Perda de backup	Baixa	Média	3	———	
Fornecedores	Falta de energia elétrica	Baixa	Alta	4	TMP= 2h NM= 90% TMR= 3h	C
	Falha na telefonia, impossibilitando comunicação	Baixa	Baixa	2	———	
	Falha no *link* externo de rede (internet)	Média	Média	4	TMP= 2h NM= 90% TMR= 4h	C
	Perda de performance no link da internet	Média	Médias	4	TMP= 4h NM= 90% TMR= 6h	
	Falha no servidor de e-mail	Baixa	Alto	4	TMP= 2h NM= 90% TMR= 3h	C

*Tempo Máximo (TMP) = de parada, até que a atividade reinicie.
Nível Mínimo (NM) = de desempenho da atividade após reinício.
Tempo Máximo (TMR) = de retomada dos níveis normais de operação.

** Atividades consideradas como críticas= AC

Quadro 20: Análise de impacto das possíveis ameaças

Depois de identificados os possíveis riscos, realizada a análise de impacto e identificadas as ameaças críticas, foram determinadas as estratégias de continuidade de negócios.

A determinação das estratégias foi realizada para os recursos da organização, conforme os quadros dos recursos abaixo.

a) Pessoas

Risco	Consequência de não se agir	Mitigação	Estratégia de continuidade de negócio
Falta de colaborador chave por motivo de doença.	- atraso nas atividades antes executadas pelo colaborador; - atraso na entrega de projeto; - pagamento de multa por não cumprimento do contrato.	- manter documentos de trabalho sempre detalhados e atualizados; - manter estes documentos em repositório no servidor interno da empresar; - manter documento detalhado contendo informações das atividades críticas do projeto; - manter em documento atualizado informações de contato com cliente e status do projeto; - manter programa de treinamentos atualizados; - manter treinamentos para cada setor, de forma a manter pessoas do mesmo setor com a mesma base de conhecimento.	- substituir o colaborador por outro da mesma equipe e que possua o mesmo nível de conhecimento, ou - substituir o colaborador por outro de equipe diferente e que possua o mesmo nível de conhecimento, ou - contratar um novo colaborador com o mesmo nível de conhecimento.
Perda de colaborador chave por desligamento /morte.	- atraso nas atividades antes executadas pelo colaborador; - atraso na entrega de projeto; - pagamento de multa por não cumprimento do contrato.	- manter documentos de trabalho sempre detalhados e atualizados; - manter estes documentos em repositório no servidor interno da empresar; - manter documento detalhado contendo informações das atividades críticas do projeto; - manter em documento atualizado informações de contato com cliente e status do projeto; - manter planejamento de sucessão; - manter programa de treinamentos atualizados; - manter treinamentos para cada setor, de	- substituir o colaborador pelo seu sucessor, conforme planejamento de sucessão; ou - contratar um novo colaborador com o mesmo nível de conhecimento.

		forma a manter pessoas do mesmo setor com a mesma base de conhecimento.	
Perda de colabora-dor chave por pedido de demissão.	- atraso nas atividades antes executadas pelo colaborador; - atraso na entrega de projeto; - pagamento de multa por não cumprimento do contrato.	- manter documentos de trabalho sempre detalhados e atualizados; - manter estes documentos em repositório no servidor interno da empresar; - manter documento detalhado contendo informações das atividades críticas do projeto; - manter em documento atualizado informações de contato com cliente e status do projeto; - manter planejamento de sucessão; - manter programa de retenção para os colaboradores; - manter programa de treinamentos atualizados; - manter treinamentos para cada setor, de forma a manter pessoas do mesmo setor com a mesma base de conhecimento.	- substituir o colaborador pelo seu sucessor, conforme planejamento de sucessão; ou - contratar um novo colaborador com o mesmo nível de conhecimento.

Quadro 21: Estratégia de continuidade dos recursos humanos

b) Instalações

Risco	Consequência de não se agir	Mitigação	Estratégia de continuidade de negócio
Perda do local por alagamen to/incênd io/desaba mento.	- multas contratuais por atraso e não entrega dos serviços; - perda da confiabilidade na empresa por colaboradores e clientes; - perda de clientes; - perda de	- não realizar alterações/manutenções na estrutura do prédio sem antes consultar especialistas; - realizar vistorias programadas na estrutura física do prédio, incluindo hidráulica e elétrica; - contratar especialistas para manutenção quando necessário; - realizar vistorias diárias na empresa ao final do expediente de forma a se certificar de que todas as torneiras estão fechadas, e cafeteiras e máquinas desligadas; - manter extintores de incêndio dentro na empresa; - realizar treinamentos para utilização de extintores; - realizar treinamentos apresentando opções de	- seguro no valor de R$80.000,00 (oitenta mil reais) a fim de cobrir as perdas de máquinas. - possível financiamento. - recurso no valor de R$50.000,00 (cinqüenta mil reais) para cobrir gastos iniciais. - aluguel de sala em

	colaboradores; - perda de parceiros; - imagem prejudicada.	saída de emergência para os colaboradores; - realizar treinamentos de primeiros socorros; - conhecimento da infaestrutura do local que será utilizado como alternativa para alocação da equipe.	Hotel (nome do Hotel) no centro de Porto Alegre.

Quadro 22: Estratégia de continuidade para as instalações

c) Informação

Risco	Consequência de não se agir	Mitigação	Estratégia de continuidade de negócio
Perda das informações do servidor "W".	- perda de informações de projetos; - multas contratuais por atraso e não entrega dos serviços; - perda da confiabilidade na empresa por colaboradores e clientes.	- manter diferentes perfis de acesso para os usuários; - liberar acesso somente das informações necessárias para o usuário; - realizar *backup* automático de uma em uma hora armazenando as informações em servidor externo.	Subir a última atualização do *backup* armazenado no servidor externo.
Avaria no servidor "W".	- perda de informações de projetos; - multas contratuais por atraso e não entrega dos serviços; - perda da confiabilidade na empresa por colaboradores e clientes.	- realizar *backup* automático de uma em uma hora armazenando as informações em servidor externo.	Compra de peça ou novo servidor. Subir a última atualização do *backup* armazenado no servidor externo em um novo servidor.
Perda das informações dos servidores "X", "Y", "Z".	- perda de informações de projetos; - perda de informações estratégicas da empresa; - multas contratuais por atraso e não entrega dos serviços; - perda da confiabilidade na empresa por	- manter diferentes perfis de acesso para os usuários; - liberar acesso somente das informações necessárias para o usuário; - realizar *backup* diário do servidor 2, armazenando em fitas DDS2 fora da empresa; - uma vez por semana armazenar o *buckup* no servidor externo da	- Subir a última atualização do *backup* armazenado no servidor externo.

	colaboradores e clientes.	empresa.	
Avaria nos servidores “X”, “Y”, “Z”.	- perda de informações de projetos; - multas contratuais por atraso e não entrega dos serviços; - perda da confiabilidade na empresa por colaboradores e clientes.	- realizar *backup* diário do servidor 2, armazenando em fitas DDS2 fora da empresa; - uma vez por semana armazenar o *buckup* no servidor externo da empresa.	- Acionar financeiro para compra de outro servidor utilizando o recurso de reserva para contingências. - Subir a última atualização do *backup* armazenado no servidor externo.

Quadro 23: Estratégia de continuidade da informação

d) Fornecedores

Risco	Consequência de não se agir	Mitigação	Estratégia de continuidade de negócio
Falta de energia elétrica	- multas contratuais por atraso e não entrega dos serviços;	- manter gerador de energia.	Acionar a empresa de energia elétrica para comunicação do ocorrido.
Falha no *link* externo de rede (internet)	- multas contratuais por atraso e não entrega dos serviços;	- manter celulares com tecnologia 3G para contingência.	- Acionar a empresa responsável e utilizar os celulares para conexão com a internet até restabelecimento normal do serviço.
Perda de perfor-mance no link da internet	- multas contratuais por atraso e não entrega dos serviços;	- manter controle de performance.	- Acionar a empresa responsável e utilizar a banda somente com os projetos essenciais até o restabelecimento normal do serviço.
Falha no servidor de e-mail	- atraso na comunicação com o cliente.	- manter controle para verificar falhas no serviço de email.	- Acionar a empresa responsável e transferir os registros de DNS que apontam para o sistema do datacenter para o servidor de *backup* da empresa.

Quadro 24: Estratégia de continuidade dos serviços terceirizados

Após a identificação dos requisitos acima, nas subseções 8.3.1 e 8.3.2 serão apresentadas as ações para elaboração dos Planos de Gerenciamento de Incidentes e Continuidade do Negócio.

8.3.1 Plano de ação para elaboração da proposta para PGI

A proposta do Plano de Gerenciamento de Incidentes (PGI) foi elaborada com o obejetivo de dar apoio ao gerenciamento de um incidente que envolva os principais recursos da organização (pessoas, tecnologia, fornecedores, instalação), conforme sugerido pela NBR 15999:2007. Esta proposta inclui o gerenciamento do risco por perda de local, que afeta diretamente os recursos de pessoas, informação e serviços prestados por fornecedores.

Para elaboração do PGI, foram utilizados os requisitos extraídos a partir dos resultados das ações apresentadas na seção 8.3. Sendo utilizadas as informações resultantes da Análise de Riscos, estratégia de contingência, prazos de recuperação.

A proposta de PGI é apresentada no APÊNDICE B.

8.3.2 Plano de ação para elaboração da proposta para PCN

A proposta do PCN é permitir que a empresa ALFA recupere e mantenha seus serviços em caso de interrupção devido à ocorrência de incidente que afete a continuidade do negócio. Para esta proposta, foi incluído em um único documento os planos para os diferentes riscos identificados para os recursos de pessoas, informação e fornecedores.

Para elaboração do PCN, foram utilizados os requisitos extraídos a partir dos resultados das ações apresentadas na seção 8.3. Sendo utilizadas as informações resultantes da Análise de Riscos, estratégia de contingência, prazos de recuperação.

A proposta de PCN é apresentada no APÊNDICE C.

