UNIVERSIDADE DE CAXIAS DO SUL

FELIPE BIONDO DA SILVA

PLANO DE CONTINUIDADE DE NEGÓCIOS PARA INDÚSTRIAS DE PEQUENO E MÉDIO PORTE

CAXIAS DO SUL

2013

UNIVERSIDADE DE CAXIAS DO SUL

FELIPE BIONDO DA SILVA

PLANO DE CONTINUIDADE DE NEGÓCIOS PARA INDÚSTRIAS DE PEQUENO E MÉDIO PORTE

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Orientadora: Profª. Iraci Cristina da Silveira de Carli

CAXIAS DO SUL

2013

DEDICATÓRIA

A todos vocês, que sempre estiveram ao meu lado, me incentivando, e contribuindo para que este trabalho atingisse seus objetivos. Em especial aos meus pais, que realizam através de mim, parte dos seus sonhos.

AGRADECIMENTOS

Quero expressar meus agradecimentos a todos aqueles que, de alguma forma, colaboraram para meu crescimento profissional e acadêmico para que este trabalho pudesse ser realizado. Em especial a minha orientadora, Prof. Iraci Cristina Silveira de Carli, por sua competência, conhecimento transmitido e orientação durante o desenvolvimento desta monografia.

Gostaria de agradecer aos meus colegas de profissão, que estão sempre dispostos a ensinar e aprender junto conosco, ao meu diretor Evandro Stumpf, que me deu oportunidade de crescimento profissional e sempre me apoiou nos momentos de indecisão.

Agradeço em especial aos meus familiares e amigos que estiveram do meu lado me apoiando. Aos meus pais, agradeço por sempre me ajudarem em todos os passos de minha vida. Agradeço também ao meu irmão que sempre esteve disposto a contribuir com o possível. Por último, e não menos importante, agradeço a minha noiva Juliana por fazer parte da minha vida e sempre estar do meu lado durante minha trajetória acadêmica.

RESUMO

A continuidade de negócios é uma área da segurança da informação para a qual, mesmo sendo de importância crucial para a operação das organizações, não é dada sua devida importância. As organizações dependem de seus processos de TI (Tecnologia da Informação) para operarem seu negócio e estes precisam estar disponíveis e ter a capacidade de serem recuperados de maneira organizada e ágil. O plano de continuidade de negócios é um conjunto de ações para evitar a interrupção dos serviços de TI e promover a recuperação de incidentes e desastres, caso estes ocorram. A continuidade de negócios é fundamentada na gestão de riscos. Um plano de continuidade de negócios define o que deve ser feito, quando deve ser feito, como deve ser feito e por quem deve ser feito. O objetivo deste trabalho é a realização de um estudo das normas e bibliotecas de melhores práticas da gestão de riscos e continuidade de negócios. A partir deste estudo, será elaborado um modelo de plano de continuidade de negócios aplicável a empresas de pequeno e médio porte que possuem um ambiente de TI simples e que estão amadurecendo o conceito de riscos e continuidade de negócios. O modelo proposto abrange a definição da organização e escopo da continuidade, a análise de riscos, a elaboração do plano de continuidade e a execução e monitoramento do plano de continuidade de negócios.

Palavras-chave: Continuidade de Negócios; Plano de continuidade de negócios; Riscos; Recuperação; Desastre; Resposta; Incidentes; Segurança; Tecnologia da Informação.

ABSTRACT

Business continuity is an area of information security which, although being critical to their business operation, is not given its due importance by organizations. Organizations rely on their IT, Information Technology, processes to run their business and these must be available and have to be recovered in a quick and organized way. The business continuity plan is a set of actions to avoid services interruption, and recover them from incidents and disasters, if these occur. Business continuity is supported by risk management. A business continuity plan defines what must be done, when it must be done, how it should be done and by whom should be done. The objective of this research project is to conduct a research of standards and libraries of best practices of risk management and business continuity. From this research, create a business continuity plan applicable to small and mid-sized companies that have a simple IT environment and are new to the concept of risk and business continuity. The proposed model covers Organization's definition and continuity scope, risk analysis, implementation of a business continuity plan and running and monitoring of the business continuity plan.

Keywords: Business continuity; Business continuity plan; Risks; Disaster; Recovery; Incidents; Response; Security; Information technology.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AD	Active Directory
BI	Business Intelligence
BPMN	Business Process Model and Notation
BS	British Standard
BSI	British Standards Institute
Cobit	Control objectives for information and related technology
CRM	Customer Relationship Management
ER	Entidade e Relacionamento
ERP	Enterprise resource planning
GCN	Gestão de continuidade de negócios
GCSTI	Gerenciamento da continuidade dos serviços de TI
HCM	Human Capital Management
HP	Hewlett Packard
IEC	International Eletrotechnical commission
IIS	Internet Information Services
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
IT	Information Technology
ITIL	Information technology infrastructure library
LTO	Linear Tape Open
NBR	Norma Brasileira
OGC	Office of Government Commerc
OLA	Operational Level Agreement
OMG	Object Management Group
PCN	Plano de Continuidade de Negócios
PDCA	Plan, do, check, act
R2	Release 2
RACI	Responsible, Accountable, Consulted, and Informed
SLA	Service Level Agreement
SQL	Structured Query Language
TI	Tecnologia da Informação
UCS	Universidade de Caxias do Sul
WMS	Warehouse Management System

SUMÁRIO

1 INTRODUÇÃO

O Plano de Continuidade de Negócios (PCN) é um conjunto de normas, operações e ações executadas pelas organizações a fim de não permitir a interrupção das atividades do negócio e proteger seus processos críticos contra falhas ou desastres significativos e, caso necessário, assegurar sua retomada em tempo hábil (BS 25999, 2006).

> Um desastre pode ser entendido como qualquer situação que afete os processos críticos do negócio de uma organização. Consequentemente, algumas ocorrências podem ser caracterizadas como sendo desastres para uma determinada empresa, mas podem não ser caracterizadas como um desastre para outra empresa (WALLACE, 2004).

Para entender Continuidade de negócio, há uma necessidade de se voltar no tempo. Na década de 60, comentava-se sobre desastres que poderiam se abater a ponto de parar com o negócio de uma organização. A partir dos anos 80, começou a ser tratado o termo recuperação de desastre, que eram medidas tomadas para retomar as atividades de uma empresa em um tempo relativamente menor. O Termo continuidade de negócios surgiu a partir da recuperação de negócios, comumente abordado na década de 90. A recuperação de negócios buscava recuperar a operação do negócio após um desastre ou outra situação que a impedisse de operar. Nesta época que o termo contingência passou a ser adotado. No final da década de 90, as organizações adotaram o termo continuidade de negócio, que é dar condições para o negócio da empresa fluir independente de desastres e, caso estes ocorram, retomar as atividades em um tempo muito menor (WALLACE, 2004).

No Brasil, a gestão da continuidade de negócios é oficialmente abordada na norma da Associação Brasileira de Normas Técnicas (ABNT) de segurança da informação NBR ISO/IEC 27002:2005. A norma trata da segurança da informação como um todo, desde os critérios básicos de segurança, gestão de riscos, gestão de ativos, gestão de pessoas, segurança física, operações, acesso, desenvolvimento de sistemas, contingência, continuidade e conformidade de negócio. (NBR ISO IEC 27002, 2005)

A continuidade de negócios também é abordada pela norma internacional BS 25999, publicada pelo British Standards Institute (BSI), Instituto Britânico de Padronização. A norma compreende a continuidade de negócios como um ciclo de gestão dentro de uma organização e apresenta um conjunto de conceitos para a elaboração de um processo de gestão da continuidade de negócios. As bibliotecas de melhores práticas de gestão de serviços de TI,

Cobit e ITIL, também apresentam processos para a gestão da continuidade de negócios e apresentam técnicas para medir e controlar sua aplicação.

A gestão de riscos é oficialmente abordada na norma brasileira ABNT NBR ISO/IEC 27005:2008. A norma, reconhecida internacionalmente, apresenta as melhores práticas para a gestão de riscos em uma organização.

O problema constatado é que as empresas não estão preparadas para enfrentar desastres e não possuem os riscos de seus processos de negócio mapeados. Nos últimos anos, em indústrias de pequeno porte, ocorreram desastres que ocasionaram perda de dados e obstrução dos processos de negócio da organização. Conforme indicadores apontados na pesquisa realizada pela empresa "Regus" com diversos executivos de tecnologia da informação (TI) no mundo, publicada na página de internet da revista CIO, menos da metade das empresas estão preparadas para enfrentar situações de desastre e mesmo com riscos mapeados, não sabem como lidar com eles e o que fazer para manter o negócio operante, resultando em prejuízo ou até mesmo situações irreparáveis. (NOW! DIGITAL, 2011)

Conforme pesquisa realizada pela OS&T Informática, publicada na página de internet do grupo Convergência Digital, aplicada em empresas de médio a grande porte, são poucas as empresas que possuem um plano de continuidade de negócios implementado, e para aquelas que possuem, o investimento em continuidade é relativamente baixo em relação a seu faturamento. (CONVERGÊNCIA DIGITAL, 2011)

Dentro deste contexto, a questão desta pesquisa é buscar uma solução para apoiar as empresas de pequeno e médio porte a lidar com situações de desastre e reduzir ao máximo sua perda no caso deste através de um modelo de plano de continuidade de negócios. Como preparar as empresas para garantir a continuidade de seu negócio em situação de desastre? Como proteger a informação da organização dos riscos relacionados ao ambiente de TI? Como tratar os incidentes que interrompem os processos de negócio da organização? O que fazer em situações de desastre? Quem deve fazer o que durante a recuperação de desastres?

O Trabalho proposto é a criação de um modelo para a elaboração de um plano de continuidade de negócios aplicado a empresas de pequeno e médio porte. O escopo definido deve-se pelo fato das empresas de até médio porte se encontrarem nos níveis "inexistente" ou "inicial" do nível da continuidade de serviços de TI, conforme o COBIT e o ITIL. Este modelo consiste em um roteiro de atividades a serem seguidos e um conjunto de artefatos. As atividades envolvem o mapeamento dos riscos nos processos de negócio, a definição das ações para tratamento destes riscos, os planos de resposta a incidentes e planos de recuperação

de desastres e o processo de execução e monitoramento das ocorrências. Os artefatos gerados serão documentos do processo, incluindo o plano concreto de continuidade de negócios.

