Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

FELIPE DAS CHAGAS

PROPOSTA DE PLANO DE CONTINUIDADE DE NEGÓCIOS PARA UMA EMPRESA PRIVADA DE BRASÍLIA

Brasília
2017

FELIPE DAS CHAGAS

PROPOSTA DE PLANO DE CONTINUIDADE DE NEGÓCIOS PARA UMA EMPRESA PRIVADA DE BRASÍLIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Rede de Computadores.

Orientador: Gilberto Oliveira Netto

Brasília
2017

FELIPE DAS CHAGAS

PROPOSTA DE PLANO DE CONTINUIDADE DE NEGÓCIOS PARA UMA EMPRESA PRIVADA DE BRASÍLIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Rede de Computadores.

Orientador: Gilberto Oliveira Netto

Brasília, 26 de setembro de 2017

Banca Examinadora

_____

Professor. Gilberto de Oliveira Netto

_____

Professor. Rafael Sarres

_____

Professor. Gilson Ciarallo

RESUMO

Este trabalho propõe um plano de continuidade de negócio para uma empresa do ramo de saúde de Brasília. Os principais instrumentos da metodologia adotada foram questionários e reuniões internas, para definição dos ativos e processos críticos ao negócio da empresa. Com os resultados obtidos, foi possível realizar uma análise de riscos, identificando as ameaças e propondo ações de controle, depois foi realizada uma análise de impacto de negócio e proposto o plano de continuidade.

Palavras-chave: Plano de Continuidade de Negócio. Análise de Riscos. Análise de Impacto de Negócio. Ameaças.

ABSTRACT

This paper proposes a business continuity plan for a company in the health branch of Brasilia. The main instruments of the methodology adopted were questionnaires and internal meetings, to define the critical assets and processes to the business. With the results obtained, it was possible to carry out a risk analysis, identifying threats and proposing control actions, then performed a business impact analysis and proposed the continuity plan.

Key words: Business Continuity Plan. Risk analysis. Business Impact Analysis. Threats.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

Atualmente, as empresas dependem cada vez mais da tecnologia da informação como forma de se manterem competitivas em um mercado globalizado. É raro encontrar organizações que não estão divulgando seus serviços na internet, compartilhando informações, vendendo produtos pela rede, dentre tantas outras alternativas que os recursos computacionais nos permitem.

A era da informação na qual nós vivemos mudou o conceito como as empresas tratam o seu negócio, cada vez mais existe a necessidade de manter os seus serviços ativos e funcionais 24 horas por dia, de forma que o comprometimento do sistema de informações pode causar grandes prejuízos ou mesmo levar a organização à falência.

Desta forma, a tecnologia da informação (TI) tem assumido um papel fundamental, pois além de prover a infraestrutura para o andamento dos negócios, ela também tem que prever os possíveis incidentes, desastres, ou até mesmo catástrofes que coloquem o negócio da instituição em risco. Neste ponto que entra o plano de continuidade de negócio (PCN), pois todos os envolvidos devem saber como lidar em situações de emergência para que os sistemas sejam reestabelecidos no menor tempo possível.

Até o ano de 2001 as empresas quase não tinham preocupações quanto à continuidade de negócio, ou quando as tinham, eram soluções básicas de segurança, como manter um backup *offsite* em outra localidade. O ataque terrorista

contra o World Trade Center mostrou que não bastava ter o seu backup a poucos quilômetros do seu site principal.

O prejuízo causado pela indisponibilidade de um serviço depende muito do ramo de atuação e o grau de importância daquele sistema. Se pensarmos em uma pequena empresa, talvez a indisponibilidade do serviço por um ou dois dias seja até aceitável, porém se imaginarmos uma instituição financeira, talvez ficar *off-line* por alguns minutos pode causar prejuízos inestimáveis.

Com isso, o PCN tem ganhado cada vez mais importância nas empresas, seja por motivos legais, financeiros ou culturais, os gestores estão cada vez mais compreendendo que investir em planos de continuidade pode salvar os seus negócios em incidentes críticos.

Engana-se quem pensa que o PCN é apenas um documento voltado para a área de tecnologia da informação (TI), ou que diz respeito apenas a equipamentos e sistemas. No PCN devem ser englobadas até mesmo responsabilidades e pessoas, afinal, em casos de catástrofe, outras pessoas devem estar aptas e orientadas em como restaurar as funcionalidades que estão no escopo do documento.

Felizmente existem muitas tecnologias nos dias atuais que auxiliam no sucesso de um plano de continuidade de negócios, podendo destacar a virtualização de servidores, que permitiu um avanço considerável para entrega de serviços bem como a computação em nuvem, onde as empresas podem transferir algumas responsabilidades a um fornecedor. Ambas abordagens serão apresentadas com mais detalhes no capítulo 3.

Justificativa

É de grande importância que empresas privadas ou públicas tenham em mente que existem riscos que rondam a todo o momento os seus negócios, e por isto deve existir um planejamento em como recuperar os seus ativos e sistemas em caso de falhas.

A empresa alvo deste estudo de caso possui uma série de redundâncias internas que previnem a ocorrência de alguns tipos de indisponibilidade, porém atualmente não existe nenhum procedimento voltado para a continuidade de negócio em caso de problemas generalizados em sua sede. Desta forma se justifica o estudo e apresentação do PCN.

Nos últimos 7 anos, a empresa estudada sempre incluiu em seu planejamento estratégico um item relacionado a continuidade de negócios, porém devido a uma série de fatores, principalmente financeiros, não houve a conclusão de um estudo ou consultoria sobre o tema. A execução deste trabalho vai de encontro à necessidade interna da organização.

Objetivo Geral

O objetivo deste trabalho é realizar um estudo de caso em uma empresa do ramo de saúde de Brasília, atuando há mais de 60 anos em rede nacional. Com base nas necessidades internas e documentações obtidas, será proposto um plano de continuidade de negócio para a alta direção, visando minimizar o tempo de parada e de recuperação que podem ocorrer.

Objetivos Específicos

Primeiramente realizou-se um levantamento de ativos e processos críticos para o negócio da empresa, na sequência foi realizado uma análise de riscos para documentar as ameaças e identificar possíveis ações de controle e mitigação dos riscos. Por fim foi realizada uma análise de impacto dos negócios para quantificar e qualificar o impacto que possíveis interrupções de serviços causariam para a organização.

Com base nos produtos obtidos, foi proposto um plano de continuidade de negócio para o sistema mais crítico da empresa, seguindo a metodologia do *Disaster Recovery Institute* (DRI) juntamente com as melhores práticas da norma ABNT NBR ISO 22301:2013, que trata especificamente sobre gestão de continuidade de negócio.

Os capítulos estão divididos da seguinte maneira: o capítulo 1 demonstra uma revisão bibliográfica sobre o tema, o capítulo 2 discorre sobre metodologias utilizadas e o capítulo 3 traz um estudo de caso.

O trabalho foi redigido a partir de pesquisas em bibliografias, normas oficiais, artigos com reputação comprovada e documentações produzidas na empresa de saúde estudada.

1 REVISÃO DA LITERATURA

Este capítulo apresenta algumas definições sobre segurança da informação e continuidade de negócio, bem como conceitua alguns assuntos correlacionados ao tema deste trabalho.

1.1 Segurança da Informação

Existem diversas definições para informação, a que melhor se adapta a esta pesquisa é a definição da Norma NBR ISO/IEC 27002:2013: "A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. ”

Baseando-se neste conceito, é possível afirmar que o sucesso de uma organização está diretamente ligado as informações, desta forma, é importante garantir que estas estejam sempre disponíveis quando necessárias, não sejam alteradas indevidamente, e que só sejam disponibilizadas a quem realmente possua direitos de acesso.

O conceito de segurança da informação, definido pela mesma Norma NBR ISO/IEC 27002:2013 é ainda mais amplo: “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

Percebe-se que na própria definição, já é abordado o tema de continuidade de negócios, conceituando de que este depende primeiramente da manutenção da segurança da informação. Para garantir a segurança da Informação é necessário

respeitar os três princípios básicos da segurança, conforme a definição de (SÊMOLA, 2003, p45):

- **Confidencialidade:** Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu aceso e uso apenas às pessoas para quem elas são destinadas.
- **Integridade:** Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
- **Disponibilidade:** Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

1.2 Ameaças e Vulnerabilidades

Para garantir a segurança da informação através de um PCN é necessário entender o que pode dar errado em um ambiente computacional, alguns conceitos segundo (BEAL, 2008, p.14):

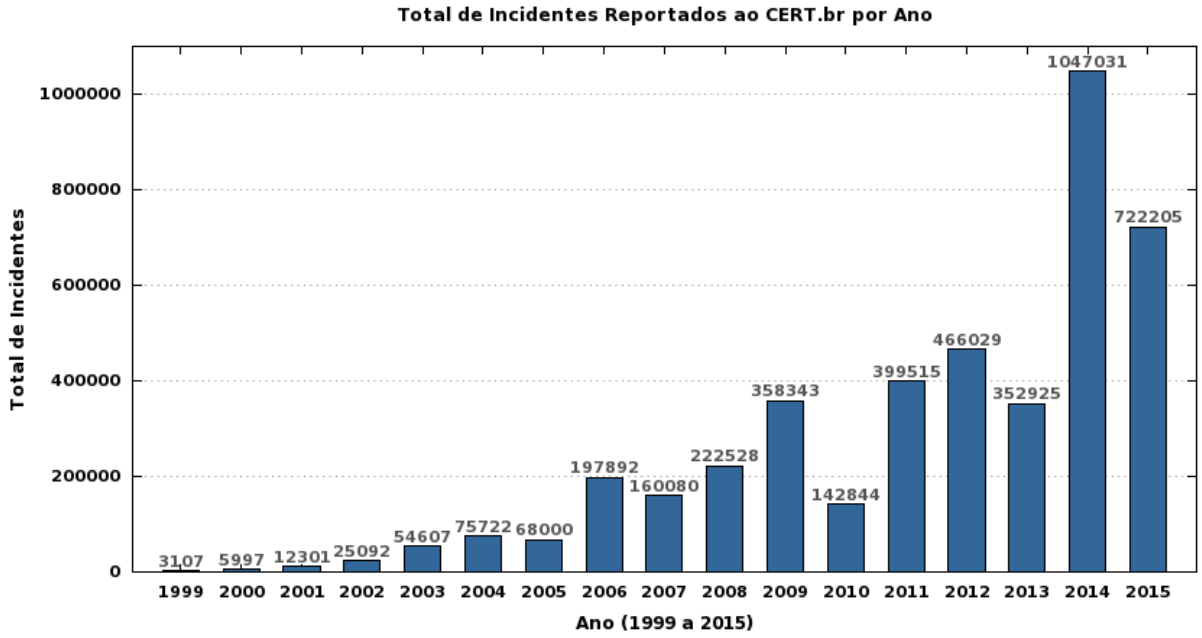
- **Ameaça:** “Expectativa de acontecimentos acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação”.
- **Vulnerabilidade:** “Fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque”.
- **Agente:** “Fonte produtora de um evento que pode ter efeitos adversos sobre um ativo de informação”.

Segundo a norma NBR ISO/IEC 27002:2013: “As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação”. Danos causados por código malicioso, hackers e ataques de negação de serviço estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

Por mais que possamos acreditar que nossas empresas estão de certa forma protegidas, existem diversos tipos de ameaças e vulnerabilidades que são cada vez

mais explorados. Podemos verificar este fato pelo aumento de incidentes de segurança reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), conforme a figura 1.

Figura 1: Incidentes de Segurança Reportados.



Fonte: Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 13 out. 2016.

Desta forma, o sucesso de um plano de continuidade de negócio, começa pela identificação de ameaças e vulnerabilidades dos processos de negócio críticos para a organização, para dimensionar corretamente o risco. Afinal como podemos nos proteger, se não soubermos quais são os riscos a que estamos vulneráveis?

