ITALO REZENDE FERREIRA DE CARVALHO

SEGURANÇA DA INFORMAÇÃO: UM INSTRUMENTO PARA AVALIAÇÃO DO PLANO DE CONTINUIDADE DO NEGÓCIO APLICADO EM UMA ORGANIZAÇÃO PÚBLICA

LAVRAS - MG
2011

ITALO REZENDE FERREIRA DE CARVALHO

SEGURANÇA DA INFORMAÇÃO: UM INSTRUMENTO PARA AVALIAÇÃO DO PLANO DE CONTINUIDADE DO NEGÓCIO APLICADO EM UMA ORGANIZAÇÃO PÚBLICA

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Sistemas de Informação para a obtenção do título de Bacharel.

Prof. Dr. Paulo Henrique de Souza Bermejo
Orientador

LAVRAS - MG
2011

ITALO REZENDE FERREIRA DE CARVALHO

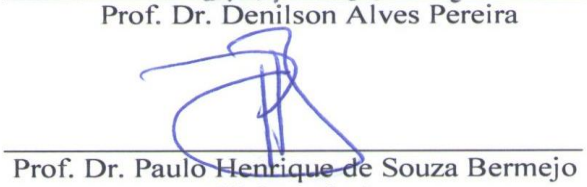
SEGURANÇA DA INFORMAÇÃO: UM INSTRUMENTO PARA AVALIAÇÃO DO PLANO DE CONTINUIDADE DO NEGÓCIO APLICADO EM UMA ORGANIZAÇÃO PÚBLICA

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Sistemas de Informação para a obtenção do título de Bacharel.

APROVADA em 17 de agosto de 2011.

Prof. Dr. André Luiz Zambalde

Prof. Dr. Denilson Alves Pereira



Prof. Dr. Paulo Henrique de Souza Bermejo
(Orientador)

LAVRAS - MG
2011

Ao meu pai, Carlinhos e à minha mãe, Máguida pela força e apoio irrestrito durante toda minha vida nos momentos alegres e tristes.

Aos meus irmãos, Vinícius e Vitor, pelo apoio e pelos momentos divertidos que me proporcionaram durante todo o tempo de convívio.

À minha namorada, Isabella, pela compreensão e pelos conselhos.

Aos meus amigos e companheiros de Carrancas, por me alegrarem quando eu me sentia triste.

Aos meus amigos e irmãos da República Riskafaka, por fazerem meus dias menos sofridos e ajudarem a suportar a distância da família.

Aos meus avós e tios, em especial, ao tio Rômulo pelo carinho e apoio.

DEDICO

AGRADECIMENTOS

À Universidade Federal de Lavras (UFLA) e ao Departamento de Ciências da Computação pela oportunidade da formação superior que sempre sonhei.

Aos professores do Departamento de Ciências da Computação, pelos ensinamentos e conselhos durante minha trajetória acadêmica.

Ao professor Dr. Paulo Henrique de Souza Bermejo, pela orientação, paciência e conselhos que foram de grande valia para a realização deste trabalho e crescimento profissional.

Aos amigos Stephania, Flávio e Marcelo, pelos conselhos e correções durante a realização deste trabalho.

Aos membros da banca examinadora.

RESUMO

No âmbito da segurança da informação, a continuidade do negócio em instituições públicas é fundamental para a manutenção de serviços essenciais à população, conferindo eficiência e credibilidade de empresas públicas perante os cidadãos. Este trabalho tem como objetivo desenvolver um instrumento de avaliação de planos de continuidade de negócio (PCNs) de instituições públicas e aplicá-lo, de modo a contribuir para o constante aprimoramento e eficiência de PCNs e auxiliar organizações públicas a se adequarem às exigências do governo federal. O instrumento de avaliação do PCN foi desenvolvido com base nas melhores práticas descritas na norma NBR ISO/IEC 27002 e na Norma Complementar 06/IN01/DSIC/GSIPR. Ele é composto de quatro fases, onde a primeira fase tem foco na gestão do plano, a segunda fase tem o objetivo de determinar possíveis cenários onde o plano deva ser colocado em ação, a terceira fase avalia a equipe e as medidas adotadas para o cenário determinado na fase anterior e a quarta fase tem o objetivo de avaliar cada medida de contingencia separadamente. Posteriormente, o instrumento foi aplicado para avaliar o plano do Aeroporto Internacional de Florianópolis a fim de identificar falhas e soluções à luz de normativas vigentes do setor público. A partir da aplicação do instrumento de avaliação, verificou-se que o plano do aeroporto cumpre com seu papel no que diz a contingenciar os principais sistemas, mas peca nas questões referentes à gestão do PCN. O instrumento de avaliação desenvolvido mostrou-se uma ferramenta importante no auxílio à avaliação e aprimoramento de PCNs de instituições públicas.

Palavras-chave: Segurança da informação. Gestão de continuidade. Plano de continuidade do negócio. Instrumento de avaliação

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O uso da informática está em crescente utilização nas empresas e a geração de informação também aumenta significativamente. A informação é considerada como um elemento essencial para a geração do conhecimento, para tomada de decisões e sua utilização alinhada à estratégia da organização, gera benefícios à imagem, à inovação, à diferenciação do produto e para a redução do custo e do risco de negócio da organização (Campos, 2007). Dessa forma, a informação é um ativo da organização, assume caráter estratégico e precisa ser tratada de forma segura. Neste sentido, a segurança da informação é um ponto crucial no aspecto estratégico para a organização.

A informação está exposta a um grande número de ameaças sejam elas de ordem física ou lógica. É importante avaliar o grau de segurança da informação na organização, bem como avaliar toda a infra-estrutura por trás da geração e armazenamento da informação.

Quando se fala em segurança da informação, é necessário analisar todas as variáveis que podem influenciar a segurança. É necessário avaliar aspectos físicos, lógicos, humanos e suas relações. O aspecto mais importante em relação à segurança da informação, é que toda e qualquer ação deve ser tomada em função do negócio, deve agregar valor ao negócio de alguma forma, caso contrário, a segurança da informação é vista pela organização como um desperdício de recursos (CAMPOS, 2007).

Uma maneira da segurança da informação agregar valor ao negócio é oferecer meios de garantir a continuidade do negócio. Para isso, são elaborados os planos de continuidade, que são um conjunto de procedimentos emergenciais a serem adotados quando ocorre um determinado incidente que possa causar a descontinuidade do negócio.

Para Campos (2007) os planos de continuidade do negócio são controles de segurança da informação e precisam se tornar um processo da organização e precisam ser geridos como qualquer outro processo. É importante que os planos evoluam junto com a organização e contribuam de maneira efetiva com ela.

1.1 Motivação e problema

Interrupções de serviços em instituições públicas podem causar sérios danos no que diz respeito à ordem pública, à ordem econômica e à integridade de assuntos relacionados à comunidade e pode também levar o público ao pânico. A adoção de uma gestão de segurança da informação se torna essencial para evitar que ocorram interrupções de qualquer espécie no setor público (XIANG, WANG, ZHANG; 2007).

Para a eficiência de um sistema de gestão de segurança da informação, é necessário que vários documentos sejam incorporados ao sistema, entre eles está o Plano de Continuidade do Negócio (PCN). De acordo com o Tribunal da Contas da União (2008) o PCN pode ser considerado como sendo um Plano de Contingência e é definido da seguinte forma: "conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a consequente prestação de serviço".

Segundo Boehmer *et al* (2009), existem diferentes tipos de PCN de acordo com o tipo de incidente que se pretende tratar. A idéia de um PCN é manter a empresa viva enquanto ela se recupera de um desastre. Boehmer *et al* (2009) afirma que ainda há pouco conhecimento comprovado sobre a eficiência de um PCN, são raros os casos em que se pôde verificar a eficiência de um PCN em situações reais.

As empresas que adotam medidas de segurança da informação muitas vezes, não possuem um PCN e quando o possuem, não são eficientes (XIANG, WANG, ZHANG; 2007). Dessa forma, é necessário conscientizar as organizações que um bom plano de continuidade do negócio é fator essencial para que a organização se mantenha ativa.

Uma forma de garantir um bom PCN é a realização de testes para verificar sua eficiência. Ernest-Jones (2005) afirma que uma em cada quatro empresa não testa seus PCN's e ainda assim, as empresas que testam, fazem isso em intervalos superiores a seis meses. Para Gibb e Buchanan (2006), os testes do PCN devem ser feitos de forma regular e exaustivamente para ver se os planos ainda são relevantes para a atual situação da organização.

Lam (2002) considera que embora as organizações mantenham um PCN, muitas delas deixam de considerá-lo como uma preocupação permanente e interrompem o ciclo de planejamento do plano.

É necessário avaliar o PCN periodicamente e alguns elementos devem ser analisados para garantir sua eficiência. Segundo Brasiliano (2009), os itens necessários de avaliar em um PCN são: 1) o conhecimento do PCN pelos colaboradores; 2) se o plano aborda os aplicativos necessários para a continuidade do negócio; 3) avaliar o funcionamento dos equipamentos e da infra-estrutura; 4) se o número de colaboradores é suficiente para a execução do PCN; 5) se o processo de comunicação é eficiente durante a execução do PCN; 6) se a preparação dos relatórios é satisfatória (BRASILIANO, 2009). Além destes itens, é importante avaliar também se o processo de recuperação das atividades críticas é realizado dentro de um intervalo de tempo que minimize ao máximo os danos causados à organização.

A necessidade de elaborar um instrumento de avaliação do plano de continuidade do negócio das organizações se mostra necessário, uma vez que PCN's mal elaborados prejudicam as organizações quando estas se vêem obrigadas a colocá-los em prática. Um bom instrumento de avaliação deve abordar os elementos citados anteriormente e deve ser passível de adaptação para cada organização ou setor que desejar utilizá-lo.

1.2 Objetivo geral

O objetivo do estudo em questão é propor um instrumento de avaliação para o Plano de Continuidade do Negócio de Instituições Públicas, visando melhorar a eficiência do plano e assim, permitir a melhoria da segurança da informação na organização.

Instrumento neste trabalho pode ser considerado como um mecanismo, um modelo, um formulário que auxilia na avaliação do PCN.

1.3 Objetivos específicos

Os objetivos específicos do trabalho para alcançar o objetivo geral são listados abaixo:

1. Identificar os principais elementos a serem considerados na avaliação de um PCN;

2. Elaborar um instrumento de avaliação do PCN;
3. Verificar o instrumento de avaliação proposto aplicando-o para avaliar um PCN.

1.4 Justificativa

Segundo Gibb e Buchanan (2006), a continuidade do negócio é fundamental para garantir que uma empresa possa se proteger contra os riscos que são inerentes ao seu ambiente. As empresas estão cada vez mais dependentes da disponibilidade de informações a fim de prestar serviços aos clientes. Uma gestão eficaz de informação requer o desenvolvimento de um ambiente no qual as informações possam ser fornecidas a qualquer pessoa autorizada, em qualquer lugar e em qualquer tempo (GIBB e BUCHANAN, 2006).

De acordo com Herbane *et al* (2004), a gestão de continuidade do negócio não está limitada a um processo sistêmico para combater incidentes. Ela pode assumir um papel estratégico na organização e garantir uma vantagem competitiva.

Nas situações em que uma ameaça atinge várias empresas, e muitas vezes, empresas concorrentes, como é o caso de terremotos, enchentes, as organizações que tiverem um PCN bem formulado, poderão recuperar suas atividades mais rapidamente que seus concorrentes. Assim sendo, suas perdas serão menores e poderão atrair a confiabilidade de seus clientes e dos clientes de empresas concorrentes (HERBANE *et al*, 2004).

Avaliar o plano de continuidade do negócio nas organizações, independentemente do seu setor de atuação, se faz necessário quando se busca a eficiência do PCN. Um PCN bem elaborado é peça fundamental para a gestão de continuidade do negócio e, consequentemente, para a competitividade e sobrevivência das organizações.

2 REFERENCIAL TEÓRICO

Neste capítulo serão apresentados os principais conceitos a respeito do tema deste trabalho. Para isto, serão abordados os assuntos segurança da informação,

políticas de segurança, padrões e normas sobre segurança da informação, gestão da continuidade do negócio, plano de continuidade do negócio.

2.1 Segurança da informação

O significado da palavra informação para o presente trabalho pode ser obtido com a definição dada pela norma NBR ISO/IEC 27002 (ABNT, 2005): "Informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegido."

A informação é utilizada tanto para administrar internamente a organização como para prever situações de mercado e concorrentes. Por esse motivo, ela é um bem poderoso para a empresa.

Por ser tão importante, a informação necessita ser segura e neste aspecto é necessário analisar a segurança da informação. A geração de informação é algo muito comum para qualquer empresa e a segurança dessas informações é vital também quanto ao caráter estratégico.

A definição dada pela norma NBR ISO/IEC 27002 (ABNT, 2005) para a segurança da informação é: "Segurança da informação é a proteção da informação de vários tipos de ameaças" cujo objetivo é garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Para Campos (2007) a segurança da informação visa garantir a integridade, confidencialidade e disponibilidade das informações processadas pela organização.

O Decreto Nº 3.505 de 13 de junho de 2000 instituído pelo presidente da República Federativa do Brasil, define segurança da informação como:

> Art. 2. Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:
> II – Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Assim sendo, a segurança da informação é imprescindível para qualquer organização tanto no caráter estratégico como no tático e operacional.

Alguns princípios básicos devem ser respeitados para que se possa garantir a segurança da informação (ABNT NBR ISO/IEC 27002, 2005):

- **Confidencialidade:** significa que a informação deve ser protegida contra sua divulgação para pessoas não autorizadas – interna ou externamente. Consiste em proteger a informação contra cópias e distribuição não autorizada. Dessa forma, a informação deve ser confidencial e sua utilização deverá ser feita por pessoas previamente autorizadas.
- **Integridade:** consiste em garantir que a informação gerada não seja modificada sem a devida autorização da(s) pessoa(s) responsável por ela. Isto implica que não deve ser permitido que a informação original sofra nenhum tipo de violação seja ela escrita, alteração de conteúdo, alteração de status, remoção e criação de informações.
- **Autenticidade:** o controle de autenticidade está ligado ao fato da informação que esteja sendo trafegada seja de fato originada do proprietário a ela relacionado. Não deve ser permitida a violação da origem da informação.
- **Disponibilidade:** garantir que a informação esteja disponível às pessoas autorizadas sem nenhum tipo de modificação e sempre que elas necessitarem. Pode ser chamado também de continuidade do serviço.

Através da garantia desses serviços, a segurança de informação poderá trazer benefícios relevantes para a organização como, por exemplo: aumentar a produtividade dos usuários através de um ambiente mais organizado, maior controle sobre os recursos de informática e, finalmente garantir a funcionalidade das aplicações críticas da empresa (FRANCISCO, 2004).

Quando se fala em segurança da informação, é importante ressaltar que aspectos humanos, tecnológicos, processuais, jurídicos e de negócios devem ser levados em consideração quando se pretende garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações (NAKAMURA e DE GEUS, 2000).

2.2 Políticas de segurança

De acordo com a norma NBR ISO/IEC 27002 (ABNT, 2005), políticas de segurança da informação têm por objetivo "fornecer uma orientação e apoio da direção para prover a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes." A política de segurança da organização deve ser clara e difundida por toda a organização, deve estar alinhada com os objetivos do negócio e ter um forte compromisso com a segurança da informação (NBR ISO/IEC 27002:2005).

O desenvolvimento de uma política de segurança deve envolver todos os *stakeholders*, desde a direção até os funcionários bem como os fornecedores e clientes com acesso aos sistemas de informação da organização. O documento de política de segurança deve ser elaborado de tal forma que seja utilizado como uma regra a ser seguida e deve passar por atualizações periódicas (CAMPOS, 2007)

A organização deve ter alguém ou uma área específica para a política de segurança responsável pela elaboração, implantação, revisão, atualização e designação de funções. É interessante que a alta gerência tenha representantes nessa equipe uma vez que a política de segurança abrange toda a organização. É importante também que esta equipe contenha desenvolvedores, auditores, usuários, especialistas em questões legais, recursos humanos, TI, gestão de riscos (LAM, 2002).

2.2.1 Elementos da política de segurança

Uma boa política de segurança tem que considerar não somente os ataques de *hackers*, mas todos os elementos que dizem respeito àquilo que é essencial quando o objetivo é combater as adversidades, como, por exemplo, controle de acesso, segurança dos equipamentos de hardware, etc. A disponibilidade da infraestrutura da organização também deve ser considerada (HUR, 1999 *apud* NAKAMURA e DE GEUS, 2000):

- Vigilância: significa que todos da organização são responsáveis por garantir e fiscalizar a segurança de informação;
- Atitude: significa a postura e a conduta quanto à segurança. Todos os envolvidos devem ter a consciência que a política de segurança não

tem efeitos se ela não for adotada de forma certa. É necessário treinamento e conscientização dos funcionários quanto à importância de se seguir a política de segurança estabelecida;

- Estratégia: significa ser criativo na elaboração da política de segurança além de ser adaptativa às mudanças no ambiente. A estratégia leva em conta também a produtividade dos usuários. Uma boa política não deve interferir negativamente no andamento dos negócios da organização;
- Tecnologia: a solução tecnológica deve ser flexível e adaptativa para suprir as necessidades da organização. Qualquer tecnologia desatualizada pode causar uma falsa sensação de segurança.