9 CONSIDERAÇÕES FINAIS

Cada vez mais as empresas de TI buscam o aperfeiçoamento e a diferenciação para manter-se competitivas no mercado. É através da adaptação e aderência das exigências e requisitos do mercado que as empresas buscam a diferenciação do seu negócio, em busca de novos setores do mercado e fidelidade dos clientes. A empresa ALFA verificou a necessidade de atender as exigências do setor bancário, setor que a empresa pretende atender, quanto ao requisito de garantir a entrega dos serviços e continuidade de negócio com um PCN.

Diante desta exigência encontrada no setor bancário, um PCN baseado em práticas de reconhecimento internacional, busca atender os requisitos encontrados para este setor e faz com que a empresa ALFA mantenha-se competitiva no mercado, atendendo as expectativas dos clientes internos e externos, com a garantia na entrega dos serviços e continuidade do negócio em caso de incidente.

A partir deste estudo, verificou-se que a cultura das organizações em relação à continuidade de negócios é muito importante. É através de uma cultura sólida que as empresas têm efetividade e sucesso na implantação de uma gestão de continuidade de negócio. Durante as entrevistas com especialistas e na busca de literaturas para elaboração do trabalho, foi verificado que a cultura de continuidade de negócio possui um grande valor e reconhecimento para empresa do exterior, sendo que no Brasil esta cultura ainda não possui o reconhecimento devido. No entanto, grandes empresas brasileiras, como Instituições Financeiras, já possuem esta cultura difundida, visto que são obrigadas a seguir as regulamentações impostas ao setor bancário.

Através das exigências encontradas nas regulamentações que as organizações brasileiras estão aderindo à cultura de continuidade de negócios, sendo que, as empresas ao aderirem a esta cultura também vão exigir a mesma garantia dos seus fornecedores, formando uma cadeia de clientes e fornecedores que aderem e exigem garantia na continuidade de negócio através de um PCN.

Durante as entrevistas com a alta direção da empresa ALFA, pôde-se verificar que há um reconhecimento da importância da segurança das informações e continuidade de negócio por parte de alguns entrevistados, no entanto não existe uma cultura dentro da organização que faça com que esta importância seja difundida entre todos os funcionários que fazem parte da alta gerência. O PCN que a empresa adotava não atendia algumas exigêngias encontradas na NBR 15999 e no COBIT. Apesar de a proposta ter como objetivo a elaboração de um PCN

baseado nas melhores práticas de mercado, verifica-se que primeiramente é necessário difundir na organização a importância de se ter um plano de continuidade de negócio, fazendo com que a empresa adote as práticas da gestão de continuidade de negócio para gerenciar de forma eficiente e eficaz o PCN proposto neste trabalho.

Durante o levantamento das informações nas literaturas, verificou-se que a NBR15999 atendeu de forma completa as necessidades encontradas para elaboração do trabalho, apresentando informações sobre a gestão da continuidade de negócios até os detalhamentos sobre as informações contidas nos planos e controles que devem ser adotados. O COBIT teve sua contribuição nos requisitos essenciais para a elaboração e controle do PCN, e o ITIL apresentou de uma forma geral os objetivos do PCN e a sua contribuição para organização. Com base nestas três referências, pode-se elaborar a proposta, sendo esta apresentada na seção 8.3.

Os objetivos propostos para o trabalho foram alcançados, sendo estes apresentados após a análise dos dados coletados e apresentados no capítulo 8.

Os objetivos específicos (a) e (b) que procuram identificar os elementos componentes do plano de continuidade de negócio e a avaliação dos pontos críticos e vulneráveis a riscos, foram expostos na subseção 8.3.

O objetivo específico (d) é apresentado nas subseções 8.3.1 e 8.3.2, onde são apresentadas as propostas para a continuidade do negócio.

Entre os fatores de limite da pesquisa, um deles é o fato do trabalho se tratar de um estudo de caso, o qual não permite generalização, pois a proposta foi elaborada com base nas necessidades e informações resultantes das entrevistas, observação e análise de documentos da empresa ALFA. Outro fator limitante é o fato de existirem poucos artigos e livros na língua portuguesa que apresentem maiores informações e detalhes sobre o assunto.

Para pesquisas futuras, sugere-se o desenvolvimento completo de um plano de gestão de continuidade de negócio, contendo o programa de gestão para análise de riscos, programa de conscientização da organização sobre a importância do assunto e planos de teste para validação do PGI, PCN e da GCN. Também se sugere a elaboração de um programa de governança de TI para empresa ALFA para aperfeiçoamento dos processos de TI.

O desenvolvimento deste trabalho proporcionou à autora novos conhecimentos e grande experiência acadêmica, sendo superada a expectativa inicial do trabalho com relação à elaboração da proposta. O trabalho, além de contribuir com os conhecimentos relacionados ao PCN, como segurança da informação, análise de riscos e estratégias de continuidade de

negócio, proporcionou uma visão maior com relação às empresas terem a necessidade de e manterem-se atualizadas e em constante pesquisa, de forma a verificar e atender as exigências de setores que pretendem atingir.

REFERÊNCIAS

ABNT NBR ISO/IEC 15999-1:2007. **Gestão da Continuidade de Negócios. Parte 1:** Código de Prática**.** Associação Brasileira de Normas Técnicas. (Pedido 171863 Impresso: 25/05/2009)

ABNT NBR ISO/IEC 15999-2:2007. **Gestão da Continuidade de Negócios. Parte 2:** Requisitos**.** Associação Brasileira de Normas Técnicas. (Pedido 171863 Impresso: 25/05/2009)

ABNT NBR ISO/IEC 17799:2005. **Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da segurança da informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro, ABNT, 2005.

ALBERTIN, Alberto Luiz; ALBERTIN, Rosa Maria de Moura**. Tecnologia de Informação:** desafios da tecnologia de informação aplicada aos Negócios. São Paulo: Atlas, 2005a.

ALBERTIN, Alberto Luiz; ALBERTIN, Rosa Maria de Moura**. Tecnologia de Informação e desempenho empresarial:** as dimensões de seu uso e a sua relação com os benefícios de negócio. São Paulo: Atlas, 2005b.

ALBERTIN, Alberto Luiz. **Benefícios do uso de Tecnologia de Informação no desempenho empresarial**. GVPesquisas. Relatório 07/2005. Disponível em <http://www.eaesp.fgvsp.br> Acesso em: 25 out.2008.

ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho científico:** elaboração de trabalhos de graduação. São Paulo: Atlas, 2003.

APPOLINÁRIO, Fabio. **Metodologia da Ciência:** Filosofia e prática da pesquisa. São Paulo: Pioneira Thomson Learning, 2006.

BORGES, Mônica Erichsen Nassif. **A informação como recurso gerencial das organizações na sociedade do conhecimento**. Ciência da Informação, Vol 24, número 2, Ibict – Instituto Brasileiro de Informação em Ciências e Tecnologia, 1995. Disponível em <http://dici.ibict.br/archive/00000601/ >. Acesso em: 25 out.2008.

CARVALHO, Rosangela Caubit de. **A aplicação de um modelo de gestão de segurança da informação e a sua influência na percepção de competitividade no setor de telecomunicações e informática**. Universidade Federal Fluminense LATEC – Laboratório de Tecnologia, Gestão de Negócios e Meio Ambiente. p. 208. Niterói, 2003. Disponível em <http://www.bdtd.ndc.uff.br/tde_busca/arquivo.php?codArquivo=1834>. Acessado em: 29 out. 2008.

COPENHAVER, John. **DRI International News**. p.17. Jan, 2007. Disponível em <https://www.drii.org/docs/DRIINewsletter1-07_9.pdf >. Acesso em: 27 out.2008.

DEVARGAS, Mario. **Survival is Not Compulsory:** An Introduction to Business Continuity Planning. Computers & Security, p. 35 – 46, 18, 1999. Disponível em < http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-3W31NRB-7&_user=10&_coverDate=12%2F31%2F1999&_alid=933512982&_rdoc=1&_fmt=high&_orig=search&_cdi=5870&_sort=d&_docanchor=&view=c&_ct=2&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=b101ed899f9622103d2b06872850f23f> Acesso em 03 nov., 2008.

CARUSO, Carlos Alberto Antônio; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. São Paulo: SENAC, 1999.

COSTA, Marco Antônio F. da; COSTA; Maria de Fátima Barrozo da. **Metodologia da Pesquisa: conceitos técnicos**. Rio de Janeiro: Interciência, 2001.

FACHIN, Odília. **Fundamentos de Metodologia**. – 5ª. ed. - São Paulo: Saraiva, 2006.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a governança de TI:** da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport, 2008.

FOINA, Paulo Rogério. **Tecnologia da Informação:** planejamento e gestão. São Paulo: Atlas, 2006.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social. -** 5 ed. – São Paulo: Atlas, 1999.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa. -** 4. ed. – São Paulo: Atlas, 2009.

HAIR JR., Joseph F.; BABIN, Barry; MONEY, Arthur H.; SAMOUEL, Phillip. **Fundamentos de métodos de pesquisa em administração.** Tradução Leon Belon Ribeiro. – Porto Alegre: Bookman, 2005.

HERBANE, Brahim; ELLIOTT, Dominic; SWARTZ, Ethné M**. Business Continuity Management:** time for a strategic role? Elsevier Ltda. All rights reserved, 2004. Disponível em < http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V6K-4DDXMGV-3&_user=10&_coverDate=10%2F31%2F2004&_alid=933512875&_rdoc=9&_fmt=high&_orig=search&_cdi=5817&_sort=d&_docanchor=&view=c&_ct=12&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=b6f402bbd59d46104e9a6549b4ecdeb0> Acesso em 05 nov., 2008.

IT GOVERNANCE INSTITUTE. **COBIT 4.1: framework, control objectives, management guidelines, maturity models**. Estados Unidos: Information Systems Audit and Control Fundation, 2007.

LAURINDO, Fernando José Barbi. **Tecnologia da informação:** eficácia nas organizações. São Paulo: Futura, 2002.