1.2.1 **Exemplos de Ameaças**

Classificando as ameaças quanto a sua intencionalidade, elas podem ser divididas nos seguintes grupos:

- **Naturais:** Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, maremotos, aquecimento, poluição, dentre outros.
- **Acidental:** Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia, dentre outros.
- **Intencional:** Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários, terroristas, dentre outros.

1.2.2 Exemplos de Vulnerabilidades

Conforme as definições dadas anteriormente, podemos entender vulnerabilidade como uma falha nos diversos componentes que regem a segurança da informação na empresa como: aplicações, softwares, equipamentos, sistemas operacionais, funcionários, dentre outros.

Alguns tipos e formas de vulnerabilidades podem ser vistos abaixo:

- **Físicas:** Instalações prediais fora do padrão, salas de CPD mal planejadas, falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio, risco de explosões, vazamentos, dentre outros.
- **Naturais:** Computadores são suscetíveis a desastres naturais, como enchentes, terremotos, tempestades, incêndio natural, e outros, como falta de energia, acumulo de poeira, aumento de umidade ou temperatura, dentre outros.

- **Hardware:** Falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou mesmo erros durante a instalação.
- **Software:** Erros na instalação ou na configuração podem acarretar acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário.
- **Mídias:** Discos, fitas, armazenamentos removíveis e relatórios impressos podem ser perdidos ou danificados. A radiação eletromagnética, por exemplo, pode afetar diversos tipos de mídias magnéticas.
- **Comunicação:** Acessos não autorizados ou perda da comunicação.
- **Humanas:** Falta de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, erros ou omissões; ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras.

Vale ressaltar que as vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças.

1.3 Análise de Riscos

Risco é a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impacto nos negócios (SÊMOLA, 2003, p.50). A Norma NBR ISO

22313:2013 que trata sobre a continuidade de negócio, define risco como algo que pode ocorrer e seus efeitos nos objetivos da organização.

Segundo a definição obtida no dicionário online Priberam da Língua Portuguesa, risco significa: perigo, inconveniente.

Desta forma, podemos afirmar que o risco é algo inesperado e que, na maioria das vezes, pode trazer uma consequência negativa. Portanto, é importante que a empresa conheça os riscos que podem dificultar ou paralisar o andamento de seus negócios.

No planejamento de um plano de continuidade de negócio é importante, no primeiro momento, levantar quais os principais ativos e processos de negócio, para saber o que proteger na empresa e, a análise de risco, têm papel fundamental para definição do que a empresa precisa de proteção, ou seja, delimitar um escopo de tudo aquilo que é vital para a continuidade de negócios da empresa, bem como definir situações de risco, sobre do que se proteger. Após a análise de risco serão utilizadas outras técnicas para saber o como se proteger e como agir em situações de paradas e/ou catástrofes.

Para que os riscos sejam reduzidos a um nível aceitável, é necessário um entendimento claro dos riscos associados a impactos graves (desastres), que levem a interrupção ou redução significativa dos serviços de informação.

1.3.1 **Gerenciando os Riscos**

Neste ponto, se faz necessária a distinção de quais são os processos críticos da empresa. Questões importantes a serem respondidas: Quais os processos que se deixarem de funcionar trazem um impacto significativo para a empresa? Quais os

ativos e sistemas que são a base para este processo crítico e, portanto, igualmente importantes para a continuidade da empresa?

Segundo as definições da Norma NBR ISO/IEC 27002:2013, é importante que a análise de risco identifique, quantifique e priorize os riscos com base em critérios de aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento de riscos de segurança da informação e para a implementação dos controles selecionados, de maneira a proteger contra esses riscos.

Podemos exemplificar esta definição desta forma: uma empresa automobilística que produza motores utilizando uma linha de produção totalmente informatizada e controlada por um sistema, obviamente colocará esse como primeiro nível no quesito priorização de riscos, deixando o sistema de e-mails, por exemplo, com um impacto baixo, visto que a indisponibilidade desse sistema não atrapalharia na linha de produção.

Desta forma, convém que as empresas definam critérios para saber quais os riscos que podem ou não serem aceitos, para isto é utilizada a técnica de análise de riscos. Uma vez identificado os processos críticos, é possível classificar os processos e seus serviços associados em ordem de importância para a organização, sendo possível ainda definir qual o período máximo e aceitável de indisponibilidade para cada processo crítico e ainda definir a ordem de recuperação dos processos para o retorno da operação de todos os serviços.

Segundo a norma NBR ISO 22301:2013, para cada um dos riscos identificados seguindo a análise/avaliação de riscos, uma decisão sobre o

tratamento do risco precisa ser tomada. Possíveis opções para um tratamento de risco incluem:

1. Aplicar controles apropriados para reduzir os riscos;
2. Conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para a aceitação do risco;
3. Evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;
4. Transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

1.4 Plano de Continuidade de Negócios

O planejamento da continuidade de negócio tem por objetivo preparar a organização para a recuperação de seus processos críticos em caso de desastre. Os detalhes a serem tratados num plano de continuidade vão variar significativamente de acordo com o tamanho da organização, o tipo de negócio e a forma de atuação no mercado (BEAL, 2008, p.137).

A definição é trivial, assim como uma política de segurança, onde existem normas que orientam na sua criação, ela vai variar de organização para organização. O mesmo ocorre na criação de um PCN, a norma NBR ISO 22313:2013 trata especificamente sobre a gestão de continuidade de negócios, porém dependendo da empresa, alguns itens serão mais importantes do que outros, portanto para o sucesso do PCN, é extremamente importante conhecer a empresa como um todo.

Exemplificando o conceito inicial, comparemos um sistema crítico de uma padaria que controle o estoque de alimentos e vendas, com um sistema crítico de um banco que controle movimentações financeiras. A parada do primeiro sistema pode significar um prejuízo, pois tudo terá que ser controlado manualmente, porém a crise mesmo que demore muito tempo, poderá ser contornada. A parada do segundo sistema representa um prejuízo de milhões, mesmo que provocada por poucos minutos ou horas. Desta forma, fica evidente que se o banco não possuir um PCN para o seu sistema, uma única situação de crise pode definir o fracasso do negócio.

Para o sucesso do plano, é necessário identificar os processos críticos da empresa, pois a criação de um PCN para todos os ativos e processos da empresa pode significar um gasto desnecessário e acima do que se quer realmente proteger, assim como, se não forem definidos todos os processos críticos da empresa, o PCN pode não funcionar adequadamente.

O plano de continuidade de negócios é imprescindível para empresas que não podem sofrer interrupção em seus processos de negócios, porque isto representaria risco de perdas financeiras, degradação da imagem no mercado e insatisfação do seu maior patrimônio: seus clientes.

Segundo Marinho (2008) o mérito do PCN não é antecipar os eventos, mas planejar ações de resposta, reduzindo o tempo de interrupção, minimizando a possibilidade de erros durante situações de crise e estresse. Como resultado, os custos de recuperação e restauração, financeiros e não financeiros, são mitigados.

1.4.1 **Elaboração do Plano de Continuidade de Negócio**

De acordo com a norma ISO/IEC 27002:2013, convém que o processo de elaboração do plano agregue os seguintes elementos-chave da gestão de continuidade de negócio:

- Entendimento dos riscos a que a organização está exposta, no que diz respeito à sua probabilidade e impacto no tempo, incluindo a identificação e priorização dos processos críticos de negócios;
- Identificação de todos os ativos envolvidos em processos críticos de negócio;
- Entendimento do impacto que incidentes de segurança da informação provavelmente terão sobre os negócios (é importante que as soluções encontradas possam tratar tanto os pequenos incidentes, como os mais sérios, que poderiam colocar em risco a continuidade da organização) e estabelecimento dos objetivos do negócio dos recursos de processamento da informação;
- Consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade de negócio, bem como a parte de gestão de risco operacional;
- Identificação e consideração da implementação de controles preventivos e de mitigação;
- Identificação de recursos financeiros, organizacionais, técnicos e ambientais suficientes para identificar os requisitos de segurança da informação;
- Garantia de segurança de pessoal e proteção de recursos de processamento das informações e bens organizacionais;
- Detalhamento e documentação de planos de continuidade que contemplem os requisitos de segurança da informação alinhados com a estratégia de continuidade de negócio estabelecida;
- Testes e atualizações dos planos e processos implantados;
- Garantia de que a gestão da continuidade de negócio esteja incorporada aos processos e estrutura da organização. Convém que a responsabilidade pela coordenação do processo de gestão de continuidade de negócio esteja atribuída a um nível adequado dentro da organização.

O PCN deve ser documentado de acordo com a criticidade de cada ameaça a processos críticos do negócio, onde devem ser definidos os responsáveis por cada ação, bem como os tempos desejáveis para início e fim de cada atividade, inclusive definindo em que situações o plano deve ser ativado. Quando novos requisitos forem identificados, é importante que o plano de continuidade seja revisto, para que o PCN reflita fielmente todas as etapas necessárias durante uma crise e/ou catástrofe.

2 METODOLOGIAS UTILIZADAS

Neste capítulo serão demonstradas as metodologias adotadas. Foi realizado um estudo de caso em uma empresa do ramo de saúde de Brasília, onde foram formados grupos de trabalho e comitês necessários para a realização de entrevistas e questionários que embasaram a construção de um plano de continuidade de negócios. O resultado foi a documentação deste plano, permitindo que a empresa estudada contenha mecanismos de controle e atuação nos casos de incidentes graves, visando a continuidade de seus negócios.

2.1 Metodologia proposta pelo *Disaster Recovery Institute (DRI)* para elaboração do PCN.

Para a elaboração do plano de continuidade seguiremos o diagrama do padrão de planejamento e desenvolvimento de um PCN de acordo com o Instituto de Recuperação de Desastres (*Disaster Recovery Institute* - DRI), conforme a figura 2.

Figura 2: Diagrama indicativo do padrão de planejamento e desenvolvimento de um plano de continuidade de negócios de acordo com o DRI Internacional.

Fonte: adaptada de Marinho (2008, p15).

O DRI foi criado por um grupo de profissionais nos Estados Unidos, com intuito de formalizar a atividade de especialista em Continuidade de Negócios, definindo conceitos, que foram consolidados na prática e que foram organizados com o objetivo de padronizar uma metodologia. Esta metodologia é atualmente utilizada pelo DRI para treinamento e certificação de profissionais de continuidade de negócio. Toda esta metodologia foi transcrita por Marinho (2008), e será adotada para execução deste projeto.

2.1.1 **Início e Administração do Projeto**

Estabelece o escopo (necessidades) para o desenvolvimento de um plano de continuidade de negócio (PCN), incluindo questões sobre aquisição de patrocínio (apoio), organização e gerenciamento do projeto para atender os limites de prazos e orçamento. (MARINHO, 2008, p.21).

Primeiramente deverão ser estabelecidas as necessidades para a continuidade de negócio da empresa, identificando leis, normas, exigências estatutárias e contratuais que devem ser atendidas pelo PCN.

Deve se realizar reuniões e/ou entrevistas junto às áreas de negócio, para identificação de todos os processos críticos para a continuidade de negócio da empresa, bem como os ativos que sustentam estes processos. Podemos resumir este procedimento como um inventário de tudo aquilo que é imprescindível para o negócio da empresa.

Nesta etapa também é importante à divulgação do projeto para desenvolver a cultura organizacional sobre o tema, demonstrando as vantagens que um plano de continuidade de negócio pode trazer para a organização. É extremamente necessário que pessoas chaves das áreas de negócio participem ativamente na definição deste escopo do projeto.

Também se faz necessária a criação de um comitê do PCN, onde serão definidas as regras e responsabilidades de cada participante pela definição e construção do plano.