O Tribunal de Contas da União (2008) considera que o conteúdo da Política de Segurança da Informação aplicável à Administração Pública Federal direta ou indireta varia de acordo com a organização, porém alguns elementos são comuns nessas políticas:

> - Definição de segurança de informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
> - Declaração do comprometimento da alta administração com a Política de Segurança da Informação, apoiando suas metas e princípios;
> - Objetivos de segurança da organização;
> - Definição de responsabilidades gerais na gestão de segurança de informações;
> - Orientações sobre análise e gerência de riscos;
> - Princípios de conformidade dos sistemas computacionais com a Política de Segurança da Informação;
> - Padrões mínimos de qualidade que esses sistemas devem possuir;
> - Políticas de controle de acesso a recursos e sistemas computacionais;
> - Classificação das informações (de uso irrestrito, interno, confidencial e secretas);
> - Procedimentos de prevenção e detecção de vírus;
> - Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
> - Princípios de supervisão constante das tentativas de violação da segurança de informações;
> - Conseqüências de violações de normas estabelecidas na política de segurança;
> - Princípios de gestão da continuidade do negócio;
> - Plano de treinamento em segurança de informações.
>
> (TRIBUNAL DE CONTAS DA UNIÃO, 2008, p.27)

Uma boa Política de Segurança da Informação é o primeiro passo para se estabelecer a segurança da informação nas organizações.

2.3 Normas relacionadas à segurança da informação utilizadas como referencia no trabalho

As normas para boas práticas e controle de TI e para implantação de processos de segurança que foram utilizados como referencia no presente trabalho estão descritas abaixo:

- ABNT NBR ISO/IEC 27002:2005 (norma brasileira baseada na ISO 17799) - Tecnologia da informação – Técnicas de segurança – código de prática para a gestão da segurança da informação;
- Norma Complementar 06/IN01/DSIC/GSIPR – Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações.

A escolha da norma NBR ISO/IEC 27002:2005 foi determinada por ela ser baseada em uma norma internacional e por ser amplamente utilizada em questões referentes a segurança da informação. A escolha da Norma Complementar 06 referente à Instrução Normativa 01 do Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil se deu ao fato da norma ser aplicável no âmbito da Administração Pública Federal, direta ou indireta, que é o objetivo do trabalho, quando este deseja elaborar um instrumento de avaliação do PCN de instituições públicas.

2.3.1 ABNT NBR ISO/IEC 27002:2005

A ISO/IEC 17799:2000 foi criada para substituir a BS 7799, no entanto, ela não inclui a segunda parte da BS 7799 (Campos, 2006). Em 2005, a norma passou por uma atualização e foi chamada de ISO/IEC 17799:2005, nesta nova versão os controles são mais distintos, separando a forma de implementação, os requisitos e as informações adicionais (Campos, 2006). Em 2007, a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração como ISO/IEC 27002.

A norma NBR ISO/IEC 27002:2005 (Tecnologia da informação – Técnicas de segurança – código de prática para a gestão da segurança da informação) é a norma brasileira equivalente à norma ISO/IEC 17799:2005, trata de técnicas de segurança no âmbito da tecnologia da informação. Os objetivos definidos nessa norma configuram as melhores práticas quando se fala em gestão da segurança da informação (TRIBUNAL DE CONTAS DA UNIÃO, 2008).

A norma tem por objetivo estabelecer "diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização" (ABNT NBR ISO/IEC 27002, 2005).

Segundo o Tribunal da Contas da União (2008), a estrutura da norma esta dividida em 11 seções:

a. Política de segurança da informação;
b. Organizando a segurança da informação;
c. Gestão de ativos;
d. Segurança em recursos humanos;
e. Segurança física e do ambiente;
f. Gestão das operações e comunicações;
g. Controle de acessos;
h. Aquisição, desenvolvimento e manutenção de sistemas de informação;
i. Gestão de incidentes de segurança da informação;
j. Gestão da continuidade do negócio;
k. Conformidade.

2.3.2 Norma Complementar 06/IN01/DSIC/GSIPR

Originária do Departamento de Segurança da Informação e Comunicação do Governo Federal do Brasil, a Norma Complementar 06/IN01/DSIC/GSIPR foi publicada no Diário Oficial da União, nº 223, de 23 de novembro de 2009 - seção 1. A Norma estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Ela é dividida em 7 seções, sendo que a primeira seção contém os objetivos da norma, a segunda seção traz as considerações iniciais, a terceira seção é chamada

Fundamento Legal da Norma Complementar, na quarta seção tem-se os conceitos e definições, a quinta seção descreve os procedimentos da norma, na sexta seção são descritas as responsabilidades e na última seção está a declaração de vigência da norma.

2.4 Gestão da continuidade do negócio

Hoje em dia, as empresas e processos de negócio dependem da TI - tecnologia da informação - mais do que nunca (WINKLER *et al*, 2010). Interrupções em infra-estrutura de TI nas organizações acarretam em rupturas em processos de negócio que levam a perdas financeiras, conseqüências legais, perdas de reputação e pode causar falências (WINKLER *et al*, 2010). Neste aspecto, se mostra necessário adotar medidas para garantir a continuidade do negócio.

Para Bajgoric (2006, p.632) o termo continuidade do negócio diz respeito "a capacidade e uma empresa continuar com suas operações, mesmo se algum tipo de falha ou desastre ocorre".

A Norma Complementar 06/IN01/DSIC/GSIPR (2009) define continuidade do negócio como sendo a capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, com o objetivo de minimizar seus impactos e recuperar perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

Segundo a NBR ISO/IEC 27002 (ABNT, 2005), a gestão da continuidade do negócio tem por objetivo "não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar sua retomada em tempo hábil, se for o caso".

Para a Norma Complementar 06/IN01/DSIC/GSIPR (2009), a gestão da continuidade pode ser definida como um processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações do negócio, caso estas ameaças se concretizem. Este processo tem o objetivo de proteger os interesses das partes envolvidas, a reputação e a marca da organização, e suas atividades de valor agregado. (NORMA COMPLEMENTAR 06/IN01/DSIC/GSIPR, 2009, p. 3)

A importância da gestão da continuidade do negócio é minimizar os impactos e auxiliar na recuperação de ativos da informação quando estes sofrem algum dano proveniente dos mais variados fatores como, por exemplo, desastres naturais, falhas em equipamentos, acidentes e ações intencionais (ABNT NBR ISO/IEC 27002, 2005).

Para que ocorra a gestão da continuidade do negócio de forma efetiva é necessário criar um plano de continuidade do negócio (PCN). Originalmente, o PCN era um conceito que caiu sobre os ombros dos departamentos de TI e se limitava a fazer backup, proteção e fornecer redundância de dados (Gill, 2006), porém, recentemente, a gestão de continuidade do negócio incluiu aspectos humanos, bem como questões técnicas e afeta todos os aspectos de uma organização (ADKINS *et al*, 2009).

Um PCN deve, segundo a NBR ISO/IEC 27002 (ABNT, 2005), ser desenvolvido e implementado para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, logo após a ocorrência de interrupções ou falhas nos processos críticos do negócio.

A Norma Complementar 06/IN01/DSIC/GSIPR (2009, p. 3) define o Plano de Continuidade de Negócio como sendo a documentação dos procedimentos e informações necessárias para que os órgãos ou entidades mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.

De acordo com ISACA (2010), o objetivo do PCN é possibilitar que a empresa continue oferecendo os serviços críticos em caso de falhas e sobreviva a interrupções causadas por desastres.

O Tribunal da Contas da União (2008) considera o PCN um Plano de Contingência e o define como sendo um conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a conseqüente prestação de serviço. O Plano de Contingência atua de forma a minimizar os impactos causados por falhas de qualquer natureza na organização. Ele é um conjunto de medidas que combinam ações preventivas e ações corretivas (TRIBUNAL DE CONTAS DA UNIÃO, 2008).

Lindström *et al* (2010) considera que o interessante para as organizações é nunca precisarem do PCN, mas, quando for necessário colocá-lo em ação, é importante

que ele seja uma ferramenta genérica para resolver qualquer tipo de situação e não servir apenas como um guia para um conjunto de situações pré-definidas.

2.4.1 Elementos do plano de continuidade do negócio

Quando se inicia a elaboração de um PCN é necessário atentar-se para alguns aspectos (TRIBUNAL DE CONTAS DA UNIÃO, 2008):

- Os riscos em que a organização está exposta, a probabilidade de ocorrência e os impactos causados;
- O que pode acarretar a interrupção de qualquer um dos sistemas operacionais;
- Identificação e priorização de recursos, sistemas e processos críticos;
- Tempo limite para recuperação de danos em qualquer recurso, sistema ou processo;
- Identificar as alternativas na recuperação de recursos, sistemas ou processos analisando qual a melhor relação custo/benefício.

A NBR ISO/IEC 27002 (ABNT, 2005) determina que todo PCN passe por testes e atualizações periódicas e que todas as revisões devam ser documentadas. É importante que cópias do PCN sejam guardadas em locais remotos bem como todo material que será utilizado para colocar o plano em ação, essas cópias devem estar atualizadas e devem ser mantidas com o mesmo nível de segurança adotado no ambiente principal (ABNT NBR ISO/IEC 27002, 2005).

É importante que o PCN siga uma estrutura básica determinada afim de que todos os planos sejam consistentes para aplicar os requisitos de segurança e identificar prioridades para testes e manutenção.

Para Lam (2002) o PCN é um processo cíclico e sempre que a organização alterar prioridades de negócio, o PCN deve ser revisto. Lam (2002) defende que o processo de elaboração do PCN pode ser dividido em 8 etapas como pode ser observado a seguir.

A primeira etapa consiste em iniciar o projeto, para isso é necessário obter o apoio da gerência, identificar os principais interessados, formar uma equipe responsável pelo plano, definir objetivos e restrições, estabelecer as estratégias para alcançar as metas, começar uma versão preliminar da política de continuidade do negócio.

Na segunda etapa são identificadas as principais ameaças ao negócio. Essas ameaças podem atuar nas tecnologias, nas informações e nas pessoas envolvidas com a organização. Na terceira etapa ocorre a análise dos riscos onde é definido a probabilidade e o impacto da ocorrência das ameaças, o nível de risco aceitável pela organização.

No quarto passo são definidos os papéis e responsabilidades e ocorre o treinamento da equipe responsável pelo plano. No quinto passo é concebido o plano de recuperação do negócio de fato.

O sexto passo consiste em documentar completamente os processos de continuidade do negócio e comunicá-los às partes interessadas.

Na fase 7 são realizados os testes para validar o plano e a fase 8 consiste em manter o plano sempre atualizado e revisado. Se necessário, o ciclo de desenvolvimento do plano pode continuar na fase 1.

Para Karakasidis (1997), alguns fatores devem ser considerados na elaboração de um PCN:

- O desenvolvimento do plano deve ter apoio da alta direção da organização.
- Estabelecer um comitê de planejamento para a continuidade do negócio. Entre as atividades do comitê estão: definir os objetivos, gerenciar o desenvolvimento, testar o plano, etc.
- Executar uma análise de impacto no negócio. Antes de construir qualquer plano de recuperação de desastres, é necessário levantar as principais ameaças e os possíveis impactos da mesma na organização.
- Avaliar as necessidades críticas do negócio. Necessidades críticas são os recursos, procedimentos e equipamentos necessários para continuar o negócio.
- Determinar as estratégias para a continuidade do negócio. Consiste em analisar todas as estratégias disponíveis para manter as principais funções do negócio.
- Preparar um plano de recuperação. Um esboço dos procedimentos de recuperação do negócio deve ser preparado para orientar o agrupamento dos insumos necessários.
- Rever os acordos de níveis de serviço. É necessário analisar os acordos fechados entre duas partes (organizações externas).

De acordo com a NBR ISO/IEC 27002 (ABNT, 2005), um PCN deve ter um gestor específico responsável pelo controle de procedimentos de emergência, de

recuperação, manual de planejamento e planos de reativação. A NBR ISO/IEC 27002 (ABNT, 2005) determina que os seguintes itens devam ser considerados na estrutura de um PCN:

> a) condições para ativação dos planos, os quais descrevem os processos a serem seguidos (como se avaliar a situação, quem deve ser acionado etc.) antes de cada plano ser ativado;
> b) procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente que coloque em risco as operações do negócio;
> c) procedimentos de recuperação que descrevam as ações necessárias para a transferência das atividades essenciais do negócio ou os serviços de infra-estrutura para localidades alternativas temporárias e para a reativação dos processos do negócio no prazo necessário;
> d) procedimentos operacionais temporários para seguir durante a conclusão de recuperação e restauração;
> e) procedimentos de recuperação que descrevam as ações a serem adotadas quando do restabelecimento das operações;
> f) uma programação de manutenção que especifique quando e como o plano deverá ser testado e a forma de se proceder à manutenção deste plano;
> g) atividades de treinamento, conscientização e educação com o propósito de criar o entendimento do processo de continuidade de negócios e de assegurar que os processos continuem a ser efetivo;
> h) designação das responsabilidades individuais, descrevendo quem é responsável pela execução de que item do plano. Convém que suplentes sejam definidos quando necessário;
> i) os ativos e recursos críticos precisam estar aptos a desempenhar os procedimentos de emergência, recuperação e reativação.
> (ABNT NBR ISO/IEC 27002, 2005).

O Tribunal de Contas da União (2008) afirma que os serviços, equipamentos, suprimentos ou quaisquer outros bens necessários para a restauração dos sistemas que são de responsabilidade de entidades externas bem como os contratos e os contatos devam fazer parte do PCN.

Existem três formas de garantir a eficiência de um PCN: treinamento e conscientização das pessoas envolvidas, realização de testes periódicos integrais ou parciais do plano, manutenção contínua (TRIBUNAL DE CONTAS DA UNIÃO, 2008).

Os testes do plano são um dos meios mais eficientes de determinar o quão aplicável é o PCN. De acordo com a NBR ISO/IEC 27002 (ABNT, 2005), os testes devem assegurar que todas as pessoas envolvidas estejam conscientes das atividades que cada uma deve desempenhar no momento em que o plano entrar em ação.

Diversas técnicas para a realização dos testes podem ser utilizadas com o objetivo de assegurar que quando for preciso que o PCN entre em ação, ele possa

assegurar que irá operar consistentemente em casos reais (ABNT NBR ISO/IEC 27002, 2005). Algumas técnicas são descritas abaixo:

> a) testes de mesa simulando diferentes cenários (verbalizando os procedimentos de recuperação para diferentes formas de interrupção);
> b) simulações (particularmente útil para o treinamento do pessoal nas suas atividades gerenciais após o incidente);
> c) testes de recuperação técnica (garantindo que os sistemas de informação possam ser efetivamente recuperados);
> d) testes de recuperação em um local alternativo (executando os processos de negócios em paralelo com a recuperação das operações distantes do local principal);
> e) testes dos recursos, serviços e instalações de fornecedores (assegurando que os serviços e produtos fornecidos por terceiros atendem aos requisitos contratados);
> f) ensaio geral (testando se a organização, o pessoal, os equipamentos, os recursos e os processos podem enfrentar interrupções).
> (ABNT NBR ISO/IEC 27002, 2005).

A realização dos testes é necessária porque os planos podem apresentar falhas geralmente devido a pressupostos incorretos, omissões ou mudanças de equipamentos, de pessoal, de prioridades (Tribunal de Contas da União, 2008). Além desses fatores a NBR ISO/IEC 27002 (ABNT, 2005) considera que mudanças de endereços ou números telefônicos; estratégia de negócio; localização, instalações e recursos; legislação; prestadores de serviços, fornecedores e clientes-chave; processos (inclusões e exclusões); risco (operacional e financeiro) também são fatores que contribuem para a realização de testes.

2.5 Trabalho relacionado

O *IT Continuity Planning Audit/Assurance Program*[1] da ISACA (2009) é considerado uma ferramenta de apoio aos auditores. Esta ferramenta é caracterizada como sendo um guia de ações e itens que os auditores devem verificar quando se pretende auditar o plano de continuidade.

De acordo com a ISACA (2009) este programa de auditoria não é uma lista de verificação ou questionário, tem apenas o intuito de auxiliar na revisão do plano de

[1] Mais informações em: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Continuity-Planning-Audit-Assurance-Program.aspx>

continuidade. Esta ferramenta pode ser adaptada às necessidades da organização que está sendo auditada.

O escopo do programa de auditoria do plano de continuidade de TI da ISACA (2009) se limita a revisar o plano de continuidade de TI e seu alinhamento com o PCN, políticas, normas, diretrizes, procedimentos, leis e regulamentos que aborda a manutenção contínua de serviços de TI (ISACA, 2009).

O programa de auditoria da ISACA (2009) usa como referencia o *framework* de boas práticas CobiT e o *framework* de controle interno COSO para validar os itens que devem ser analisados pelo auditor.

A diferença entre o programa da ISACA (2009) e o trabalho que se segue, é que ele não é considerado como um instrumento de avaliação, apenas identifica os itens que devem ser avaliados de acordo com o CobiT e o COSO. A forma como é realizada essa avaliação fica a critério do auditor e ele pode usar de diversos mecanismos, entre eles, um instrumento de avaliação.

3 METODOLOGIA

A metodologia de pesquisa mostra como é desenvolvido o trabalho. A forma como os dados são levantados, formas de analisá-los e expô-los são descritas na metodologia.

O método científico de pesquisa diz respeito ao caminho que deve ser seguido para atingir os objetivos do trabalho (GIL, 1999 apud BERMEJO, 2009, p.20). Dessa forma, várias maneiras de classificar uma pesquisa podem ser utilizadas como pode ser observado nas seções seguintes.