O NUSIS, Núcleo de Avaliação, Seleção, Desenvolvimento e Aplicação de Sistemas de Informação, da Universidade de Caxias do Sul (UCS), é um projeto cujo objetivo é disponibilizar sistemas de informação para utilização em empresas de pequeno porte através de desenvolvimento, implantação, consultoria e assessoria, sendo seu produto gerado de domínio público. O NUSIS busca integrar diversas áreas do conhecimento em um único trabalho, gerando um único produto, unindo alunos e professores em projetos de atuação em empresas de pequeno porte. O trabalho em questão visa criar um Modelo de Plano de Continuidade de Negócios aplicável às empresas associadas ao NUSIS (NUSIS, 2012).

Para a criação do modelo de plano de gestão de continuidade de negócios foi realizado um estudo aprofundado das Normas ABNT ISO/IEC 27002:2005, ABNT ISO/IEC 27005:2008 e BS 23999, dos padrões de riscos e continuidade abordados nas bibliotecas ITIL e Cobit, bem como em livros especializados no assunto e estudo de caso de planos de continuidade de negócios já aplicados em empresas. A partir deste estudo foi possível a elaboração de uma proposta do modelo de elaboração de um plano de continuidade.

A partir da proposta elaborada, o modelo pôde ser desenvolvido e disponibilizado na ferramenta de colaboração Microsoft Sharepoint 2010 Foundation. O modelo foi validado através do estudo de caso de sua aplicação em uma indústria de médio porte na cidade de Caxias do Sul. Uma indústria de médio porte é aquela que possui um número de funcionários superior a 100 e inferior a 500, ou que sua receita bruta anual supere R$ 3.500.000,00 (CHIAVENATO, 2011). O resultado do modelo, o plano de continuidade de negócios, foi avaliado pelo gestor de área funcional e pelo seu superior responsável através de questionário qualitativo. O modelo de plano de gestão da continuidade de negócios está disponibilizado para uso do NUSIS.

O presente trabalho divide-se em quatro capítulos. O capítulo 1 compreende a introdução do trabalho. O capítulo 2 aborda o estudo científico das normas e bibliotecas utilizadas para a elaboração do plano de continuidade de negócios. Ainda neste capítulo há uma comparação entre cada uma das bibliografias e suas contribuições para a elaboração da solução proposta.

O capítulo 3 compreende o projeto de solução proposto. Este capítulo divide-se em cinco sessões, correspondente a aplicação do trabalho, a definição do escopo para a continuidade, a análise de riscos, a elaboração do plano de continuidade e a execução e monitoramento da continuidade de negócios.

O capítulo 4 refere-se ao desenvolvimento do sistema PCN através de uma ferramenta de colaboração e ao estudo de caso de sua aplicação em uma empresa de médio porte. A partir deste capítulo é possível concluir a eficiência do modelo proposto.

2 CONTINUIDADE DE NEGÓCIOS

O Plano de continuidade de Negócios, PCN, é um conjunto de normas, operações e ações executadas pelas organizações a fim de não permitir a interrupção das atividades do negócio e proteger seus processos críticos contra falhas ou desastres significativos e, caso necessário, assegurar sua retomada em tempo hábil (BS 25999, 2006). Um desastre pode ser entendido como qualquer situação que afete os processos críticos do negócio de uma organização. Consequentemente, algumas ocorrências podem ser caracterizadas como sendo desastres para uma determinada empresa, mas podem não ser caracterizadas como um desastre para outra empresa (Wallace, 2004). Podem-se chamar de críticos aqueles processos que representam perigos sérios para a vida humana e ao ambiente, ou que colocam em risco grande quantidades de recursos. Processos críticos são aqueles cujos resultados geram maior impacto nos clientes internos e externos (ISO IEC 27005, 2005).

Há uma semelhança entre contingência e continuidade quando se fala em segurança da informação. Um plano de contingência é uma resposta formal a uma ou várias ameaças previamente identificadas. Já o plano de continuidade de negócios vai um passo além, prevendo, planejando e formalizando a restauração ou recuperação da empresa conforme tempos acordados pela organização, ao mesmo que tempo em que esta executa as ações de contingência, caso a empresa possuir um plano concreto ou não (WALLACE, 2004). Entende-se como ameaça qualquer fator externo que possa comprometer uma operação de negócio (ISO IEC 27005, 2005).

O plano de continuidade de negócios é o resultado de um processo de Gestão da continuidade de negócios (GCN). As organizações devem estar preparadas para enfrentar situações inesperadas que possam vir a interromper os serviços de TI, Tecnologia da Informação, e ativos críticos dos processos de negócio. A gestão da continuidade de negócios é responsável por organizar os recursos da organização para minimizar ao máximo as consequências de possíveis desastres. O objetivo do plano de continuidade de negócio é determinar os pontos críticos das áreas de TI relacionadas aos processos de negócio da organização. O processo de gestão da continuidade de negócios deve obter e analisar as informações para resultar em uma estratégia integrada com planos de ação correspondente para reagir a incidentes não programados, desastres, nos processos de negócio (MAGALHÃES, 2007).

Para obter os melhores resultados da GCN, a organização deve identificar seus processos e suas relações com o ambiente de TI. Conforme a GCN, os pontos críticos do

negócio podem ser a visão do negócio, compreendendo o atendimento aos clientes e o atendimento a leis e regulamentações, processos de negócio, que compreendem os processos de negócio de missão-crítica e o plano de continuidade de negócios, aplicações, que corresponde às aplicações e bases de dados, processamento de dados e procedimentos de contingência e recuperação, e de infraestrutura, referente à segurança física e lógica, comunicações, segurança da informação e redundância de hardware e software (BS 25999, 2006).

O plano de continuidade de negócios possui como parte crucial a gestão de riscos, abordada detalhadamente na sessão dois deste capítulo, pois é através dela que os riscos são identificados e geram-se os planos de ação para tratamento dos riscos. Um desastre pode ocorrer a partir da consequência de uma vulnerabilidade explorada por uma ameaça. Os planos de continuidade de negócios devem ser implementados para assegurar que ao menos as operações essenciais ao processo de negócio estejam disponíveis o maior tempo possível. Um plano de continuidade de negócios pode ser aplicado na organização toda, bem como em uma área funcional, processo de negócio ou um ativo específico apenas (NBR ISO IEC 27002 , 2005).

O trabalho proposto apresenta um modelo para a elaboração de um plano de continuidade de negócios em uma organização de pequeno ou médio porte. Para a elaboração do modelo foram realizadas pesquisas bibliográficas em livros, mas principalmente nas normas e guias de melhores práticas como as normas NBR ISO IEC 27002, NBR ISO IEC 27005, a norma internacional BS 25999, e os guias de melhores práticas de gestão de TI, ITIL e Cobit.

2.1 NORMA NBR ISO IEC 27005, GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

Para a elaboração do plano de continuidade de negócios, é necessário conhecer os riscos envolvidos. A gestão de riscos em sistemas da informação é abordada na norma brasileira NBR ISO/IEC 27005 de forma ampla e genérica, fornecendo diretrizes para o processo de gestão de riscos em segurança da informação. A norma é uma publicação da Associação Brasileira de Normas Técnicas, ABNT A gestão de riscos deve estrar alinhada com a estratégia da organização em que ela é implantada, tornando-se um processo contínuo.

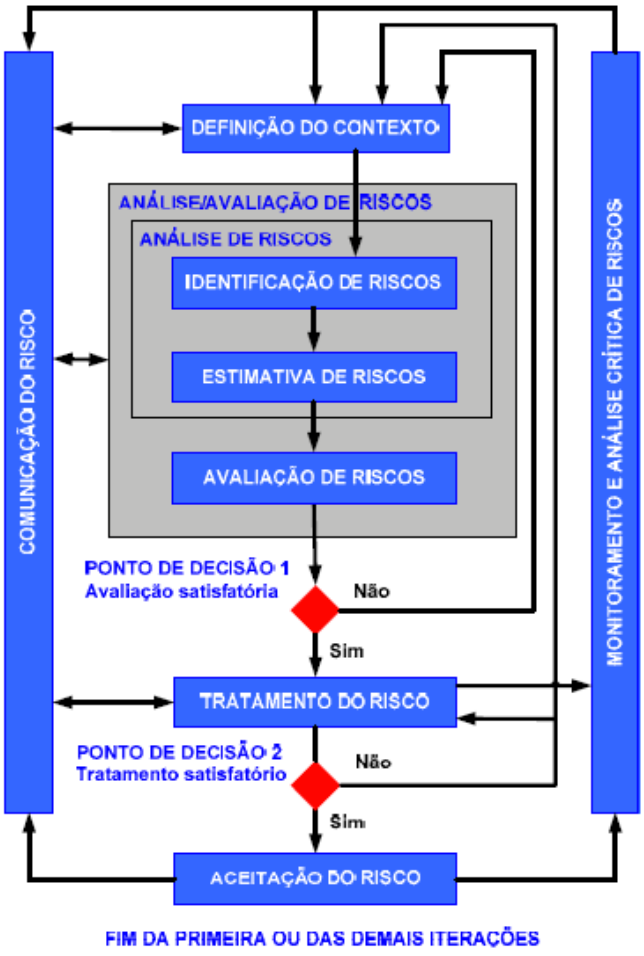
A norma NBR ISO IEC 27005:2008 é um conjunto de melhores práticas em gestão de risco reconhecido internacionalmente e compõe o conjunto de normas de segurança da informação ISO 27000 publicado pelo International Organization for Standarization (ISO) e International Electrotechnical Comission (IEC). A norma foi publicada em 2008 e reescrita em 2011 (NBR ISO IEC 27005, 2008). A norma serve como referência bibliográfica para as bibliotecas Cobit e ITIL.

Conforme a NBR ISO IEC 27005, a gestão de riscos busca prover à empresa identificação dos riscos, análise e avaliação dos riscos em função do seu impacto no processo de negócio em conjunto com a probabilidade de sua ocorrência, comunicação e entendimento da probabilidade e consequência dos riscos, estabelecimento da ordem prioritária para tratamento do risco, priorização das ações para reduzir a ocorrência dos riscos, envolvimento das partes interessadas nas decisões de gestão de riscos e comunicação entre elas, eficácia no monitoramento do tratamento de risco, monitoramento e análise crítica de riscos e do seu processo de gestão, coleta de informações de forma a melhorar a abordagem da gestão de riscos e treinamento de gestores e pessoal a respeito dos riscos e das ações para mitiga-los (NBR ISO IEC 27005, 2008).

2.1.1 Processo de gestão de riscos segundo a NBR ISO IEC 27005

O processo de gestão de riscos de segurança da informação se divide em seis partes: definição do contexto, análise e avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e monitoramento e análise crítica de riscos. Os processos não necessariamente seguem esta ordem, as atividades de análise de riscos e tratamento de riscos podem ser realizadas diversas vezes durante o processo. Essas iterações ocorrem para aprofundar e detalhar melhor o processo em cada repetição. As atividades de comunicação e monitoramento e análise seguem em paralelo com o processo geral. O processo está exemplificado na figura 1.