Segundo Marinho (2008, p.21). É importante neste início de projeto, esclarecer entre os integrantes do comitê e as pessoas que atuarão de forma operacional a diferença entre:

1. Recuperação de desastres e continuidade de negócios;
2. Respostas a crises e gerenciamento de crises;
3. Reduzir e impedir riscos de ocorrência de eventos.

Com relação à administração do projeto, se faz necessária a adoção de alguma metodologia para controlar a execução das tarefas, onde o gerente do projeto deve possuir meios de checar se tudo está sendo feito conforme definido no escopo e início do projeto.

A alta direção da empresa deve demonstrar o total comprometimento em todas as fases do projeto de construção e gerenciamento do PCN, porém nesta etapa inicial é que fica mais evidente a necessidade deste apoio.

2.1.2 **Avaliação e Controle dos Riscos**

As atividades relacionadas à avaliação e controle dos riscos definem os possíveis e prováveis cenários que fazem parte do ambiente corporativo e que podem afetar a organização, tanto com interrupções, quanto com desastres. Elencando os possíveis danos relacionados a cada evento e quais as medidas necessárias para prevenir e reduzir os efeitos de uma potencial perda. (MARINHO, 2008, p.27).

Observamos pela definição que esta etapa está diretamente ligada à execução de uma análise de risco, para identificação de ameaças, vulnerabilidades, riscos e consequências.

Quando citamos a expressão níveis aceitáveis de risco, estamos nos referindo à importância dos processos de negócio e também o valor dos ativos e da segurança embutida. Exemplo: Uma universidade quer proteger um computador de

sala de aulas, este ativo não possui um valor elevado, então resolve colocar apenas uma proteção com chave. Existe um risco de que alguém tente danificar esta proteção e levar o computador embora, mas devido ao valor baixo ativo e do preço alto que outras soluções de segurança teriam, a Universidade define que este risco é aceitável. Se este computador armazenasse todos os vídeos de entrada e saída de alunos, o ativo passaria a ter maior importância, com certeza o nível de aceitação do risco seria outro, e outros tipos de segurança seriam implementados.

Durante a execução da análise de risco, verificamos que algumas ações que minimizem os riscos, já podem ser identificadas e executadas, sem estarem ligadas propriamente com um plano de continuidade de negócios. Exemplo: É identificado que o backup de um sistema crítico não está atendendo a requisitos legais (retenção de 5 anos), ações corretivas são realizadas antes mesmo das próximas ações do PCN.

2.1.3 **Análise de Impacto nos Negócios (Bussiness Impact Analysis - BIA)**

Nesta etapa serão identificados e avaliados os impactos resultantes da interrupção e dos cenários de desastres que podem afetar a organização, bem como as técnicas para quantificar e qualificar esses impactos. Define a criticidade dos processos de negócios, suas prioridades de recuperação e interdependências, para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos. (MARINHO, 2008, p.35).

A análise de impacto de negócios (BIA) é uma parte fundamental do processo de continuidade de negócios que analisa as funções de negócios de missão crítica e

identifica e quantifica o impacto de uma perda dessas funções (por exemplo, operacional, financeira) pode ter sobre a organização.

Existem diversos modelos (templates) disponíveis na internet, porém cada empresa possui a sua singularidade, cada funcionário ou gestor possui uma concepção de riscos ou de processo crítico, portanto, para execução deste trabalho acadêmico, utilizaremos o modelo proposto pelo guia de boas práticas para planos de continuidade de negócio, desenvolvido pela Associação Brasileira das Entidades Fechadas de Previdência Complementar (ABRAPP), que será adaptado para este trabalho acadêmico, abaixo estão as 5 fases do modelo:

1. Definição do projeto:

Momento em que a organização define o responsável pelo BIA, estipula qual a sua autoridade e estabelece o escopo, objetivos e prazos para a entrega dos resultados.

2. Elaboração de questionário

Este questionário visa extrair a maior quantidade de informação sobre os sistemas críticos da empresa, de forma que seja possível quantificar e qualificar os impactos, sejam eles financeiros, de imagem, legais ou operacionais. Com os resultados destes questionamentos, será possível construir outras matrizes de dados para elencar e priorizar os sistemas.

3. Entrevista

Uma vez que o questionário esteja pronto, uma forma de melhorar os resultados, é entrevistar diretamente os responsáveis pelas atividades críticas. Desta forma, as respostas terão uma consistência mais coerente, pois dúvidas e esclarecimentos podem ser trabalhados.

4. Determinação dos tempos de recuperação (*Recovery Time Objectives* RTO).

Segundo a definição do próprio guia de boas práticas da ABRAPP: “É o período dentro do qual um processo deve ser reestabelecido após um acidente, a fim de evitar consequências inaceitáveis relacionadas com a quebra de continuidade de negócios”. Ou seja, é o período máximo que um sistema pode ficar indisponível.

Lembrando que neste período já está englobado o tempo que seria gasto, tentando recuperar o sistema, a empresa deve possuir métricas e horários bem definidos, de quando o PCN deve ser acionado a fim de garantir que o RTO seja atingido.

5. Estabelecimento do “ponto real de recuperação” (*Recovery Point Objective* RPO).

Este seria o período máximo de informações que poderiam ser perdidas, sem que houvesse prejuízo que impactasse na continuidade de negócio. É claro que qualquer perda de informação causa transtornos para as empresas, porém o RPO é o tempo em que os prejuízos ainda são contornáveis.

Destes 5 passos propostos pela ABRAPP foi realizada uma única adaptação. Enquanto no modelo as definições dos tempos de RTO e RPO só são realizadas após os questionários e as entrevistas, no presente estudo foi optado por inclui-las no próprio questionário, buscando desta forma, que o resultado fosse o mais fidedigno possível com as necessidades das áreas de negócio.

Após o resultado destes questionamentos, deve ser definida uma métrica para elencar os sistemas e suas criticidades, para que seja possível em uma situação de emergência priorizar o restabelecimento de um sistema em comparação a outro, ou enxergar os seus relacionamentos, para garantir que o RTO não ultrapasse o seu valor máximo.

2.1.4 **Desenvolvendo Estratégias de Continuidade de Negócio**

Define e orienta a seleção de estratégias operacionais alternativas para a recuperação dos processos e dos componentes de negócio dentro dos prazos de recuperação desejados enquanto processos corporativos críticos são mantidos em atividade. (MARINHO, 2008, p.43).

Nesta etapa é importante que a empresa identifique as possíveis alternativas para Continuidade de Negócio disponíveis, suas vantagens e desvantagens, com as respectivas características de custo, incluindo a mitigação (redução de riscos) como estratégia de recuperação.

Até mesmo nesta fase do projeto, cada empresa poderá se enquadrar em uma estratégia, melhor do que a outra, por isso é importante entender sobre as características da empresa para que a escolha seja desenvolvida após esta etapa.

Novamente é de crucial importância que a alta direção esteja comprometida com o projeto do PCN, pois agora serão conhecidos os custos de cada abordagem para garantir a continuidade de negócio, e geralmente os custos com continuidade são um investimento em que a empresa não terá um retorno, a não ser que ela passe por uma crise e veja o quanto economizou e manteve seu negócio após uma situação de catástrofe.

2.1.5 **Respostas e Operações de Emergência**

Desenvolve e implementa procedimentos de resposta e estabilização de situações por meio de um incidente ou evento, incluindo a criação e a especificação

de normas para o gerenciamento de um centro operacional de emergência (COE) utilizado como central de comando durante uma crise. (MARINHO, 2008, p.51).

As respostas necessárias para cada tipo de situação identificada na análise de risco devem ser trabalhadas e treinadas, para que numa situação real de emergência, exista uma equipe especifica de monitoramento, que acione os responsáveis pelo gerenciamento de crise, ou acione até mesmo os bombeiros em casos de incêndio por exemplo.

Todos os procedimentos devem ser documentados, para que esta equipe de monitoramento, tenha condições de dar a primeira resposta a situação de crise. Ao acionar a equipe de gerenciamento de crise, esta equipe também tem que estar treinada e possuir documentação sobre como atuar em cada situação de emergência. Provavelmente esta equipe acionará, um grupo de trabalho que iniciará a recuperação do desastre, e em algum tempo já definido acionará a equipe de PCN para iniciar a movimentação dos sistemas, processos ou pessoas para um outro ambiente que permita o funcionamento do sistema até que seja possível a recuperação total do sistema no seu local de origem.

2.1.6 **Desenvolvendo e Implementando PCN**

Planeja, elabora e integra os componentes de um Plano de Continuidade de Negócios, visando o atendimento às janelas de recuperação dos componentes e dos processos da organização. (MARINHO, 2008, p.57).

Cada sistema crítico identificado pela organização terá o seu próprio PCN, pois cada sistema funciona de uma maneira específica, possui as suas interdependências, e pessoas que o gerenciam.

Nesta etapa que será escolhida uma metodologia para documentar o plano, deverá ser organizado uma estrutura em função do tempo sobre as atividades a serem executadas, bem como deve estar presente os nomes e contatos de todas as pessoas envolvidas que terão papel importante na execução do PCN em uma situação real de emergência.

É neste ponto que o PCN é produzido, implementado e testado. Também devem ser definidas as ações relacionadas a manutenção do plano, pois os sistemas, processos e pessoas, são dinâmicos. Qualquer alteração deve ser documentada e o plano revisto, para garantir que sua utilização garanta a continuidade de um processo crítico.

Uma metodologia muito utilizada: é um *checklist* das atividades em ordem cronológica a serem seguidas, o responsável vai sinalizando as atividades já executadas, e após a conclusão do plano, este documento já será disponibilizado aos responsáveis, que checarão se o plano está atendendo as necessidades, ou já precisa de melhorias ou adaptações.

2.1.7 **Implementando a Consciência e os Programas de Treinamento**

Desenvolve um programa para incrementar a cultura corporativa, incentivando as habilidades necessárias para elaborar, implementar, atualizar e executar um Plano de Continuidade de Negócios. (MARINHO, 2008, p.69).

O tema continuidade de negócio, por muito tempo esteve mais vinculado a área de TI, porém nos últimos anos as empresas compreenderam que o lado humano está vinculado a quase que todos os processos e setores das organizações,

afinal do que adianta investir em segurança, redundância, processos internos se a equipe que opera um sistema não agir de acordo com as melhores práticas.

A consciência corporativa é algo que deve ser constantemente trabalhada, pois pessoas entram e saem a todo momento das empresas, desta forma, é importante que a organização identifique formas de sempre estar divulgando e trabalhando a importância do PCN.

Outro fator importante é o treinamento das pessoas que integrarão as equipes relacionadas a continuidade de negócio, a empresa deve investir em cursos internos ou externos para preparar os seus funcionários, quanto mais aptos eles estiverem, melhor será o resultado da atuação em uma situação de crise.

2.1.8 **Mantendo e Exercitando o PCN**

Elabora um pré-plano e coordena exercícios do PCN, avaliando os resultados obtidos. Desenvolve processos para a manutenção das variáveis dos planos de acordo com os objetivos estratégicos da empresa. Apresenta uma comparação entre o resultado obtido e um ambiente corporativo convencional, relatando as diferenças de forma concisa e clara. (MARINHO, 2008, p.71).

Como qualquer instrumento de segurança, o PCN deve ser constantemente testado e revisado. Podemos comparar esta necessidade a um sistema de backup, a empresa realiza backups diários, semanais, mensais, mas nunca exercita um teste de recuperação (*restore*), no dia em que ela necessitar destes dados poderão ocorrer surpresas indesejáveis. No PCN é a mesma coisa, como se trata de um teste, poderão ser agendados horários menos críticos, para simular a ocorrência de crise.

Os resultados dos testes devem ser documentados, analisados e se necessário os planos serão readequados. Isto fará com que a alta direção fique confiante em que em uma situação real de utilização do plano, tudo sairá conforme o planejado.