3.1 A natureza da pesquisa

Com relação à natureza da pesquisa, ela pode ser dividida em pesquisa básica ou fundamental e em pesquisa aplicada ou tecnológica (SILVA e MENEZES, 2001; JUNG, 2004).

Para Silva e Menezes (2001) a pesquisa aplicada ou tecnológica tem por finalidade gerar conhecimento para a aplicação prática que será utilizada para solução de problemas específicos envolvendo verdades e interesses locais. Segundo Jung

(2004), a pesquisa tecnológica utiliza conhecimentos básicos, tecnologias existentes e busca como resultado um novo produto ou processo.

Considerando-se os objetivos propostos neste trabalho que inclui a formulação de um instrumento para avaliação de PCN, o trabalho foi enquadrado na pesquisa aplicada.

3.2 A abordagem do problema de pesquisa

A forma de abordagem da pesquisa se divide em qualitativa e quantitativa. No trabalho que se segue, a abordagem qualitativa se torna mais aplicável uma vez que Silva e Menezes (2001) afirmam que a abordagem qualitativa é descritiva e o pesquisador é o instrumento-chave. Na pesquisa qualitativa, a quantificação dos dados é dificultada já que ela considera que o mundo objetivo e a subjetividade do sujeito não podem ser traduzidos em números (SILVA e MENEZES, 2001).

De acordo com Jung (2004) os valores do pesquisador são permitidos quando se realiza a interpretação dos dados na pesquisa qualitativa. Appolinário (2006) citado por Bermejo (2009, p. 21) afirma que na pesquisa qualitativa, a coleta dos dados é proporcionada por interações sociais com o fenômeno estudado e que a interpretação dos mesmos é feita com base nas percepções do próprio pesquisador.

Assim sendo, a pesquisa qualitativa melhor se aplica ao trabalho, uma vez que a interpretação dos dados far-se-á pelo próprio pesquisador.

3.3 Caracterização dos objetivos da pesquisa

Os objetivos da pesquisa podem ser classificados como sendo do tipo descritivo (JUNG, 2004) e exploratório (POLIT; HUNGLER, 1987 apud BERMEJO, 2009, p. 21).

Segundo Jung (2004) a pesquisa descritiva busca a "identificação, o registro e a análise de características, fatores e variáveis" que mantêm algum tipo de relação com o fenômeno pesquisado.

Em relação à pesquisa exploratória, Polit e Hungler (1987) citado por Bermejo (2009, p. 22), ela é caracterizada como sendo uma extensão da pesquisa descritiva e a

sua intenção é “desenvolver ou refinar hipóteses” e pode também ser utilizada para “testar e definir os métodos de coleção de dados”.

Segundo Silva e Menezes (2001) a pesquisa exploratória proporciona maior familiaridade com o problema e tem como objetivo formular hipóteses. Envolvem levantamento bibliográfico, entrevistas e normalmente assume a forma de pesquisa bibliográfica e estudo de caso.

A pesquisa definida como “descritiva exploratória” melhor se enquadra no presente trabalho, uma vez que ela descreve como está implantado os Planos de Continuidade do Negócio na organização estudada e como se adequar às normas relacionadas à segurança da informação.

3.4 Procedimentos técnicos

Como citado por Silva e Menezes (2001) a pesquisa exploratória pode assumir a forma de pesquisa bibliográfica ou estudo de caso.

Do ponto de vista dos procedimentos técnicos, Gil (1991) citado por Silva e Menezes (2001, p. 21), o estudo de caso é caracterizado por uma análise profunda e exaustiva de um ou mais objetos que se deseja conhecer.

Segundo Jung (2004), o estudo de caso é uma importante ferramenta para os pesquisadores quando este deseja saber “como” e “por que” as “coisas” funcionam. Jung (2004) define estudo de caso como sendo um procedimento de pesquisa que estuda um fenômeno local e real.

A técnica de estudo de caso é aplicável quando se busca adquirir os conhecimentos básicos a cerca do objeto da pesquisa básica (JUNG, 2004). Em síntese, parte-se do princípio que o estudo proposto visa explicar ou descrever uma determinada situação a partir da identificação de uma necessidade. Para isto, é necessário selecionar uma amostra do universo em questão, elaborar um instrumento para coletar os dados, aplicar o instrumento, efetuar um tratamento estatístico, e realizar uma análise comparativa entre os dados, uma análise do padrão de referência e bibliografias. Realizadas estas atividades, conclui-se o trabalho obtendo-se então as descobertas (JUNG, 2004).

A caracterização do presente trabalho como sendo um estudo de caso se deu pelo fato de ter sido feita a análise do plano de continuidade do negócio de uma organização.

3.5 Técnicas de pesquisa

A metodologia de pesquisa é mais bem entendida quando se apresenta seus detalhes na fase de desenvolvimento (BERMEJO, 2009). O desenho da pesquisa é uma forma eficiente de se explicar as fases da pesquisa.

3.5.1 Desenho da pesquisa

"O desenho da pesquisa contempla os seus componentes que são demonstrados em sequências lógicas" (YIN, 2005 apud BERMEJO, 2009, p. 23). A representação gráfica do desenho da pesquisa pode ser observada na Figura 1.

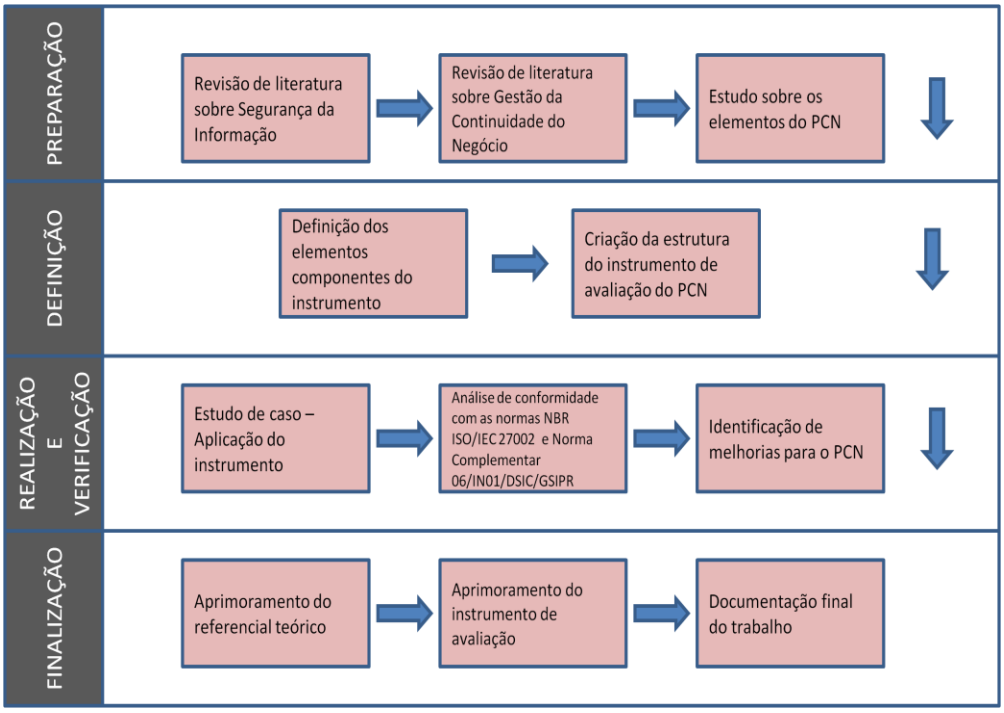


Figura 1 - Desenho da pesquisa. Adaptado de Bermejo (2009)

Conforme observado na Figura 1, o trabalho foi realizado em quatro etapas: 1) preparação; 2) definição; 3) realização e verificação; 4) finalização. A descrição de cada etapa e suas atividades podem ser observadas na seção seguinte.

3.5.2 Etapas e atividades da pesquisa

A seguir, está a descrição das atividades realizadas em cada fase da pesquisa.

1) Etapa de preparação: essa etapa foi composta por três atividades principais:
    - Revisão de literatura sobre segurança da informação: coleta de materiais bibliográficos, revisão conceitual sobre segurança da informação, revisão dos principais conceitos, revisão conceitual sobre políticas de segurança da informação, revisão sobre os principais padrões e normas relacionados à segurança da informação;
    - Revisão sobre Gestão da Continuidade do Negócio: coleta de materiais bibliográficos, revisão conceitual sobre gestão da continuidade do negócio, revisão sobre PCN;
    - Estudo sobre os elementos do PCN: coleta de materiais bibliográficos, revisão conceitual sobre os elementos de um PCN, revisão epistemológica sobre a estrutura do PCN, seleção e verificação das características principais do PCN.
2) Etapa de definição: composta por duas atividades principais, a saber:
    - Definição dos elementos componentes do instrumento: a partir dos resultados obtidos na etapa de preparação, foram definidos os elementos principais para compor o instrumento de avaliação do PCN;
    - Criação da estrutura do instrumento de avaliação do PCN: essa atividade consiste em definir a estrutura do instrumento de avaliação de acordo com os elementos identificados na atividade anterior.
3) Etapa de realização e verificação: esta etapa foi formada por três atividades principais:

- Estudo de caso – aplicação do instrumento: esta atividade consiste em realizar um estudo de caso da aplicação do instrumento na avaliação do PCN selecionado;
- Análise de conformidade com a norma NBR ISO/IEC 27002 e Norma Complementar 06/IN01/DSIC/GSIPR: esta atividade consiste em analisar se o resultado da avaliação do PCN das organizações está em conformidade com a norma NBR ISO/IEC 27002 e com a Norma Complementar 06/IN01/DSIC/GSIPR;
- Identificação de melhorias para o PCN: esta atividade tem por objetivo identificar melhorias no que diz respeito ao PCN avaliado através do resultado da avaliação.

4) Etapa de finalização: composta por três atividades principais:
   - Aprimoramento do referencial teórico: a partir da contribuição das etapas anteriores, o referencial teórico pode ser melhorado;
   - Aprimoramento do instrumento de avaliação: a partir da contribuição das etapas anteriores, o instrumento de avaliação pode ser melhorado;
   - Documentação final do trabalho: após todas as atividades descritas, ocorreu o encerramento do trabalho com a atividade de documentação final do trabalho, onde está incluso a validação do trabalho, conclusão das atividades, proposta para trabalhos futuros.

3.6 Abrangência da pesquisa

A abrangência da pesquisa também chamada delimitação da pesquisa estabelece os limites da investigação (MARCONI e LAKATOS, 2010).

O campo de investigação limitou-se a aplicar o instrumento e avaliar o PCN do Aeroporto Internacional de Florianópolis.[2] A amostragem utilizada foi do tipo casual simples (Silvia e Menezes, 2001; Jung, 2004), que correspondeu à seleção do aeroporto para realização do estudo de caso numa população finita de organizações

[2] O PCN avaliado pode ser encontrado no endereço eletrônico: <http://sites.google.com/site/sbflpcn/Home/plano-de-contingencia>.

reais. O critério utilizado para a escolha da organização obedeceu à disponibilidade para fornecimento das condições necessárias para a realização da verificação, além do fato do aeroporto ser administrado pela INFRAERO, o que caracteriza a organização como sendo componente da Administração Pública Federal.

3.7 Verificação e validação

A verificação deste trabalho foi feita em três etapas que podem ser verificadas abaixo:

- A primeira etapa consiste em aplicar o instrumento de avaliação no PCN selecionado, conforme justificado na seção anterior;
- Na segunda etapa, será realizada uma análise de conformidade dos resultados alcançados na etapa anterior com a norma NBR ISO/IEC 27002 (ABNT, 2005) e uma análise verificando as exigências e expectativas em relação ao PCN de acordo com a Norma Complementar 06/IN01/DSIC/GSIPR (2009).
- Na terceira etapa, o resultado da avaliação dos PCN's será validado e o objetivo desta etapa é mostrar como está o PCN das organizações e identificar quais pontos podem ou devem ser melhorados. Nesse momento, poderá ser verificado se o PCN atende aos objetivos de negócio e se está alinhado com a estratégia das organizações.

Com a verificação do trabalho, será possível identificar se o instrumento de avaliação do PCN proposto atingiu seu objetivo que é realizar a avaliação de PCN's em instituições públicas de acordo com a norma NBR ISO/IEC 27002 e a Norma Complementar 06/IN01/DSIC/GSIPR e sugerir melhorias.

4 RESULTADOS E DISCUSSÃO

Neste capítulo, serão relatados os resultados obtidos no desenvolvimento do instrumento de avaliação do PCN de instituições públicas. Também serão expostos os resultados do estudo de caso e a discussão da aplicação do instrumento.

4.1 Instrumento para avaliação do PCN

Este trabalho tem por objetivo fornecer um instrumento para avaliar o plano de continuidade do negócio em organizações públicas, identificando melhorias com o intuito de torná-lo mais eficiente. Um PCN eficiente é peça fundamental para auxiliar na garantia da segurança da informação. Avaliar o PCN é parte integrante no ciclo de desenvolvimento do plano. Ele pode ser usado sempre que a organização sentir a necessidade de avaliar e ou atualizar o PCN.

Ele foi desenvolvido para ser usado por empresas do setor público que desejam avaliar os seus PCN's. Pode ser aplicado por auditores internos das organizações ou mesmo por algum responsável do setor de segurança da informação. Pode ser aplicado também por auditores externos ou por qualquer pessoa/organização que deseja verificar a eficiência do PCN da organização com a qual esteja firmando algum tipo de acordo.

Ao terminar a aplicação do instrumento, espera-se que a organização seja capaz de identificar pontos falhos no seu PCN. Através das análises dos resultados, a organização será capaz de propor melhorias que atendam às suas necessidades e reduza os pontos falhos identificados.

A estrutura geral do instrumento é composta de quatro fases, onde cada fase é composta por diversas etapas como pode ser observado na Figura 2.

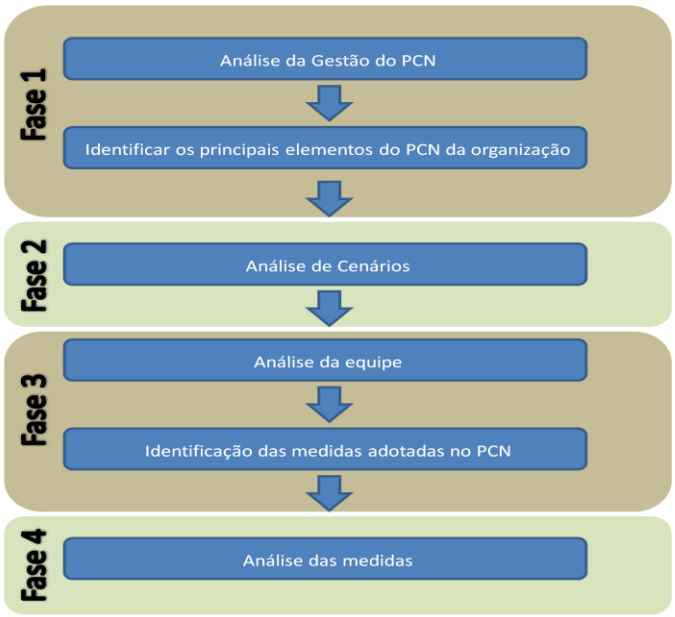


Figura 2 - Fases do instrumento de avaliação do plano de continuidade do negócio

Para elaboração deste instrumento, diversos materiais foram analisados durante a fase de revisão bibliográfica, dentre eles, os que forneceram as principais contribuições na definição das questões importantes de serem analisadas no PCN foram Devargas (1999); Herbane *et al* (2004); Lindström *et al* (2010); McDonald (2008); Brasiliano (2009); Gibb e Buchanan (2006); Lam (2002); Norma Complementar 06/IN01/DSIC/GSIPR (2009); NBR ISO/IEC 27002 (2005); Tribunal de Contas da União (2008); Karakasidis (1997); Ernest-Jones (2005); Wiboonrat (2008); Kepenach (2007).

A Figura 3 mostra onde os materiais analisados contribuíram na elaboração da estrutura do instrumento de avaliação e identifica o relacionamento das fases do instrumento com as fases de elaboração do PCN.