LUCIANO, Edimara Mezzomo; FREITAS, Henrique. Application Solution Provider: uma nova estratégia para agregar valor ao negócio e reduzir custos de TI. In: **Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação**, 2, 2005, São Paulo-SP. **Anais** São Paulo: TECSI/FEA/USP, 2005, p. 77 resumos (Anais em CD-ROM). Disponível em < http://www.adm.ufrgs.br/professores/hfreitas/files/artigos/2005/2005_176_TECSI.pdf>. Acesso em: 25 out.2008. ARTIGO

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerencimento de Serviços de TI na Prática: uma obordagem com base no ITIL**. São Paulo: Novatec Editora Ltda, 2007.

MANSUR, Ricardo. **Governança de TI:** metodologia, frameworks e melhores práticas. Rio de Janeiro: Brasport, 2007.

NEGRINE, Airton. Instrumentos de coleta de informações na pesquisa qualitativa**.** In: TRIVIÑOS, Augusto Nibaldo Silva; MOLINA NETO, Vicente (org.). **A pesquisa qualitativa na educação física**: Alternativas metodológicas. Porto Alegre: Ed. Universidade/UFRGS/Sulina, 1999 p. 61-93.

OFFICE OF GOVERNMENT COMMERCE. **Planning to Implement Service Management**. v2.0 Reino Unido: The Stationery Office, 2005a. Disponível em <http://www.tso.co.uk/pism/app/frames.htm> Acesso em 01 out., 2008.

OFFICE OF GOVERNMENT COMMERCE. **Business Perspective:** The IS View on Delivering Services to the Business. v2.0 Reino Unido: The Stationery Office, 2005b.

PASQUALETTO, Loimar; LUCIANO, Edimara M. Implantação de Práticas ITIL: o caso do TRF4. In.: **CATI - Congresso Anual de Tecnologia da Informação**, São Paulo - SP. Anais do 3º CATI, 2006.

RECH, Ionara; SOUZA, Alessandro Nunes de. Gestão de TI. In: FOSSATTI, Nelson Costa; LUCIANO, Edimara Mezzomo (org.). **Prática Profissional em Administração:** ciência, método e técnica. Porto Alegre: Sulina, 2008, p. 157-174.

ROESCH, Sylvia Maria Azevedo. **Projetos de Estágio e de Administração:** guia para estágios, trabalhos de conclusão e estudos de caso. São Paulo: Atlas, 2006.

SILVA, Luiz Gustavo Cordeiro da; SILVA, Paulo Caetano da; BATISTA, Eduardo Mazza; HOMOLKA, Herbert Otto; JÚNIOR, Ivanildo Jose de Souza Aquino; LIMA, Marcelo Ferreira de. **Certificação Digital - Conceitos e Aplicações - Modelos Brasileiro e Australiano.**Editora Ciência Moderna: Rio de Janeiro, 2008.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** visão executiva da segurança da informação: aplicada a Security Officer. Rio de Janeiro: Elsevier, 2003, oitava reimpressão.

SMITH, Martin; SHERWOOD, John**. Business Continuity Planning**. Computer & Security, p. 14-23. Elsevier Science Ltda, 1995. Disponível em < http://www.sciencedirect.com/> Acesso em 01 nov., 2008

SNEDAKER, Susan. **Business Continuity and Disaster Recovery Planning for IT Professionals.** Elsevier, 2007. Disponível em <http://www.sciencedirect.com/science/book/9781597491723> Acesso em 1º nov., 2008.

STANTON, Ray. **Continuity in a disaster.** INFORSECURITY. Volume 4, Issue 8, November-December 2007, p. 24-*25* Nov/Dec. 2007. Disponível em <http://www.sciencedirect.com/> Acesso em 1º nov., 2008.

TESTA, Mauricio Gregianin; LUCIANO, Edimara Mezzomo; RECH, Ionara. Técnicas de coleta de dados. In: FOSSATTI, Nelson Costa; LUCIANO, Edimara Mezzomo (org.). **Prática Profissional em Administração:** ciência, método e técnica. Porto Alegre: Sulina, 2008, p. 67-85.

TEXAS DEPARTMENT OF INFORMATION RESOURCES. **Businnes Continuity Planning**. Rev. December, 2004. Austin, Texas. Disponível em <http://www.dir.state.tx.us/pubs/bcpg/bcpg.pdf> Acesso em 6 nov., 2008.

WEILL, Peter; ROSS, Jeanne W. **Governança de TI, Tecnologia da Inoformação**. São Paulo: M. Books do Brasil Editora Ltda, 2006.

YIN, Robert K. **Estudo de caso:** planejamento e métodos. Porto Alegre: Bookman, 2005.

APÊNDICE A – DADOS DE IDENTIFICAÇÃO

DADOS DE IDENTIFICAÇÃO DA ALUNA

Nome: Patrícia Marques da Silveira

Endereço: Rua Visconde de Pelotas, 155/ap. 308

Data de nascimento: 26/04/1980

Fone para contato: (51) 91010948

Email: pati.marques@hotmail.com

DADOS DE IDENTIFICAÇÃO DO SUPERVISOR

Nome: Rafael Krug Marques

Endereço: Praça Dr. Julio de Aragão Bozzano, 25/14

Data de nascimento: 05/03/1979

Fone para contato: (51) 3388-3269

Email: rkm79@terra.com.br

APÊNDICE B – PROPOSTA PARA PLANO DE GERENCIAMENTO DE INCIDENTE

1 OBJETIVO

Este documento tem por objetivo dar suporte ao gerenciamento da fase crítica de um incidente.

Na ocorrência de um incidente maior que afete o local onde está instalada a empresa, consequentemente o dano causado atingirá de alguma forma a continuidade dos serviços e do negócio, atingindo recursos e atividades críticas da organização, pois são nas instalações da empresa que estão localizados os colaboradores, os servidores com as informações de clientes, projetos, pesquisas, informações administrativas, estratégias, entre outras que possuem valor para a organização.

A execução das atividades contidas neste documento deve garantir a continuidade do negócio, satisfazendo os interesses do cliente (interno/externo).

2 RESPONSÁVEIS DO PGI

Nesta seção serão apresentados os responsáveis pela análise do PGI, assim como pelas correções e manutenções que ocorram. Abaixo são apresentados os responsáveis e as suas atividades com relação ao PGI:

- Diretor Administrativo (nome) – análise crítica do plano.
- Diretor de TI (nome) – análise crítica do plano, correção e atualização do plano.

3 ESCOPO

O escopo de gerenciamento de incidente deste documento refere-se à perda do local de trabalho, onde está incluída a ativação do plano, com os primeiros contatos que devem ser realizados na ocorrência do incidente, comunicações das equipes e clientes, atividades e ações para execução do plano. Outros planos podem ser ativados em paralelo a este, sendo apontado o documento de Plano de Continuidade de Negócios (PCN) e a seção correspondente, visto que o incidente pode afetar os recursos internos do local.

4 ANÁLISE DE RISCOS E IMPACTOS

A análise dos riscos foi realizada determinando a prioridade do risco através da análise da probabilidade de ocorrência do risco e os impactos causados pela ocorrência do mesmo. Foram determinados indicativos (baixo=1, médio =2 e alto=3) para qualificação da probabilidade e impacto, onde a soma dos indicadores resultou na prioridade do risco. Para os riscos que afetam as atividades críticas da empresa, foram elaborados os planos de contingências com os seus respectivos responsáveis e atividades.

Abaixo são apresentadas as informações pertinentes ao risco contido neste documento, assim como as informações pertinentes de mitigação e continuidade do negócio quando ocorre a impossibilidade de uso do local original de instalação da empresa.

5 GERENCIAMENTO DE INCIDENTE PARA PERDA DAS INSTALAÇÕES

Nas subseções abaixo serão apresentadas as informações úteis para o gerenciamento inicial do incidente, assim com as atividades subsequentes. Na seção 5.1 serão apresentadas as informações referentes ao risco, conseqüências de não se agir, as mitigações para minimizar a ocorrência do risco e as estratégias de continuidade, assim como os responsáveis pela ativação e execução do plano.

Na seção 5.2 serão apresentadas as atividades pertinentes a cada um dos responsáveis, desde o início de ativação do PGI até a ativação do PCN para alguns recursos. Nas subseções sequentes é apresentado o plano de comunicação, indicando a sequência de realização das comunicações e responsáveis, desenho de sequência das atividades, recursos financeiros disponíveis para contingência, equipamentos necessários e serviços que devem ser contratados.

5.1 PERDA DO LOCAL POR ALAGAMENTO/INCÊNDIO/DESABAMENTO

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre incidente maior que afete o local das instalações da empresa.

Risco	Perda do local por alagamento/incêndio/desabamento.	
Probabilidade: Baixa	**Impacto:** Alto	**Prioridade:** 4
Consequências de não se agir	• multas contratuais por atraso e não entrega dos serviços; • perda da confiabilidade na empresa por colaboradores e clientes; • perda de clientes; • perda de colaboradores; • perda de parceiros; • imagem prejudicada.	
Mitigação	• não realizar alterações/manutenções na estrutura do prédio sem antes consultar especialistas; • realizar vistorias programadas na estrutura física do prédio, incluindo hidráulica e elétrica; • contratar especialistas para manutenção quando necessário; • realizar vistorias diárias na empresa ao final do expediente, de forma a se certificar de que todas as torneiras estão fechas, cafeteiras e máquinas desligadas; • manter extintores de incêndio dentro na empresa; • realizar treinamentos para utilização de extintores; • realizar treinamentos apresentando opções de saída de emergência para os colaboradores no caso de evacuação do local; • realizar treinamentos de primeiros socorros; • conhecimento da infaestrutura do local que será utilizado como alternativa para alocação da equipe.	
ESTRATÉGIA DE CONTINUIDADE	• seguro no valor de R$80.000,00 (oitenta mil reais) a fim de cobrir as perdas de máquinas; • recurso de contingência no valor de R$50.000,00 (cinquenta mil reais) para cobrir gastos iniciais com compras de equipamentos, máquinas e servidores necessários; • financiamento (caso necessário); • aluguel de sala em Hotel (nome do Hotel) no centro de Porto Alegre, priorizando a proximidade do local afetado.	
Responsáveis	• Diretor Administrativo (nome) • Gerente de Projetos (nome) • Diretor de TI (nome) • Gerente Financeiro (nome) • Especialista 1 (nome) • Recursos Humanos (nome) • Suporte (nome)	
Tempo de Recuperação*	TMP = 4 dias NM = 80% TMR = 6 dias	
*Tempo de Recuperação: Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.		