Figura 1: Processo da gestão de riscos



Fonte: NBR ISO IEC 27005, 2008

Conforme a ISO/IEC 27002, os controles implementados em seu escopo, limite e contexto de um plano de continuidade de negócios devem ser baseados em riscos. O processo abordado na ISO/IEC 27005 atende este requisito em diversas situações e ambientes, conforme a sua aplicação. Em um conceito de PDCA, sigla para "*Plan, Do, Check, Act*", a definição de contexto, análise e avaliação do risco, e a aceitação do risco se classificam na fase "planejar", as ações e controles necessários para atender o tratamento do risco e mitiga-los são classificados na fase "executar". A fase "verificar" do PDCA retrata a definição das necessidades de revisão das avaliações e tratamento de risco pelos gestores baseando-se nos incidentes e mudanças no ambiente. A última fase, "agir", são executadas as ações necessárias para manter e melhorar o processo de gestão de risco em segurança da informação. A tabela 1 representa as etapas do PDCA na gestão de riscos.

Tabela 1: Fases da gestão de risco conforme etapas do PDCA

Etapas do PDCA	**Processo de gestão de riscos**
Planejar	Definição do contexto Análise / avaliação de riscos Plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos

2.1.2 Definição do contexto

Esta etapa é uma definição do escopo da análise de riscos. Na definição do contexto, são identificados qual a aplicação da gestão de riscos, quais os ativos que deverão ser verificados, o limite da análise de risco, as restrições da organização e qual a equipe envolvida com suas devidas responsabilidades. A definição do escopo deve considerar os objetivos estratégicos da organização e questões que podem afetar no processo da gestão de riscos. A organização deve definir quais são os critérios que serão utilizados para identificar e avaliar os riscos.

O resultado desta etapa é o escopo da gestão de risco, suas restrições organizacionais e a equipe definida com as devidas responsabilidades e os critérios de análise e avaliação dos riscos.

2.1.3 Análise e avaliação de riscos

A etapa de análise e avaliação de riscos consiste em análise de ricos, composta pelas atividades de identificação de riscos e estimativa de riscos, e a avaliação de riscos. Esta etapa determina. Esta etapa é executada frequentemente em diversas iterações, sendo a avaliação de alto nível a primeira a ser executada para identificar os riscos de alto impacto que mereçam uma segunda avaliação mais aprofundada. As demais iterações focam-se em um nível mais baixo e nos já revelados na primeira iteração, sendo realizadas até obterem-se informações o suficiente para uma avaliação detalhada. O método selecionado para análise e avaliação de riscos fica a critério da organização.

2.1.3.1 Análise de riscos

A etapa de análise de riscos é fundamental para a elaboração de um plano de continuidade de negócios pois é através dela que são identificados os riscos que podem levar a um desastre.

A análise de riscos se inicia a partir dos critérios básicos e do escopo definido do processo que se pretende aplicar a gestão de risco. Esta etapa tem como ação a identificação dos riscos, ordenados por prioridade conforme os critérios definidos para que se possa realizar uma avaliação de riscos apropriada. Esta etapa identifica e determina o valor dos ativos da informação, identifica ameaças e vulnerabilidades existentes ou de possível existência, identifica os controles existentes e seus impactos no risco, determina as consequências e prioriza os riscos derivados ordenando-os conforme critérios de avaliação pré-estabelecidos.

A identificação dos ativos tem como objetivo classificar todos os ativos envolvidos no processo de negócio em prioridades. A partir da identificação dos ativos, deve ser realizada a identificação das ameaças relacionadas a estes ativos, as ameaças deverão ser tratadas nas etapas subsequentes. A identificação das vulnerabilidades analisa quais são os pontos dos ativos que podem ser explorados por uma ameaça, seja esta vulnerabilidade existente ou não. A identificação dos controles existentes identifica quais ações a organização já toma para tratar os riscos pré-identificados. A partir das ameaças e vulnerabilidades, devem ser identificadas as consequências da ocorrência de um risco.

Com os riscos previamente identificados, a NBR ISO IEC 27005 propõe uma atividade de estimativa de riscos, para avaliação das consequências e de suas probabilidades. Estas atividades servem para estimar um nível de risco baseado na consequência e sua probabilidade de ocorrência. Para a estimativa do risco, pode ser utilizada a abordagem qualitativa, classificando os riscos como alto, médio e baixo, ou a abordagem quantitativa, atribuindo valores numéricos para os riscos.

2.1.3.2 Avaliação de riscos

A avaliação de riscos compreende atribuir comparações dos riscos identificados na análise de riscos com os critérios de avaliação e de aceitação de risco. Nesta etapa são analisados os riscos identificados na análise de riscos e então avaliados conforme os critérios estabelecidos pela organização na definição do escopo. O nível de risco estabelecido na

estimativa é revisto e devidamente avaliado. A avaliação de riscos usa o conhecimento do risco identificado na análise de riscos para a tomada de decisões sobre ações futuras, tomando a decisão do empreendimento de uma atividade e quais as prioridades para o tratamento do risco, levando em consideração os níveis estimados de risco.

O Resultado desta etapa é a lista de riscos avaliados e com o nível de risco estabelecido para direcionar as ações de tratamento do risco.

2.1.4 Tratamento do risco

O processo de tratamento do risco inicia-se a partir da lista de riscos ordenados por prioridades, resultado da análise e avaliação dos riscos, associadas aos cenários de incidentes relacionados. A atividade tem como objetivo a definição de controles para reduzir, reter, evitar ou transferir os riscos, juntamente com a definição de um plano de tratamento do risco. O resultado do tratamento de risco é o plano de tratamento de risco e uma relação dos riscos residuais. Existem quatro formas de tratar os riscos segundo a NBR ISO IEC 27005, que são a redução do risco, a retenção do risco, evitar o risco e a transferência do risco.

A redução do risco é um conjunto de ações que visam reduzir seu nível de risco, reduzindo sua probabilidade de ocorrência ou a sua consequência. As ações de redução do risco devem ser elaboradas conforme as restrições da organização definidas do escopo.

A retenção do risco consta em definir o risco da forma que está tratado, sem decisões adicionais, baseando-se na avaliação de riscos, é muito semelhante à aceitação do risco. Se um risco atende os critérios de aceitação, não há por que executar controles desnecessários.

A ação de evitar o risco é conter a atividade que inicia um risco para não ser executada. Esta opção deve ser tomada quando o risco identificado é considerado extremamente alto, tornando-se necessário evita-lo por completo. As ações para evitar o risco podem ser muito custosas, porém se há uma probabilidade mediana de ocorrência devem ser adotadas.

A transferência do risco é a terceirização de um risco para entidades que possam gerenciá-lo de maneira mais eficaz. Estas ações devem ser tomadas com base nas restrições organizacionais definidas no escopo. Com a transferência do risco para terceiros, a responsabilidade por seu tratamento varia conforme acordo formado com terceiros, porém a responsabilidade legal continua sendo da organização.

2.1.5 Aceitação do risco

Esta etapa consiste em analisar os controles sugeridos no tratamento do risco e sujeita-los à aprovação dos gestores da organização. A decisão de se aceitar os riscos deve ser devidamente registrada formalmente juntamente com a sua responsabilidade. O objetivo desta etapa é a aceitação do tratamento do risco proposto ou dos riscos residuais. Os critérios de avaliação podem ser muito mais complexos do que aparentam, em alguns casos, o risco residual pode não atender os critérios de aceitação pois no momento não levam em conta as circunstancias predominantes, cita-se como exemplo o custo comparado com o momento financeiro da organização.

Toda e qualquer decisão tomada a respeito de um risco ou tratamento do mesmo deverá ser analisada profundamente pelos gestores e estressadas ao máximo antes de ser realizada. O resultado desta etapa é uma lista com os riscos aceitos e com as devidas justificativas para os que não forem aprovados

2.1.6 Comunicação do risco

A comunicação é uma etapa crucial na gestão de riscos, executada paralelamente com as demais atividades, visa compartilhar as informações do processo de gestão de risco entre os tomadores de decisão e as demais partes envolvidas. Uma comunicação bem realizada pode indicar o sucesso de um processo de gestão de riscos, certificando de que todas as ações realizadas estejam sob ciência de todos os envolvidos, evitando desencontro de informações.

Para aperfeiçoar a comunicação e tirar maior proveito da mesma é essencial a criação de um plano de comunicação, tanto para acompanhamento das atividades rotineiras quanto para a comunicação de emergências. A comunicação deve ser transparente entre todos os envolvidos para melhor desempenho em caso de situações de desastre. O resultado desta etapa é o entendimento continuo do processo pelos envolvidos e pelos gestores.

2.1.7 Monitoramento e análise crítica de riscos

Os riscos dificilmente permanecem estáticos, esta etapa serve para monitorar os fatores como valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de

ocorrência dos riscos mapeados a fim de identificar mudanças no processo. O monitoramento é importante para evitar que ameaças aumentem o nível de riscos considerados pequenos. Todos os riscos devem ser considerados individualmente e em conjunto, pois o impacto agregado pode resultar em uma consequência maior.

O resultado desta atividade pode fornecer dados para uma análise crítica dos riscos, que deve ser realizada periodicamente conforme as mudanças vão ocorrendo, este resultado é o alinhamento contínuo da gestão de riscos com os objetivos de negócio da organização e dos critérios de aceitação do risco.

2.2 ISO IEC 17799 e ISO IEC 27002

No Brasil, a gestão da continuidade de negócios é oficialmente abordada na norma ABNT de segurança da informação ABNT NBR ISO/IEC 17799:2005 e na sua edição mais nova, a NBR ISO IEC 27002. A norma trata da segurança da informação como um todo, é dividida em onze seções: política de segurança da informação, organizando a segurança da informação, gestão de ativos, segurança em recursos humanos, segurança física e do ambiente, gestão de operações e comunicações, controle de acessos, aquisição, desenvolvimento e manutenção de sistemas de informação, gestão de incidentes de segurança da informação, gestão da continuidade do negócio e conformidade. Por se tratar de uma norma técnica, a ISO IEC 27002 tende a abranger diversos cenários possíveis, podendo ser aplicada em diferentes organizações com realidades financeiras e processos distintos, o seu processo é definido pela organização e deve ser seguido à risca e anualmente auditado para garantir a certificação da mesma (NBR ISO IEC 27002, 2005).