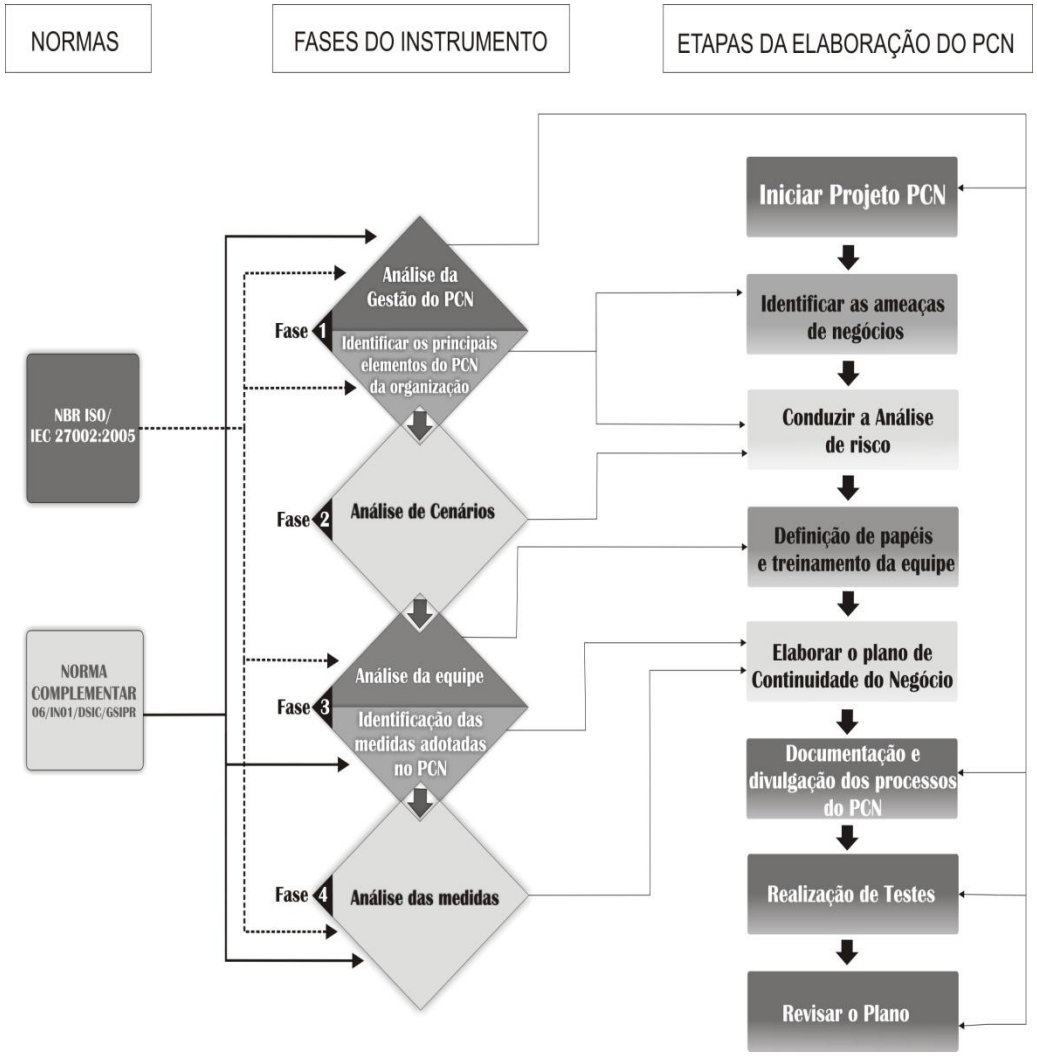


Figura 3 - Relação entre as normas, o instrumento e as fases de elaboração do PCN

4.1.1 Fases da avaliação do PCN

A avaliação do PCN contempla a aplicação do instrumento desenvolvido e, posteriormente, será feita a análise de conformidade com as normas NBR ISO/IEC 27002 e Norma Complementar 06/IN01/DSIC/GSIPR onde será verificado se o PCN avaliado atende às recomendações das normas.

As fases do instrumento de avaliação bem com suas etapas são descritas abaixo:

FASE 1 – Etapa 1: Análise da gestão do PCN.

Nesta etapa, será analisada como é a gestão do PCN na organização. Questões relacionadas à atualização do PCN, equipe responsável, orçamento disponível, divulgação serão abordadas. Segundo o Tribunal de Contas da União (2008), a organização deve ter uma equipe responsável e orçamento disponível para o PCN. Para Lam (2002), Ernest-Jones (2005), o PCN é um processo cíclico e deve passar por atualizações periódicas, preferencialmente a cada seis meses. Ao fim desta etapa, será possível identificar o grau de envolvimento da organização com o seu PCN.

FASE 1 – Etapa 2: Identificar os principais elementos do PCN da organização.

O objetivo dessa fase é identificar os principais elementos, definir e classificar as principais ameaças abordadas no PCN. Para Karakasidis (1997), Lam (2002), Lindström *et al* (2010), Tribunal de Contas da União (2008) definir as principais ameaças e os possíveis impactos que elas podem causar no negócio caracteriza como uma das principais fases na elaboração de um PCN. Para executar esta fase, é necessário avaliar no PCN da organização quais as ameaças que ele busca mitigar. Como resultado desta etapa, obtém-se uma lista das ameaças que o PCN considera crítico para o negócio.

FASE 2 – Etapa única: Análise de cenários.

O objetivo dessa fase é analisar os cenários em que as ameaças identificadas na fase anterior possam se concretizar e gerar impactos negativos para a organização. Para Kepenach (2007), afirma que a organização deve iniciar o desenvolvimento do plano em torno do cenário de pior caso. Alguns cenários possíveis estão associados a diferentes ameaças, como, por exemplo, 1) fatores humanos: roubos, sabotagens, insatisfação; 2) capacidade de processamento: as empresas devem estar cientes da atual capacidade de processamento; 3) desastres naturais: incêndios, enchentes, terremotos,

etc (DEVARGAS, 1999). De acordo com a norma NBR ISO/IEC 27002 (ABNT, 2005), testes de mesa onde são simulados diferentes cenários é uma das formas mais baratas de testar o PCN.

Para realizar esta fase, o responsável pela avaliação deve identificar os possíveis cenários em que as ameaças identificadas na fase anterior possam se concretizar. Um exemplo de cenário seria a ruptura de cabos de energia ocasionado por obras nas proximidades da organização, este cenário concretizaria a ameaça de falta de energia na empresa. Como resultado desta fase, os principais cenários serão identificados.

FASE 3 – Etapa 1: Análise da equipe.

Nesta etapa, o objetivo é identificar se a organização tem uma equipe definida para atuar caso o cenário descrito na fase anterior se concretize e se a divulgação do PCN entre as equipes é efetiva. A formação de uma equipe responsável pela continuidade do negócio é fator determinante e pode influenciar o potencial do PCN (HERBANE, 2004). É importante que toda a organização tenha a mesma compreensão da metodologia e do plano de continuidade do negócio para poder manter um nível de maturidade do PCN (LINDSTRÖM *et al*, 2010). Questões relativas à divulgação do plano na organização devem ser avaliadas no PCN (HERBANE *et al*, 2004). Devargas (1999) afirma que é extremamente importante que os funcionários da organização sejam informados de suas responsabilidades e como reagir em caso de um desastre. É necessário conscientizar todos os envolvidos da necessidade de proteger o sistema e os recursos.

Como resultado dessa etapa, será possível identificar se o PCN define uma equipe para atuar frente ao cenário desfavorável e se a divulgação das ações a serem tomadas é efetiva.

FASE 3 – Etapa 2: Identificação das medidas adotadas no PCN

O objetivo dessa etapa é identificar no PCN quais as medidas adotas caso o cenário identificado na fase anterior se confirme. De acordo com a Norma Complementar 06/IN01/DSIC/GSIPR (2009); Karakasidis (1997); Wiboonrat (2008); Gibb e Buchanan (2006) a identificação das medidas e estratégias para garantir a continuidade do negócio é parte integrante do PCN.

A execução desta etapa é feita analisando quais as medidas contempladas no PCN da organização para garantir a continuidade do negócio caso o cenário

identificado na fase 2 de confirme. Ao término desta etapa, será possível identificar todas as medidas contempladas no plano.

FASE 4 – Etapa única: Análise das medidas.

Nessa etapa, será realizada a análise de cada medida identificada na fase anterior. Questões referentes a contratos, custo das alternativas, empecilhos legais serão analisadas.

É importante analisar a dependência de serviços externos e como esses serviços poderiam afetar a resposta e recuperação da organização (McDonald, 2008). Segundo Devargas (1999), todas as empresas têm contratos e o PCN deve considerá-los quando se formula as estratégias de recuperação. As empresas, normalmente, recebem serviços de terceiros e fornecem serviços a terceiros, dessa forma, as medidas de recuperação devem avaliar se os contratos não serão violados

Avaliar o custo das alternativas é importante quando se avalia o PCN (BRASILIANO, 2009). Um Plano de Continuidade do Negócio deve documentar o custo das alternativas que serão implementadas para assegurar a continuidade das operações caso ocorra alguma interrupção no serviço. (McDonald, 2008)

Nessa etapa, também é analisado se os recursos necessários e a equipe responsável por colocar a medida que garante a continuidade do negócio em prática estão disponíveis e se a equipe tem conhecimento das ações a serem tomadas (BRASILIANO, 2009).

Como resultado dessa fase, será possível avaliar se as medidas adotadas estão bem definidas e se são eficientes.

4.2 Aplicação do instrumento para avaliação do PCN

Nesta seção, será apresentado o estudo de caso realizado para verificar o instrumento de avaliação do PCN de instituições públicas desenvolvido neste trabalho.

4.2.1 Estudo de caso no Aeroporto Internacional de Florianópolis

O Aeroporto Internacional de Florianópolis – Hercílio Luz é um terminal aeroportuário administrado pela Infraero. Este aeroporto retrata os primórdios da aviação na América do Sul.

O terminal foi inaugurado em 1976, é considerado o 14º aeroporto mais movimentado do Brasil e está na lista dos que mais recebem vôos durante o verão (Infraero, 2011). Devido às excelentes condições meteorológicas da região onde o aeroporto se encontra, ele mantém uma taxa de alta operacionalidade ao longo dos anos, acima de 99% (Infraero, 2011). Esta situação faz com que ele seja escolhido como principal alternativa para empresas aéreas, quando estas desejam alterar vôos devido a condições climáticas desfavoráveis em outras pistas (INFRAERO, 2011).

Segundo a Infraero (2011), o aeroporto não acompanhou o crescimento da cidade onde se localiza, por esse motivo, um novo aeroporto será construído, com capacidade para 2,7 milhões de passageiros por ano. O novo aeroporto terá uma área de 35.817m^2 e um pátio de estacionamento de aeronaves com 12 posições para aviões de grande porte (INFRAERO, 2011).

No ano de 2009, o aeroporto teve um movimento de mais de 2 milhões de passageiros (Infraero, 2011). Uma paralisação no funcionamento de algum sistema ligado à operação do aeroporto acarretaria em enormes transtornos para os passageiros e para as companhias aéreas. Visto a importância de se manter a continuidade do serviço prestado pelo aeroporto, um plano de continuidade do negócio se mostrou um mecanismo propício para ser implantado na organização.

4.2.1.1 O PCN do aeroporto

O Aeroporto Internacional de Florianópolis, por ser uma organização prestadora de serviço para a comunidade, necessita que seus serviços estejam em pleno funcionamento. Quaisquer paralisações nos seus serviços podem causar sérios transtornos aos seus clientes e aos usuários de seus serviços no âmbito nacional e internacional.

Visto a importância de manter seus serviços em pleno funcionamento, foi elaborado um plano de continuidade do negócio para garantir a continuidade de seus principais sistemas.

O PCN do aeroporto foi desenvolvido através do levantamento de informações obtidas através dos colaboradores do setor de TI da empresa e dos colaborados das demais empresas envolvidas nos sistemas contingenciados (MARTINS *et al*, s.d).

Os objetivos do plano são 1) maximizar as ações de recuperação através de um plano que contem as fases de notificação/ativação, de recuperação e de reconstrução; 2) identificar as atividades, recursos e procedimentos necessários para manter os sistemas em funcionamento; 3) atribuir responsabilidades para agir durante a execução do plano; 4) firmar contatos e contratos externos que possibilitam apoio técnico e estratégias de recuperação (MARTINS *et al*, s.d).

A estrutura do PCN do aeroporto pode ser observada na sequência:

- Apresentação – realiza uma pequena apresentação dos objetivos e sistemas contingenciados pelo plano;
    - Sistemas contingenciados – relaciona os sistemas que serão contingenciados pela PCN da organização;
    - Equipe técnica – estabelece os responsáveis pelo plano e seus contatos;
    - Contato dos responsáveis pelos sistemas – estabelece os meios de contato dos responsáveis por cada sistema contingenciado;
    - Contato dos fornecedores de equipamentos – estabelece os meios de contato das empresas fornecedoras de equipamentos necessários para o funcionamento dos sistemas contingenciados;
    - Ambientes – caracteriza os ambientes nos quais os sistemas contingenciados estão inseridos.
- Princípios do plano – são identificados os princípios da elaboração do plano;
- Notificação e Ativação – são listadas as ações tomadas para detectar e avaliar os danos causados por uma interrupção e a sequência para notificações quando se pretende colocar o plano em ação. Nesta fase também é determinado as medidas de contingência que devem ser tomadas para cada ameaça identificada;
- Normativas do backup – são determinadas as regras e procedimentos para a realização de backups.

4.2.1.2 Avaliação do PCN da organização utilizando o instrumento

Tendo em mãos o PCN do aeroporto, foi possível realizar a avaliação do mesmo aplicando o instrumento desenvolvido. O resultado da avaliação pode ser observado a seguir.

Fase 1, etapa 1 – análise da gestão do PCN.

Não foi possível determinar a avaliação das questões: "A organização incorpora o PCN nos seus processos e em sua estrutura?" e "Toda a organização está ciente da existência do PCN?" devido ao fato de não ter sido possível entrar em contato direto com a organização.

A questão "As responsabilidades pelo plano são bem difundidas e identificadas no PCN?" e a questão "O plano tem um responsável específico?" atendem de forma satisfatória a avaliação. As evidências que confirmam estas questões podem ser encontradas na seção 1.2 Equipe Técnica do plano.

O PCN avaliado não atendeu as questões referentes à realização de atividades de treinamento, conscientização e educação dos colaboradores com o propósito de criar entendimento sobre continuidade do negócio, à identificação dos recursos financeiros necessários para colocar as medidas de contingencia em ação e a questão relativa às atividades de testes e atualizações do plano. Não foram encontradas no PCN evidências que mostrassem se e como estas atividades são feitas.

Fase 1, etapa 2 – identificar os principais elementos do PCN da organização.

O PCN avaliado atende de forma satisfatória a questão: "O plano identifica as principais ameaças que podem causar interrupções aos processos de negócio?". As evidências para esta questão podem ser encontradas nas tabelas: Tabela A – Sistema SISO/BDO: coluna Risco; Tabela B – Sistema SGTC: coluna Risco; Tabela C – Sistema GEST: coluna Risco.

As principais ameaças identificadas no PCN são:

- Indisponibilidade do ponto de cabeamento estruturado que atende a rede de computadores.
- Indisponibilidade de alguma estação operacional.
- Indisponibilidade da estação STAFF.
- Monitores de TV com defeito ou a imagem da estação de partida ou chegada não estão sendo projetadas nas telas das TVs

- Indisponibilidade da(as) tela(as) LCD inteligente(es).
- Indisponibilidade do sistema de som.
- Indisponibilidade do servidor de banco de dados (s-flbn07).
- Indisponibilidade do servidor de distribuição de telas (s-flgn08).
- Indisponibilidade do link de dados ou roteador
- Indisponibilidade do switch de rede.
- Interrupção do servidor reserva (s-flbn10).
- Interrupção da energia elétrica comercial.
- Indisponibilidade do BIMTRA ou Link de Dados Rede INTRAER.
- Indisponibilidade do servidor de banco de dados (s_flbn50).
- Indisponibilidade de alguma estação Totem.
- Indisponibilidade de algum computador do caixa.
- Indisponibilidade do conversor de mídia.
- Indisponibilidade do switch de rede (desembarque)
- Indisponibilidade do switch de rede (sala técnica principal)

Fase 2 – análise de cenários.

Foi determinado um possível cenário que pudesse afetar o funcionamento normal da organização. O cenário determinado foi a interrupção da energia elétrica comercial ocasionada por fortes ventos na região. Este cenário foi determinado por ele afetar todos os sistemas contingenciados.

Fase 3, etapa 1 – análise da equipe.

A questão referente a: "O PCN determina uma equipe específica para atuar no cenário identificado?" foi atendida parcialmente, a evidência encontrada para esta questão no plano avaliado pode ser encontrada na página 7 do PCN, nos procedimentos de avaliação de danos, onde as pessoas e procedimentos que devem ser seguidos são expostos, porém, as pessoas e os procedimentos são seguidos para qualquer cenário, por esse motivo, a avaliação conclui que esta questão é atendida parcialmente.

Para a questão: "As pessoas envolvidas diretamente no cenário possuem treinamento/educação adequados?", a avaliação concluiu que o PCN avaliado atende pouco a esta questão, uma vez que não existe informação sobre o grau de conhecimento que as pessoas têm em relação ao cenário proposto, infere-se que o conhecimento dos responsáveis seja genérico, independe do cenário.

Fase 3, etapa 2 – identificação das medidas adotadas no PCN.

Nessa etapa, todas as questões atendem de forma satisfatória a avaliação. Para as questões: “As estratégias de continuidade para as atividades críticas são definidas no PCN?” e “Os procedimentos operacionais que permitem a restauração e recuperação das atividades são identificados no PCN?”, as evidências podem ser encontradas na página 11 do plano, onde os procedimentos que precisam ser executados após a avaliação dos danos são identificados.

Para a questão: “As medidas adotadas para recuperar e restaurar as operações do negócio são identificadas no PCN?”, as evidências podem ser encontradas na página 11 do plano, como citado no parágrafo anterior e também podem ser encontradas nas tabelas contidas no plano, na coluna: medida de contingência.

As principais medidas de contingência identificadas no plano para atuar frente ao cenário determinado durante a fase 2 da avaliação são:

- Servidores terão suprimento de energia dos no-breaks por até 30 minutos;
- Caso o gerador do aeroporto não entre em funcionamento nesse intervalo de tempo, os servidores deverão ser desligados até que a energia volte;
- Esperar que a energia seja restabelecida totalmente para não correr o risco de oscilações na rede elétrica ou de súbitas paralisações da energia.