Se possível a empresa deve optar por realizar periodicamente auditorias internas e externas de seus planos, onde uma equipe diferente da que construiu o PCN, irá checar se o plano está atendendo ao que foi proposto.

2.1.9 **Relações Públicas e Gerenciamento de Crises**

Desenvolve, coordena, avalia e exercita o manuseio de mídias e documentos durante situações de crise, bem como os possíveis meios de comunicação que minimizem impactos traumáticos entre a organização, seus funcionários e suas famílias clientes-chave, fornecedores, investidores e gestores corporativos. Assegura o fornecimento de informações para todos os investidores, por meio de uma fonte única e constantemente atualizada. (MARINHO, 2008, p.81).

Durante uma situação de crise, muito provavelmente ocorrerá um impacto negativo para a empresa, o PCN tem como função garantir que estes impactos sejam controláveis e aceitáveis, porém é necessário saber lidar com as situações de crise, pois uma declaração errada pode acentuar os impactos relacionados a imagem da empresa, por isso é importante definir como a empresa falará com a imprensa, órgãos reguladores, clientes, dentre outros.

Geralmente as empresas que contém uma área específica de comunicação, controlam este caso, criando uma cultura na organização em que apenas este setor pode falar em nome da empresa, desta forma, as respostas são tratadas antes de serem divulgadas. Caso a empresa não contenha este dispositivo, devem ser

criados métodos de divulgação, e principalmente responsabilizando uma equipe que atue com esta função.

2.1.10 **Parceria com Entidades Públicas**

Estabelece os procedimentos necessários e as políticas de coordenação de resposta, atividades de Continuidade e Restauração de Negócios, com auxílio de autoridades públicas para o atendimento de normas e leis. (MARINHO, 2008, p.83).

Necessário identificar se existe alguma legislação em que a empresa atue em conjunto com órgãos públicos e que seja possível algum acordo de cooperação entre as partes, visando a continuidade de negócios.

2.1.11 **Parceria com Entidades Privadas**

Estabelece diretrizes de procedimentos e coordenação de resposta, atividades de Continuidade e Restauração de Negócios, com o auxílio de organizações que compartilham interesses comuns e de terceiros contratados para a execução de tarefas e serviços devido à especialização de sua estrutura e objetivo de negócio para limitação de responsabilidades e funções. (MARINHO, 2008, p.89).

Este é o ponto onde a empresa pode transferir uma responsabilidade relacionada a continuidade de negócios para uma empresa de terceiros, seja através da contratação de serviços, ou até mesmo de acordos de cooperação. Duas empresas em que exista uma relação de confiança mútua, podem, por exemplo, armazenar o site backup uma da outra.

3 ESTUDO DE CASO

3.1 A empresa

A organização estudada atua com convênios de plano de saúde complementar, possui sede em Brasília no seu escritório central (matriz) e escritórios remotos em cada capital brasileira, totalizando 28 localidades. Possui mais de 650 mil beneficiários, que são os principais clientes do serviço da empresa. Alguns sistemas também são acessados pelos prestadores de serviços médicos que atendem os beneficiários e aceitam o plano de saúde.

Apesar de a empresa possuir vários escritórios remotos, e todos estarem diretamente ligados a matriz, todos os sistemas de informação estão centralizados no escritório central, onde a equipe de informática prove as soluções de infraestrutura de rede, segurança, backup, desenvolvimento de sistemas, dentre outras.

Como a empresa atua no ramo de saúde, a mesma é regulada pela Agência Nacional de Saúde Suplementar (ANS), que é vinculada ao Ministério da Saúde, responsável pelo setor de planos de saúde no Brasil.

3.1.1 Início e Administração do Projeto

O projeto iniciou-se com a apresentação do tema de continuidade de negócio aos gestores e alguns colaboradores com grande conhecimento do negócio da instituição, o objetivo desta apresentação inicial era definir as responsabilidades, identificando as pessoas que deveriam participar do projeto. Foram demonstrados

alguns riscos que a empresa estava correndo, a diferença entre recuperação de desastres e a continuidade de negócios.

Nesta apresentação houve um consenso dos ouvintes sobre a importância de que o plano seria construído em conjunto entre as áreas, uma vez que as áreas fim conhecem os sistemas e a área meio TI conhece sobre as interligações entre os sistemas e a infraestrutura. O quadro 1 demonstra como ficaram definidas as responsabilidades.

Quadro 1 – Responsabilidades no PCN

Responsabilidade	**Nome ou Função**
Projeto plano de continuidade de negócio	Gerente de TI e equipe TI
Identificação de processos críticos	Equipe de TI Gerente de Advocacia Gerente de RH Gerente de Arrecadação Gerente Financeiro Gerente de Materiais Gerente de Auditorias médicas Gerente de Comunicação Ouvidoria
Projeto orçamentário	Gerente Financeiro e Arrecadação
Aquisições / locações / contratações	Gerente de Materiais e equipe de TI
Comunicação e treinamento	Gerente de Comunicação e RH

Fonte: Documentação produzida internamente na empresa.

Com base no quadro de responsabilidades, foi criado um comitê gestor do plano de continuidade de negócios (CGPCN). Apesar do documento principal do PCN ser de responsabilidade do gerente de TI e sua equipe, ficou estipulado que durante todo o projeto, seriam realizadas reuniões quinzenais entre os membros do comitê, além de encontros extraordinários dependendo da necessidade.

Através de entrevistas com os membros do comitê, foi realizado um levantamento de ativos, buscando identificar os principais sistemas da empresa,

suas interligações, sua infraestrutura e principalmente, as pessoas chave que gerenciam e mantém estes sistemas.

Nesta etapa foram definidos pelo comitê os sistemas que deveriam fazer parte do escopo do PCN, não significando necessariamente que novos sistemas ou subsistemas não pudessem ser incluídos nas próximas etapas do projeto, visto que a análise de risco e análise de impacto de negócios poderiam apontar para outros produtos capazes de entender o relacionamento de sistemas necessários para a continuidade de negócios.

Sistemas (nomes fictícios) incluídos no escopo e suas funções:

SAPM - Sistema responsável por autorização de procedimentos médicos. Alguns procedimentos médicos podem ser liberados pelo site pelo prestador de serviço (clínicas e hospitais), ou em alguns casos o prestador entra em contato com a central de atendimento, onde os atendentes do callcenter utilizam o sistema para autorizar os exames, cirurgias, procedimentos, dentre outros.

SAM - Sistema que permite auditar os procedimentos médicos que estão sendo realizados pelos prestadores, visando o combate de superfaturamento e procedimentos desnecessários. Médicos auditores contratados pela empresa utilizam este sistema de dentro e fora da instituição para periciar os prestadores. A empresa deixa de perder dinheiro, descredenciando os prestadores que estão agindo de má fé.

SAR - Sistema responsável pela arrecadação de dinheiro junto aos próprios beneficiários do plano, bem como com os patrocinadores (empresas públicas e privadas com planos de saúde corporativos). Dependendo do contrato, os

patrocinadores proveem o pagamento de até 50% do plano de saúde do funcionário, devendo o sistema subsidiar meios de cobrança e controle por parte da empresa.

SO - Sistema de ouvidoria seguindo as legislações da ANS, onde todas as reclamações enviadas por este canal devem ser tratadas e respondidas dentro do prazo estipulado pela agência. O sistema gerencia protocolos e notificações, facilitando o tratamento de cada caso. Além dos canais disponíveis no site, também pode ser utilizado pelo callcenter para registro de reclamações originadas via telefone.

SOPME - Sistema responsável pelo controle de compra de órteses, próteses e matérias especiais. Alguns insumos na área de saúde possuem um custo muito elevado, portanto, este sistema permite que sejam efetuados leilões de compra e controle de fornecedores. Permite que um mesmo produto não seja adquirido com uma diferença tão grande de preço e também controla o preço e a qualidade dos produtos solicitados pelos prestadores de serviço.

SCALL - Sistema 0800 para recebimento de ligações telefônicas. Sistema de entrada de ligações para marcações de exames, reclamações, dúvidas, dentre outros. Muitos dos demais sistemas só são “alimentados” após a chegada da ligação oriunda do beneficiário ou prestador.

SES - Sistema de envio de e-mail e SMS para notificações. A ANS não possui uma regulamentação específica sobre este assunto, porém uma exigência recente solicita que todas as marcações de exames e cancelamentos sejam notificadas para o beneficiário, dessa forma este sistema também foi elegível a constar no PCN.

SWEB – Sistema web de internet e intranet responsável pela interface de acesso entre a operadora do plano de saúde e seus beneficiários/prestadores. Este

é o portal que integra todos os demais sistemas, permitindo que eles sejam acessados via web e intranet, alimentando os bancos de dados que fornecem informações aos demais sistemas.

Os sistemas que são fornecidos por empresas terceirizadas, que já possuem em seus contratos itens específicos relacionados a continuidade de negócio, não serão tratados no PCN. Exemplo: SJUD (sistema jurídico) acessado via web para gerência dos processos jurídicos, controlando prazos e ações a serem tomadas pelos advogados da organização. Para garantir um melhor controle sobre esses sistemas de terceiros, como trabalhos futuros, a empresa implantará formas de testar a continuidade de negócio relacionada a eles.

Com base nos sistemas incluídos no escopo, a equipe de TI identificou os itens de infraestrutura tecnológica. Os servidores ficam armazenados em uma sala adaptada como o centro de processamento de dados (CPD), possuindo sistemas de refrigeração redundantes, são 4 equipamentos de ar-condicionado que funcionam alternadamente em duplas, caso ocorra alguma falha existe um sistema de controle para acionar a manutenção. Existem sensores de controle de temperatura e umidade, porém não foram criados controles de combate a incêndio. A energia elétrica da sala é estabilizada e possui nobreaks que possuem uma autonomia de aproximadamente 2 horas.

Todos os bancos de dados estão consolidados de forma redundante em um *failover cluster* Microsoft com a tecnologia *SQL Always On* em dois servidores físicos. Todas as aplicações (web, arquivos, sistemas), estão armazenadas em um cluster de alta disponibilidade de máquinas virtuais Vmware, em um ambiente construído em 7 servidores físicos Dell.

A empresa possui ainda sistemas de segurança como firewall de borda (protegendo o perímetro da rede), antivírus para servidores e estações de trabalho, antispam para controle de e-mails recebidos e entregues, webgateway para controle de acesso a páginas de internet.

3.1.2 **Avaliação e Controle dos Riscos**

Através da técnica *Facilitated Risk Analysis Process* (FRAP) descrita por Peltier, foram identificados os principais riscos aos quais a empresa se encontra vulnerável, para que fossem definidas métricas e ações de controle, bem como definir responsabilidades e prazos de atuação.

A análise de risco está descrita no apêndice A, mas será detalhada abaixo:

1. Interrupção de energia no site principal – A empresa já possui nobreaks corporativos que possuem autonomia de manter o centro de processamento de dados (CPD) principal e o SCALL (callcenter) ativos por cerca de duas horas, porém se faz necessário a aquisição de um gerador elétrico para aumentar a autonomia, principalmente nos períodos de chuva, onde são frequentes as quedas de energia no local da matriz.

2. Falha no link de acesso à internet – Apesar de não ser constante a falha de acesso à internet por parte do fornecedor contratado, devido aos sistemas críticos da empresa dependerem exclusivamente do acesso à internet, se faz necessário a aquisição de link redundante.

3. Incêndio ou desabamento do site principal – Principal razão pela qual a empresa está buscando um PCN, as situações de catástrofe devem ser tratadas, pois atualmente a organização não possui nem ao menos a cópia de seus backups em outra localidade que não seja o site principal.

4. Roubo ou vazamento de informação. A empresa já efetua há alguns meses a checagem de acessos aos seus sistemas, porém devido a diversas substituições de função e o controle inadequado de permissões, se faz necessário a criação de profiles (usuários modelo) para garantir que os usuários só possuam acesso aos

quais realmente necessitem, minimizando possíveis roubos de dados. Existe também o interesse em aquisição de ferramenta de *Data Loss Prevention* (DLP), onde seja possível configurar políticas para evitar o vazamento de informações privilegiadas.