A norma divide a continuidade de negócio em seis subseções com diretrizes para a elaboração de um plano de continuidade: aspectos da gestão da continuidade de negócios relativos à segurança da informação, incluindo segurança da informação no processo de gestão de continuidade de negócios, continuidade de negócios e análise e avaliação de riscos, desenvolvimento e implementação de planos de continuidade relativos à segurança da informação, estrutura do plano de continuidade de negócio e testes, manutenção e reativação dos planos de continuidade do negócio.

2.2.1 Aspectos da gestão da continuidade do negócio relativos à segurança da informação

O plano de continuidade de negócios é um conjunto de ações que uma organização realizada para evitar a interrupção do seu processo de negócio, reduzir a probabilidade de desastres e , caso ocorram, se recuperar de desastres em um tempo hábil aceitável pela organização. O plano de continuidade de negócios possui como parte crucial a gestão de riscos, pois é através dela que os riscos são identificados e geram-se os planos de ação para tratamento dos riscos. Um desastre pode ocorrer a partir da consequência de uma vulnerabilidade explorada por uma ameaça, é muito importante que as consequências de um desastre estejam devidamente documentadas e analisadas de maneira crítica. Um plano de continuidade de negócios pode ser aplicado na organização toda, bem como em uma área funcional, processo de negócio ou um ativo específico apenas.

2.2.2 Incluindo segurança da informação no processo de gestão de continuidade de negócios

O processo de gestão de continuidade de negócios tem como artefato os planos de continuidade de negócio, todo processo deverá seguir os requisitos de segurança da informação e se basear nos princípios da organização. O plano de continuidade deve levar em consideração a gestão de riscos, as restrições da organização como situação financeira, aspectos culturais e recursos humanos. A gestão do processo de continuidade de negócios deve ser atribuída a um nível que possua autonomia adequada para tomar as ações.

2.2.3 Continuidade de negócios e análise e avaliação de riscos

A análise e avaliação de riscos ocupam uma importância muito grande na gestão de continuidade de negócios, ela visa identificar os e ventos que podem ocasionar interrupção no processo de negócio. Todo processo de continuidade de negócios é baseado na gestão de riscos em segurança da informação, ela é responsável por identificar os ativos do processo de negócio, as vulnerabilidades, as ameaças, as probabilidade, as consequências e os cenários de incidente possíveis. A gestão do risco ainda é responsável por prover o tratamento do risco e sua aceitação perante a gestão da organização. O artefato gerado da gestão de riscos, o plano

de tratamento do risco, é essencial para o processo de gestão de continuidade de negócios. A partir da gestão do risco, deve ser realizada uma análise do que foi identificado e determinado a probabilidade e o possível impacto das interrupções, tanto em termos de escala quanto em relação ao período de recuperação.

Toda e qualquer avaliação de risco deve ser acompanhada pelos responsáveis pelos processos de negócio que estão em análise. A análise não deve se limitar aos recursos de processamento, mas também deve levar em consideração fatores de segurança como pessoas, capacidade técnica, controle de acessos, entre outros. A junção de diferentes riscos é muito importante, pois um processo pode afetar diretamente o outro, a análise deve priorizar os riscos baseados na criticidade dos processos e nos objetivos da organização, incluindo recursos críticos, impactos, possibilidade de ausência de tempo e prioridade de recuperação. Em função dos resultados da gestão do risco, deve ser desenvolvido um plano estratégico para determinar a abordagem a ser adotada na continuidade dos negócios. Uma vez criada, a estratégia deve ser validada pela direção para a elaboração de um plano de implementação desta estratégia.

2.2.4 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

Os planos de continuidade desenvolvidos devem ser implementados para a manutenção ou recuperação dos processos críticos e assegurar a disponibilidade dos mesmos no nível acordado e em tempo aceitável em situações de desastre.

O plano de continuidade deve levar em consideração questões como a definição das responsabilidades de cada envolvido nas ações, a definição de um desastre, a implementação de controles para tratar os riscos e ações para recuperar a operação de negócio, os procedimentos operacionais envolvidos, a documentação dos processos e a disseminação da cultura na organização.

Todo o processo de planejamento deve focar nos objetivos de negócio e ter suas ações identificadas com os prazos acordados, este processo deve identificar os recursos necessários para realizar estas ações, como pessoas ou ferramentas. Os procedimentos de recuperação devem conter todo o detalhamento das operações a serem realizadas tanto internamente quanto por equipes terceirizadas, em caso de terceirização, deve haver um contrato de atendimento com o fornecedor para que o processo de recuperação não sofra

quaisquer atrasos. O plano de continuidade deve conter uma análise crítica das vulnerabilidades da organização e os planos para seu tratamento, encontrados também na gestão de riscos.

Da mesma forma que os dados críticos da organização devem estar armazenados em locais seguros, os planos de continuidade e os recursos necessários para ativá-los também devem ser protegidos e atualizados para que no momento de sua ativação possam estar sempre disponíveis, as melhores práticas indicam o seu armazenamento em locais distantes da organização. Em situações de armazenamento alternativo, devem ser aplicados os mesmos requisitos de segurança do ambiente de produção.

2.2.5 Estrutura para um plano de continuidade de negócio

Para a criação de planos de continuidade de negócios deve-se criar e manter uma estrutura básica para eles. Cada plano de continuidade deve descrever o seu enfoque, seja qual ele for, e também quais as condições necessárias para sua ativação, quem são os responsáveis por suas atividades. Novos requisitos deverão ser ajustados nos planos conforme forem surgindo. É importante que cada plano possua um gestor específico e a responsabilidade de executar os procedimentos de emergência, recuperação, planejamento e planos de reativação sejam de responsabilidade deste gestor. O gestor deve saber delegar as tarefas e gerenciar que tudo seja cumprido conforme estabelecido nos planos.

2.2.6 Testes, manutenção e reativação dos planos de continuidade do negócio

Para um plano de continuidade de negócios ser realmente eficiente, este precisa ser testado e atualizado regularmente. Os testes de um plano de continuidade de negócios devem assegurar que todos os membros da equipe e demais envolvidos relevantes estejam conscientes dos planos e de suas responsabilidades, conhecendo e dominando suas atividades em caso de emergência. Os testes devem mapear quando e como cada membro deverá agir.

A responsabilidade para análises críticas deve ser definida, todas as mudanças nas atividades do negócio que ainda não tenham sido contempladas devem ser inseridas nos planos seguidas de uma atualização apropriada das atividades. Este processo de mudanças deve ser estabelecido através de um controle formal, assegurando que toda mudança passe por todos os envolvidos e devidamente analisados.

2.3 BS 25999-1

A norma BS 25999 foi desenvolvida pela British Standards Institute (BSI), em 2006, com o intuito de criar padrões para o gerenciamento da continuidade de negócios, de sigla GCN. A norma se divide em duas partes, a BS 25999-1, que apresenta as normas e melhores práticas para a criação de um processo de gestão da continuidade de negócios, e a BS 25999-2 que apresenta as especificações obrigatórias para a certificação em gestão da continuidade de negócios adequada à dimensão da organização. O objetivo da continuidade de negócios segundo a BS 25999 é reduzir os prejuízos causados por desastres, protegendo seu pessoal, preservando a reputação da organização e provendo ações que permitam que a operação continue em operação (BS 25999, 2006).

As organizações que possuem dependência de seus processos de TI precisam, de alguma forma, ter a preocupação em mantê-lo operando durante todo o seu período de trabalho. A gestão da continuidade de negócios possui três fundamentos que são melhorar a resistência de uma organização frente a desastres que causem interrupções em seu processo de negócio, fornecer uma metodologia para recuperar suas operações em situações de desastre com interrupção e comprovar a sua capacidade de gerenciar as interrupções de negócio. A GCN, gestão da continuidade de negócios, é um guia de riscos e seus respectivos tratamentos, englobando dois programas, o programa de recuperação de desastres, focado na infraestrutura de TI, e o plano de continuidade de negócios que identificam riscos que possam prejudicar as operações da organização e estabelece seu devido tratamento.

Segundo a BS 25999, a gestão da continuidade de negócios se baseia em três características, disponibilidade, confiabilidade e recuperação. A disponibilidade, que é a capacidade do ambiente de produção se manter disponível para uso dos seus usuários o maior tempo possível através do uso de tecnologias de proteção, redundância e replicação de dados. A confiabilidade trata as ações previsíveis e a garantia de retorno rápido dos recursos de TI em situações de desastre. A recuperação é a opção mais rigorosa, compreende proteção e cópias de seguranças dos dados para situações de recuperação completa ou parcial do ambiente tecnológico.

A primeira parte da norma BS 25999 compreende as melhores práticas para o gerenciamento da continuidade de negócios. Segundo a norma, o processo de gestão da continuidade de negócios deve compreender um ciclo de vida composto por seis etapas, conforme a figura 2: gestão do programa de GCN, entendendo a organização, determinando a estratégia da continuidade de negócios, desenvolvendo e implantando uma resposta de GCN,

testando, mantendo e analisando os preparativos de GCN e incluindo a GCN na cultura da organização.

Figura 2: Ciclo de vida da gestão da continuidade de negócios

Fonte: BS 25999, 2006.

2.3.1 Gestão do programa de GCN

A primeira etapa do ciclo é a gestão do programa, onde são definidas as responsabilidades pela implementação da gestão da continuidade de negócios. Nesta etapa é nomeado um gestor responsável por todo o processo de implementação e é elaborada uma política com diretrizes básicas, definição do escopo e alocação dos recursos envolvidos. A gestão deve compreender não só a implantação do GCN mas também a sua manutenção e melhoria contínua.

2.3.2 Entendendo a organização

A segunda etapa do ciclo compreende o entendimento dos processos da organização que serão abordados no GCN. Nesta etapa é realizada uma análise de impacto onde são identificados os processos fundamentais e as atividades de TI que suportam estes processos, estimando o tempo necessário de recuperação em situação de desastre. Outra atividade fundamental desta etapa é a análise de riscos dos processos que estão sendo tratados pelo GCN, visando identificar, analisar e avaliar as ameaças que podem explorar vulnerabilidades resultando na interrupção dos processos organizacionais. Na análise de riscos deve-se levar

em consideração o impacto que um risco pode levar à organização em caso de ocorrência, esta análise é essencial para determinar o período de interrupção máximo tolerável e os tempos e recursos necessários para sua recuperação.