5.2 ATIVIDADES E AÇÕES DOS RESPONSÁVEIS

Abaixo são apresentadas as atividades que cada envolvido deve executar, assim como a comunicação dos interessados. Nas atividades não estão listadas ações de primeiros socorros, pois todos os colaboradores da empresa devem estar preparados para prestar este atendimento quando necessário.

Responsável	Responsabilidade de atividades/ações
Diretor Administrativo (nome)	1- Avaliar a ocorrência do risco. 2- Ativar o PGI e PCN quando confirmado o incidente. 3- Evacuação do local (opção 1)*. 4- Comunicar serviços de emergência (consultar seção 6). 5- Comunicar responsáveis pela execução das atividades e ativação de outros planos (consultar seção 7). 6- Disponibilizar o *backup* das máquinas e servidores. 7- Efetuar as instalações dos *backups.*
Gerente Financeiro (nome)	1- Evacuação do local (opção 2)*. 2- Comunicar seguradora (consultar seção 8). 3- Comunicar local secundário (Hotel) sobre a utilização do local (consultar seção 8). 4- Marcar local e hora para reunião de comunicação já no local secundário (consultar seção 8). 5- Disponibilizar os recursos financeiros de contingência (consultar seção 5.2.3) para compra de equipamentos já definidos (consultar seção 5.2.4), como máquinas e servidores. 6- Contratar Datacenter para hospedagem das informações do servidor “W” (consultar seção 5.2.5). 7- Contratar serviço de internet 3G (consultar seção 5.2.5).
Gerente de Projetos (nome)	1- Comunicar equipes de trabalho e marcar a reunião de comunicação no local secundário (consultar seção 9). 2- Comunicar e tranqüilizar clientes (consultar seção 10). 3- Comunicar familiares de colaboradores quando necessário (consultar seção 9). 4- Acompanhar as instalações e preparação do ambiente secundário. 5- Realizar processo seleção quando verificada necessidade por morte de colaborador (consultar PCN, seção 6.2 e 6.2.1).
Diretor de TI (nome)	1- Avaliar as perdas e, conforme as necessidades dos projetos em execução, verificar o número de máquinas necessárias para compra. 2- Pegar o recurso financeiro e comprar equipamentos, máquinas e servidores identificados como necessários (consultar seção 5.2.3 e 5.2.4). 3- Auxiliar todas as instalações de máquinas, configurações e atualização do *backup* das máquinas e servidores. 4- Acompanhar e auxiliar todas as atividades de instalações das máquinas e preparação do ambiente até a estabilidade para o reinício das atividades.
Suporte (nome)	1- Auxiliar na compra dos equipamentos, máquinas e servidores necessários. 2- Preparar local secundário (Hotel) para receber equipamentos. 3- Realizar instalação e configuração das máquinas e servidores. 4- Colorar em um roteador o serviço de banda larga 3G (consultar 5.2.5). 5- Auxiliar nas instalações dos *backups* das máquinas e servidores. 6- Certificar-se do funcionamento correto de todas as máquinas e servidores.
Especialista 1 (nome)	1- Realiza treinamentos quando realizado contratados novos colaboradores por motivo de perda dos anteriores (consultar PCN índice 6.2 e 6.2.1).
* Todos os colaboradores devem ter treinamento indicando local e procedimentos de saída no caso de evacuação do local. São dois os responsáveis pelo alerta de orientação de evacuação, mas na ausência dos responsáveis, outros colaboradores podem iniciar o processo de evacuação.	

5.2.1 Plano De Comunicação Do Incidente

Abaixo é apresentado o desenho do Fluxo de Comunicação que deverá ocorrer assim que identificado o início do incidente de perda do local

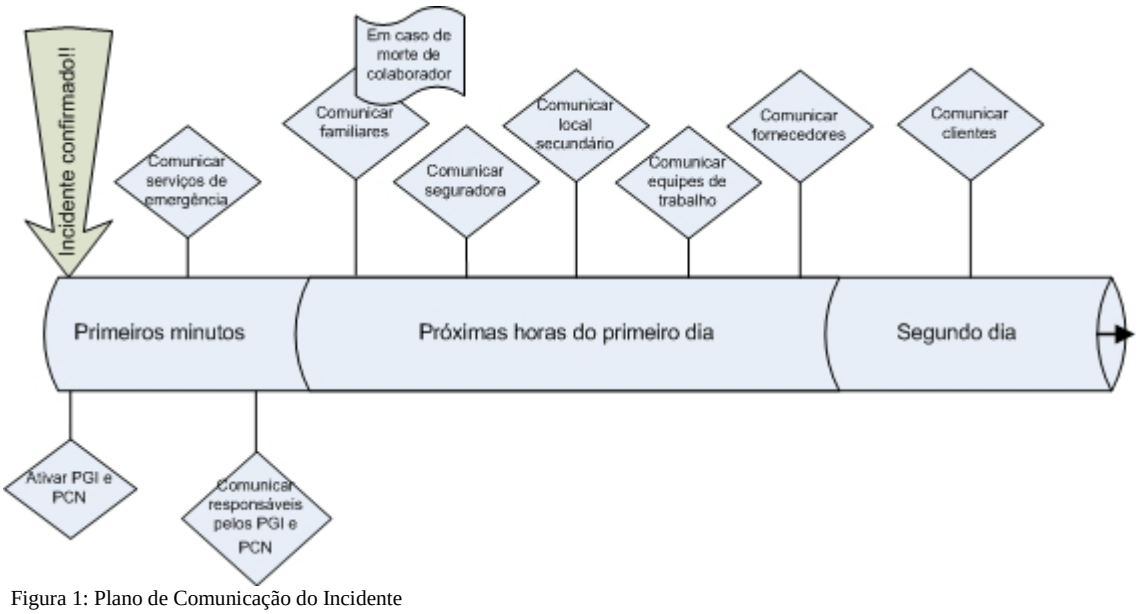

Figura 1: Plano de Comunicação do Incidente

Responsável pela comunicação	Quem recebe a comunicação
Diretor Administrativo (nome)	1- Comunicar serviços de emergência (consultar seção 6). 2- Comunicar responsáveis pelo PGI e PCN (consultar seção 7).
Gerente Financeiro (nome)	1- Comunicar seguradora (consultar seção 8). 2- Comunicar local secundário (Hotel) sobre a utilização do local (consultar seção 8). 3- Comunicar fornecedores (consultar seção 5.2.5).
Gerente de Projetos (nome)	1- Comunicar equipes de trabalho e marcar a reunião de comunicação no local secundário (consultar seção 9). 2- Comunicar familiares quando ocorrer morte de colaborador. 3- Comunicar e tranqüilizar clientes (consultar seção 10).

5.2.2 Desenho De Sequência Das Atividades

Abaixo é apresentado o desenho da sequência de atividades e ações apresentadas no item 5.6 deste documento. Estas atividades devem ser realizadas pelos responsáveis conforme o prazo determinado.

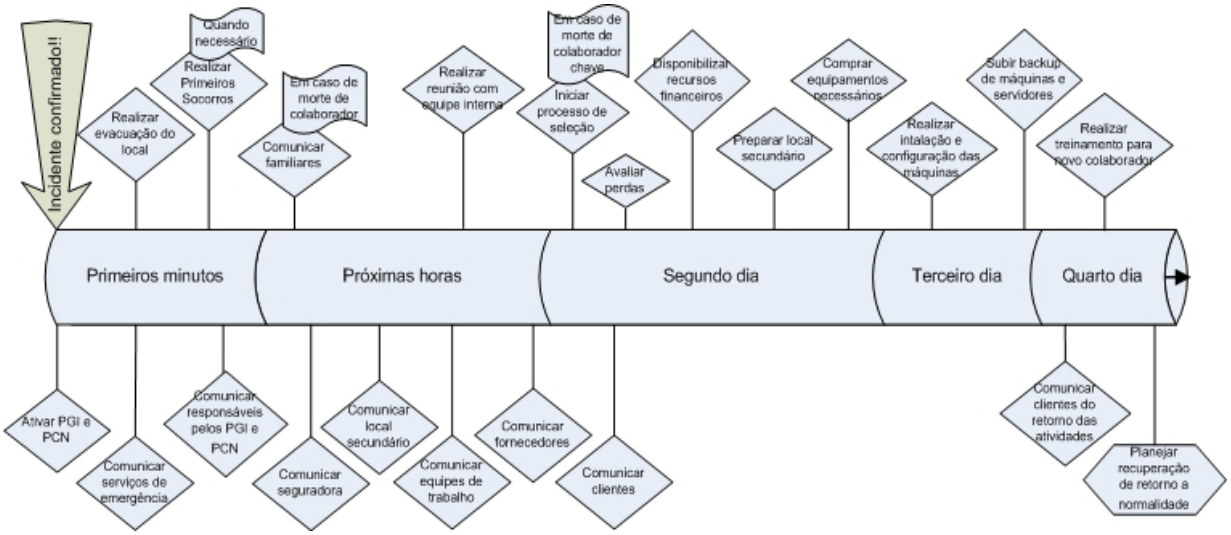

Figura 2: Desenho de sequência das atividades

5.2.3 Recursos Financeiros de contingência

Como forma de garantir a continuidade dos serviços e consequentemente do negócio, a empresa disponibiliza recursos financeiros de forma contingenciar as perdas ocasionadas pelo incidente. Abaixo são apresentados os recursos disponíveis para os gastos emergenciais.