Fase 4 – análise das medidas

Para a questão: “Os ativos e recursos críticos que apóiam a medida são identificados no PCN?”, a avaliação concluiu que o PCN avaliado atende parcialmente a esta questão uma vez que o plano apenas cita superficialmente os ativos e recursos nas tabelas, na coluna: medida de contingência.

Para a questão: “As medidas dependem de terceiros?”, a avaliação concluiu que o plano atende de forma satisfatória este item. O plano deixa claro que para o cenário determinado durante a fase 2 da avaliação, as medidas de contingencia dependem em partes do fornecedor de energia elétrica e do gerador do aeroporto.

Para a questão: “Existem cláusulas nos contratos que define exatamente quais as responsabilidades de terceiros para garantir a continuidade no negócio?”, a avaliação concluiu que o PCN avaliado atende pouco a este item. As únicas evidências encontradas é que o plano apenas estabelece os contatos dos fornecedores de equipamentos para reposição de peças.

O resultado da avaliação da questão: “O PCN determina como a equipe responsável pela medida deve atuar?”, concluiu que o plano atende parcialmente a este item. As evidências podem ser encontradas no diagrama da página 13, que estabelece

quais as ações devem ser tomadas pelos responsáveis, independente da medida de contingência que deva ser colocada em ação.

O PCN avaliado não atende às questões: “O custo da implantação das medidas é identificado?” e “Possíveis empecilhos legais para colocar a medida em prática são abordados pelo PCN?”. Não foram encontrados indícios no plano sobre o custo a implantação das medidas e sobre possíveis empecilhos legais para colocar a medida em ação.

Para a questão: “Medidas alternativas são identificadas no PCN caso a medida principal falhe?”, a avaliação concluiu que o plano atende parcialmente a este item. São identificadas medidas alternativas nas tabelas do PCN, porém, de forma muito superficial.

4.2.1.3 Proposição de melhorias para adequação do PCN avaliado

Com a aplicação do instrumento de avaliação do PCN no plano de continuidade do negócio do Aeroporto Internacional de Florianópolis, foi possível identificar questões que podem ser melhoradas a fim de prover uma melhor adequação do plano com a norma NBR ISO/IEC 27002:2005 e com a Norma Complementar 06/IN01/DSIC/GSIPR.

É aconselhável acrescentar questões relativas às maneiras de divulgar o plano entre os membros da organização. Uma maneira seria estabelecer reuniões periódicas entre os membros da organização a fim de debater questões relativas à gestão da continuidade da empresa e fornecer treinamento, conscientização, educação a respeito do PCN da organização.

É interessante identificar no plano, os recursos financeiros que a empresa disponibiliza para a gestão da continuidade. Dessa forma, a equipe responsável pelo plano, terá em mãos todo o orçamento disponível para a gestão da continuidade e poderá distribuí-lo de forma a otimizar o PCN. Uma sugestão seria determinar a porcentagem dos recursos financeiros destinados a atuar na contingencia de cada ameaça identificada durante a elaboração do plano.

A realização de testes e atualizações do PCN são de suma importância para que ele continue eficaz. Durante a avaliação, não foi identificado no plano da organização, questões relativas a testes e atualizações do plano. O ideal é que estes planos passem por testes e atualizações frequentemente. Os intervalos entre os testes e atualizações

são determinados pela importância dos sistemas contingenciados. Uma sugestão seria reunir a equipe e realizar testes de mesa onde ocorre a simulação de eventos que causem a descontinuidade dos serviços e assim, poder verificar se as medidas e procedimentos relatados no plano atendem as expectativas. Simulações reais se tornam inviável devido à constante operação do aeroporto.

As medidas de contingencia necessitam, na maioria das vezes, de recursos financeiros, recursos tecnológicos e recursos humanos para serem colocadas em ação. O PCN da organização não identifica estes recursos. Uma sugestão seria montar uma tabela com os componentes tecnológicos e seus valores, associados a cada medida de contingencia, alem disso, o plano deve determinar onde estão armazenados estes componentes e caso alguns deles estejam em falta, quais os procedimentos que devem ser seguidos para poder adquiri-los.

Outra melhoria sugerida para o PCN do aeroporto é identificar em seu plano quais as medidas de contingência que possam ter algum empecilho legal ou no caso de não haver nenhuma restrição legal, deixar isso documentado no plano.

Por último, todo PCN tem que garantir que suas medidas funcionem, caso não possam fornecer essa garantia, é importante que ele determine medidas alternativas. O PCN da organização fornece medidas alternativas apenas para poucas medidas de contingencia principal, o ideal seria estabelecer medidas alternativas para todas as medidas principais.

4.3 Discussão

Os elementos encontrados em um plano de continuidade do negócio podem ser classificados em essenciais, obrigatórios e desejados de acordo com as implicações futuras ocasionados pela inconformidade destes elementos.

Na avaliação do PCN, foi possível identificar a ausência de alguns elementos e estes podem ser classificados como descrito no parágrafo anterior.

As questões referentes à divulgação do plano entre os membros da organização e a realização de treinamento, educação, conscientização em relação à gestão da continuidade é essencial. A ausência deste elemento provocaria uma desorganização quando algum incidente ocorresse e os membros da organização precisassem aplicar as

ações descritas no plano sem ao menos saber o porquê de estarem realizando essas ações.

É desejado que o plano contenha itens que identifiquem os recursos financeiros que a organização disponibiliza para a gestão da continuidade do negócio. A ausência de itens relacionados a este assunto no PCN implicaria em uma má distribuição dos recursos entre as atividades de contingencia estabelecidas no plano.

É obrigatório que o plano de continuidade do negócio contenha elementos que tratem da realização de testes para verificar a eficiência do plano e elementos que tratem a realização de atualizações do plano. A inconformidade destes itens no plano acarretaria em sérias implicações no futuro. Um PCN desatualizado e nunca testado pode causar mais danos à continuidade do negócio do que a ausência de um PCN. Isso é explicado porque quando um PCN desatualizado e não testado é colocado em ação, o tempo para corrigir suas falhas durante sua execução pode ser maior do que começar do zero.

Toda medida de contingencia necessita de recursos financeiros, tecnológicos e humanos e estes itens são essenciais em um PCN. A ausência de itens no plano que estabeleçam os recursos para cada medida de contingencia pode acarretar em um atraso e em uma má implementação das medidas.

Existem medidas de contingencia que podem sofrer algum empecilho legal e é desejado que o plano identifique estas medidas e seus empecilhos legais. A ausência deste item no PCN pode acarretar implicações quando o plano precisar ser colocado em ação e a medida de contingencia adotada sofrer algum impedimento devido a alguma legislação vigente, isso acarretaria em um atraso na execução do plano.

É desejado que o PCN acrescente em seu escopo medidas de contingencia alternativas às medidas de contingencia principais. A inconformidade deste item pode tornar o PCN incompleto e se por ventura, as medidas adotadas falharem em algum momento, o plano não terá estabelecido as medidas alternativas e a continuidade do negócio poderá ser afetada.

Com a avaliação do PCN do Aeroporto Internacional de Florianópolis foi possível identificar que ele mostra maior interesse em contingenciar falhas em equipamentos componentes dos sistemas contingenciados. Ele não se preocupa tanto com falhas de caráter humano, como por exemplo, sabotagens, imperícia, imprudência.

De forma geral, o PCN avaliado estabelece de forma clara as medidas e ações a serem tomadas frente a uma situação de descontinuidade dos serviços porém, existe

certa carência no que diz respeito às questões que tangenciam o plano, como por exemplo, determinar a freqüência de realização dos testes e atualizações do plano, bem como realizar treinamentos das pessoas envolvidas com a continuidade nas empresas.

O instrumento de avaliação desenvolvido permitiu identificar os elementos importantes que o plano contempla e os que estão ausentes ou incompletos. Isso permite que o avaliador determine ações que possam melhorar o PCN avaliado. Dessa forma, o instrumento de avaliação se mostrou uma ferramenta interessante para realizar a avaliação de PCNs.

A utilização do instrumento desenvolvido na avaliação do PCN do Aeroporto Internacional de Florianópolis foi de fácil aplicação, uma vez que ele aborda de forma seqüencial todas as etapas do plano de continuidade do negócio. Através de sua aplicação, foi possível identificar quais etapas do PCN avaliado podem ser melhoradas para melhor adequação às normas utilizadas como referencia na elaboração do instrumento de avaliação.

O fato do instrumento de avaliação abordar de forma seqüencial todas as etapas do PCN permite ao avaliador identificar em quais etapas da elaboração do plano ocorre um maior número de falhas. Assim, a organização pode melhorar seu plano e fornecer treinamento com foco nas etapas onde ocorrem mais falhas.

O instrumento de avaliação desenvolvido permite que a organização avalie seu PCN por etapas e permite que ela estabeleça diferentes avaliadores, onde cada avaliador fica responsável por uma fase da avaliação. Dessa forma, a avaliação se torna mais completa e menos tendenciosa.

5 CONSIDERAÇÕES FINAIS

Garantir a continuidade do negócio nas organizações é essencial para que a organização se mantenha ativa no mercado. A descontinuidade de suas atividades pode acarretar danos referentes à imagem da empresa, além de perdas financeiras, de clientes e de confiabilidade.

Com a realização deste trabalho foi possível identificar a importância do Plano de Continuidade do Negócio nas organizações. Foi possível verificar que o PCN é considerado muitas vezes como uma *commodity*, mas, visto que seu uso ainda não está

enraizado nas empresas, no cenário atual ele ainda é considerado como um diferencial estratégico.

O objetivo deste trabalho foi criar um instrumento de avaliação do PCN para poder ser utilizado por qualquer colaborador da empresa, sendo este interno ou externo. O objetivo foi alcançado, sendo possível elaborar um instrumento de avaliação que segue as melhores práticas sugeridas pela norma NBR ISO/IEC 27002:2005 e pela Norma Complementar 06/IN01/DSIC/GSIPR. Foi possível realizar um estudo de caso de sua aplicação, onde foi verificado que ele atende ao propósito para o qual foi concebido.

O instrumento desenvolvido cumpre com seu objetivo que é fornecer um mecanismo de avaliação de Planos de Continuidade do Negócio.

Este trabalho contribuiu para a teoria no que se refere à segurança da informação, com foco para a gestão da continuidade do negócio. Foi possível realizar um levantamento na literatura dos principais componentes de um PCN, confrontando visões de diferentes autores.

Com a elaboração do instrumento de avaliação, foi possível determinar quais elementos do PCN devem ser avaliados e o instrumento desenvolvido oferece um mecanismo de avaliação quando se pretende avaliar o plano de continuidade do negócio em instituições públicas.

O trabalho limitou-se a desenvolver um instrumento de avaliação do plano de continuidade do negócio de instituições públicas e verificá-lo em um estudo de caso do PCN do Aeroporto Internacional de Florianópolis, obtido através da web.

Como trabalhos futuros, podem ser realizadas aplicações do instrumento de avaliação em organizações do mesmo segmento para poder identificar semelhanças e diferenças no PCN das organizações. É interessante também realizar avaliações do PCN de empresas públicas e privadas e analisar se existe diferença acentuada nos planos.

Seria interessante também utilizar o instrumento de avaliação do PCN no processo de elaboração do PCN, desta forma, seria possível identificar quais itens são passíveis de avaliação e o plano elaborado já teria a preocupação de acrescentar estes itens no seu escopo.

BIBLIOGRAFIA

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT, 2005.

ADKINS, G. L.; THORNTON, T. J.; BLAKE, K. **A Content Analysis Investigating Relationships Between Communication and Business Continuity Planning.** Journal of Business Communication. Julho 2009, vol 46, nº 3, p. 362-403

BAJGORIC, N. **Information systems for e-business continuance : a systems approach.** Kybernetes, vol 35, 2006, p. 632-652.

BERMEJO, P. H. S. **Planejamento estratégico de tecnologia da informação com ênfase em conhecimento**. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, Florianópolis, 2009 (Tese)

BOEHMER, W.; BRANDT, C.; GROOTE, J. F. "**Evaluation of a business continuity plan using process algebra and modal logic.**" 2009 IEEE Toronto International Conference Science and Technology for Humanity TICSTH. IEEE, 2009. p. 147-152.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Secretaria de Fiscalização de Tecnologia da Informação. 3ª Ed. Brasília, 2008, 75 p.

BRASIL. Norma Complementar 06/IN01/DSIC/GSIPR de 11 de novembro de 2009. Estabelece diretrizes para Gestão de Continuidade de Negócio, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta ou indireta – APF. **Diário Oficial [da] República Federativa do Brasil**, Brasília, n. 223, p. 20, 23/Nov/2009. Seção 1

BRASIL. Decreto nº 3.505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, nº 114, pag. 2, 14 jun. 2000. Seção 1.

BRASIL. Infraero Aeroportos. 2011. Disponível em http://www.infraero.gov.br/index.php/br/aeroportos/santa-catarina/aeroporto-internacional-de-florianopolis.html. Acessado em julho de 2011

BRASILIANO, A. C. R. **Método Brasiliano: Plano de Continuidade do Negócio.** Brasiliano&Associados, março 2009. Disponível em: http://www.brasiliano.com.br/pdf/metodo_brasiliano_plano_de_continuidade_de_negocios.pdf. Acesso em: 12/04/2011

CAMPOS, A. **Sistema de segurança da informação: controlando os riscos**. Florianópolis: Visual Books, 2ª ed, 2007.

DEVARGAS, M. **Survival is not compulsory: an introduction to business continuity planning.** Computers & Security, Volume 18, 1999, Pag 35-46.

ERNESTJONES, T. **Business continuity strategy – the life line.** Network Security, Volume 2005, Agosto 2005, Pag. 5-9

FRANCISCO, R. **A importância de um plano de continuidade do negócio da organização.** Estado de Santa Catarina. Instituto Superior Tupy, 2004. (Monografia)

GIBB, F.; BUCHANAN, S. **A framework for business continuity management.** International Journal of Information Management, Vol 26, Abril 2006, Pag 128-141

GILL, T. J. **Workplace continuity: how risk and technology will affect facilities strategy.** Journal of Facilities Management, vol. 4, 2006 , pp.110 - 125

HERBANE, B.; ELLIOTT, D.; M. SWARTZ, E. M. **Business Continuity Management: time for a strategic role?** Long Range Planning. Vol. 37, out 2004, Pag 435-457

ISACA. **Certified Information Systems Auditor – CISA**. 2010

ISACA. **IT Continuity Planning Audit/Assurance Program.** Disponível em http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Continuity-Planning-Audit-Assurance-Program.aspx Acessado em maio de 2011. USA, 2009

JUNG, C. F. **Metodologia para pesquisa & desenvolvimento:** aplicada a novas tecnologias, produtos e processos. Rio de Janeiro: Axcel Books do Brasil, 2004.

KARAKASIDIS, K. "**A project planning process for business continuity**", Information Management & Computer Security, Vol. 5, pp.72 – 78, 1997

KEPENACH, R. J. **Business Continuity Plan Design**. Second International Conference on Internet Monitoring and Protection ICIMP 2007 Icimp (2007)

LAM, W. **Ensuring business continuity**. IT Professional , vol.4, no.3, pp.19-25, Mai/Jun 2002

LINDSTRÖM, J.; SAMUELSSON, S.; HÄGERFORS, A. **Business continuity planning methodology.** Disaster Prevention and Management, Vol. 19, p.243 – 255, 2010

MCDONALD, R. **New considerations for security compliance, reliability and business continuity**. 2008 IEEE Rural Electric Power Conference. IEEE, 2008.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica.** 7. ed. São Paulo: Atlas, 2010. xvi, 297 p.

MARTINS, R. F.; WANGHAM, M. S.; FAVARIM, F. **Plano de Continuidade de Negócio para a TI do Aeroporto Internacional de Florianópolis**. In: Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, 2009, Campinas - SP. IX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, 2009. v. 9.

NAKAMURA, E. T.; DE GEUS, P. L. **Um modelo de segurança de redes para ambientes cooperativos.** Instituto de Computação – Universidade Estadual de Campinas. Campinas, SP. 2000. (Dissertação)

SILVA, E. L.; MENEZES, E. M. **Metodologia de Pesquisa e Elaboração de Dissertação.** 3ª ed. ver. atual. Laboratório de Ensino a Distância da UFSC. Florianópolis, 2001, 121 p.

UNIVERSIDADE FEDERAL DE LAVRAS. Biblioteca da UFLA. **Manual de normalização e estrutura de trabalhos acadêmicos: TCC, monografias, dissertações e teses**. Lavras, 2010. Disponível em: <http://www.biblioteca.ufla.br/site/index.php>. Acesso em janeiro de 2011.