2.3.3 Determinando a estratégia da continuidade de negócios

Na terceira etapa do ciclo, a organização deve definir uma série de estratégias e procedimentos a serem seguidos em caso de uma interrupção. Com todas as estratégias possíveis identificadas, devem ser selecionadas as que melhor se aplicam ao processo contemplado no GCN a fim de permitir que a organização tenha o menor tempo de interrupção possível. A escolha das melhores estratégias devem considerar os recursos da organização como pessoas, tecnologias, instalações, informações, suprimentos, o seu tempo de implementação e ativação e os custos envolvidos. Nas estratégias são descritos métodos de operação alternativos para atender a necessidade de operação durante ou após um desastre, além de métodos para proteger os processos críticos previamente identificados e mitigar os riscos. As estratégias englobam o nível corporativo, sendo muito importante a questão de tempo de restauração para cada atividade.

2.3.4 Desenvolvendo e implementando uma resposta de GCN

Após a definição da estratégia, a organização deve operacionaliza-la através da criação de um plano operacional de resposta para os incidentes que atenda as expectativas dos gestores e o que foi acordado na análise de impacto ao negócio. Este plano operacional deve conter as atividades que serão realizadas, identificando os recursos tecnológicos, os responsáveis pelas atividades, o procedimento de ativação e manutenção do plano. Como todo processo organizacional, deve ser definido um responsável por manter e atualizar o plano regularmente levando em consideração novos riscos e alterações no ambiente, bem como se responsabilizar pela comunicação do desempenho do processo com os gestores do processo de negócio. O objetivo dos planos de resposta é lidar com o maior número possível de tipos de interrupção, independente de sua origem e com isso minimizar ou evitar interrupções nos processos de negócio.

2.3.5 Testando, mantendo e analisando os preparativos de GCN

O ciclo de continuidade de negócios contém uma etapa para validar e manter os processos implantados de GCN. A organização deve criar uma agenda de testes para a simulação de situação de desastre envolvendo todos os responsáveis pelas atividades do plano de continuidade. Os resultados dos testes devem passar por análise crítica e gerar informações para manutenção e melhorias nos processos de resposta. Esta etapa do processo também deve definir o processo de auditoria para verificar as conformidades do GCN de acordo com a legislação, padrões ou certificações caso sejam aplicáveis.

2.3.6 Incluindo a GCN na cultura da organização

Como parte que envolve todo o ciclo de vida do processo de GCN, a conscientização dos colaboradores no que diz respeito à continuidade de negócios é essencial para um melhor desempenho do plano de continuidade. A organização deve adotar a continuidade como valor básico e parte de seu processo de gestão. A disseminação desta cultura pode ser realizada através de treinamentos, conscientização e da simulação de situações de desastres com intuito de mostrar aos colaboradores o impacto da falta da gestão de continuidade em caso de desastre.

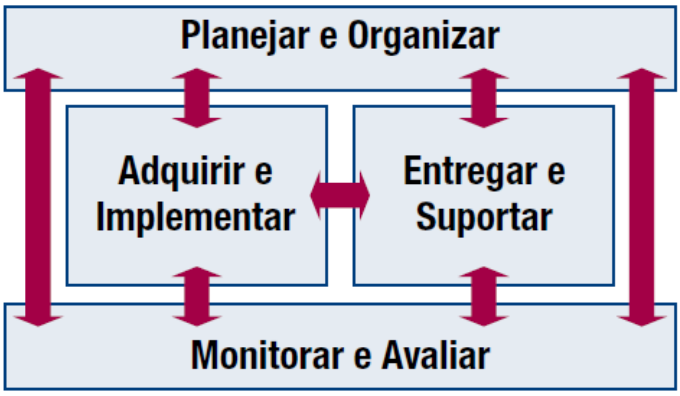
O sumário executivo, é um resumo de toda a definição da continuidade. Este sumário deve ser apresentado para os gestores e patrocinadores, portanto deve ser escrito de forma clara sem a utilização de termos técnicos de TI. O sumário executivo se inicia com a definição da continuidade de negócios, onde devem constar exemplos de situações de risco que podem prejudicar a organização, qual é o objetivo em se implantar a continuidade de negócios e a descrição das fases da implantação da continuidade de negócios na organização.

A norma BS 25999 deve ser considerada por organizações que procuram criar um processo de gestão da continuidade de negócios. A GCN deve ser definida dentro da própria organização e estar alinhada com o planejamento estratégico e com a gestão e risco. A norma BS 25999 pode ser utilizada tanto para processos de TI quanto para outros processos organizacionais. A elaboração do GCN irá resultar na criação de um ou mais planos de continuidade de negócios.

2.4 COBIT – CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY

O Control Objectives for Information and Related Technology (COBIT), é um guia com as melhores práticas de gerenciamento da governança de tecnologia da informação criado pelo Information Systems Audit and Control Association (ISACA). O Cobit se divide em quatro domínios: Planejamento e organização, aquisição e implementação, entregar e suportar e monitoração e avaliação, conforme ilustrado na figura 3 (COBIT, 2007).

Figura 3: Os quatro domínios inter-relacionados do Cobit



Fonte: Cobit, 2007

O Cobit tem sua aplicação baseada em níveis de maturidade, cada um de seus processos pode ser avaliado conforme sua aplicação na organização. O Cobit também fornece técnicas para medição e monitoramento de cada um de seus processos, define os responsáveis pelas atividades conforme as melhores práticas de mercado.

O gerenciamento da continuidade de serviços de TI é abordado dentro do seu domínio de entrega e suporte. O domínio de entrega e suporte tem como objetivo assegurar que os serviços de TI estejam disponíveis conforme definido em um nível de serviço. O Cobit também possui um conjunto de melhores práticas para o gerenciamento de riscos de TI, abordadas no domínio planejar e organizar.

2.4.1 Definir e gerenciar níveis de serviços

Para compreender a continuidade de negócios, os serviços de TI devem possuir um acordo de níveis de serviço, Service Level Agreement (SLA). O acordo de nível de serviço é

uma definição de tempo para que os serviços de TI, sejam quais eles forem, possam ser executados a fim de comprometer o mínimo possível os processos de negócio da organização. Este processo deve ser documentado e incluso nos planos de continuidade de negócios, sendo seu monitoramento e relatório de desempenho partes importantes na avaliação do serviço.

O processo de definição e gerenciamento de níveis de serviço deve assegurar o alinhamento dos principais serviços de TI com a estratégia de negócio, possuindo foco em identificar os requisitos de serviço, acordar os níveis de serviço e monitorar o atendimento desses níveis de serviço. Para realizar este processo, é importante que haja a formalização de acordos de níveis de serviços internos e externos alinhados com os requisitos e com a capacidade de entrega dos mesmos, reporte do atendimento aos níveis de serviços acordados, através do plano de comunicação, identificação e comunicação de requisitos de serviços novos e atualizados para o planejamento estratégico.

São resultados do processo o catálogo de serviços, essencial para determinar os processos para a continuidade de negócios, o relatório de desempenho de processos, podendo medir o atendimento dos serviços envolvidos na continuidade, requisitos novos ou atualizados de serviços, fornecendo informação de novos serviços e tecnologias que poderão ser abordadas no processo de continuidade de negócios, os SLAs, que são chave para determinar o tempo de recuperação dos serviços de TI em caso de situação de desastre, e os acordos de níveis operacionais, Operational Level Agreement (OLA), que servem como roteiro operacional para executar as atividades de recuperação e continuidade.

2.4.2 Assegurar a continuidade dos serviços

O processo de assegurar a continuidade dos serviços, abordado no domínio “Entregar e suportar”, deve garantir um impacto mínimo nos negócios em caso de desastre tendo foco em incorporar a capacidade de recuperação através de soluções automatizadas e de planos de continuidade de negócios. Para alcançar a continuidade deve-se desenvolver, manter e melhorar a contingencia de TI, treinar e testar os planos de contingencia, manter uma estrutura de armazenamento de cópias de segurança dos dados e dos planos de contingencia em ambientes remotos.

O processo de assegurar a continuidade de serviços de TI compreende atividades como a análise de impacto e avaliação de riscos, elaboração e manutenção dos planos de continuidade, identificação de recursos necessários para a recuperação de desastres, realização

de testes e promoção de melhorias a partir destes, planejamento e implementação de controles de cópias de segurança e elaboração e manutenção de procedimentos de revisão do processo de continuidade.

A continuidade de serviços pode ser mensurada pela quantidade de horas perdidas pelos usuários devido à inoperância não planejada de sistemas em um mês, pela quantidade de processos críticos de negócio dependentes de TI não contemplados nos planos de continuidade, o percentual de SLAs de disponibilidade alcançados, a quantidade de processos críticos de negócio cobertos pelo plano de continuidade, o percentual dos testes de recuperação bem sucedidos e a frequência de interrupção dos serviços nos sistemas críticos.

2.4.3 Avaliar e gerenciar os riscos de TI

O Cobit possui um guia de melhores práticas para criar e manter uma estrutura de gestão de risco. O processo de gerenciamento dos riscos de TI é uma documentação do nível comum acordado dos riscos de TI, suas estratégias de mitigação e seus riscos residuais. Qualquer evento que cause um impacto no processo de negócio da organização deve ser identificado, analisado, avaliado e então elaboradas as estratégias de mitigação do risco a níveis aceitáveis. Todo resultado deve ser avaliado pelas partes interessadas e expressos em termos financeiros para que o risco seja alinhado à condição da organização.

Avaliar e gerenciar os riscos de TI é analisar e comunicar os riscos do ambiente de TI e seus possíveis impactos nos processos de negócio buscando desenvolver um processo de gerenciamento de riscos alinhado ao negócio que contemple a identificação, avaliação, mitigação e comunicação dos riscos. O gerenciamento dos riscos de TI é atingido pela garantia da integração do gerenciamento com os processos de negócio, a realização das avaliações do risco e a elaboração e decisão dos planos de ação para tratamento dos riscos.

O processo de avaliação e gerenciamento dos riscos de TI é formado por diversas atividades como promover o alinhamento da gestão de riscos de TI com os processos de negócio, identificar os objetivos de TI e estabelecer o contexto de risco, identificar eventos associados a TI e ao negócio, avaliar criticamente os riscos, avaliar as respostas aos eventos, planejar e priorizar as atividades de tratamento de risco, aprovar e assegurar o financiamento dos planos de tratamento de riscos e manter e monitorar os planos de tratamento dos riscos.