5. Comprometimento dos sistemas ocasionados por ataques externos e/ou internos. A organização já possui ferramentas que permitem minimizar os ataques bem-sucedidos, contudo é importante que as políticas de *backup, firewall* e *intrusion prevention system* (IPS) sejam revistas e testadas periodicamente, para evitar possíveis surpresas relacionadas ao comprometimento dos sistemas.

6. Ataques ocasionados devido a vulnerabilidades em softwares desatualizados. A empresa já possui rotinas de atualização dos sistemas operacionais de servidores, porém se faz necessário o planejamento de atualização de softwares em geral.

3.1.3 **Análise de Impacto nos Negócios (*Bussiness Impact Analysis* - BIA)**

Foi definido o coordenador de TI como responsável pela execução do BIA. O escopo definido foi a execução de questionário e entrevista com todos os responsáveis dos sistemas críticos que integrarão o PCN, nessa etapa serão confirmados se os sistemas definidos no item 3.1.1 realmente satisfazem a continuidade de negócios da organização, bem como a identificação de subsistemas e infraestrutura necessários para o funcionamento do sistema “pai”. Também foi definido um prazo de 15 dias para a conclusão do BIA.

O questionário submetido por meio de entrevista buscou quantificar e qualificar os prejuízos causados pela interrupção dos sistemas.

O quadro 2 consolidou as respostas ao questionário referente ao sistema de autorização de procedimentos médicos (SAPM).

Quadro 2 - Questionário referente ao sistema de autorização de procedimentos médicos (SAPM).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema responsável por autorização de procedimentos médicos.
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Consulta a base de procedimentos aprovados pela ANS; Consulta as regras de negócio; Aprova ou não aprova um procedimento.
2. Identificar possíveis impactos financeiros.	Além de multa estipulada pela ANS, a indisponibilidade deste sistema acarreta que exames e procedimentos sejam feitos sem a devida análise. Impacto financeiro médio
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Banco de dados (SQL), servidores de aplicação web (IIS), internet. Sistema gerido por pessoas da área de tecnologia, reguladores médicos e atendentes do callcenter.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	Multas da ANS, procedimentos executados sem a devida análise (custo adicional) e possíveis processos jurídicos.
5. Existe alguma interdependência com outro processo interno da organização.	Existe interdependência com os sistemas de callcenter, portal e envio de SMS. • SCALL / SWEB / SES
6. Estabelecer o tempo máximo de parada.	24 horas.
7. Existem requisitos legais e regulamentares?	Sim, regulamentação da ANS.
8. Existem prazos de recuperação?	48 horas.

Fonte: Documentação interna produzida com base em entrevista.

O sistema SAPM é regulamentado pela resolução normativa da ANS de Nº 395 de 14 de janeiro de 2016.

O quadro 3 consolidou as respostas ao questionário referente ao sistema de auditorias médicas (SAM).

Quadro 3 - Questionário referente ao sistema de auditorias médicas (SAM).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema responsável por auditoria médica.
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Auditar guias médicas por amostragem. Prover dados estatísticos para avaliação de prestadores de serviços.
2. Identificar possíveis impactos financeiros.	Não há impactos financeiros diretos, apenas indiretos, uma vez que a função do sistema é justamente auditar gastos e ajudar na redução de custos.
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Banco de dados (SQL), servidores de aplicação web (IIS). Sistema gerido por pessoas da área de tecnologia e médicos auditores.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	Falta de informações que permitam tomar ações referentes a má utilização do plano por parte dos beneficiários e prestadores de serviço.
5. Existe alguma interdependência com outro processo interno da organização.	Interdependência com os dados gravados nos sistemas do portal (SWEB).
6. Estabelecer o tempo máximo de parada.	48 horas.
7. Existem requisitos legais e regulamentares?	Não.
8. Existem prazos de recuperação?	72 horas.

Fonte: Documentação interna produzida com base em entrevista.

O quadro 4 consolidou as respostas ao questionário referente ao sistema de arrecadação (SAR).

Quadro 4 - Questionário referente ao sistema de arrecadação (SAR).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema de arrecadação.
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Arrecadar provisões financeiras junto a patrocinadoras e beneficiários. Emitir guias de cobrança.
2. Identificar possíveis impactos financeiros.	Impacto alto, pois a arrecadação que libera recursos para que a empresa mantenha suas contas em dia. Possíveis processos jurídicos relacionados a cobranças indevidas. Juros bancários.
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Banco de dados (SQL), servidores de aplicação web (IIS). Sistema gerido por pessoas da área de tecnologia, contadores e analistas financeiros.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	A ruptura deste sistema pode inviabilizar a continuidade da empresa caso a indisponibilidade dure mais que 1 dia.
5. Existe alguma interdependência com outro processo interno da organização.	Sim, sistema utiliza os dados internos para checar cobranças e emitir boletos bancários. Também é consultado pelo callcenter para dúvidas relacionadas a cobrança.
6. Estabelecer o tempo máximo de parada.	12 horas
7. Existem requisitos legais e regulamentares?	Não
8. Existem prazos de recuperação?	48 horas

Fonte: Documentação interna produzida com base em entrevista.

O quadro 5 consolidou as respostas ao questionário referente ao sistema de ouvidoria (SO).

Quadro 5 - Questionário referente ao sistema de ouvidoria (SO).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema de ouvidoria
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Receber reclamações, dúvidas, elogios. Transferir demanda para as áreas de negócio.
2. Identificar possíveis impactos financeiros.	Multas da agência reguladora e processos judiciais.
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Banco de dados (SQL), servidores de aplicação web (IIS). Sistema gerido por pessoas da área de tecnologia e ouvidores.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	Impacto médio, devido as regulamentações da ANS possuírem um prazo para resposta aos questionamentos efetuados.
5. Existe alguma interdependência com outro processo interno da organização.	Sim. • SCALL / SWEB
6. Estabelecer o tempo máximo de parada.	48 horas.
7. Existem requisitos legais e regulamentares?	Sim, definidos pela ANS.
8. Existem prazos de recuperação?	72 horas.

Fonte: Documentação interna produzida com base em entrevista.

O sistema SO é regulamentado pela resolução normativa da ANS de Nº 323 de 03 de abril de 2013.

O quadro 6 consolidou as respostas ao questionário referente ao sistema de órteses, próteses e materiais especiais (SOPME).

Quadro 6 - Questionário referente ao sistema de órteses, próteses e materiais especiais (SOPME).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema de órteses, próteses e materiais especiais.
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Realizar a compra de insumos relacionados a saúde com custo elevado. Controlar gastos e fornecedores.
2. Identificar possíveis impactos financeiros.	Impacto indireto, pois o sistema funciona justamente para redução de gastos com a compra de materiais.
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Banco de dados (SQL), servidores de aplicação web (IIS). Sistema gerido por pessoas da área de tecnologia, gerencia de compras, operadores de regulação e médicos auditores.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	Impacto alto, pois o sistema fornece como produto uma grande economia na compra de alguns materiais.
5. Existe alguma interdependência com outro processo interno da organização.	Sim, sistema diretamente integrado ao sistema de auditoria. • SAM / SWEB
6. Estabelecer o tempo máximo de parada.	24 horas.
7. Existem requisitos legais e regulamentares?	Não.
8. Existem prazos de recuperação?	48 horas.

Fonte: Documentação interna produzida com base em entrevista.

O quadro 7 consolidou as respostas ao questionário referente ao sistema de callcenter (SCALL).

Quadro 7 - Questionário referente ao sistema de callcenter (SCALL).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema de callcenter
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Receber os contatos de beneficiários e prestadores.
2. Identificar possíveis impactos financeiros.	Impacto alto, devido à legislação da ANS que obriga que este sistema tenha indisponibilidade mínima.
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Central telefônica, URA[1]. Sistema gerido por empresa terceirizada de telefonia e URA, teleatendentes e gerencia de tecnologia.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	Impacto grande, pois, é o principal meio de interface entre os clientes da empresa, a sua indisponibilidade praticamente inviabiliza os demais sistemas.
5. Existe alguma interdependência com outro processo interno da organização.	Sim, teleatendentes utilizam o SWEB para checar e visualizar todos os tipos de informação para resposta aos beneficiários.
6. Estabelecer o tempo máximo de parada.	4 horas.
7. Existem requisitos legais e regulamentares?	Sim.
8. Existem prazos de recuperação?	8 horas.

Fonte: Documentação interna produzida com base em entrevista.

O quadro 8 consolidou as respostas ao questionário referente ao sistema de e-mail e SMS (SES).

Quadro 8 - Questionário referente ao sistema de e-mail e SMS (SES).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema de envio de e-mail e SMS
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Envio de e-mail e SMS
2. Identificar possíveis impactos financeiros.	Multas e processos judiciais.
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Servidores de e-mail e integração a central telefônica para envio de SMS. Sistema gerido pela gerência de tecnologia.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	Impacto baixo, visto que a notificação ainda é uma exigência recente da ANS, porém em breve será alterado para um impacto maior.
5. Existe alguma interdependência com outro processo interno da organização.	Sim, todos os sistemas que utilizam o envio de notificação se integram com o SES. • SAPM, SAR, SOPME, SO.
6. Estabelecer o tempo máximo de parada.	48 horas.
7. Existem requisitos legais e regulamentares?	Não.
8. Existem prazos de recuperação?	72 horas.

Fonte: Documentação interna produzida com base em entrevista.

O quadro 9 consolidou as respostas ao questionário referente ao sistema de e-mail e SMS (SES).

Quadro 9 - Questionário referente ao sistema de portal (SWEB).

Relatório de Análise de Impacto de Negócio	
Descrição do sistema ou serviço crítico	Sistema web de integração da intranet e internet.
Questionamento	**Resposta**
1. Quais são as funções críticas do sistema?	Interface entre clientes e organização. Acesso aos demais sistemas.
2. Identificar possíveis impactos financeiros.	Impacto alto, pois muitos beneficiários só utilizam este tipo de acesso.
3. Realizar o levantamento dos recursos necessários (tecnologia, infraestrutura e pessoal).	Banco de dados (SQL), servidores de aplicação web (IIS). Sistema gerido por pessoas da área de tecnologia.
4. Avaliar o impacto de uma ruptura do negócio ao longo do tempo	Impacto grande, pois, a indisponibilidade de um dos principais meios de acesso, pode gerar impacto negativo da imagem da empresa.
5. Existe alguma interdependência com outro processo interno da organização.	Sim, o SWEB que permite o acesso aos demais sistemas via web.
6. Estabelecer o tempo máximo de parada.	2 horas.
7. Existem requisitos legais e regulamentares?	Não.
8. Existem prazos de recuperação?	4 horas.

Fonte: Documentação interna produzida com base em entrevista.

Após as entrevistas, os dados obtidos foram consolidados, permitindo gerar a tabela 1, que buscou quantificar o impacto de cada sistema em função do tempo de parada, assumindo 4 níveis de impacto (baixo, médio, alto e catastrófico).

Tabela 1 - Impacto dos sistemas em função do tempo de parada.

Sistema	**>4 horas**	**>8horas**	**>16horas**	**>1dia**	**>2dias**	**>3dias**
SAPM	1	2	3	3	3	4
SAM	1	1	2	2	3	3
SAR	3	3	4	4	4	4
SO	1	1	2	2	3	3
SOPME	2	2	3	3	4	4
SCALL	3	4	4	4	4	4
SES	1	2	2	3	3	4
SWEB	3	4	4	4	4	4

Impacto. (1) baixo (2) médio (3) alto (4) catastrófico

Fonte: Documentação interna produzida após consolidação dos dados.