Recurso Financeiro	Responsável pelo recurso	Valor (R$)	Quando acionar
Seguro de bens físicos	Gerente Financeiro	80.000,00	Quando ocorrer perda do local de trabalho, o seguro cobre as perdas físicas de máquinas e servidores (consultar seção 8).
Reserva de contingência	Gerente Financeiro	50.000,00	Para contingenciar gastos emergenciais.
Financiamento	Gerente Financeiro	-	A empresa possui credibilidade no mercado financeiro, ficando viável um financiamento para cobrir gastos emergenciais.

5.2.4 Lista de equipamentos necessários

Para o reinício das atividades no ambiente secundário, é necessário preparar o ambiente com equipamentos e máquinas necessárias para o início das atividades. Então, após a avaliação das perdas e identificação das necessidades de cada projeto que está sendo executado, é identificada a necessidade de compras extras, além das que já estavam planejadas para o gerenciamento do incidente. Para os equipamentos, pode ser utilizado o

recurso financeiro de continuidade já disponível ou um financiamento extra. Abaixo é apresentada a lista dos equipamentos já programados para compra.

Equipamentos	Qnt.	Configuração	Funcionalidade
Máquina	1	Core 2DUO 2400+2.40GHz com 160 GB e 8GB de RAM	Para virtualizar as informações dos servidores “X”, “Y” e ”Z” perdidos e subir os *backups*.
Notebooks	4	AMD Turion 64 Mobile 1.58 GHz, com HD 160GB e 2GB de RAM	Para restabelecimento dos *backups* do administrativo.
Máquina	1	Pentium 3 de 550MHZ Xenon com 2MD de Cachê, um HD de 20 GB SCSI mais um HD de 9GB SCSI e 1,50GB de RAM	Para recuperação do ambiente do servidor “W” e que deve ser hospedado em Datacenter contratado. Ver(índice 5.6.3)

Além das máquinas previstas listadas acima e as específicas conforme a verificação de necessidade dos projetos devem ser comprados cabos de rede e hubs suficientes para preparação do local secundário de forma a atender os projetos em andamento.

5.2.5 Serviços que devem ser contratados

Para recuperação e disponibilização das informações aos usuários que estarão operando durante o período de contingências, é necessário a hospedagem das informações do servidor “W” e disponibilização de acesso a internet. Para estes serviços serão contratados os serviços listados abaixo:

Serviço	Fornecedor	Telefones	Endereço	Função
Datacenter	uolHost	4003.9011	Rua General Bento Martins, 24. Porto Alegre	Para hospedagem das informações do servidor “W”.
Banda larga 3G sem fio	CLARO	1052	Rua: Andradas, 1501, Centro. Porto Alegre	Para disponibilização de acesso a internet.

6 TELEFONES DE EMERGÊNCIA

Abaixo é apresentada a lista dos contatos dos serviços de emergências, que deve ser acionado assim que for detectado o incidente.

TELEFONES DE EMERGÊNCIA	
Corpo de Bombeiros	193
Polícia Civil	197
Polícia Militar	190
Serviço de Atendimento Médico de Urgência (SAMU)	192

7 CONTATO DOS RESPONSÁVEIS PELA ATIVAÇÃO/EXECUÇÃO

Abaixo é apresentada a lista dos primeiros contatos que devem ser realizados quando identificado que o local de trabalho foi afetado por um incidente. Estas pessoas são responsáveis direta ou indiretamente pelo gerenciamento do incidente, por isto a importância da primeira comunicação.

Responsável	Telef. Cel.	Telef. Resid.	Endereço
Diretor Administrativo (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Gerente de Projetos (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Diretor de TI (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Gerente Financeiro (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Especialista 1 (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Recursos Humanos (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Suporte (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA

8 CONTATO DA SEGURADORA E LOCAL SECUNDÁRIO

Abaixo é apresentado o telefone de contato da seguradora, para acionamento do seguro e o telefone do local secundário onde vai ser montada as instalações para continuidade do negócio.

Nome do recurso	Telefone 1	Telefone 2	Endereço
Banco seguradora (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Hotel (nome)	5191010102	5133727272	Rua: Beta, 2 - Centro – POA

9 CONTATO DE COLABORADORES

Abaixo é apresentado o telefone dos colaboradores da empresa para comunicação do incidente e agendamento da primeira reunião de comunicação. Também é apresentado o contato de um familiar dos colaboradores, para comunicação caso o incidente afete diretamente o colaborador.

Nome	Telef. Cel.	Telef. Resid.	Contato Familiar	Endereço
Diretor Administrativo (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Gerente de Projetos (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Diretor de TI (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Gerente Financeiro (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Recursos Humanos (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Suporte (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Analista de Projeto 2 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Analista de Projeto 3 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Analista de Projeto 3 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Testador 1 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Testador 2 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Testador 3 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Testador 4 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Especialista 1 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Especialista 2 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA
Especialista 3 (nome)	51-99999999	51-3333.3333	51-3333.3333 (nome)	Rua: Beta, 2 - Centro – POA

10 CONTATO DE CLIENTES

Abaixo são apresentados os telefones dos clientes da ALFA, onde o Gerente de Projetos deverá realizar a comunicação do incidente e tranquilizar o cliente em relação à garantia de entrega dos projetos que estão sendo executados. Após o reinício das atividades, o Gerente de Projetos também deve comunicar o cliente.

Nome	Telef. 1	Telef. 2
Empresa Beta	51-99999999	51-3333.3333
Empresa Gama	51-99999999	51-3333.3333
Empresa XYZ	51-99999999	51-3333.3333
Empresa ABC	51-99999999	51-3333.3333
Empresa JKM	51-99999999	51-3333.3333
Empresa OPQ	51-99999999	51-3333.3333
Empresa RST	51-99999999	51-3333.3333

APÊNDICE C – PROPOSTA PARA PLANO DE CONTINUIDADE DE NEGÓCIOS

1 OBJETIVO

Este documento tem por objetivo dar suporte ao restabelecimento dos serviços no caso de incidente que afete as instalações, garantindo a continuidade do negócio da empresa. Desta forma a empresa mantém o cumprimento dos contratos, fazendo com que o cliente receba os serviços com a qualidade e o prazo planejado.

2 RESPONSÁVEIS DO PCN

Nesta seção serão apresentados os responsáveis pelo PCN e as suas atividades com relação ao documento.

- Diretor Administrativo (nome) – análise crítica do plano.
- Diretor de TI (nome) – análise crítica do plano, correção e atualização do plano.

3 ESCOPO

O escopo de continuidade deste documento refere-se à recuperação dos recursos que influenciam diretamente nas atividades consideradas como críticas para organização. A determinação deste escopo ocorreu através da análise dos riscos e impactos. Abaixo é apresentado o escopo de continuidade:

- Pessoas;
- Instalações;
- Informação; e
- Fornecedores.

4 ANÁLISE DE RISCOS

A análise dos riscos foi realizada determinando a prioridade do risco através da análise da probabilidade de ocorrência do risco e os impactos causados pela ocorrência do mesmo.

Foram determinados indicativos (baixo=1, médio =2 e alto=3) para qualificação da probabilidade e impacto, onde a soma dos indicadores resultou na prioridade do risco. Para os riscos que afetam as atividades críticas da empresa, foram elaborados os planos de contingências com os seus respectivos responsáveis e atividades.

Para cada risco considerado como crítico foi elaborado um plano de contingência. Todas as contingências para os possíveis riscos são apresentadas nas seções 6 a 9. Nestas seções, também é apresentada a prioridade do risco, probabilidade e impacto identificados durante a análise e as consequências por não se tomar as ações devidas.

Na próxima seção serão apresentados os responsáveis pela ativação dos planos de contingência, conforme o escopo dos recursos.

5 RESPONSABILIDADES DE ATIVAÇÃO/EXECUÇÃO

Abaixo são apresentados os papéis e as responsabilidades das pessoas quanto à tomada de decisão durante e após incidente. Estas pessoas são os responsáveis pela ativação dos planos, envolvimento com relação aos gastos financeiros necessários para determinadas contingências ou no auxilio para execução de determinadas ações do plano.

Recurso	Responsável	Responsabilidade
Pessoas	Gerente de Projetos (nome)	1- Ativar o Plano. 2- Analisar criticidade de projetos. 3- Realizar processo de seleção. 4- Realizar comunicação interna/externa.
	Recursos Humanos (nome)	1- Realiza processo de seleção. 2- Avaliar plano de sucessão.
	Especialista 1 (nome)	1- Realizar treinamentos.
Informação	Diretor Administrativo (nome)	1- Ativar o Plano. 2- Disponibilizar *backup* do servidor. 3- Efetuar a instalação de *backup*.
	Diretor de TI (nome)	1- Pegar recurso financeiro para compra de servidor. 2- Auxiliar nas instalações de *backup* até que o ambiente esteja estável para início das atividades.
	Gerente de Projetos (nome)	1- Realizar comunicação interna/externa.
	Gerente Financeiro (nome)	1- Liberar verbas de contingência.
	Suporte (nome)	1- Auxiliar na instalação do *backup*.
Fornecedores	Diretor de TI (nome)	1- Ativar Plano 2- Comunicar fornecedor.

	Suporte (nome)	1- Ativar gerador de energia. 2- Entrar em contato com fornecedor
	Gerente de Projetos (nome)	1- Realizar comunicação interna/externa.

5.1 CONTATO DOS RESPONSÁVEIS PELA ATIVAÇÃO/EXECUÇÃO

Abaixo é apresentada a lista para contato dos responsáveis pela ativação e execução dos planos de contingência contidos neste documento.

Responsável	Telef. Cel.	Telef. Resid.	Endereço
Diretor Administrativo (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Gerente de Projetos (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Diretor de TI (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Gerente Financeiro (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Especialista 1 (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Recursos Humanos (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA
Suporte (nome)	51-99999999	51-3333.3333	Rua: Beta, 2 - Centro – POA

6 CONTINGÊNCIA PARA PERDA DE COLABORADOR CHAVE

Na falta de colaborador chave por motivo de doença, ausência temporária, demissão ou morte, a empresa tem como garantir a continuidade dos serviços prestados ao cliente, pois as informações e conhecimentos adquiridos durante a execução de um projeto são documentados e armazenados em repositório interno da empresa. Este repositório está localizado em um servidor dentro da organização e o acesso a estas informações são controladas, podendo o usuário acessar somente as informações pertinentes ao seu projeto em execução. Desta forma, outra pessoa com conhecimentos técnicos tem a possibilidade de dar continuidade ao andamento de um projeto, mesmo que este projeto tenha sido iniciado por outra pessoa, pois a base de conhecimento necessário para o andamento de um projeto está dentro da empresa. Ficando o cliente assegurando quanto ao andamento dos projetos.