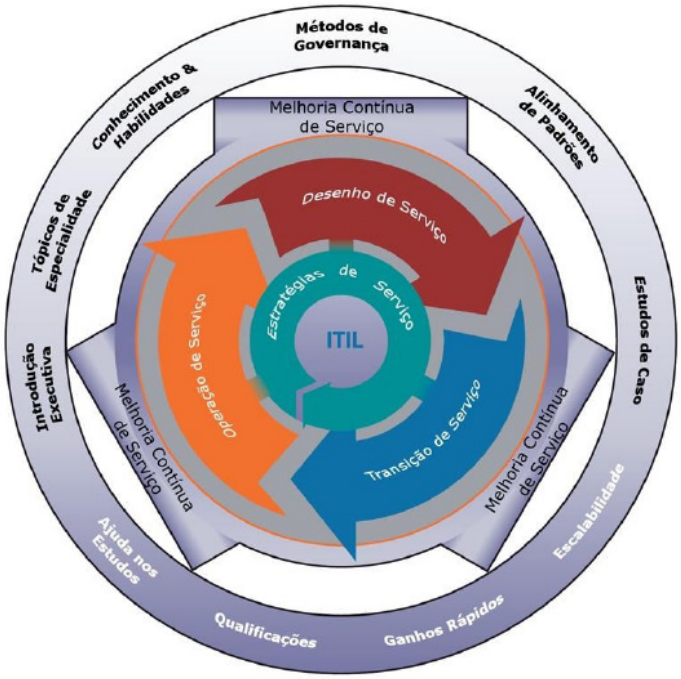
O processo tem como indicadores de desempenho o percentual dos serviços de TI cobertos pela avaliação de risco, o percentual de riscos críticos identificados e que haja

tratamento, o percentual dos planos de tratamento aprovados para implementação e a quantidade de desastres causados por riscos não mapeados.

2.5 ITIL – INFORMATION TECHNOLOGY INFRA-STRUCTURE LIBRARY

O Information Technology Infrastructure Library (ITIL), é um conjunto de melhores práticas da gestão de serviços de TI, criado pelo Office of Government Commerce (OGC), Câmara de Comércio Britânico, nos meados da década de 80. O ITIL foi reformulado no ano de 2002 e passou a ser adotado com maior frequência, sendo dividida em oito volumes: Suporte aos serviços, entrega de serviços, planejamento e implementação, gerenciamento de aplicações, gerenciamento de segurança, gerenciamento da infraestrutura de TI e de comunicações, perspectiva do negócio e gerenciamento dos ativos de software. Em 2007, o ITIL sofreu nova revisão e passou a abordar a gestão do serviço através de um ciclo de vida do serviço. A terceira versão do ITIL dividiu o modelo em cinco livros: Estratégia de serviços, desenho de serviços, transição de serviços, operação de serviços e melhoria continua de serviços, conforme ilustrado na figura 4 (ITIL, 2007).

Figura 4: Visão geral do ciclo de vida da biblioteca das melhores práticas ITIL v3



Fonte: ITIL, 2007

No ITIL, tratando-se de plano de continuidade, três processos são de suma importância para a elaboração do plano de continuidade. A gestão da continuidade de serviços é abordada no desenho de serviços, possuindo um processo detalhado de continuidade. O gerenciamento do nível de serviço, que fornece suporte para a continuidade, também abordado no desenho de serviços. O processo de gerenciamento de incidentes é abordado nas operações de serviço. O ITIL não possui um processo definido para a gestão de riscos.

2.5.1 Gerenciamento de nível de serviço

O gerenciamento do nível de serviço é um processo fundamental do desenho de serviço. É neste processo que são alinhadas as necessidades do cliente com os serviços prestados e então estes são negociados, acordados e documentados. Objetivo do gerenciamento do nível de serviço é determinar acordo de nível de serviços, SLAs, o que é uma garantia de que um serviço será executado de uma forma dentro de um período de tempo aceitável. Os SLA são base para todos os processos do ITIL. O processo traz benefícios tanto para o cliente, que sabe o que pode esperar e exigir do prestador de serviço, e para o prestador, que saberá exatamente o que deve entregar e quando executá-lo. É de extrema importância que o nível de serviço seja especificado corretamente para garantir uma melhor entrega.

Os objetivos do processo de gerenciamento de nível de serviço são desenvolver relações de negócio, onde são negociados e acordados os requisitos anuais e os requisitos de nível de serviço para requisitos futuros, desenvolver e gerenciar as metas estabelecendo os acordos de nível operacional, OLAs, com as demais áreas da organização, revisar contratos de terceiros para avaliar as metas de fornecedores, prevenir pró ativamente falhas nos serviços, reportar e gerenciar serviços e elaborar o plano de aperfeiçoamento de serviço para gerenciar, planejar e implantar melhorias nos serviços e processos.

2.5.2 Gerenciamento da continuidade dos serviços de TI

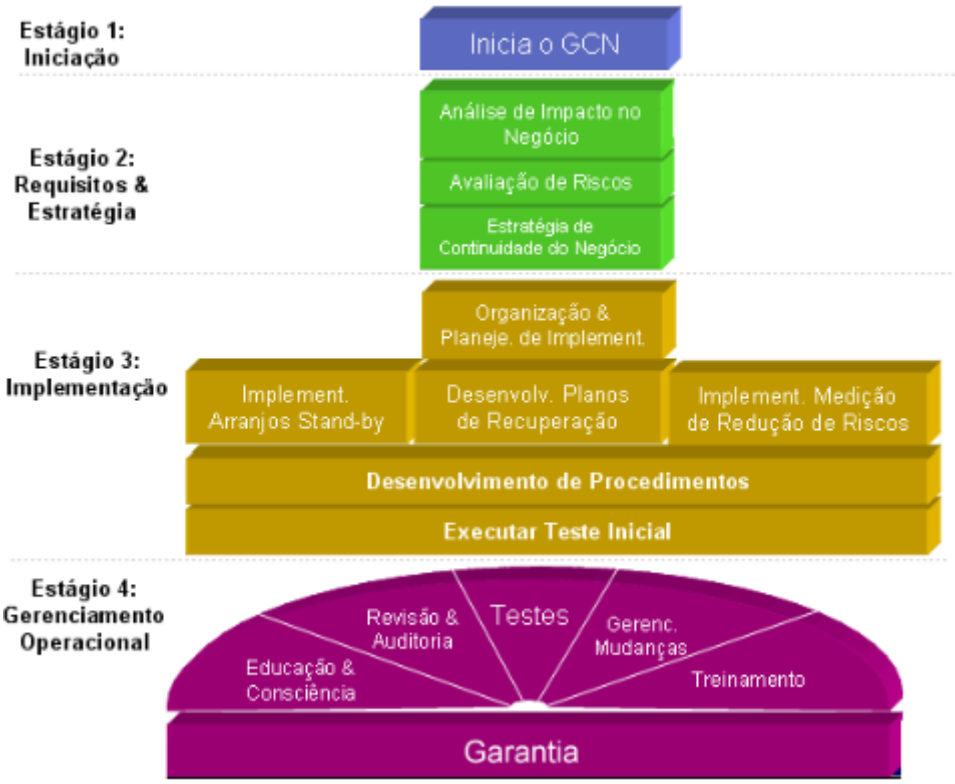
Os objetivos do processo de gerenciamento de continuidade de serviços de TI (GCSTI), são desenvolver e manter os planos de continuidades de serviços de TI e suas ações de recuperação, realizar revisões regulares da análise dos riscos que impactam o negócio e atualizar seus planos de continuidade, aconselhar às demais áreas de negócio a importância da

continuidade de negócios, garantir que os mecanismos de continuidade e recuperação são eficientes em situações de desastre e operem dentro dos SLA definidos, avaliar o impacto das alterações nos planos de continuidade, assegurar medidas proativas parar otimizar a disponibilidade de serviços conforme custo e benefício e negociar os contratos necessários para atender os requisitos de recuperação para dar suporte em situações de desastre.

O foco do gerenciamento da continuidade de serviços são os eventos que podem interferir de maneira drástica no processo de negócios, um desastre, podendo variar de organização para organização. Eventos com menor impacto são lidados no processo de gerenciamento de incidentes. O impacto de um desastre com perda de serviços é medido através de análise de impacto, parte do processo de gestão de riscos.

O ITIL define um fluxo de atividades para a continuidade de serviços, ilustrados na figura 5. São quatro estágios: iniciação, requisitos e estratégia, implementação e gerenciamento operacional.

Figura 5: O processo de gerenciamento da continuidade de negócios



Fonte: ITIL, 2007

O ciclo de vida da continuidade se inicia na fase de iniciação, nesta fase deve-se estabelecer uma política para os planos de continuidade, estabelecer o escopo que os planos

terão e se iniciar um projeto para o desenvolvimento dos planos. Este processo contempla a organização como um todo.

A segunda fase, requisitos e estratégia, é quando se define a estratégia de continuidade do negócio, nela são realizadas as atividades de análise de impacto do negócio, a avaliação de riscos e a estratégia de continuidade dos serviços de TI.

A terceira fase, de implementação, é a etapa em que se desenvolvem os planos de continuidade de negócio, os planos de recuperação de desastre e se testa a estratégia. Nesta fase são criados os planos para implantar o processo de continuidade como os procedimentos de emergência, avaliação de danos, planos de recuperação, entre outros. Também são abordados nesta fase a implantação de medidas para a redução dos riscos e acordos para atender os requisitos de disponibilidade.

O plano de continuidade de serviços de TI é desenvolvido nesta fase, incluindo o plano de recuperação. Este plano deve incluir o seu período de atualização, a lista dos responsáveis para definir as ações, a iniciação da recuperação e o grupo de especialistas para cobrir as ações e suas responsabilidades. Estes envolvidos podem ser internos ou terceirizados, conforme a politica da organização. Os testes iniciais são executados nesta fase com objetivo de garantir que a estratégia implantada é eficiente em situações de desastre.

Como todo processo do ITIL, a ultima fase do ciclo é o gerenciamento operacional, são práticas cabíveis a educação, conscientização e treinamento dos envolvidos, buscando capacitar a equipe em operar os planos e lidar com as situações de desastre, a revisão e auditoria, os testes e simulações, contemplando não apenas a eficácia mas sim como a equipe se comportará em situações de desastre e como utilizar os recursos, o gerenciamento da mudança, procurando identificar as alterações de processo e de tecnologia que influenciam na continuidade de serviços de TI, e por último a garantia de que o processo está atingindo os requisitos de negócio de forma satisfatória.

O GCSTI pode ser medido em duas situações, durante a operação normal e durante / após um desastre. Em situações de operação normal são métricas os resultados dos testes feitos no plano e o custo do processo. Em situações de desastre pode-se avaliar os pontos fracos no plano, o tempo de recuperação em comparação com o tempo estimado e as perdas devido ao desastre.