A tabela 2 foi construída com base na tabela de impactos e tempos de RPO/RTO, permitindo definir as criticidades dos sistemas.

Tabela 2 - Criticidade dos sistemas.

Criticidade	**Sistemas**	**RPO**	**RTO**
1	SCALL/ SWEB	2 horas	4 horas
2	SAR	12 horas	24 horas
3	SAPM / SOPME / SES	24 horas	48 horas
4	SAM / SO	48 horas	72 horas

Criticidade. (1) crítico (2) alta (3) média (4) baixa

Fonte: Documentação interna produzida após consolidação dos dados.

Com base nos questionários, planilha de impacto dos sistemas em função do tempo de parada e tabela de criticidade, foi possível elencar a ordem de criticidades, permitindo definir a ordem de priorização da continuidade de negócio.

Os dois sistemas mais críticos para a empresa estudada são o sistema de callcenter (SCALL) e o sistema web (SWEB), porém como o sistema SCALL possui suas funcionalidades geridas por empresas terceirizadas (Central telefônica e URA), concluímos que o sistema de maior criticidade gerido internamente pela empresa é o (SWEB), fornecendo informações importantes para o funcionamento dos demais sistemas.

3.1.4 **Desenvolvendo Estratégias de Continuidade de Negócio**

Através da análise de risco, foi evidenciada a necessidade de duas aquisições para proteção ao site principal da organização. A primeira diz respeito a proteção contra falhas de energia, com a aquisição de um gerador de energia. A segunda aquisição seria um link de acesso redundante a internet.

Nos últimos anos, houve mais de dez ocorrências de indisponibilidade no site principal onde as causas foram justamente a falta de energia e problemas com o acesso à internet. Estas duas ações minimizariam a interrupção de operação do site principal, mas não seriam suficientes para os casos de catástrofe (incêndio, desabamento, dentre outros), para esses casos serão abordados dois tipos de estratégia: 1. Criação de site backup; 2. Contratação de empresa para computação em nuvem.

3.1.4.1. Estratégia1: Criação de escritório backup

Para a criação do site backup será necessário a locação de um espaço que possa alocar os novos equipamentos, bem como acomodar metade do pessoal responsável pela gerência e operação dos sistemas. Essas pessoas permaneceriam com as suas atuais funções, mas em caso de catástrofe do site principal, atuariam no reestabelecimento da operação do negócio através do site backup.

Por se tratar de uma nova localidade, seriam necessários alguns gastos adicionais relacionados a infraestrutura para que o ambiente backup pudesse operar na falta de qualquer tipo de comunicação ou equipamento do site principal. Por uma questão de padronização e compatibilidade os equipamentos a serem adquiridos seriam dos mesmos fabricantes já utilizados na matriz, pois isso facilitaria o processo de replicação, backup, gerência e manutenção.

No quadro 10 foi realizada uma estimativa de preços para a implementação desta estratégia, os custos de imóveis se basearam nos preços pagos pela empresa nos seus escritórios de Brasília, os custos com aquisições de equipamentos se basearam em uma cotação de preços levantada junto a um dos parceiros da organização no mês de outubro de 2016.

Quadro 10 - Estimativa de preços utilizando a estratégia 1 no período de um ano.

Item	**Gasto mensal**	**Gasto anual**	**Gasto total**
Locação de prédio comercial com espaço para cerca de 50 pessoas e espaço adicional para a criação de uma sala de servidores e equipamentos.	R$25.000	R$300.000	R$300.000
Reforma para criação de sala de servidores.			R$300.000
Aquisição de storage de discos (Dell) com armazenamento mínimo de 30 TB de dados com Raid 5.			R$328.000
Aquisição de dois servidores físicos (Dell) compatíveis com virtualização (Vmware).			R$302.000
Aquisição de dois switches core (Dell).			R$125.000
Aquisição de dois switches de LAN (Dell).			R$16.000
Aquisição de firewall de borda (Aker).			R$60.000
Aquisição de licenças Windows, Vmware.			R$125.000
Contratação de link de dados com dupla abordagem de 100MB entre a matriz e a filial.	R$25.000	R$300.000	R$300.000
Movimentação de 50 estações de trabalho da localidade matriz para o site backup, com seguro de transferência.			R$100.000
Total			**R1.956.000**

Fonte: Documentação interna produzida com auxílio de fornecedores.

Nesta estratégia a empresa utilizará equipamentos e/ou softwares que auxiliarão no processo de réplica de dados entre o escritório principal (matriz) e o escritório backup, conforme citado nos itens abaixo:

A) Microsoft *failover cluster* geográfico + Microsoft SQL Server 2016 com *Always On.*

O serviço de *failover cluster* da Microsoft nada mais é do que dois ou mais servidores desempenhando a mesma função, com alta disponibilidade. Geralmente um dos servidores assume a função ativo e o outro a função passivo, caso o servidor ativo apresente falhas, o sistema possui um mecanismo que transfere para o servidor passivo a carga de trabalho e este passa a responder como ativo.

Até o ano de 2008 o serviço de failover cluster exigia que os servidores com este recurso estivessem próximos um ao outro, pois era necessária uma ligação de cabo crossover[1] entre os servidores, além deles terem que compartilhar o mesmo disco no storage[2]. A partir da versão 2008 do Windows, foi criado o conceito de cluster geográfico, onde cada servidor poderia estar em uma localidade distante.

Em paralelo a esta tecnologia, a Microsoft a partir da versão 2012 do SQL server criou o conceito de *Always On*, onde cada servidor não precisa mais compartilhar o mesmo disco, cada um grava no seu próprio disco disponibilizado no storage, assim a replicação é feita de forma síncrona, pois os dados só serão gravados no banco somente quando ambos servidores estiverem sincronizados.

B) Virtualização de servidores com Vmware.

A virtualização de servidores possibilitou uma série de vantagens ao mercado de TI, das quais podemos destacar: redução de energia, espaço físico, cabeamento e também o tempo para criar ou modificar a estrutura de um servidor. Utilizando a virtualização, podemos por exemplo aumentar ou diminuir alguns recursos computacionais como disco, placa de rede, memória, CPU, dentre outros.

Em um mesmo servidor, você pode ter bancos de dados incluídos neste recurso de replicação e outros bancos que não se repliquem via *Always On*. Desta forma os bancos relacionados aos sistemas críticos ao invés de se replicarem apenas aos servidores da matriz, também seriam replicados para a localidade remota (backup).

1. Cabo crossover – É um cabo de rede par trançado que permite que dois computadores sejam ligados pelas respectivas placas de rede, sem a necessidade de um switch ou hub.

2. Storage – Conjunto de discos com redundâncias que fornece espaço de armazenamento para servidores em rede.

Essa tecnologia facilita o processo de réplica para a localidade backup, pois podem ser criadas políticas para copiar um servidor completo em determinados horários do dia, desta forma em caso de indisponibilidade do site principal o mesmo servidor poderia ser ligado ou colocado em status ativo.

Obs.: Dependendo da criticidade do sistema, também é possível utilizar o conceito de *cluster* para que os servidores fiquem ativos em ambas as localidades, como backup um do outro.

C) Backup Dell + linha de equipamento DS

A empresa atualmente utiliza a suíte de produtos Dell para backup.

- NetVault (em nível de arquivos, granulares).
- Vranger (máquinas virtuais).
- AppSure (*snapshots* configuráveis).

Com o barateamento do custo de discos ocorrido nos últimos anos, alguns fabricantes estão investindo no backup direto em disco em vez de fitas. Isto possibilita uma série de vantagens, como, por exemplo, redução da janela, replicação síncrona ou assíncrona para outra área de disco.

A empresa já possui dois equipamentos de backup DS4100, um replica ao outro os dados, porém atualmente eles estão alocados na mesma localidade. Com a criação do escritório secundário seria necessário apenas a movimentação de um destes equipamentos e adaptação das políticas atuais de backup.

3.1.4.2. Estratégia2: Contratação de empresa com dados na nuvem

Apesar de nesta estratégia não ser necessário um espaço para novos equipamentos, se faz necessário um novo escritório para as 50 pessoas que seriam as responsáveis por gerir e operar o sistema em caso de catástrofe do site principal.

O quadro 11 traz uma estimativa de custos para a estratégia 2. Os preços dos serviços em nuvem se basearam na calculadora disponível na internet no site do Windows Azure (Serviço de nuvem da Microsoft). Disponível em: https://azure.microsoft.com/pt-br/pricing/calculator/?service=cloud-services

Quadro 11 – Estimativa de preços utilizando a estratégia 2 no período de um ano.

Item	Gasto mensal	Gasto anual	Gasto total
Locação de prédio comercial com espaço para cerca de 50 pessoas.	R$15.000	R$180.000	R$180.000
Aquisição de firewall de borda (Aker).			R$60.000
Aumentar o link de internet do site principal para 200MB.	R$20.000	R$240.000	R$240.000
Contratação de link de internet com dupla abordagem de 100MB, para o novo escritório.	R$20.000	R$240.000	R$240.000
Aquisição de dois switches de LAN (Dell).			R$16.000
Contratação de serviço em nuvem com tamanho e performance compatível para o bom funcionamento dos sistemas críticos. Calculado sobre o valor de 10 instancias A7 totalizando 20 TB de espaço disponível.	R$48.546.00	R$582.552	R$582.552
Movimentação de 50 estações de trabalho da localidade matriz para o site backup, com seguro de transferência.			R$100.000
Total			**R$1.318.652**

Fonte: Documentação interna produzida com auxílio de fornecedores.

Nesta abordagem seriam necessários ajustes para configurar a replicação de dados entre o site principal e os sistemas armazenados em nuvem.

Tanto o *failover cluster*, quanto o SQL poderiam ser utilizados para a réplica de bancos de dados, porém cada fornecedor de serviços em nuvem possui as suas próprias regras, devendo ser verificado se poderia ser utilizado a virtualização vmware e o backup Dell para auxiliar neste processo de réplica, ou se mais algum ajuste seria necessário.

3.1.4.3. Comparação e definição da estratégia

Para comparação das duas estratégias propostas, foram levantadas as principais vantagens e desvantagens das duas abordagens, descritas no quadro 12.

Quadro 12 – Vantagens e desvantagens das estratégias propostas.

Estratégia 1: Site backup	
Vantagens	Desvantagens
• Compatibilidade. Empresa já possui ferramentas para replicação de dados. • Capacitação. Funcionários já sabem operar a tecnologia. • Segurança. Dados armazenados internamente.	• Custo inicial. • Necessidade de renovação do parque tecnológico a cada 5 anos.
Estratégia 2: Serviços em nuvem	
Vantagens	Desvantagens
• Custo. • Escalabilidade. Possibilidade de aumentar os recursos por demanda.	• Capacitação da tecnologia aos funcionários. • Dependência de um terceiro. • Segurança. Dados críticos na nuvem.

Fonte: Documentação interna produzida com auxílio de fornecedores.

Observação: Apesar da estratégia 1 apresentar um custo mais elevado no seu primeiro ano de vigência, os maiores custos estão relacionados a aquisição de equipamentos, uma renovação completa do parque tecnológico deveria ser realizada a cada 5 anos. Já a estratégia 2 apresenta um custo menor no primeiro ano, porém

o custo da contratação do serviço em nuvem de quase 600 mil reais será aplicado anualmente.

Ambas abordagens foram explicitadas primeiramente aos membros do comitê gestor do PCN, onde foram tiradas possíveis dúvidas e efetuados os ajustes necessários. Após esta etapa foram submetidas à alta direção as planilhas de estimativas de custo, bem como as vantagens e desvantagens de cada estratégia, para que fosse escolhida qual estratégia a ser implementada.