Abaixo são apresentados os tipos de incidentes que podem ocorrer e as mitigações adotadas para cada tipo de ocorrência, como forma de minimizar os efeitos do incidente. Também são apresentadas as estratégias de continuidade adotadas após início do incidente, as consequências de não se agir e o prazo para restabelecimento do serviço.

6.1 FALTA DE COLABORADOR CHAVE

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre falta de colaborador chave.

Risco	Falta de colabora-dor chave por motivo de doença.	
Probabilidade: Baixa	**Impacto:** Alto	**Prioridade:** 4
Consequências de não se agir	• atraso nas atividades antes executadas pelo colaborador; • atraso na entrega de projeto; • pagamento de multa por não cumprimento do contrato.	
Mitigação	• manter documentos de trabalho sempre detalhados e atualizados; • manter estes documentos em repositório no servidor interno da empresar; • manter documento detalhado contendo informações das atividades críticas do projeto; • manter em documento atualizado informações de contato com cliente e status do projeto; • manter programa de treinamentos atualizados; • manter treinamentos para cada setor, de forma a manter pessoas do mesmo setor com a mesma base de conhecimento.	
ESTRATÉGIA DE CONTINUIDADE	• substituir o colaborador por outro da mesma equipe e que possua o mesmo nível de conhecimento, ou • substituir o colaborador por outro de equipe diferente e que possua o mesmo nível de conhecimento, ou • contratar um novo colaborador com o mesmo nível de conhecimento.	
Responsáveis	• Gerente de Projetos (nome) • Recursos Humanos (nome) • Especialista 1 (nome)	
Tempo de Recuperação*	TMP = 2 dias NM = 70% TMR = 3dias	
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.		

6.1.1 LISTA DE TAREFAS

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente, de forma a contingenciar a falta/ausência do colaborador chave.

Passo	Responsável	Procedimento
1	Recursos Humanos (nome)	**1.1-** Assim que detectada a ausência do colaborador, Recursos Humanos deve entrar em contato com o colaborador para verificar a situação de saúde e tempo de ausência. **1.2-** Colaborador confirmou doença e ausência temporária, passar para próximo passo (2).

2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve avaliar o nível de criticidade do projeto e tomar as decisões entre aguardar por 2 dias o retorno ou colaborador ou ativar o plano de continuidade. **2.2-** Projeto é identificado como crítico e colaborador necessita ficar afastado por mais de 2 dias, Gerente de Projetos ativa o plano de continuidade. Passa para o passo (3).
3	Gerente de Projetos (nome)	**3.1-** Gerente de Projetos avalia se tem recurso capacitado dentro da própria equipe de projeto para substituir colaborador chave. **3.1.1-** Tendo recurso disponível na própria equipe, comunica ao substituto, a equipe e ao cliente sobre a substituição (fim). **3.1.2-** Não tendo recurso dentro da própria equipe de projeto, passa para passo 3.2. **3.2-** Gerente de Projetos avalia se tem recurso capacitado e disponível dentro de outra equipe de projeto para substituir colaborador chave. **3.2.1-** Tendo recurso disponível em outra equipe, comunica ao substituto, a equipe e ao cliente sobre a substituição (fim). **3.2.2-** Não tendo recurso dentro da outra equipe, passa para o passo (4).
4	Recursos Humanos (nome) Gerente de Projetos (nome)	**4.1**- Recursos Humanos e Gerente de Projetos reavaliam os currículos de pessoas já entrevistadas pela empresa. **4.2-** Recursos Humanos marca entrevistas. **4.3-** Recursos Humanos e Gerente de Projetos realizam a entrevista e seleção. **4.4-** Recursos Humanos comunica para a empresa o novo colaborador. Passa para passo (5). **4.5 -** Gerente de Projetos comunica a equipe e ao cliente sobre o novo colaborador que irá realizar a substituição.
5	Especialista 1 (nome)	**5.1**- Especialista 1 realiza treinamento para o novo colaborador e apresenta o projeto que vai ser continuado por ele (fim).

6.2 PERDA DE COLABORADOR CHAVE POR DESLIGAMENTO/MORTE

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre a perda do colaborador chave por desligamento ou morte.

Risco	Perda de colaborador chave por desligamento /morte.	
Probabilidade: Baixa	**Impacto:** Alto	**Prioridade:** 4
Consequências de não se agir	• atraso nas atividades antes executadas pelo colaborador; • atraso na entrega de projeto; • pagamento de multa por não cumprimento do contrato.	
Mitigação	• manter documentos de trabalho sempre detalhados e atualizados; • manter estes documentos em repositório no servidor interno da empresar; • manter documento detalhado contendo informações das atividades críticas do projeto; • manter em documento atualizado informações de contato com cliente e status do projeto; • manter planejamento de sucessão; • manter programa de treinamentos atualizados; • manter treinamentos para cada setor, de forma a manter pessoas do mesmo setor com a mesma base de conhecimento.	

ESTRATÉGIA DE CONTINUIDADE	• substituir o colaborador pelo seu sucessor, conforme planejamento de sucessão; ou • contratar um novo colaborador com o mesmo nível de conhecimento.
Responsáveis	• Gerente de Projetos (nome) • Recursos Humanos (nome) • Especialista 1 (nome)
Tempo de Recuperação*	TMP = 3 dias NM = 60% TMR = 4dias
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.	

6.2.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificada a ocorrência do incidente, de forma a contingenciar o desligamento ou a morte do colaborador chave.

Passo	Responsável	Procedimento
1	Gerente de Projetos (nome)	**1.1 -** Assim que for confirmada a ausência do colaborador, Gerente de Projetos deve ativar o plano. **1.2** - Gerente de projetos deve comunicar Recursos Humanos e Especialista 1.
2	Recursos Humanos (nome)	**2.1-** Recursos Humanos deve avaliar plano de sucessão e verificar o sucessor para o colaborador ausente. **2.2-** Recursos Humanos identificou que há sucessor para o colaborador. Passar para o próximo passo (3). **2.3-** Recursos Humanos não identificou sucessor para o colaborador . Passar para o próximo passo (4).
3	Gerente de Projetos (nome) Especialista 1 (nome)	**3.1-** Gerente de Projetos deve comunicar ao sucessor, a equipe e ao cliente sobre a substituição. **3.2-** Especialista 1 deve realizar treinamento para o novo sucessor (fim).
4	Recursos Humanos (nome) Gerente de Projetos (nome)	**4.1**- Recursos Humanos e Gerente de Projetos reavaliam os currículos de pessoas já entrevistadas pela empresa. **4.2-** Recursos Humanos marca entrevistas. **4.3-** Recursos Humanos e Gerente de Projetos realizam a entrevista e seleção. **4.4-** Recursos Humanos comunica para a empresa o novo colaborador. Passa para passo (4) **4.5 -** Gerente de Projetos comunica a equipe e ao cliente sobre o novo colaborador que irá realizar a substituição.
5	Especialista 1 (nome)	**5.1**- Especialista 1 passa treinamento para o novo colaborador e apresenta o projeto que vai ser continuado por ele (fim).

6.3 PERDA DE COLABORADOR CHAVE POR PEDIDO DE DEMISSÃO

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre a perda do colaborador chave por pedido de demissão.

Risco	Perda de colaborador chave por pedido de demissão.	
Probabilidade: Baixa	**Impacto:** Alto	**Prioridade:** 4
Consequências de não se agir	• atraso nas atividades antes executadas pelo colaborador; • atraso na entrega de projeto; • pagamento de multa por não cumprimento do contrato.	
Mitigação	• manter documentos de trabalho sempre detalhados e atualizados; • manter estes documentos em repositório no servidor interno da empresar; • manter documento detalhado contendo informações das atividades críticas do projeto; • manter em documento atualizado informações de contato com cliente e status do projeto; • manter planejamento de sucessão; • manter programa de retenção para os colaboradores; • manter programa de treinamentos atualizados; • manter treinamentos para cada setor, de forma a manter pessoas do mesmo setor com a mesma base de conhecimento.	
ESTRATÉGIA DE CONTINUIDADE	• substituir o colaborador pelo seu sucessor, conforme planejamento de sucessão; ou • contratar um novo colaborador com o mesmo nível de conhecimento.	
Responsáveis	• Gerente de Projetos (nome) • Recursos Humanos (nome) • Especialista 1 (nome)	
Tempo de Recuperação*	TMP = 3 dias NM = 60% TMR = 4dias	
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.		

6.3.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificada o incidente, de forma a contingenciar o pedido de demissão do colaborador chave.

Passo	Responsável	Procedimento
1	Gerente de Projetos (nome)	**1.1-** Assim que for confirmada demissão do colaborador, Gerente de Projetos deve ativar o plano.
2	Recursos Humanos (nome)	**2.1-** Recursos Humanos deve avaliar plano de sucessão e verificar o sucessor para o colaborador ausente. **2.2-** Recursos Humanos identificou que há sucessor para o colaborador. Passar para o próximo passo (3).

		2.3- Recursos Humanos não identificou sucessor para o colaborador . Passar para o próximo passo (4).
3	Gerente de Projetos (nome) Especialista 1 (nome)	**3.1-** Gerente de Projetos deve comunicar ao sucessor, a equipe e ao cliente sobre a substituição. **3.2-** Especialista 1 deve passar treinamento para o novo sucessor (fim).
4	Recursos Humanos (nome) Gerente de Projetos (nome)	**4.1**- Recursos Humanos e Gerente de Projetos reavaliam os currículos de pessoas já entrevistadas pela empresa. **4.2-** Recursos Humanos marca entrevistas. **4.3-** Recursos Humanos e Gerente de Projetos realizam a entrevista e seleção. **4.4-** Recursos Humanos comunica para a empresa o novo colaborador. Passa para passo (5)
5	Especialista 1 (nome)	**5.1**- Especialista 1 passa treinamento para o novo colaborador e apresenta o projeto que vai ser continuado por ele (fim).