XIANG, W.; WANG, Y.; ZHANG, Z. "**The Research on Business Continuity Planning of E-government Based on Information Security Risk Management,**" Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on , vol., no., pp.446-450, 6-8 Abril 2008

WIBOONRAT, M. **"An empirical IT contingency planning model for disaster recovery strategy selection"** Engineering Management Conference, 2008. IEMC Europe 2008. IEEE International , vol., no., pp.1-5, 28-30 Junho 2008

WINKLER, U.; et al. **Process-centric Business Continuity Management : A Model-Driven Approach.** Seventh International Conference on the Quality of Information and Communications Technology. IEEE, 2010. p. 248-252

APÊNDICE A: Instrumento de Avaliação do PCN – Fase 1

Avaliação do Plano de Continuidade do Negócio do Aeroporto Internacional de Florianópolis Data:22/07/2011					
Instruções para o preenchimento: 1)Marque com "X" o campo que mais se adéqüe à pergunta. 2)Marque apenas uma alternativa, para cada campo avaliado. 3) No campo "evidências", disserte sobre as evidências que proporcionaram a resposta para a questão.					
FASE 1					
Etapa 1: Análise da gestão do PCN.	Avaliação				
	Não atendeu	Atendeu pouco	Atendeu parcialmente	Atendeu	Evidências
A organização incorpora o PCN nos seus processos e em sua estrutura? (NBR ISO/IEC 27002:2005)					Não foi possível determinar
Toda a organização está ciente da existência do PCN? (NBR ISO/IEC 27002:2005)					Não foi possível determinar
As responsabilidades pelo plano são bem difundidas e identificadas no PCN? (NBR ISO/IEC 27002:2005; Norma Complementar 06/IN01/DSIC/GSIPR)				x	Seção 1.2 Equipe Técnica
O plano tem um responsável específico? (Norma Complementar 06/IN01/DSIC/GSIPR)				x	Seção 1.2 Equipe Técnica
Atividades de treinamento, conscientização e educação com o propósito de criar o entendimento sobre continuidade do negócio são abordados no PCN? (NBR ISO/IEC 27002:2005)	x				Não foi possível encontrar nenhum indício no plano de atividades de treinamento, conscientização e educação para criar entendimento sobre continuidade do negócio
Os recursos financeiros para viabilizar o plano são identificados? (Norma Complementar 06/IN01/DSIC/GSIPR)	x				Não foi encontrado nenhum indício no plano sobre os recursos financeiros destinados ao plano de contingência
Os testes e atualizações do plano são realizados com freqüência? (NBR ISO/IEC 27002:2005; Norma Complementar	x				Não foi encontrado nenhum indício no plano de ações relacionadas a testes e atualizações do plano

06/IN01/DSIC/GSIPR)					
Etapa 2: Identificar os principais elementos do PCN da organização.	Avaliação				
	Não atendeu	Atendeu pouco	Atendeu parcialmente	Atendeu	Evidências
O plano identifica as principais ameaças que podem causar interrupções aos processos de negócio? (NBR ISO/IEC 27002:2005; Norma Complementar 06/IN01/DSIC/GSIPR)				x	Tabela A – Sistema SISO/BDO: coluna Risco Tabela B – Sistema SGTC: coluna Risco Tabela C – Sistema GEST: coluna Risco

Cite as principais ameaças identificadas:

1) Indisponibilidade do ponto de cabeamento estruturado que atende a rede de computadores.
2) Indisponibilidade de alguma estação operacional.
3) Indisponibilidade da estação STAFF.
4) Monitores de TV com defeito ou a imagem da estação de partida ou chegada não estão sendo projetadas nas telas das TVs
5) Indisponibilidade da(as) tela(as) LCD inteligente(es).
6) Indisponibilidade do sistema de som.
7) Indisponibilidade do servidor de banco de dados (s-flbn07).
8) Indisponibilidade do servidor de distribuição de telas (s-flgn08).
9) Indisponibilidade do link de dados ou roteador
10) Indisponibilidade do switch de rede.
11) Interrupção do servidor reserva.(s-flbn10).
12) Interrupção da energia elétrica comercial.
13) Indisponibilidade do BIMTRA ou Link de Dados Rede INTRAER.
14) Indisponibilidade do servidor de banco de dados (s_flbn50).
15) Indisponibilidade de alguma estação Totem.
16) Indisponibilidade de algum computador do caixa.
17) Indisponibilidade do conversor de mídia.
18) Indisponibilidade do switch de rede (desembarque)
19) Indisponibilidade do switch de rede (sala técnica principal)

APÊNDICE B: Instrumento de Avaliação do PCN – Fase 2

Avaliação do Plano de Continuidade do Negócio do Aeroporto Internacional de Florianópolis Data:22/07/2011
Instruções para o preenchimento: 1)Para cada ameaça identificada na fase 1, determine possíveis cenários onde possa ocorrer sua concretização
FASE 2
Cenário1: Interrupção da energia elétrica comercial ocasionada pela queda de uma árvore na linha de transmissão devido aos fortes ventos na região.

APÊNDICE C: Instrumento de Avaliação do PCN – Fase 3

Avaliação do Plano de Continuidade do Negócio do Aeroporto Internacional de Florianópolis Data:22/07/2011					
Instruções para o preenchimento: 1)Marque com "X" o campo que mais se adéqüe à pergunta. 2)Marque apenas uma alternativa, para cada campo avaliado. 3) No campo "evidências", disserte sobre as evidências que proporcionaram a resposta para a questão. 4) Responda estas questões para cada cenário identificado na fase 2					
FASE 3					
Etapa 1: Análise da equipe	Avaliação				
	Não atendeu	Atendeu pouco	Atendeu parcialmente	Atendeu	Evidências
O PCN determina uma equipe específica para atuar no cenário identificado? (NBR ISO/IEC 27002:2005; Norma Complementar 06/IN01/DSIC/GSIPR)			x		Na página 7, nos procedimentos de avaliação de danos, as pessoas e procedimentos que devem ser seguidos são expostos, porém, eles são seguidos pra qualquer cenário
As pessoas envolvidas diretamente no cenário possuem treinamento/educação adequados? (NBR ISO/IEC 27002:2005)		x			Não existe informação sobre o grau de conhecimentos que as pessoas têm em relação ao cenário, infere-se que o conhecimento dos responsáveis é genérico, independe do cenário
Etapa 2: Identificação das medidas adotadas no PCN	Avaliação				
	Não atendeu	Atendeu pouco	Atendeu parcialmente	Atendeu	Evidências
As estratégias de continuidade para as atividades críticas são definidas no PCN? (Norma Complementar 06/IN01/DSIC/GSIPR)				x	Na página 11, os procedimentos que precisam ser executados após a avaliação dos danos são identificados
Os procedimentos operacionais que permitem a restauração e recuperação das atividades são identificados no PCN? (NBR ISO/IEC 27002:2005)				x	Na página 11, os procedimentos que precisam ser executados após a avaliação dos danos são identificados
As medidas adotadas para recuperar e				x	Na página 11, os procedimentos que

restaurar as operações do negócio são identificadas no PCN? (NBR ISO/IEC 27002:2005)					precisam ser executados após a avaliação dos danos são identificados; Nas tabelas, na coluna: medida de contingência

Cite as principais medidas identificadas:

1) servidores terão suprimento de energia dos no-breaks por até 30 minutos

2) caso o gerador do aeroporto não entre em funcionamento nesse intervalo de tempo, os servidores deverão ser desligados até que a energia volte

3) esperar que a energia seja restabelecida totalmente para não correr o risco de oscilações na rede elétrica ou de súbitas paralisações da energia.

APÊNDICE D: Instrumento de Avaliação do PCN – Fase 4

Avaliação do Plano de Continuidade do Negócio do Aeroporto Internacional de Florianópolis Data:22/07/2011					
Instruções para o preenchimento: 1)Marque com "X" o campo que mais se adéqüe à pergunta. 2)Marque apenas uma alternativa, para cada campo avaliado. 3) No campo "evidências", disserte sobre as evidências que proporcionaram a resposta para a questão. 4) Responda estas questões para cada medida identificada na fase 3					
FASE 4					
Análise das medidas	Avaliação				
	Não atendeu	Atendeu pouco	Atendeu parcialmente	Atendeu	Evidências
Os ativos e recursos críticos que apóiam a medida são identificados no PCN? (NBR ISO/IEC 27002:2005; Norma Complementar 06/IN01/DSIC/GSIPR)			x		O plano apenas cita superficialmente os ativos e recursos nas tabelas, coluna: medida de contingência
O PCN deixa claro se as medidas de contingência dependem de terceiros? (NBR ISO/IEC 27002:2005)				x	Depende do fornecedor de energia elétrica e do gerador do aeroporto
Existem cláusulas nos contratos que define exatamente quais as responsabilidades de terceiros para garantir a continuidade no negócio? (Norma Complementar 06/IN01/DSIC/GSIPR)		x			O PCN só estabelece os contatos dos fornece-dores de equipamentos para reposição de peças
O PCN determina como a equipe responsável pela medida deve atuar? (NBR ISO/IEC 27002:2005; Norma Complementar 06/IN01/DSIC/GSIPR)			x		O diagrama da página 13 estabelece quais as ações devem ser tomadas pelos responsáveis, independente da medida que deve ser colocada em ação
O custo da implantação das medidas é identificado? (Norma Complementar 06/IN01/DSIC/GSIPR)	x				Não foi encontrado nenhum indício no plano sobre o custo da implantação das medidas
Possíveis empecilhos legais para colocar a medida em prática são abordados pelo PCN?	x				Não foi encontrado nenhum indício no plano sobre possíveis empecilhos legais

Medidas alternativas são identificadas no PCN caso a medida principal falhe?			X		São identificadas medidas alternativas nas tabelas, porém, de forma muito superficial

ANEXO A – Plano de Continuidade do Negócio do Aeroporto Internacional de Florianópolis

PLANO DE CONTINGÊNCIA PARA TI DO AEROPORTO INTERNACIONAL DE FLORIANÓPOLIS

1 APRESENTAÇÃO

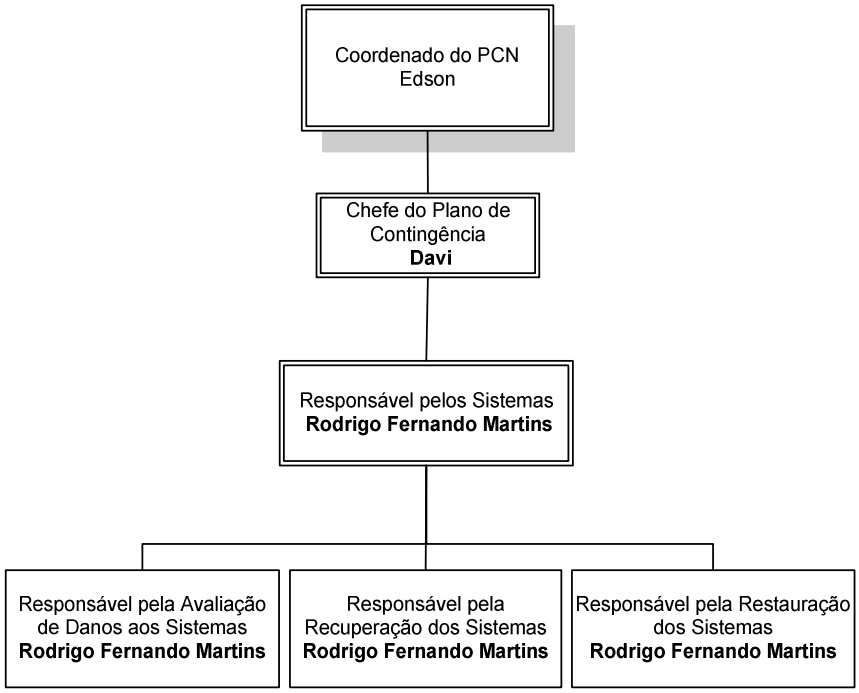
Este documento foi elaborado para contingenciar os sistemas SISO/BDO, GEST e SGTC do Aeroporto Internacional de Florianópolis, com base na análise de riscos realizada, na criticidade dos processos de cada sistema e no impacto gerado caso algum sistema ou parte deste fique indisponível. Com base nestes aspectos, um plano de contingência específico foi elaborado.

1.1 Sistemas Contigênciados

Os sistemas que serão contingenciados para o Aeroporto Internacional de Florianópolis estão descritos abaixo:

SISO/BDO – Sistema Integrado de Solução Operacional e Banco de Dados Operacional;
GEST – Sistema Gestor de Estacionamento;
SGTC – Sistema de Gerenciador de Torre de Controle.

1.2 Equipe Técnica



Edson – Coordenando do Plano de Continuidade de Negócios

Av. Severo Dulius, 90010 São João – Porto Alegre – RS – CEP 90200-310

Telefones:

PABX (51) 3358-2000

DDR: (51) 3358-0000

FAX:(51) 3358-1111

E-mail: edsonxx.cnpa@infraero.gov.br

Davi – Chefe do Plano de Contingência

AV Diomício Freitas, 3393 Carianos – Florianópolis – SC – CEP 88700-900

Telefones:

Trabalho:(48) 2221-1234

Casa: (48) 3357-2222

Celular: (48) 9999-8888

E-mail: davi.cnpa@infraero.gov.br

davi@gmail.com

Rodrigo Fernando Martins – Responsável pelos Sistemas

Rua São Paulo, 32 Bela Vista 2 – São José SC – CEP 88110-455

Telefones:

Trabalho: (48) 3331-4029

Casa: (48) 324-5678

Celular: (48) 88269066

E-mail: rodrigofm.cnpa@infraero.gov.br

rodrigo.rodrigo@gmail.com

1.3 Contato Sistemas Dos Responsáveis Pelos Sistemas

SISO/BDO

Eduardo Gonçalves – TIGL - Telefone: (21) 3398-4275

Ângela Quintana – TIGL – Telefone: (21) 3398-4280

GEST

Escala TIRF - Telefone: (81) 3322-4522

SGTC

HELP DESK TIPA – Telefone (51) 3358-1274

NAPA – Telefone (51) 3358-2398

1.4 Contato Dos Fornecedores De Equipamentos

Em caso de problemas com os equipamentos as seguintes empresas deverão ser contatadas para reposição:

Computadores:

HP – Telefone 0800-7097751

Positivo – Telefone 0800-644-6591

Switch de rede:

Redisul – Telefone (41) 3362-2728

1.5 Ambientes

Os ambientes nos quais os sistemas alvo se encontram são:

Sala técnica principal:

- localizada na administração da Infraero ao lado da sala da tecnologia da informação de Florianópolis. Na sala técnica principal estão localizados os servidores principais (SISO/BDO, GEST).

Sala de operações da torre de controle de Florianópolis:

- localizada no ponto mais alto do prédio da torre de controle, nesta sala estão as duas estações no qual os operadores utilizam os módulos do sistema SGTC. Nesta sala, também está o servidor principal do SGTC.

Sala técnica de contingência Site B:

- localizada no prédio antigo da VASP, nesta temos toda a infra-estrutura no qual manterá a estratégia de espelhamento dos servidores dos sistemas SISO/BDO, GEST e SGTC, haverá três servidores, sendo que cada um destes é destinado para um sistema específico. Os servidores deverão ter seus sistemas operacionais e banco de dados idênticos aos do sistema original. A rede local chegará ao local no Site B através de um par de fibras óticas partindo da sala técnica próxima ao desembarque doméstico RACK C, interligando com outro par te fibra que segue até o RACK A. Também terá mais dois pares de fibras partindo do RACK A e chegando direto ao local alternativo. O Site B também é provido de equipamentos de segurança como câmeras de vídeo, controle de acesso biométrico, sistema de ar-condicionado, sensores de fumaça, no-break, gerador de energia elétrica, sistemas de comunicação telefônica e via rádio.

2 PRINCÍPIOS DO PLANO

São consideradas várias situações que constituem uma base para o plano.

- a principal situação é aquela que atinge os clientes, se os sistemas situados na Infraero de Florianópolis não estão operantes; por conseqüência, a Infraero não está executando os processos de negócios relacionados aos sistemas;
- outra situação que deve ser considerado, mas não menos importante é manter estratégias de prevenção e recuperação que serão usadas para contornar a crise e sustentar o funcionamento dos sistemas.

Com base nos princípios do plano, as seguintes suposições foram utilizadas ao desenvolver o plano de contingência para os sistemas SISO/BDO, SGTC e GEST:

- se os sistemas (SISO/BDO, GEST e/ou SGTC) estiverem inoperantes devido uma falha no servidor, seja *hardware* ou *software* e o servidor não seja recuperado no prazo de duas (2) horas o Site B deverá ser ativado;
- caso ocorra uma indisponibilidade no ativo de rede (*switch*), que interliga o servidor do sistema aos demais switches de rede, e conseqüentemente as estações de trabalho dos usuários envolvidos aos processos operacionais do sistema, e este ativo de rede não seja restabelecido no prazo de duas (2) horas o switch deverá ser substituído pelo reserva que encontra-se no armário da TI na prateleira de equipamentos de rede de contingência.
- sistemas preventivos (por exemplo, geradores, aparelhos de ar-condicionado, *no-break*, sensores de fumaça, sistemas

sprinkler, extintores de incêndio e assistência de bombeiros) devem estar plenamente operacionais a todo momento;

- todos equipamentos envolvidos pelo sistema, seja o servidor, os ativos de rede ou a estações de trabalho devem estar ligados a um abastecimento de fonte de alimentação ininterrupta, *uninterrupted power supply* (UPS), que fornece alimentação elétrica de 45 minutos à 1 hora durante uma falha de energia do fornecimento externo;

O PCN não é aplicável nas seguintes situações:

- caso ocorra uma catástrofe que envolva a parte operacional, as estações de trabalho e/ou usuários dos sistemas (por exemplo incêndio nas áreas operacional do aeroporto);
- caso o plano de evacuação de ocupação do terminal de passageiros e/ou administração da Infraero sejam ativados.