O GCSTI possui diversas funções, conforme o ITIL, o papel responsável pela continuidade é o gerente de continuidade de serviços. Este responsável possui papéis diferentes em situações rotineiras e em situações de desastre. O gerente tem como responsabilidade desenvolver, implantar e manter o processo de gerenciamento da

continuidade do serviço conforme os SLA definidos, assegurar de que todos os envolvidos estejam preparados para situações de desastre, ajudar na execução da análise de riscos dos serviços existentes e de novos a serem implantados, gerenciar os testes de TI para todos os planos de continuidade, gerenciar os serviços de TI entregues durante o período de crise e avaliar as mudanças do ambiente e seus impactos nos planos de continuidade de negócio.

2.5.3 Gerenciamento de incidentes

O processo de gerenciamento de incidentes lida com todos os incidentes. Entende-se como incidente as falhas nos serviços de TI que impactam no processo de negócio. A meta deste processo é restaurar o serviço de acordo com os SLA definidos no gerenciamento de nível de serviço minimizando o impacto nas operações de negócio. O escopo deste processo inclui qualquer evento que possa interromper um serviço de TI, incluindo eventos conhecidos ou não e problemas identificados no gerenciamento de problemas.

O processo de gerenciamento de incidente consiste de nove etapas: a identificação do incidente, o registro do incidente, a classificação do incidente, a priorização do incidente conforme seu impacto no processo de negócio, o diagnóstico do incidente, a escalação ou transferência do incidente, a investigação e diagnóstico, a resolução e recuperação, e o encerramento da demanda do incidente.

O gerenciamento de incidentes deve levar em consideração os limites de tempo conforme o seu SLA, os modelos de incidente e as operações necessárias para trata-los, e incidentes graves, com maior impacto no processo de negócio da organização. Este ultimo deve ser tratado como desastre e ser o maior foco na gestão de riscos e continuidade de negócios. São atribuições do processo de gerenciamento de incidentes buscar a eficiência e eficácia do processo, produzir informações gerenciais, gerenciar o trabalho das equipes de suporte, gerenciar os incidentes graves, e desenvolver e manter processo e procedimentos para tratamento dos incidentes.

2.6 RELAÇÃO ENTRE AS REFERENCIAS BIBLIOGRÁFICAS

No presente trabalho foram estudadas as melhores práticas para a gestão da continuidade de negócios e da gestão de riscos no que se refere à Tecnologia da Informação. As normas ISO IEC 27002 e 27005 abordam respectivamente a gestão da continuidade de

negócios e a gestão de riscos de forma a fornecer as práticas certificadas de mercado no que se refere à segurança da informação. A norma internacional BS 25999 fornece um guia de melhores praticas no que se trata em continuidade de negócios. O ITIL e o COBIT trazem as melhores práticas na gestão da tecnologia da informação, tratando todo e qualquer ativo de TI como um serviço.

A continuidade de negócios é tratada de forma semelhante nas normas, no ITIL e no Cobit. Cada uma das bibliografias possuem sua maneira própria de tratar a continuidade de negócios, porém todas elas trabalham com o mesmo conceito.

A ISO IEC 27002 tem um foco na continuidade de negócios como um todo, unindo conceitos de disponibilidade e de contingência a fim de entender a continuidade. Por ser uma norma de segurança da informação, esta compreende muito dos conceitos de segurança citados nas normas ISO 27000 e tem como base a gestão de riscos abordada na norma ISO IEC 27005. Por ser uma norma técnica, seus conceitos são muito amplos e buscam o desenvolvimento de um processo de continuidade na organização, tendo este processo elaborado, a norma oferece as melhores técnicas para manter este ambiente em funcionamento adequado. A ISO IEC 27002 não define um nível de serviço como o ITIL e o Cobit, porém todas as etapas da continuidade de serviços se baseiam em um conceito de tempo aceitável para a recuperação de desastres conforme a criticidade do ativo avaliado. A ISO IEC 27002 não define um processo de continuidade, mas sim, um conjunto de práticas a serem consideradas na criação de um plano de continuidade. Esta norma tem como base a ISO IEC 27005, gestão de riscos.

A ISO IEC 27005, referente à gestão de riscos, define um processo para a gestão dos riscos em um ambiente organizacional, baseado nas práticas de segurança da informação. Por ser uma norma técnica específica, é a melhor fonte para se basear o processo de gestão de riscos. A ISO IEC 27005 define um processo contínuo e cíclico para identificar, analisar e tratar os riscos de uma forma detalhista.

A BS25999 trata a continuidade de negócios como um processo de gestão com um ciclo de vida bem definido e contínuo. Sua principal diferença é o reconhecimento mundial do seu guia de melhores práticas, contemplado em sua primeira parte, BS 25999-1, e a certificação em continuidade de negócios baseada em sua segunda parte, BS 25999-2. A BS 25999 é bastante ampla e não se foca apenas nos processos de TI, podendo ser aplicada em outras áreas da organização. O ciclo do processo propõe o entendimento dos processos da organização, onde é realizada a análise de riscos e impactos de negócio, como o base para suas atividades e seus planos, sendo depois dividido em estratégia, operacionalização e testes,

sendo envolvido por um processo de disseminação da cultura de continuidade de negócios na organização.

Tanto o Cobit quanto o ITIL trabalham com base em serviços de TI, cada serviço possui um SLA, acordo de nível de serviço, que irá definir os controles a serem implementados. O foco de ambos é o serviço de TI propriamente dito, que são todos os processos, sistemas, infraestrutura e ferramentas fornecidas pela TI para operacionalizar os objetivos de negócio.

O Cobit possui um conjunto de práticas baseado em objetivos e medições de TI, processo e das atividades, sendo que um acaba direcionando o outro. O Cobit avalia o ambiente de TI com base em um modelo de maturidade para cada um dos processos de seus quatro domínios. Os processos do Cobit detalham bastante o que executar e como medir seus resultados. A continuidade de negócios no Cobit é tratada na entrega e suporte do serviço, que são os processos que devem ser realizados para assegurar o funcionamento da organização e sua recuperação em caso de falhas. As práticas de continuidade segundo o Cobit englobam toda a área de TI e se baseia nas práticas de gestão de TI com conceito de apoio ao negócio, tratando conceito como a gestão de segurança da informação, a gestão de riscos como base para a criação de um plano de continuidade, e o gerenciamento do desempenho como base para a disponibilidade. O Cobit usa as normas ISO IEC 27002, ISO IEC 27005 e a BS 25999-1 como referencia bibliográfica para a sua elaboração.

O ITIL, em sua versão mais recente, utiliza o conceito de ciclo de vida do serviço, sendo todo o seu processo de continuidade baseado nos SLAs definidos. O ITIL foca nos serviços diários realizados para garantir o funcionamento da infraestrutura e sistemas de TI, englobando a gestão da continuidade em seu livro do desenho do serviço. Diferente do Cobit, o ITIL detalha bastante os processos e foca em como executar. O desenho do serviço descreve os objetivos e planos e cria um desenho do serviço detalhando seus processos. O ITIL trata a continuidade de negócios principalmente como uma operação de recuperação de desastres, tendo um processo separado para tratar da disponibilidade dos serviços.

O ITIL não tem um processo próprio para a gestão de risco porém é incorporado no gerenciamento financeiro dos serviços de TI, no gerenciamento de incidentes e problemas, no gerenciamento de mudanças e no gerenciamento da continuidade de serviço. Uma característica que identifica o ITIL é a definição de um papel de gerencia em cada processo, sendo este gerente o responsável pelos seus processos e sua integração com os objetivos de negócio. O ITIL também utiliza as normas ISO IEC 27002 e 27005 e a BS 25999-1 como referencia bibliográfica.

A tabela 2 apresenta algumas características essenciais de um plano de continuidade de negócios conforme sua presença nas referencias bibliográficas adotadas.

Tabela 2: Comparação entre as referencias bibliográficas

Características	**ISO 27002**	**ISO 27005**	**BS 25999**	**Cobit**	**ITIL**
Gestão de Continuidade de Negócios	X		X	X	X
Gestão de Riscos		X	X	X	
Define um processo e o trata como um ciclo		X	X		X
Definem claramente os responsáveis por gerenciar os processos e atividades					X
Classifica o processo de continuidade em níveis de maturidade				X	
Detalha métricas de avaliação				X	X
Baseia-se nos acordos de nível de serviço, SLAs				X	X
Priorização de atividades baseada na relação de custo, probabilidade e impacto	X	X	X		
Trata continuidade, contingência e resposta a incidentes separadamente				X	X
Abrange a etapa de mapeamento organizacional		X	X	X	
Abrange a etapa de elaboração de catálogos de serviços				X	X
Abrange uma fase de testes e simulações	X		X	X	X
Planeja a manutenção e melhoria contínua	X	X	X	X	X
Abrange processos de recuperação de desastres	X		X	X	X
Abrange a gestão da mudança	X	X	X	X	X
Sugere uma estrutura de plano de continuidade			X		
Abrange processos de cópias de segurança			X	X	X
Abrange planos de comunicação e disseminação de cultura na organização		X	X		
Identificam ativos organizacionais e suas relações com os processos de negócio		X	X		
Abrange diferentes conceitos de tratamento de risco / desastre	X	X	X	X	X
Abrange atividades operacionais da gestão de TI					X

As quatro referências bibliográficas têm seu estilo de lidar com a continuidade de negócios, porém todas elas seguem o mesmo conceito. Não se pode definir qual delas é a mais adequada, esta decisão dependerá da situação da organização e qual o seu objetivo ao implantar um plano de continuidade de negócios. No modelo sugerido neste trabalho estarão sendo adotados conceitos encontrados nas quatro referencias a fim de desenvolver um processo que possa adequar-se à realidade mais comum da indústria de pequeno e médio porte.

3 MODELO PARA ELABORAÇÃO DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

A partir das normas e bibliotecas estudadas no capítulo 2 é proposto um modelo para a elaboração de um plano de continuidade de negócios apropriado para empresas de pequeno a médio porte. A grande maioria das empresas de médio porte não possui cultura de continuidade de negócios (CONVERGÊNCIA DIGITAL, 2011).