7 CONTINGÊNCIA PARA PERDA DAS INFORMAÇÕES

Na ocorrência de incidente que afete as informações, este plano de contingência deverá ser ativado de modo a garantir a continuidade dos serviços e entrega dos projetos. Além do plano de continuidade, a empresa mantém uma lista de mitigações de forma a minimizar os danos que venham a ocorrer no caso de incidente.

Abaixo são apresentadas, para cada uma das ocorrências, as mitigações adotadas e as consequências de não se agir caso os eventos ocorram.

7.1 PERDA DOS DADOS/INFORMAÇÕES DO SERVIDOR “W”

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre perda dos dados/informações do servidor “W”.

Risco	Perda dos dados/informações do servidor “W”.	
Probabilidade: Média	**Impacto:** Alto	**Prioridade:** 5
Consequências de não se agir	• perda de informações de projetos; • multas contratuais por atraso e não entrega dos serviços; • perda da confiabilidade na empresa por colaboradores e clientes.	
Mitigação	• manter diferentes perfis de acesso para os usuários; • liberar acesso somente das informações necessárias para o usuário; • realizar *backup* automático de uma em uma hora armazenando as informações em servidor externo.	
ESTRATÉGIA DE CONTINUIDADE	• subir a última atualização do *backup* armazenado no servidor externo.	
Responsáveis	• Diretor Administrativo (nome) • Gerente de Projetos (nome)	

	• Diretor de TI (nome) • Suporte (nome)
Tempo de Recuperação*	TMP = 1 dia NM = 90% TMR = 2 dias
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.	

7.1.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente, de forma a contingenciar a perda dos dados/informações do servidor “W”.

Passo	Responsável	Procedimento
1	Diretor Administrativo (nome)	**1.1-**Assim que for confirmada a perda das informações do servidor “W”, Diretor Administrativo deve ativar o Plano. **1.2-**Diretor Administrativo de comunicar Gerente de Projetos, Gerente de TI e Suporte.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve comunicar as equipes. **2.2-** Gerente de Projetos deve comunicar a indisponibilidade do ambiente e o prazo para o cliente.
3	Diretor Administrativo (nome) Suporte (nome)	**3.1-** Diretor Administrativo deve disponibilizar *backup* do servidor “W”. **3.2**- Diretor Administrativo deve instalar o *backup* no servidor. **3.3**- Suporte deve auxiliar na instalação do *backup*.
4	Diretor de TI (nome)	**4.1**- Diretor de TI deve auxiliar nas instalações até que o ambiente esteja estável para início das atividades.
5	Gerente de Projetos (nome)	**5.1**- Gerente de Projetos comunica as equipes à disponibilização do ambiente. **5.2**- Gerente de Projetos comunica ao cliente a disponibilização do ambiente.

7.2 AVARIA DO SERVIDOR “W”

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre avaria no servidor “W”.

Risco	Avaria do servidor “W”.	
Probabilidade: Média	**Impacto:** Alto	**Prioridade:** 5
Consequências de não se agir	• perda de informações de projetos; • multas contratuais por atraso e não entrega dos serviços; • perda da confiabilidade na empresa por colaboradores e clientes.	

Mitigação	• realizar *backup* automático de uma em uma hora armazenando as informações em servidor externo.
ESTRATÉGIA DE CONTINUIDADE	• comprar novo servidor ou peça de substituição. • subir a última atualização do *backup* armazenado no servidor externo.
Responsáveis	• Diretor Administrativo (nome) • Gerente de Projetos (nome) • Diretor de TI (nome) • Suporte (nome) • Financeiro (nome)
Tempo de Recuperação*	TMP = 2 dias NM = 90% TMR = 3 dias
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.	

7.2.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas no momento de identificação do incidente de forma a contingenciar a avaria do servidor “W”.

Passo	Responsável	Procedimento
1	Diretor Administrativo (nome)	**1.1-** Assim que for confirmada a avaria do servidor “W”, Diretor Administrativo deve ativar o Plano. **1.2-** Diretor Administrativo de comunicar Gerente Financeiro, Gerente de Projetos, Gerente de TI e Suporte. **1.3-** Diretor Administrativo deve avaliar os danos do servidor e decidir compra de peça de substituição ou troca de servidor.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve comunicar as equipes. **2.2-** Gerente de Projetos deve comunicar a indisponibilidade do ambiente e o prazo para o cliente.
3	Gerente Financeiro (nome)	**3.1-** Gerente Financeiro deve liberar recurso de contingência para compra de peça ou compra de servidor.
4	Diretor Administrativo (nome) Suporte (nome)	**4.1-** Diretor Administrativo deve disponibilizar *backup* do servidor “W”. **4.2**- Diretor Administrativo deve instalar o *backup* no servidor. **4.3**- Suporte deve auxiliar na instalação do *backup.*
5	Diretor de TI (nome)	**5.1**- Diretor de TI deve auxiliar nas instalações até que o ambiente esteja estável para início das atividades.
6	Gerente de Projetos (nome)	**6.1**- Gerente de Projetos comunica as equipes à disponibilização do ambiente. **6.2**- Gerente de Projetos comunica ao cliente a disponibilização do ambiente.

7.3 PERDA DOS DADOS/INFORMAÇÕES DOS SERVIDORES “X”, “Y” E “Z”

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre perda dos dados/informações dos servidores “X”, “Y”ou “Z”.

Risco	Perda dos dados/informações do servidor “X”, “Y” ou “Z”.	
Probabilidade: Média	**Impacto:** Alto	**Prioridade:** 5
Consequências de não se agir	• perda de informações de projetos e administrativas; • multas contratuais por atraso e não entrega dos serviços; • perda da confiabilidade na empresa por colaboradores e clientes.	
Mitigação	• manter diferentes perfis de acesso para os usuários; • liberar acesso somente das informações necessárias para o usuário; • realizar *backup* diário do servidor 2, armazenando em fitas DDS2 fora da empresa; • uma vez por semana armazenar o *backup* no servidor externo da empresa.	
ESTRATÉGIA DE CONTINUIDADE	• subir a última atualização do *backup* armazenado no servidor externo ou das fitas DDS2.	
Responsáveis	• Diretor Administrativo (nome) • Gerente de Projetos (nome) • Diretor de TI (nome) • Suporte (nome)	
Tempo de Recuperação*	TMP = 1 dia NM = 90% TMR = 2 dias	
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.		

7.3.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente, de forma a contingenciar a perda dos dados/informações dos servidores “X”, “Y” ou “Z”.

Passo	Responsável	Procedimento
1	Diretor Administrativo (nome)	**1.1-** Assim que for confirmada a perda das informações de um dos servidores: “X”, “Y”, ou “Z”, Diretor Administrativo deve ativar o Plano. **1.2-**Diretor Administrativo de comunicar Gerente de Projetos, Gerente de TI e Suporte.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve comunicar as equipes de projeto e administrativas.
3	Diretor Administrativo (nome) Suporte (nome)	**3.1-** Diretor Administrativo deve disponibilizar *backup* dos servidores que ocorreu a perda das informações: “X”, “Y”, ou “Z”. **3.2**- Diretor Administrativo deve instalar o *backup* nos servidores em que ocorreu

		o incidente. **3.3**- Suporte deve auxiliar na instalação do *backup*.
4	Diretor de TI (nome)	**4.1**- Diretor de TI deve auxiliar nas instalações até que o ambiente esteja estável para início das atividades.
5	Gerente de Projetos (nome)	**5.1**- Gerente de Projetos comunica as equipes de projetos e administrativas sobre a disponibilização do ambiente.

7.4 AVARIA DOS SERVIDORES “X”, “Y” OU “Z”

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre avaria em um dos servidores “X”, “Y” ou “Z”.

Risco	Avaria dos servidores “X”, “Y” ou “Z”.	
Probabilidade: Média	**Impacto:** Alto	**Prioridade:** 5
Consequências de não se agir	• perda de informações de projetos; • multas contratuais por atraso e não entrega dos serviços; • perda da confiabilidade na empresa por colaboradores e clientes.	
Mitigação	• realizar *backup* diário do servidor 2, armazenando em fitas DDS2 fora da empresa; • uma vez por semana armazenar o *backup* no servidor externo da empresa.	
ESTRATÉGIA DE CONTINUIDADE	• comprar novo servidor ou peça de substituição. • subir a última atualização do *backup* armazenado no servidor externo.	
Responsáveis	• Diretor Administrativo (nome) • Gerente de Projetos (nome) • Diretor de TI (nome) • Suporte (nome) • Financeiro (nome)	
Tempo de Recuperação*	TMP = 2 dias NM = 90% TMR = 3 dias	
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.		

7.4.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente,de forma a contingenciar a avaria dos servidores “X”, “Y” e “Z”.

Passo	**Responsável**	**Procedimento**
1	Diretor Administrativo (nome)	**1.1-** Assim que for confirmada a avaria de um dos servidores: “X”, “Y” ou “Z”. Diretor Administrativo deve ativar o Plano. **1.2-** Diretor Administrativo de comunicar Gerente Financeiro, Gerente de

		Projetos, Gerente de TI e Suporte. **1.3-** Diretor Administrativo deve avaliar os danos do servidor e decidir compra de peça de substituição ou troca de servidor.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve comunicar as equipes.
3	Gerente Financeiro (nome)	**3.1-** Gerente Financeiro deve liberar recurso de contingência para compra de peça ou compra de servidor.
4	Diretor Administrativo (nome) Suporte (nome)	**4.1-** Diretor Administrativo deve disponibilizar *backup* do servidor "W". **4.2**- Diretor Administrativo deve instalar o *backup* no servidor. **4.3**- Suporte deve auxiliar na instalação do *backup*.
5	Diretor de TI (nome)	**5.1**- Diretor de TI deve auxiliar nas instalações até que o ambiente esteja estável para início das atividades.
6	Gerente de Projetos (nome)	**6.1**- Gerente de Projetos comunica as equipes a disponibilização do ambiente.