3 NOTIFICAÇÃO E ATIVAÇÃO

Nesta fase, são descritos as ações tomadas para detectar e avaliar os danos causados por uma interrupção de algum dos sistemas. Com base na avaliação do evento, o plano pode ser ativado pelo chefe do plano de contingência, Sr. Davi. Em caso de emergência, a prioridade da Infraero é preservar a saúde e a segurança das pessoas, antes que possa dar procedimento as fases de notificação e de ativação. As informações de contato da equipe do PCN estão localizadas no início deste documento na subseção 1.2 (equipe técnica). A **seqüência para notificação** está listada abaixo:

1. a primeira medida é notificar o coordenador do PCN Sr. Edson, caso não esteja disponível o chefe do plano de contingência Sr. Davi deve ser notificado em seu lugar. Todas as informações observadas relacionadas à indisponibilidade do sistema devem ser repassadas ao Sr. Davi;

2. o gerente da área operacional envolvida (setor de operações do aeroporto no caso do sistema SISO e SGTC, ou setor comercial no caso do sistema GEST) é contatado pelo coordenador do PCN para avaliação de danos para informa-lhe o ocorrido. O chefe do plano de contingência deve instruir o responsável pelos sistemas Sr. Rodrigo Fernando Martins para começar os procedimentos de avaliação de danos;
3. o chefe do plano de continência Sr. Davi deve notificar o técnico responsável pela avaliação de danos (Sr. Rodrigo Fernando Martins) e encaminhá-lo para os procedimentos esboçados a seguir, para determinar a extensão de dano e estimar o tempo de recuperação.

Fluxograma 1: Seqüência para notificação

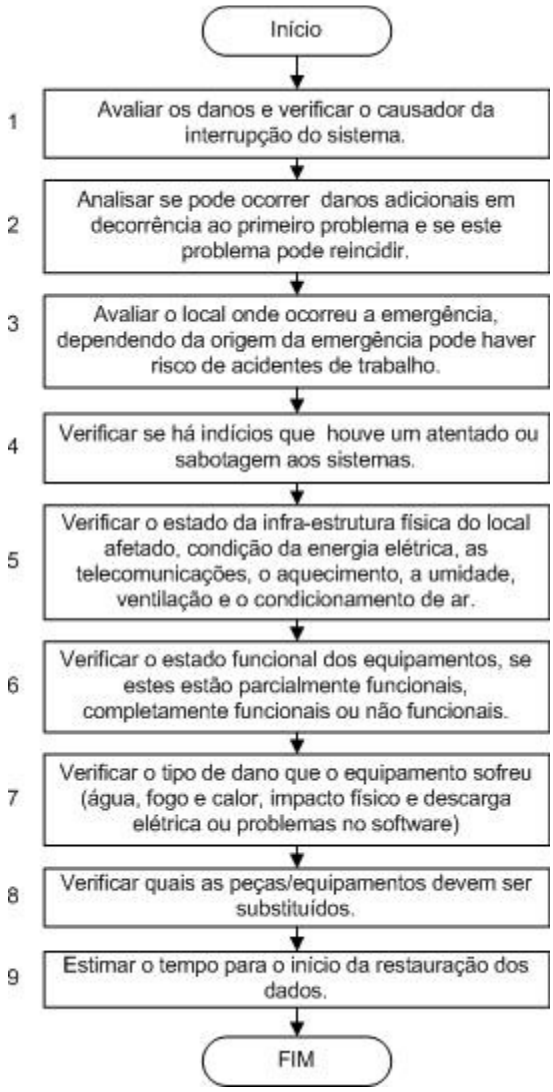
Os procedimentos de **avaliação de danos** são:

1. o técnico Sr. Rodrigo Fernando Martins deve avaliar os danos e verificar o causador da interrupção do sistema. Inicialmente, através de uma análise ao diagrama do sistema (ver Figura A,

B e C), o técnico deve verificar se o problema é no servidor, ou em uma das estações de operação, posteriormente, o técnico deve verificar se a falha é causada por *software*, *hardware*, rede de dados ou outro agente externo;

2. o técnico Sr. Rodrigo Fernando Martins deve analisar se pode ocorrer danos adicionais em decorrência ao primeiro problema e se este problema pode reincidir;
3. o técnico Sr. Rodrigo Fernando Martins deve avaliar o local onde ocorreu a emergência, dependendo da origem da emergência pode haver risco de acidentes de trabalho, verificar se há indícios que houve um atentado ou sabotagem aos sistemas, informações que vão complementar o laudo técnico pós emergência;
4. o técnico Sr. Rodrigo Fernando Martins deve verificar o estado da infra-estrutura física do local afetado (seja a sala dos operadores de algum dos sistemas tratados ou a sala dos servidores localizada na administração da Infraero), tais como a condição da energia elétrica, as telecomunicações, o aquecimento, a umidade, ventilação e o condicionamento de ar;
5. o técnico Sr. Rodrigo Fernando Martins deve verificar o estado funcional dos equipamentos, verificando se estes estão parcialmente funcionais, completamente funcionais ou não funcionais;
6. o técnico Sr. Rodrigo Fernando Martins deve verificar o tipo de dano que o equipamento sofreu, os danos causados, como por exemplo por água, fogo e calor, impacto físico e descarga elétrica ou problemas no *software*;
7. após analisar os equipamentos afetados, o técnico Sr. Rodrigo Fernando Martins deve verificar quais as peças/equipamentos devem ser substituídos, sejam estas da parte estrutural da sala, do *hardware* computador/servidor ou do *software*;

8. o técnico Sr. Rodrigo Fernando Martins que avalia os danos deve estimar o tempo para o início da restauração dos dados.



Fluxograma 2: Avaliação de danos.

A seguir, são apresentados os diagramas de rede dos sistemas alvo (referência para o item 1 dos procedimentos de avaliação de danos).

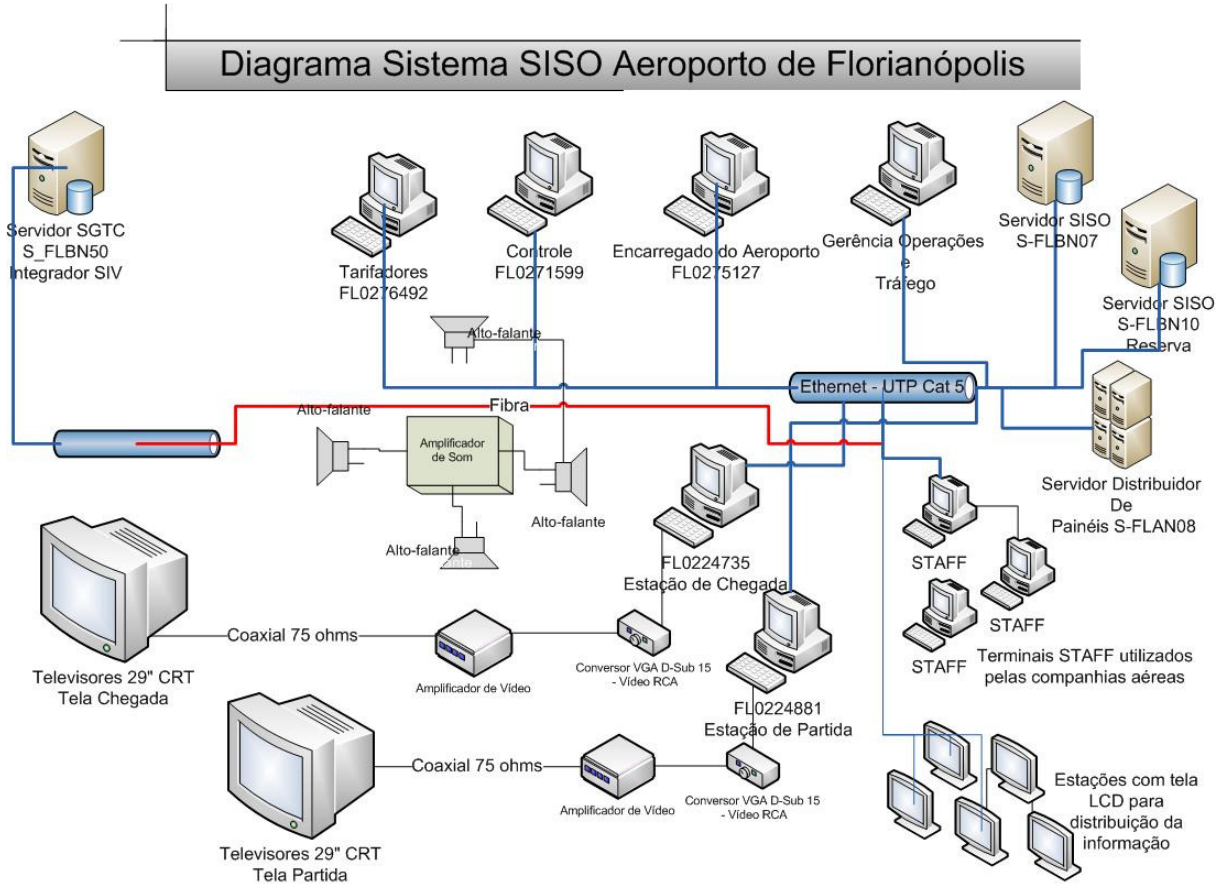


Figura A

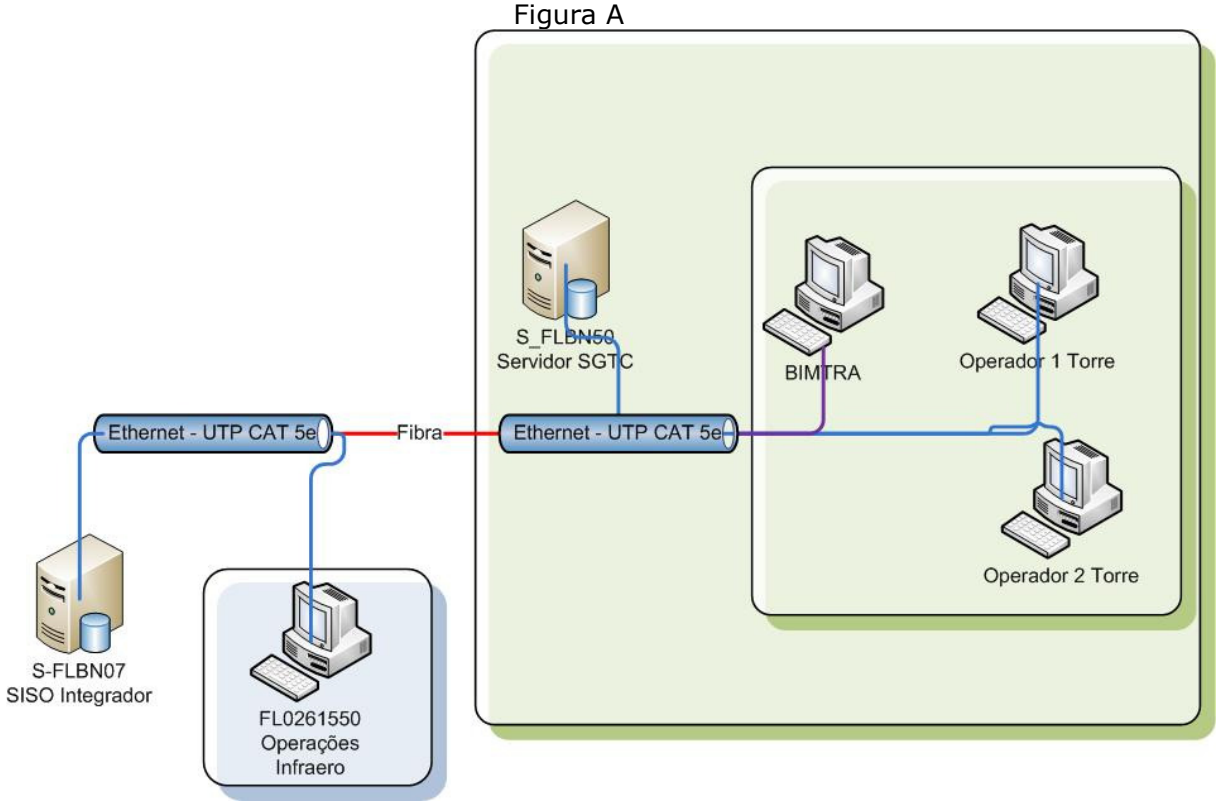


Figura B

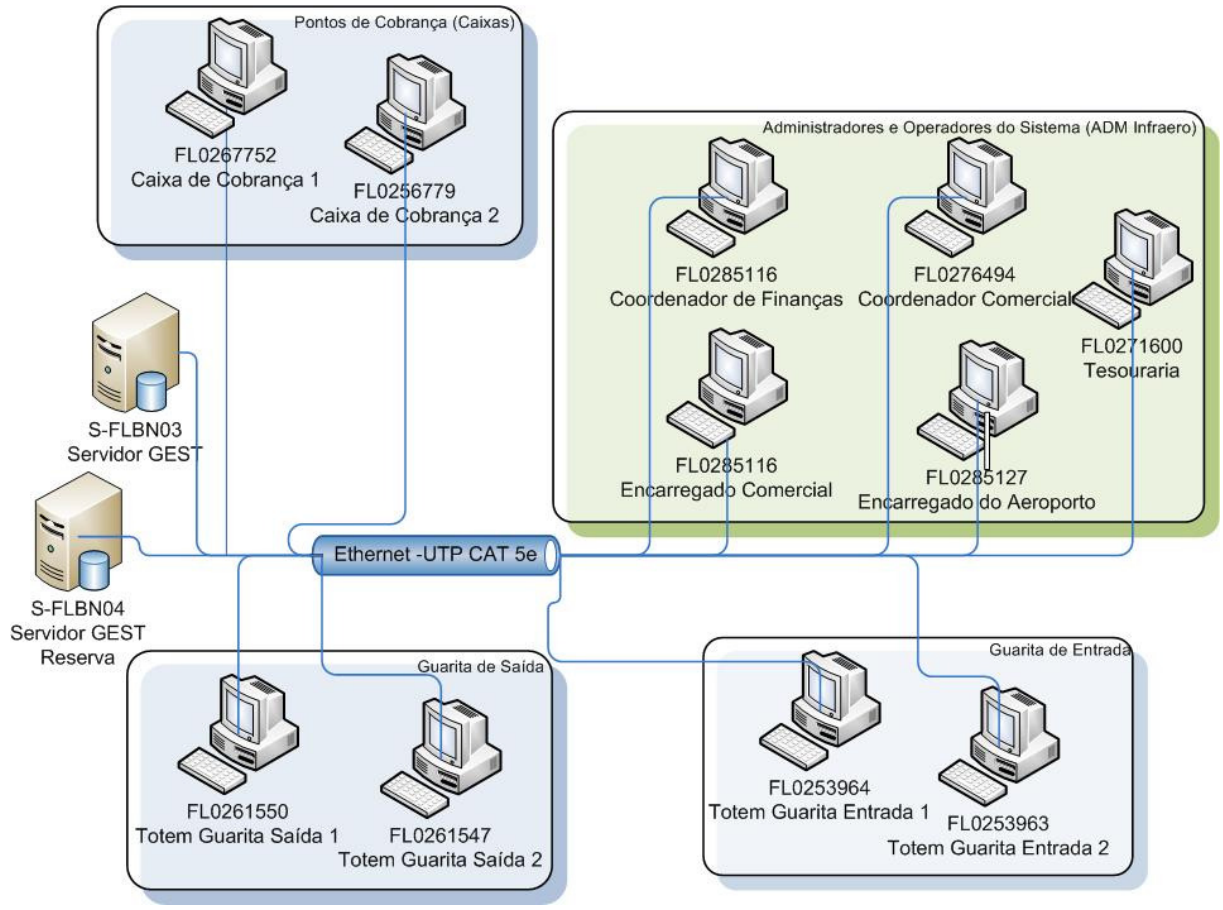
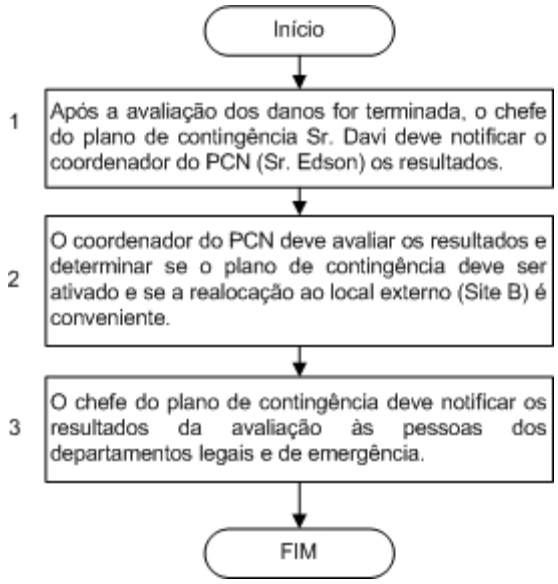


Figura C

Os procedimentos que precisam ser executados **após a avaliação dos danos** são:

1. quando a avaliação dos danos for terminada, o chefe do plano de contingência Sr. Davi deve notificar o coordenador do PCN (Sr. Edson) os resultados;
2. o Sr. Edson, coordenador do PCN deve avaliar os resultados e determinar se o plano de contingência deve ser ativado e se a realocação ao local externo (Site B) é conveniente;
3. baseado na avaliação dos resultados, o chefe do plano de contingência deve notificar os resultados da avaliação às pessoas dos departamentos legais e de emergência. No caso de roubo ou atentado, deve-se comunicar a polícia, em caso de incêndio deve-se avisar aos bombeiros, neste caso através da seção contra incêndio localizada no aeródromo deste aeroporto.



Fluxograma 3: Procedimento pós avaliação dos danos.