Após reuniões internas, a alta direção optou para que fosse implementada a estratégia de número 1 (criação de escritório backup). Os principais motivos para esta escolha apontados pelos diretores, foram a falta de confiança em deixar os dados fora do ambiente interno e a falta de profissionais capacitados para operar a tecnologia em nuvem. Os dados armazenados pela empresa são sigilosos, pois envolvem informações relacionadas a saúde dos beneficiários, exames, materias médicos, dentre outros.

3.1.4.4. Backup *offsite*

Independentemente da estratégia escolhida, ficou evidenciada a necessidade de adoção de um backup offsite em que os dados mais importantes serão gravados em fitas magnéticas e enviados para outra unidade da empresa. Até que os planos de continuidade sejam implementados, este backup externo garantiria condições mínimas para retomada do negócio em caso de catástrofe no site principal.

Na situação atual, em caso de grave crise na matriz, a organização não teria como recriar seus sistemas em outro ponto; não existiriam informações sobre clientes, fornecedores, devedores, contas a pagar, dentre tantas outras informações importantes para a continuidade de operação do plano de saúde.

3.1.5 **Respostas e Operações de Emergência**

A empresa já possui uma equipe de monitoramento 24/7 responsável por algumas ações de recuperação de pequenos incidentes e, em casos mais graves, acionamento de analistas para atuação na resolução dos problemas. Esta abordagem, resolve a grande maioria dos casos, porém quando adicionado o conceito de um PCN, se faz necessário que esta equipe esteja nas duas localidades (escritório matriz e escritório backup).

Após reuniões internas, foi nomeada a equipe do escritório matriz (principal) como equipe de monitoramento 1, e a equipe do escritório backup (secundário) como equipe de monitoramento 2. O quadro 13 demonstra os procedimentos e principais atribuições das equipes de monitoramento.

Quadro 13 – Procedimentos das equipes de monitoramento

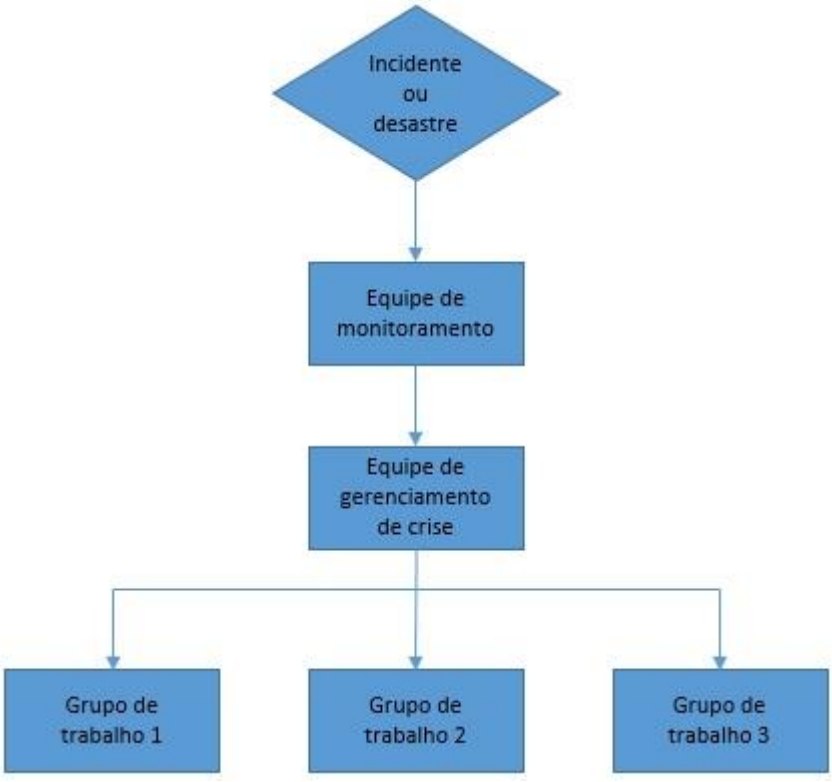
Incidente	Equipe	Ação
Falha em um ou mais sistemas críticos.	Monitoramento 1	1. Acionar a equipe de gerenciamento de crise.
	Monitoramento 2	1. Confirmar com a equipe de monitoramento 1 se já foi dado tratamento ao incidente.
Falta de energia site principal	Monitoramento 1	1. Checar funcionamento dos geradores e *nobreaks.* 2. Acionar empresa de manutenção do gerador para possíveis reabastecimentos de combustível. 3. Acionar equipe de gerenciamento de crise para sobreaviso. 4. Notificar equipe de monitoramento 2 para ficar atenta ao monitoramento, enquanto a equipe 1 fica dedicada ao monitoramento de autonomia do gerador.
	Monitoramento 2	1. Ao ser acionada assume o papel principal de monitoramento.
Catástrofe no site principal	Monitoramento 1	1. Caso seja possível, acionar os responsáveis pelo controle da causa. Exemplo: Acionar bombeiros em caso de incêndio, acionar manutenção em caso de inundação.
	Monitoramento 2	1. Caso não seja possível contato com a equipe do site principal para checar as condições, acionar o gerenciamento de crise.

Fonte: Documentação interna produzida com base nas necessidades de monitoramento.

Para o sucesso do plano de respostas a situações de emergência se faz necessário o treinamento contínuo das equipes de monitoramento, bem como que este plano esteja impresso e de fácil acesso a todos os envolvidos. Como forma de treinamento e checagem contínua, a empresa fará uma simulação por mês em datas pré-estipuladas para que o processo fique claro para os funcionários responsáveis por esta função.

O plano de respostas a incidentes buscou seguir o fluxograma representado na figura 3, onde na ocorrência de um incidente a equipe de monitoramento acionaria a equipe de gerenciamento de crise e esta equipe acionaria os grupos de trabalho necessários para a atuação na resolução do problema ou acionamento do PCN.

Figura 3 - Fluxograma utilizado em caso de incidentes ou desastres



Fonte: Documentação interna produzida com base nas necessidades de monitoramento.

1. Após a ocorrência de um incidente, a equipe de monitoramento deve acionar a equipe de gerenciamento de crise com no máximo 5 minutos.

2. Após serem acionados, a equipe de gerenciamento de crise aciona dois grupos de trabalho, o primeiro iniciará as tentativas de restaurar o sistema no próprio escritório matriz, o segundo iniciará as checagens do PCN e após um tempo pré-estabelecido de acordo com cada sistema iniciará a execução do PCN para migração do sistema para o escritório backup, ou nuvem. O tempo máximo de acionamento das duas equipes deve ser de no máximo 10 minutos.

3.1.6 **Desenvolvendo e Implementando PCN**

Por uma questão de prazos deste trabalho acadêmico, não será possível trabalhar com um PCN para cada sistema crítico, portanto, trabalharemos no desenvolvimento e implementação do PCN do sistema de maior criticidade (SWEB).

O sistema web (SWEB), possui o seu Recovery Time Objectives (RTO), definido como 2 horas, isto significa que entre a ocorrência de uma falha e o funcionamento total do sistema, seja no escritório principal ou no escritório backup ou nuvem, este é o tempo máximo para que o sistema esteja normalizado. Portanto deve ser previsto todo o tempo em que as equipes de monitoramento, gerenciamento de crises e grupos de trabalho terão para se comunicar, mais o tempo necessário para reestabelecimento do sistema. Verificando estes tempos, definimos os horários em que obrigatoriamente temos que iniciar o PCN para transferência do sistema para o site redundante ou nuvem.

Como visto anteriormente existe uma replicação síncrona proporcionada pela tecnologia failover cluster geográfico com SQL always on, entre o site principal e o

site redundante, porém como o tempo de Recovery Point Objective (RPO) está definido como 4 horas, isto significa que temos que ter um backup de logs do SQL, e que este backup também seja replicado para a segunda localidade ou nuvem. Foram definidos que estes backups ocorreriam de 2 em 2 horas, e seriam replicados em aproximadamente 1 hora para o site de redundância. Mesmo existindo a sincronização de SQL em tempo real, o backup completo (full) seria replicado pela tecnologia de redundância de backup Dell.

O plano de continuidade de negócios proposto para o sistema SWEB foi descrito no quadro 14.

Quadro 14 – Plano de continuidade de negócios para o sistema SWEB

Plano de Continuidade de Negócios – Sistema web SWEB			
Equipe:	Atividade:	Tempo máximo esperado:	Status:
Gerenciamento de crise.	1. Acionar o grupo de trabalho de banco de dados.	5 minutos	☐ OK.
	2. Acionar o grupo de trabalho infraestrutura.	5 minutos	☐ OK.
	3. Acionar o grupo de trabalho de comunicação.	5 minutos	☐ OK.
	4. Gerenciar as equipes em atuação.	Continuo	☐ OK.
	5. Notificar equipes ao término da restauração completa.	15 minutos	☐ OK.
Grupo de trabalho banco de dados (BD).	1. Checar se o banco de dados do site backup está sincronizado.	10 minutos	☐ OK, seguir para o passo 5. ☐ Negativo.
	2. Checar se a restauração do backup de logs das últimas 2 horas tornaria o banco sincronizado.	5 minutos	☐ OK, seguir para o passo 4. ☐ Negativo.
	3. Restaurar backup completo (full)	60 minutos	☐ OK.
	4. Restaurar backup de logs.	20 minutos	☐ OK.
	5. Notificar equipe de gerenciamento de crise.	5 minutos	☐ OK.

	6. Monitorar o ambiente	Continuo	☐ OK.
Grupo de trabalho Infraestrutura.	1. Checar se os servidores virtuais de IIS do site backup estão ativos	10 minutos	☐ OK. Seguir para o passo 3. ☐ Negativo
	2. Iniciar os servidores virtuais necessários para o sistema.	10 minutos	☐ OK.
	3. Alterar entradas DNS externas, para que a internet aponte para a nova localidade.	30 minutos	☐ OK.
	4. Notificar equipe de gerenciamento de crise.	5 minutos	☐ OK.
	5. Monitorar o ambiente	Continuo	☐ OK.
Grupo de trabalho comunicação	1. Preparar respostas para público interno e externo.	30 minutos	☐ OK.
	2. Responder imprensa, agências, dentre outros, caso houver a necessidade	Continuo	☐ OK.

Fonte: Documentação interna produzida por este trabalho acadêmico.

Esta foi a documentação inicial proposta para o PCN, onde cada equipe iniciaria a elaboração de planos detalhados de como executar estas atividades relacionadas. Devido à falta de tempo para a execução deste trabalho acadêmico, estas atividades serão objeto de trabalhos posteriores.

3.1.7 **Implementando a Consciência e os Programas de Treinamento**

O comitê gestor do PCN utilizará as próprias ferramentas internas da empresa (intranet e e-mail) para divulgar campanhas de conscientização aos funcionários que não estão diretamente ligados ao PCN, para que seja criada uma cultura onde cada empregado entenda que a continuidade de negócios depende de todos, treinando os colaboradores, inclusive em como agir em situações de crise.

Para os funcionários que atuarão no monitoramento, gerência de crises e grupos de trabalho na recuperação dos sistemas, serão aplicados treinamentos semestrais explicando que o conceito de continuidade deve ser parte integrante do dia-a-dia de suas funções.

Como a manutenção e recuperação de sistemas está diretamente ligada a tecnologia fornecida por alguns fabricantes (Microsoft, Vmware, Dell), serão fornecidos cursos anuais para as equipes de trabalho que atuam com as ferramentas e disponibilizado gratificações para os funcionários que obterem certificações ligadas a tecnologia utilizada pela empresa.

3.1.8 **Mantendo e Exercitando o PCN**

A alta direção estipulou que as equipes diretamente envolvidas com o PCN deveriam simular a indisponibilidade de um sistema crítico pelo menos uma vez ao mês, checando a replicação, processos de recuperação e possibilidade de utilização do sistema através do site redundante.

Além desses testes, quadrimestralmente em datas pré-agendadas deveria ser feita a transferência de todos os sistemas críticos para o escritório secundário, isto possibilitaria treinar toda a equipe continuadamente sobre como agir em situações de crise. Todo este processo deveria ser documentado, através de check lists, para descobrir se tudo está funcionando conforme o esperado, e corrigindo possíveis problemas.