8 CONTINGÊNCIA PARA PERDA DE SERVIÇO DO FORNECEDOR

Este plano de continuidade deve ser ativado de modo a garantir a continuidade dos serviços terceirizados, pois estes afetam diretamente no andamento dos projetos executados pela ALFA.

Abaixo é apresentado, para cada uma das ocorrências referente a perda de serviço do fornecedor, as mitigações adotadas e as consequências de não se agir caso os eventos ocorram.

8.1 FALTA DE ENERGIA ELÉTRICA

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre a falta de energia elétrica. O respectivo fornecedor e contato são apresentados na seção 10.

Risco	Falta de energia elétrica.	
Probabilidade: Média	**Impacto:** Média	**Prioridade:** 4
Consequências de não se agir	• multas contratuais por atraso e não entrega dos serviços.	
Mitigação	• manter celulares com tecnologia 3G para contingência.	
ESTRATÉGIA DE CONTINUIDADE	• acionar a empresa de energia elétrica comunicando o ocorrido e verificando prazos de retorno. • Utilizar celulares de tecnologia 3G para acesso à internet.	
Responsáveis	• Gerente de Projetos (nome) • Diretor de TI (nome) • Suporte (nome)	

Tempo de Recuperação*	TMP = 2 horas NM = 90% TMR = 4 horas
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.	

8.1.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente, de forma a contingenciar a falta de energia elétrica.

Passo	Responsável	Procedimento
1	Diretor de TI (nome)	**1.1-** Assim que for confirmada a falta de energia elétrica, Diretor de TI deve ativar o Plano. **1.2-** Diretor de TI de comunicar Gerente de Projetos e Suporte. **1.3-** Diretor de TI deve comunicar o fornecedor sobre a ocorrência.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve comunicar as equipes. **2.2-** Gerente de Projetos deve comunicar a indisponibilidade do ambiente e o prazo para o cliente. **2.3-** Gerente de Projetos deve avaliar os projetos críticos para o uso do gerador.
3	Suporte (nome)	**3.1-** Suporte deve verificar e acionar o gerador de energia para ser utilizado com os projetos críticos.
4	Gerente de Projetos (nome)	**4.1**- Gerente de Projetos comunica as equipes à disponibilização do ambiente. **4.2**- Gerente de Projetos comunica ao cliente a disponibilização do ambiente.

8.2 FALHA NO LINK EXTERNO DE REDE (INTERNET)

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre falha no serviço de internet. O respectivo fornecedor e contato são apresentados na seção 10.

Risco	Falha no *link* externo de rede (internet).	
Probabilidade: Baixa	**Impacto:** Alto	**Prioridade:** 4
Consequências de não se agir	• multas contratuais por atraso e não entrega dos serviços.	
Mitigação	• manter celulares com tecnologia EDGE.	
ESTRATÉGIA DE CONTINUIDADE	• acionar a empresa fornecedora de internet comunicando o ocorrido e verificando prazos de retorno. • Utilizar celulares de tecnologia EDGE para emular internet para toda empresa.	
	• Gerente de Projetos (nome)	

	• Diretor de TI (nome) • Suporte (nome)
Tempo de Recuperação*	TMP = 2 horas NM = 90% TMR = 4 horas
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.	

8.2.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente, de forma a contingenciar a falha no *link* de internet.

Passo	Responsável	Procedimento
1	Diretor de TI (nome)	**1.1-** Assim que for confirmada a falha internet, Diretor de TI deve ativar o Plano. **1.2-** Diretor de TI de comunicar Gerente de Projetos e Suporte. **1.3-** Diretor de TI deve comunicar o fornecedor da ocorrência.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve comunicar as equipes.
3	Suporte (nome)	**3.1-** Suporte deve verificar os celulares para acesso a internet. **3.2-** Suporte deve conectar o celular com tecnologia EDGE no servidor de *gateway* da ALFA. **3.3-** Suporte deve definir interface de rede fixa da empresa com DHCP para obtenção de endereço dinâmico.
4	Gerente de Projetos (nome)	**4.1**- Gerente de Projetos comunica as equipes a disponibilização do ambiente.

8.3 FALHA NO SERVIDOR DE EMAIL

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre falha no servidor de email. O respectivo fornecedor e contato são apresentados na seção 10.

Risco	Falha no servidor de email.	
Probabilidade: Baixa	**Impacto:** Alta	**Prioridade:** 4
Consequências de não se agir	• atraso na comunicação com o cliente.	
Mitigação	• manter controle para verificar falhas no serviço de email.	
ESTRATÉGIA DE CONTINUIDADE	• acionar a empresa fornecedora do serviço de email comunicando o ocorrido e verificando prazos de retorno. • transferir os registros de DNS que apontam para o sistema do datacenter para o servidor de *backup* da empresa.	

	• Gerente de Projetos (nome) • Diretor de TI (nome) • Suporte (nome)
Tempo de Recuperação*	TMP = 2 horas NM = 90% TMR = 3 horas
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.	

8.3.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente, de forma a contingenciar a falta dos serviços de email.

Passo	Responsável	Procedimento
1	Diretor de TI (nome)	**1.1-** Assim que for confirmada a falha de email, Diretor de TI deve ativar o Plano. **1.2-** Diretor de TI de comunicar Gerente de Projetos e Suporte. **1.3-** Diretor de TI deve comunicar o fornecedor da ocorrência.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve comunicar as equipes sobre a indisponibilidade. **2.2-** Gerente de Projetos deve comunicar o cliente sobre a indisponibilidade.
3	Suporte (nome)	**2.1-** Suporte deve entrar em contato com o datacenter e pedir alteração dos registros MX da empresa para o endereço IP XXX.YYY.XXX.YYY. **2.2-** Suporte deve modificar todas as configurações dos clientes internos da ALFA para obter os novos emails no servidor interno da ALFA.
4	Gerente de Projetos (nome)	**4.1**- Gerente de Projetos comunica as equipes a disponibilização do serviço. **4.2-** Gerente de Projetos deve comunicar cliente do retorno do serviço.

8.4 PERDA DE PERFORMANCE NO LINK DE INTERNET

Abaixo são apresentadas as informações pertinentes de mitigação e continuidade quanto ocorre perda de performance no link de internet.

Risco	Perda de performance no *link* de internet.	
Probabilidade: Média	**Impacto:** Médias	**Prioridade:** 4
Consequências de não se agir	• multas contratuais por atraso e não entrega dos serviços.	
Mitigação	• manter controle de performance do serviço de internet.	
ESTRATÉGIA DE CONTINUIDADE	• acionar a empresa fornecedora do serviço internet comunicando o ocorrido e verificando prazos de retorno. • Utilizar a banda somente com os projetos essenciais até o restabelecimento normal	

	do serviço.
	• Gerente de Projetos (nome) • Diretor de TI (nome) • Suporte (nome)
Tempo de Recuperação*	TMP = 4 horas NM = 90% TMR = 6 horas
*Tempo Máximo (TMP) = de parada, até que a atividade reinicie. Nível Mínimo (NM) = de desempenho da atividade após reinício. Tempo Máximo (TMR) = de retomada dos níveis normais de operação.	

8.4.1 Lista de Tarefas

Abaixo está a lista de ações e tarefas a serem tomadas, assim que identificado o incidente, de forma a contingenciar a falha de performance no *link* de internet.

Passo	Responsável	Procedimento
1	Diretor de TI (nome)	**1.4-** Assim que for confirmada a falha de email, Diretor de TI deve ativar o Plano. **1.5-** Diretor de TI de comunicar Gerente de Projetos e Suporte. **1.6-** Diretor de TI deve comunicar o fornecedor da ocorrência.
2	Gerente de Projetos (nome)	**2.1-** Gerente de Projetos deve avaliar os projetos críticos para utilização da banda com estes projetos. **2.2-** Gerente de Projetos deve comunicar as equipes sobre a falha de performance e informar que somente os projetos essenciais deve continuar operando .
3	Suporte (nome)	**2.1-** Suporte deve fechar range de IP dos projetos não essenciais para acesso a internet.
4	Gerente de Projetos (nome)	**4.1**- Gerente de Projetos comunica as equipes a disponibilização do serviço.

9 RECURSO FINANCEIRO DE CONTINGÊNCIA

Como forma de garantir a continuidade dos serviços e consequentemente do negócio, a empresa disponibiliza recursos financeiros de forma contingenciar as perdas ocasionadas pelo incidente. Abaixo é apresentado o recurso disponível para os gastos emergenciais.

Recurso Financeiro	Responsável pelo recurso	Valor (R$)	Quando acionar
Reserva de contingência	Gerente Financeiro	50.000,00	Para contingenciar gastos emergenciais, como compra de peças para manutenção em servidores e compra de servidor.

10 CONTATO DE FORNECEDORES

Abaixo é apresenta a lista dos fornecedores e telefones para contato. Os fornecedores devem ser comunicados assim que identificada a indisponibilidade dos serviços prestados por eles.

Fornecedor	Serviço	Telefone 1	Telefone 2
CEEE	Energia elétrica	51-3382.4900	0800 72 12333
uol Host	email	4003.9011	-
Southtech	Internet	51-3026.2006	0800 88 78324

11 CONTATO DE CLIENTES

Abaixo são apresentados os telefones dos clientes da ALFA, onde o Gerente de Projetos deverá realizar a comunicação do incidente e tranqüilizar o cliente em relação à garantia de entrega dos projetos que estão sendo executados. Após o reinício das atividades, o Gerente de Projetos também deve comunicar o cliente.

Nome	Telef. 1	Telef. 2
Empresa Beta	51-99999999	51-3333.3333
Empresa Gama	51-99999999	51-3333.3333
Empresa XYZ	51-99999999	51-3333.3333
Empresa ABC	51-99999999	51-3333.3333
Empresa JKM	51-99999999	51-3333.3333
Empresa OPQ	51-99999999	51-3333.3333
Empresa RST	51-99999999	51-3333.3333