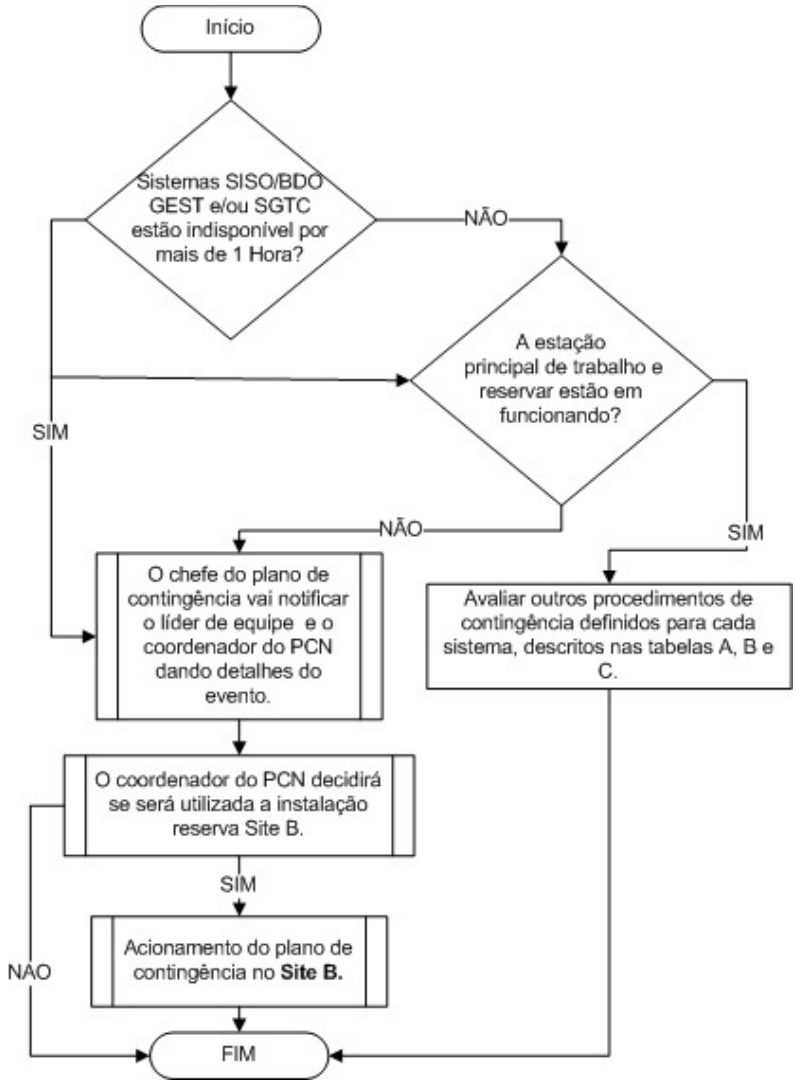
O **plano de contingência será ativado** caso um dos critérios abaixo forem válidos e mediante a aprovação do coordenador do PCN:

1. se algum dos três sistemas ficar indisponível por mais de 2 hora, independente do causador do problema, sejam estes relacionados a redes de dados, a problemas elétricos, condições ambientes ou dos próprios servidores dos sistemas sendo estes um problema de *hardware* ou de *software*;
2. se a estação principal e a estação reserva de trabalho não estiverem em funcionamento.

   É importante lembrar que para cada sistema, seja este o GEST, SISO ou SGTC, têm-se sempre duas estações de trabalho uma sendo a principal e a outra a reserva, em alguns casos a reserva é utilizada simultaneamente com a principal.
3. caso o plano seja ativado, o chefe do plano de contingência notifica o líder de equipe sobre os detalhes do evento e informa-o caso seja necessário o deslocamento da equipe.
4. o coordenador do PCN informa que será utilizada a instalação reserva e caso precise de materiais auxiliares (conforme

determinado na avaliação de danos) deverão ser deslocados ao lugar alternativo.

5. quando necessário, o chefe do plano de contingência deve lembrar a equipe de plano de contingência o lugar da instalação alternativa (o espelhamento dos sistemas), em que este será utilizado caso um evento de emergência ocorra aos sistemas, e este lugar alternativo deve estar preparado para a chegada da equipe.
6. o chefe do plano de contingência deve notificar as pessoas restantes (através dos procedimentos de notificação) o estado geral do incidente, o que foi afetado.



Fluxograma 4: Procedimentos para ativação do plano de contingência.

As tabelas apresentadas a seguir descrevem as medidas de contingência para cada um dos sistemas. Estas medidas de contingência baseiam-se na análise de impacto que foi apresentada no documento do PCN para o Aeroporto Internacional de Florianópolis, são medidas para contornar situações críticas de uma forma imediata.

Tabela A: Sistema SISO/BDO

Risco	Medida de Contingência
Indisponibilidade do ponto de cabeamento estruturado que atende a rede de computadores.	Verificar se existe outro ponto de rede próximo para o remanejamento deste cabeamento a estação, ou providenciar uma rede alternativa com Path Cord longo.
Indisponibilidade de alguma estação operacional.	Caso uma das estações pare de funcionar, deve-se auxiliar a realocação dos operadores para a segunda estação, se a segunda estação também falhar utilizar o procedimento manual até que uma estação nova seja providenciada.
Indisponibilidade da estação STAFF.	Se alguma estação STAFF falhar, o usuário da estação (companhia aérea) deve notificar o Centro de Operações Aeroportuária (COA) no Ramal 4095 e solicitar que seja dado a manutenção ao computador e que as devidas alteração e cadastro dos vôos daquela companhia seja realizado pelo operador do COA através do sistema que o mesmo também pode acessar.
Monitores de TV com defeito ou a imagem da estação de partida ou chegada não estão sendo projetadas nas telas das TVs	Verificar se o problema é na estação de distribuição de telas de partida ou chegada de vôo. Caso seja em alguma dessas duas estações, deve-se providenciar o mais breve possível a manutenção desta ou a substituição da mesma. Se o problema for na TV ou no cabo coaxial que saí do conversor PC/TV, deve-se notificar o setor de manutenção do aeroporto através do Supervisor do aeroporto em serviço para realizar a manutenção da TV ou do cabo coaxial.
Indisponibilidade da(as) tela(as) LCD inteligente(es).	O supervisor do aeroporto ou os agentes de proteção devem notificar a TI, informando quais estações de telas inteligentes estão indisponíveis. A TI deve verificar se o problema e na tela LCD ou no computador, caso o problema seja na tela de LCD esta deve ser retirada para manutenção externa e no lugar desta deves-se colocar a tela reserva, que encontra-se no depósito de equipamentos novos da TI. Se o problema é de hardware ou software do computador, deve-se tentar resolver este no local onde o equipamento se encontra, caso contrário deverá ser colocado a estação reserva, substituindo a estação defeituosa e prontificar o reparo da mesma.
Indisponibilidade do sistema de som.	Ao identificar o problema, o centro de operações aeroportuárias deve notificar a TI através do ramal 4029 para que esta verifique se o problema é no computador anunciador que utiliza o módulo do SISO o PADS, ou no sistema de amplificação do som. Caso o defeito seja no computador este deve ser reparado no local ou então substituído pela estação reserva que se encontra no depósito de equipamentos novos da TI, se o problema for no sistema de som (amplificadores) o supervisor do aeroporto em exercício deverá ficar ciente e este deve notificar o problema ao setor de manutenção da Infraero.
Indisponibilidade do servidor de banco de dados (s-flbn07).	A TI verificará qual o causador dessa indisponibilidade do servidor (fonte, disco rígido, memória, processador ou placa mãe) caso o tempo de manutenção desse equipamento seja maior que 15 minutos então deverá ser alterada as configurações da estações clientes apontando para conectar ao servidor reserva s-flbn10.
Indisponibilidade do servidor de distribuição de telas (s-flgn08).	A TI verificará qual o causador dessa indisponibilidade do servidor, caso seja hardware (fonte, disco rígido, memória, processador ou placa mãe) deve-se providenciar o mais rápido possível a substituição da peça com defeito. Caso o problema seja no software deverão ser realizados os procedimentos necessários para a restauração do sistema no servidor com auxílio do técnico responsável pelos servidores da regional sul (TIPA).

Indisponibilidade do link de dados ou roteador	Caso o link com a operadora da Embratel esteja indisponível, deve-se notificar a área de redes da TIPA para que analisem o problema e se for necessário façam solicitação a operadora para manutenção do link. Se o problema for no roteador da Cisco, este deve ser substituído pelo roteador reserva que fica no armário da TI na prateleira de equipamentos de rede de contingência e o defeituoso deve ser encaminhado a área de redes na regional
Indisponibilidade do switch de rede.	Verificar quais computadores foram afetados pela indisponibilidade do switch, anotar todas as portas que serão remanejadas para as portas disponíveis do switch em funcionamento, caso não tenha porta vaga deve-se utilizar o switch reserva que está no armário da TI na prateleira de equipamentos de rede de contingência.
Interrupção do servidor reserva. (s-flbn10).	Se for encontrado um problema no servidor reserva, este problema deve ser avaliado pela TI e a manutenção deve ser providenciada o mais breve possível. Se o servidor reserva s-flbn10 estiver servindo como servidor principal para os computadores clientes, todos os processos do sistema SISO deverão ser realizados manualmente utilizando as fichas de preenchimento e as chamadas de som através do operador que fica na sala do COA, utilizando o microfone que fica ligado ao sistema de amplificação do som.
Interrupção da energia elétrica comercial.	Caso o abastecimento comercial seja interrompido, os servidores terão suprimento de energia dos no-breaks por até 30 minutos, caso o gerador do aeroporto não entre em funcionamento nesse intervalo de tempo, os servidores deverão ser desligados até que a energia volte. É importante esperar que a energia seja restabelecida totalmente para não correr o risco de oscilações na rede elétrica ou de súbitas paralisações da energia.

TABELA B: SISTEMA SGTC

Risco	Medida de Contingência
Indisponibilidade do ponto de cabeamento estruturado que atende a rede de computadores.	Caso o problema seja na torre de controle, o cabeamento deverá ser consertado pelos técnicos da TI do Comando da Aeronáutica. Caso seja um problema com o cabeamento do terminal de passageiros, os técnicos deverão remanejar o ponto de rede danificado para outro disponível.
Indisponibilidade de alguma estação operacional.	Quanto ao hardware das estações que ficam na torre de controle é de responsabilidade do Comando da Aeronáutica mantê-los, porém o software instalado deve ser mantido pela TI do SBFL. A TI deverá atuar nos procedimentos de manutenção do software, já a estação que fica disponível no terminal de passageiros essa deverá ser mantida pela TI do aeroporto (tanto o hardware quanto o software). Caso o hardware esteja danificado, este deve ser substituído o mais breve possível.
Indisponibilidade do BIMTRA ou Link de Dados Rede INTRAER.	Quanto a disponibilidade dos dados (informação que trafega), é de responsabilidade do Comando da Aeronáutica mantê-los.
Indisponibilidade do switch de rede.	Tanto o *switch* que está na torre de controle quanto o *switch* que está na sala técnica principal deverá ser substituído pelo reserva que está no armário da TI na prateleira de equipamentos de rede de contingência.
Indisponibilidade do servidor de banco de dados (s_flbn50).	Como não há servidor reserva (contingência), este dependerá da manutenção dos técnicos do Comando da Aeronáutica no caso de um problema no *hardware* e dos dos técnicos da TI do SBFL, caso o problema seja o *software*.
Interrupção da energia elétrica comercial.	Caso o abastecimento comercial seja interrompido, o servidor terá suprimento de energia dos no-breaks por até 30 minutos, caso o gerador do aeroporto não entre em funcionamento nesse intervalo de tempo, o servidor devera ser desligado até que a energia volte. É importante esperar que a energia seja restabelecida totalmente para não correr o risco de oscilações na rede elétrica ou de súbitas paralisações da energia.

TABELA C: SISTEMA GEST

Risco	Medida de Contingência
Indisponibilidade do ponto de cabeamento estruturado que atende a rede de computadores.	Verificar se existe outro ponto de rede próximo para o remanejamento deste cabeamento a estação, ou providenciar uma rede alternativa com Path Cord longo. Caso o problema seja na rede que atende os Totens localizados nas guaritas de entrada ou saída do estacionamento, deve-se analisar se não houve rompimento da fibra ótica, ou algum problema com os conversores de mídia. Caso seja identificado o problema no meio físico de comunicação, então será adotada a medida de contingência manual em que o vigilante deverá anotar os dados do veículo num formulário já definido pelo setor comercial do aeroporto.
Indisponibilidade de alguma estação operacional.	Caso uma das estações pare de funcionar, deve-se auxiliar a realocação dos operadores para a segunda estação, se esta estação estiver disponível.
Indisponibilidade de alguma estação Totem.	Caso uma (1) estação da entrada ou saída do estacionamento esteja indisponível, fecha-se este acesso e deixa apenas a segunda entrada ou saída aberta. Caso as duas (2) estações da entrada ou saída estejam com problema deve-se passar para o procedimento manual, de acordo com as orientações que o setor comercial da Infraero passou aos vigilantes. A equipe de TI deverá providenciar a solução do problema o mais breve possível.
Indisponibilidade de algum computador do caixa.	Caso ocorra com apenas uma das posições, utiliza-se a posição reserva, caso ocorra com as duas, o cálculo para cobrança deverá ser realizado manualmente, e a equipe de TI deverá providenciar a solução do problema o mais breve possível. Após ter restabelecido o funcionamento do sistema, os operadores que trabalham no caixa deverão inserir no sistema todas as cobranças realizadas manualmente.
Indisponibilidade do conversor de mídia.	Caso ocorra uma indisponibilidade em algum dos 4 conversores de mídia que atende os Totens do estacionamento, este deverá ser utilizado o conversor de mídia reserva que está no armário da TI na prateleira de equipamentos de rede de contingência.
Indisponibilidade do switch de rede (desembarque)	Verificar qual dos dois computadores foram afetados pela indisponibilidade do *switch* ou da porta do *switch*, anotar todas as portas que serão remanejadas para as portas disponíveis do *switch* em funcionamento. Caso não tenha porta vaga, deve-se utilizar o switch reserva que está no armário da TI na prateleira de equipamentos de rede de contingência.
Indisponibilidade do switch de rede (sala técnica principal)	Verificar quais computadores foram afetados pela indisponibilidade do switch, anotar todas as portas que serão remanejadas para as portas disponíveis do switch em funcionamento, caso não tenha porta vaga deve-se utilizar o switch reserva que está no armário da TI na prateleira de equipamentos de rede de contingência.
Indisponibilidade do switch de rede (Guaritas)	Utilizar o switch reserva que está no armário da TI na prateleira de equipamentos de rede de contingência.
Interrupção da energia elétrica comercial.	Caso o abastecimento comercial seja interrompido, os servidores terão suprimento de energia dos no-breaks por até 30 minutos, caso o gerador do aeroporto não entre em funcionamento nesse intervalo de tempo, os servidores deverão ser desligados até que a energia volte. É importante esperar que a energia seja restabelecida totalmente para não correr o risco de oscilações na rede elétrica ou de súbitas paralisações da energia.

4 NORMATIVAS DO BACKUP

As cópias de segurança (*backups*) são gravadas em mídias magnéticas do tipo DAT DDS 36/72 GBytes em uma unidade da HP (DW027A) externa com interface USB para facilitar a remoção e a instalação em outro servidor. O servidor que possui a rotina de *backup* (agendamento das tarefas) é o S-FLGN01. Durante os cinco

primeiros dias da semana (segunda à sexta) são realizados os *backup*s diários do tipo diferencial, sendo copiados os arquivos que foram alterados desde o último *backup* total do sistema. Para a sua restauração, é necessário que se tenha o *backup* total juntamente com a fita de *backup* diferencial, a retenção de cada mídia diária é de uma semana. Além da rotina de *backup* diário (diferencial), são feitos ainda os *backup*s semanais do tipo total e a retenção é de quatro semanas. A rotina de *backup* mensal é do tipo total e sua retenção é ilimitada, sendo a mesma armazenada em outro prédio. Neste caso, foi escolhido à edificação do terminal de carga da Infraero que fica a um quilômetro de distância, as fitas são armazenadas em um armário com chave, na sala do coordenador da área do terminal de carga.

O conteúdo a ser copiado nas fitas de *backup* dos sistemas são:

SISO\BDO: pasta \\S-FLBN07\D:\MSSQL2005\BACKUP\;

GEST: pasta \\S-FLBN03\D:\MSSQL\BACKUP\;

SGTC: pasta \\S-FLBN07\D:\BACKUPSGTC\;

Apesar do servidor do SGTC ser o S-FLBN50 os arquivos de *backup* do SQL são copiados para o diretório D:\BACKUPSGTC\ do servidor S-FLBN07, pois a rede do sistema SGTC não é a mesma da Infraero, e como o servidor S-FLBN07 possui um segunda placa de rede e esta está conectada a uma rede local virtual (VLAN) da rede do SGTC, é possível copiar estes dados para a mídia na rede da Infraero, através do S-FLGN01 (servidor de *backup*).

O controle de backup é realizado numa base de registros localizada no aplicativo Lotus Notes. Nesta base, são registrados diariamente pelo técnico Rodrigo Fernando Martins os backups realizados nos sistemas que estão sendo contingenciados. Neste registro, está identificado o dia da realização do backup e a duração, em caso de falha, deve-se anotar na observação quais arquivos não foram copiados.

Os *backups* dos sistemas são testados semanalmente por amostragem. Por exemplo, a cada semana é escolhida uma fita para

fazer a restauração em uma pasta alternativa e observar se os dados foram corretamente restaurados (estão íntegros).