Essa transferência também permitiria o acompanhamento de performance da utilização dos sistemas através do escritório secundário, para checar se também não seriam necessários ajustes ou aquisições para que os serviços atendessem a contento as necessidades da empresa. Exemplo: poderia ser verificado que os

sistemas no escritório remoto estivessem lentos demais para operação do negócio e fossem necessários ajustes na quantidade de servidores ou links de comunicação.

Com base nos testes e movimentações, também seriam feitas reuniões quadrimestrais com o comitê gestor do PCN para checar se haveria a necessidade de melhorias ou alterações no PCN.

3.1.9 **Relações Públicas e Gerenciamento de Crises**

A empresa já tem como prática que apenas o setor de comunicação pode falar em nome da empresa, seja para jornalistas ou em mídias sociais. Esse procedimento foi reforçado principalmente para em casos de crise, onde os colaboradores envolvidos ou não na situação de crise deveriam repassar qualquer solicitação de informação para a comunicação.

O gerenciamento de crises foi um grupo formado pelos 3 principais analistas de segurança da empresa, foi disponibilizado um celular corporativo onde os 3 funcionários trabalhariam em escala de plantão, recebendo para ficar em disponibilidade da empresa. Caso fossem acionados fora de seus horários de trabalho receberiam conforme a legislação vigente. Esse grupo seria o responsável pela atuação nas possíveis crises, seguindo o PCN para acionar e acompanhar o processo de restauração de sistemas.

O mesmo processo de plantão com disponibilidade foi incluso para as pessoas que atuariam nos grupos de trabalho, pois caso uma crise ocorresse fora do horário de trabalho e não fosse possível contato com ninguém, de nada adiantaria a criação de prazos e processos.

3.1.10 **Parceria com Entidades Públicas**

Apesar de a empresa estar diretamente ligada a um órgão público regulador (ANS), durante a execução do trabalho não foi deslumbrada a possibilidade de parceria com entidades públicas, relacionadas ao PCN.

3.1.11 **Parceria com Entidades Privadas**

A empresa já possui alguns contratos com entidades privadas, transferindo a responsabilidade de alguns sistemas e/ou infraestrutura para empresas que fornecem um serviço específico. Podemos destacar o sistema de callcenter (SCALL), onde o serviço de centrais telefônicas e canais de comunicação é fornecido por uma empresa que atua no segmento, se integrando com a unidade de resposta audível (URA) fornecida por outra empresa específica.

Caso a alta direção optasse pela estratégia de número 2 de aquisição de serviços em nuvem, outro grande contrato seria firmado com uma entidade privada, que proveria a infraestrutura necessária para rodar os sistemas em caso de ativação do PCN em momentos de crise.

CONCLUSÃO

Segundo o DRI – *Disaster Recovery Institute* - de cada cinco empresas que possuem interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos. Este dado demonstra como uma situação de crise grave pode impactar na continuidade de negócio. Uma indisponibilidade dos sistemas críticos, pode afetar não somente o lado financeiro, como também pode gerar um impacto irreversível para a imagem da instituição.

Como resultado deste trabalho acadêmico, a empresa do estudo de caso conseguiu gerar uma análise de riscos, a partir da qual documentou as principais falhas a que estava exposta e adotou medidas para minimizar as ocorrências e impactos de possíveis paradas, tais como falta de energia, falha no link de acesso à internet, dentre outras. A geração do documento de impacto de negócios possibilitou que a organização conhecesse melhor os seus sistemas e as integrações existentes, permitindo definir uma maneira mais eficaz de priorizar o restabelecimento dos sistemas na ordem de importância. A definição de uma estratégia de continuidade de negócios, bem como o primeiro plano de continuidade de negócios proposto, permitiu à empresa definir uma forma sobre como atuar em casos de crise.

Como recomendações, a organização deverá iniciar as tratativas de locação de um prédio comercial que possa acomodar a sala de servidores de contingência (backup), e as estações de trabalho de 50 pessoas que ficarão alocadas nesta nova localidade. Deverá ser realizada uma reforma para a criação dessa sala e será necessário adquirir os novos equipamentos (storage, servidores, switches de comunicação, firewall) e licenças de software, que permitirão a criação da infraestrutura tecnológica do site redundante. A empresa deverá detalhar o plano de

continuidade dos demais sistemas críticos. Após a criação deste escritório backup, os planos deverão ser testados e adaptados, e finalmente os funcionários deverão ser treinados e orientados a participar de programas de conscientização.

O desenvolvimento do presente estudo demonstrou que existe um custo elevado para a criação de um plano de continuidade de negócios, uma vez que não existe continuidade sem redundância de dados, equipamentos, dentre outras. O grande desafio atual é convencer os gestores empresariais de que a ausência desses planos e da sua correta execução pode significar o encerramento das atividades da empresa em casos de desastres.

Serão executados como trabalhos futuros estudos dentro da empresa para quantificar o custo de uma parada no serviço dos sistemas críticos, tal procedimento visará obter uma tabela de custo benefício entre a implantação do plano proposto por este trabalho acadêmico e o custo de uma grande parada no ambiente de produção.

REFERÊNCIAS

ABNT NBR ISO 22301, Associação Brasileira de Normas Técnicas. 2013

ABNT NBR ISO 22313, Associação Brasileira de Normas Técnicas. 2015

ABNT NBR ISO/IEC 27001, Associação Brasileira de Normas Técnicas. 2013

ABNT NBR ISO/IEC 27002, Associação Brasileira de Normas Técnicas. 2013

ABRAPP. Guia de Boas Práticas para Planos de Continuidade de Negócios. Disponível em: <http://www.abrapp.org.br/Documentos%20Pblicos/guiaboaspraticas.pdf>. Acesso em 20 out. 2016.

ANS. RN Nº 323, DE 3 DE ABRIL DE 2013
Disponível em: <http://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MjQwNA==>. Acesso em 30 set. 2017.

ANS. RN Nº 395, DE 14 DE JANEIRO DE 2016
Disponível em: <http://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MzE2OA==>. Acesso em 30 set. 2017.

BEAL, Adriana. ***Segurança da Informação - Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações*****.** Rio de Janeiro: Atlas, 2008.

CERT. Estatísticas dos incidentes reportados ao CERT.br. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 13 out. 2016.

MARINHO, Fernando. ***Como Proteger e Manter seus Negócios - Um plano Básico Para Contingências e Continuidade nas Empresas***. Rio de Janeiro: Ciência Moderna, 2008.

MICROSOFT. Cotação de serviços em nuvem Microsoft. Disponível em: https://azure.microsoft.com/pt-br/pricing/calculator/?service=cloud-services. Acesso em: 28 out. 2016.

PELTIER, Thomas R. **Facilitated Risk Analysys Process (FRAP).** Disponivel em: <http://www.ittoday.info/AIMS/DSM/85-01-21.pdf>. Acesso em: 02 out. 2016.

SÊMOLA, Marcos. ***Gestão da Segurança da Informação*** **- Uma visão Executiva.** Rio de Janeiro: Campus, 2003.

APÊNDICE A – Avaliação e Controle dos Riscos

Quadro 15 – Avaliação e Controle dos Riscos da Empresa Estudada

ID	Risco	Tipo (C/D/I)	Prioridade (A/B)	Medida de Controle	Ação	Responsável	Prazo
01	Interrupção de energia no site principal.	C/D/I	A	1. Aquisição de gerador elétrico	1. Especificar gerador. 2. Adquirir novo gerador. 3. Implantar equipamento. 4. Testes.	1 Engenheiro elétrico. 2. Gerência de materiais. 3. Gerência de materiais e engenheiro elétrico. 4. Engenheiro elétrico.	1. 7 dias. 2. 90 dias. 3. 15 dias. 4. 2 dias.
				2. Capacitação da equipe responsável pelo gerador	5. Contratar empresa para capacitação da equipe responsável pelas rotinas semanais de checagem do gerador.	5. Gerência de educação corporativa.	5. 15 dias
02	Falha no link de acesso à internet.	C/D	A	1. Aquisição de link de acesso redundante.	1. Efetuar levantamento de necessidades. 2. Adquirir link de acesso redundante. 3. Implementar novo link. 4. Testes.	1. Gerência de tecnologia. 2. Gerência de materiais. 3. Gerência de tecnologia. 4. Gerência de tecnologia.	1. 7 dias. 2. 90 dias. 3. 15 dias. 4. 7 dias.
03	Incêndio ou desabamento do site principal.	C/D/I	A	1. Criação de planos de continuidade de negócios para os sistemas mais críticos da empresa.	1. Efetuar uma análise de risco e analise de impacto de negócios para definição dos sistemas críticos da empresa. 2. Escolher a melhor estratégia de continuidade de acordo com as necessidades da empresa. 3. Aquisição de equipamentos	1. Gerência de tecnologia em conjunto com as áreas de negócio. 2. Gerência de tecnologia.	1. 30 dias. 2. 15 dias.

					e/ou contratação de serviços que subsidiem o PCN. 4. Criação e implantação dos PCNs. 5. Testes.	3. Gerência de materiais. 4. Gerência de tecnologia. 5. Gerência de tecnologia.	3. 90 dias. 4. 90 dias. 5. 15 dias.
				2. Treinamento de funcionários.	6. Solicitar o treinamento dos funcionários da brigada de incêndio junto ao corpo de bombeiros. 7. Capacitar os funcionários que atuarão na execução dos PCNs.	6. Gerência de educação corporativa. 7. Gerência de tecnologia.	6. 15 dias. 7. 30 dias.
04	Roubo ou vazamento de informação.	C / I	A	1. Segregação de acessos dos funcionários.	1. Criar políticas de acesso, que limitem as permissões dos colaboradores a apenas, a sua área de atuação. 2. Criar grupos de acesso e implementar os níveis de permissionamento.	1. Gerência de Tecnologia. 2. Gerência de tecnologia.	1. 40 dias. 2. 90 dias.
				2. Aquisição de ferramenta de *Data Loss Prevention* (DLP).	1. Levantar necessidades. 2. Adquirir ferramenta. 3. Implementar. 4. Testar.	1. Gerência de tecnologia. 2. Gerência de materiais. 3. Gerência de tecnologia. 4. Gerência de tecnologia.	1. 7 dias. 2. 90 dias. 3. 15 dias. 4. 7 dias.
05	Comprometimento dos sistemas ocasionados por ataques externos e/ou internos	C / D / I	B	1. Checagem das políticas de backup e firewall.	1. Checar se as políticas de backup e de firewall estão atendendo as necessidades da empresa.	1. Gerência de tecnologia.	1. 10 dias.

					2. Criar rotinas diárias de monitoramento. 3. Testar a execução da recuperação dos backups, avaliando tempo e integridade dos dados.	2. Gerência de tecnologia. 3. Grupo de trabalho de backup.	2. 2 dias. 3. Pelo menos uma vez na semana.
				2. Treinamento dos colaboradores nas ferramentas de segurança.	1. Cotar treinamentos oficiais para a equipe de tecnologia responsável pelo suporte. 2. Criar políticas de incentivo a obtenção de certificações técnicas.	1. Gerência de educação corporativa. 2. Diretoria de administração.	1. 10 dias 2. 90 dias.
06	Ataques ocasionados devido a vulnerabilidades em softwares desatualizados.	C / D / I	B	1. Implementação de software de instalação e gerenciamento de softwares.	1. Configuração do modulo do software *System Center Configuration Manager*, para atualização de softwares desatualizados. 2. Criar rotinas de controle para monitoramento e atualização dos softwares.	1. Gerência de tecnologia 2. Gerência de tecnologia.	1. 30 dias. 2. 10 dias.

Fonte: Documentação interna produzida durante este trabalho.