O modelo em questão visa atingir organizações de pequeno ou médio porte que normalmente se encontram nos níveis “inexiste” ou “inicial” em relação aos seguintes processos do Cobit (Cobit, 2007):

a) Planejamento estratégico da TI: O guia se aplica a organizações que não possuem um planejamento estratégico de TI formalizado, mas entendem que a TI é importante para o seu negócio.
b) Diretrizes da tecnologia e infraestrutura: A organização não possui um planejamento de infraestrutura tecnológica para atender requisitos de sistemas. A necessidade do uso da tecnologia é existente porem é emergente, o uso é isolado e geralmente mal planejado. O direcionamento da tecnologia geralmente é ditado por planos de evolução de fornecedores de software e hardware.
c) Processos e organização da TI: A organização da TI não é relacionada aos objetivos de negócio, as áreas de TI e suas ações geralmente são reativas e implementadas de maneira inconsistente. A TI é considerada como uma área de apoio e geralmente é envolvida nos estágios finais de projetos ou novas implementações.
d) Gerenciamento dos investimentos de TI: A organização não possui um planejamento dos investimentos a serem realizados em TI. Os investimentos são geralmente reativos ou para demandas isoladas. A necessidade de investimento é conhecida porém não é formalizada.
e) Recursos humanos de TI: As equipes de TI são pequenas ou inexistentes, a organização enxerga a TI como fornecedora de suporte reativo e não busca a capacitação de seus profissionais e seu alinhamento com o processo de negócio.
f) Gerenciamento de riscos: A organização não enxerga vantagem em um processo de gerenciamento de riscos porém compreende que os riscos mais críticos devem ser tratados. A relação custo e probabilidade é levada em consideração porém é preferível arriscar a realizar um investimento alto.

g) Gerenciamento de Níveis de Serviço – SLA: A organização não reconhece a necessidade da definição de níveis de serviço, conhece os serviços que utiliza porem estes são realizados conforme a capacidade ou urgência momentânea.
h) Gerenciamento de desempenho da Infraestrutura: A organização não compreende que os processos de negócio dependem do desempenho da sua estrutura de TI. Os usuários possuem reclamações devido à limitação da estrutura, porém sua melhoria ocorre através de necessidade de contorno ou em situações de desastre.
i) Continuidade de Negócios: A organização tem noção dos riscos mas não compreende o seu impacto no processo de negócio, possui alguns controles para evitar a perda mas não pode garantir a sua eficiência. As respostas para situações de desastre são reativas.
j) Segurança da informação: A segurança da informação não é um conceito compreendido por todos na organização porém sua necessidade é conhecida. Há poucos controles de segurança da informação mas não há uma política formalizada.

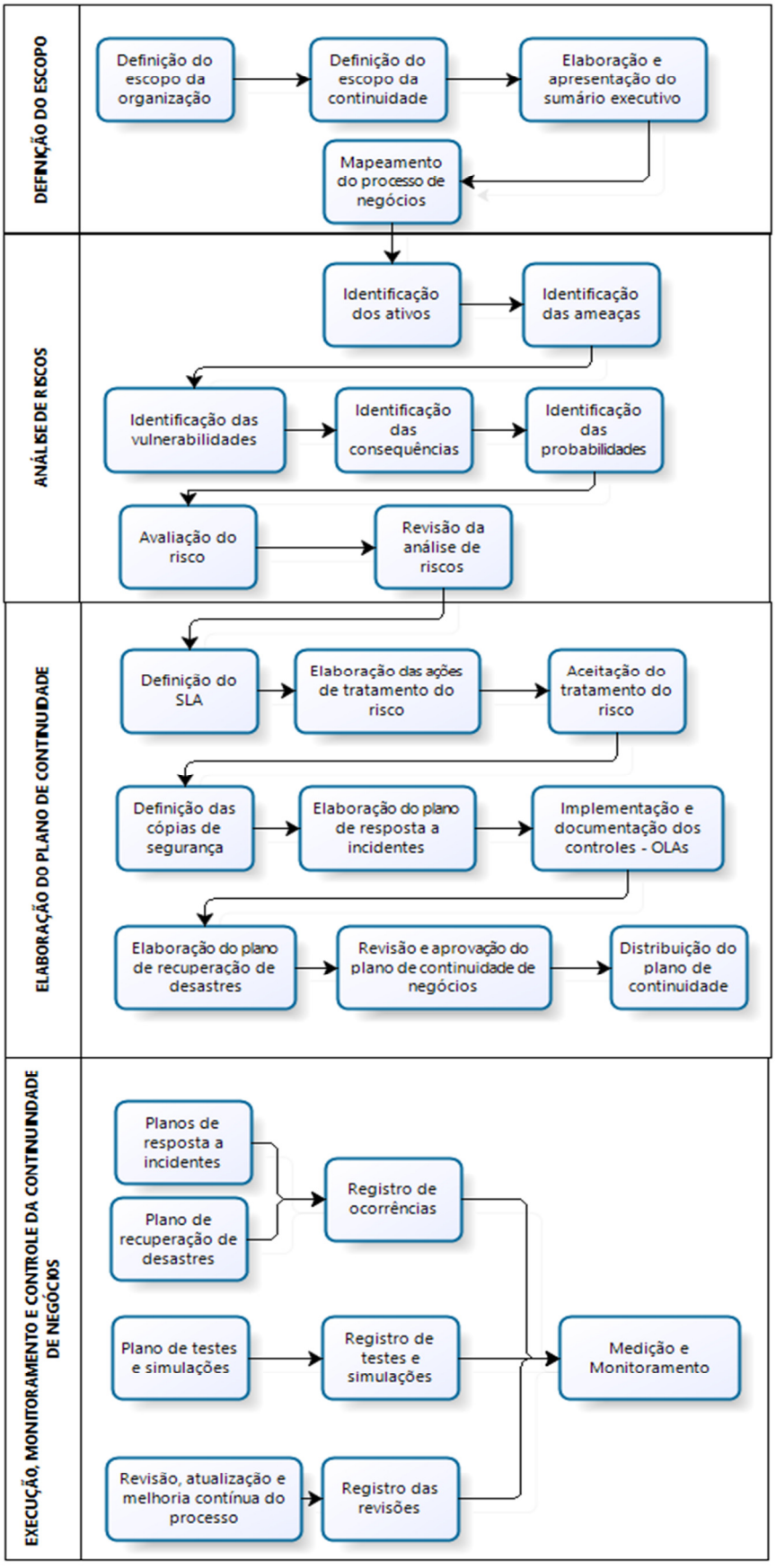
O modelo de plano de continuidade possui quatro fases, a definição do escopo, a análise de riscos, o plano de continuidade e a execução e monitoramento da continuidade. A fase de elaboração do escopo é formada pelas etapas de definição do escopo da organização, definição do escopo da continuidade, elaboração do sumário executivo e mapeamento do processo.

A Fase de análise de risco é composta pelo mapeamento do processo de negócios, pela identificação dos ativos, suas ameaças, vulnerabilidades e consequências, pela identificação da probabilidade dos riscos, pela avaliação do risco e por sua revisão. Esta fase direciona as ações da fase subsequente.

A terceira fase compreende as etapas para a definição do SLA, a elaboração das ações de tratamento do risco, a aceitação do tratamento do risco, a definição das cópias de segurança, a elaboração do plano de resposta a incidentes, a implementação e documentação dos OLAs, a elaboração do plano de recuperação de desastres, a revisão e aprovação do plano de continuidade de negócios e a sua distribuição e armazenamento.

A quarta e última fase é um conjunto de etapas para realizar os registros de execução e medir o desempenho, composta pelo registro de ocorrências, elaboração e registro dos planos de teste, elaboração e registro dos planos de revisão e manutenção e pela medição através dos indicadores de desempenho. As fases foram definidas a partir do estudo das referências bibliográficas e das necessidades das organizações de pequeno e médio porte. A figura 6 representa o processo proposto para a elaboração dos planos de continuidade.

Figura 6: Etapas propostas para a elaboração do plano de continuidade de negócios



O modelo é composto por três partes:

a) Guia de elaboração: a primeira parte do modelo compreende um guia contendo uma lista de atividades necessárias para a elaboração do plano. A elaboração do plano de continuidade deve seguir os passos descritos no guia de elaboração. É composto por diversas atividades sequenciais que seguidas irão dar condições de se criar um plano de continuidade de negócios, porém em algumas situações deve-se retornar a atividades anteriores para revisão o complemento. O guia proposto possui quatro colunas de informação, a primeira e a segunda coluna representam a fase e a etapa do modelo respectivamente, a terceira coluna se subdivide em outras quatro que apresentam os responsáveis pela realização das atividades, onde GC é o gestor da continuidade, P é o patrocinador, GP é o gestor de processo, UC é o usuário chave e TI é a equipe de TI, e a quarta coluna apresenta as atividades a serem executadas. O cabeçalho do guia está representado na figura 7. O guia está presente no anexo A, Guia para elaboração de um plano de continuidade de negócios.

Figura 7: Guia para a elaboração de um plano de continuidade de negócios

ANEXO A. GUIA PARA A CRIAÇÃO DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

Fase	Etapa	Papéis				Atividades
		R	A	C	I	
Definição do escopo	Definição da Organização	GC				Utilizar a lista Definições da Organização para registrar o levantamento realizado nesta etapa.
		GC		P , GP		Organizar uma reunião com os possíveis patrocinadores da implantação da continuidade para levantar pontos do escopo.
		GC		P , GP		Identificar qual a unidade organizacional a ser aplicada, seu propósito, sua missão, seu negócio e seus valores.
		GC		P , GP , TI		Identificar a posição da TI na organização.
		GC		P , GP		Identificar o organograma e a estrutura organizacional da organização.
		GC				Registrar o levantamento na lista Definições da Organização . Podem ser realizados múltiplos registros em caso de múltiplas unidades organizacionais.
	Definição do	GC		P , GP , UC , TI		Através de reunião, definir com os patrocinadores e envolvidos quais os processos ou sistemas deverão ser abordados pelo plano de continuidade de negócios. O escopo define o plano de continuidade.

b) Conjunto de Artefatos: O guia, ao ser executado, apresenta um conjunto de artefatos onde são registradas todas as definições e atividades realizadas na elaboração do plano de continuidade. São dezesseis documentos que amparam a elaboração do plano de continuidade de negócios. Os artefatos combinados representam o plano de continuidade de negócio formalizado. O conjunto de artefatos está presente no anexo B, Artefatos do plano de continuidade de negócios.

c) Informações complementares: conjunto de informações que auxiliam nas definições e registros das atividades do guia tratando-se de gestão de riscos, estes são frequentemente acionados durante a execução do guia proposto (NBR ISO IEC 27005: 2008). O conjunto de informações complementares está presente no Anexo C, Informações complementares.

As atividades propostas pelo guia estão atribuídas a responsáveis por sua execução. Segundo o Cobit, utiliza-se uma matriz denominada RACI, Responsible, Accountable, Consulted, and Informed, que indica os responsáveis(R), quem deve prestar contas e realizar atividades (A), quem deve ser consultado (C) e quem deve ser informado (I) (Cobit, 2007).

3.1 DEFINIÇÃO DO ESCOPO

O modelo de plano de continuidade de negócios se inicia com a definição da organização e do escopo do plano a ser desenvolvido.

Nesta primeira etapa, deve-se analisar o ambiente em que a organização se insere e quais os seus processos críticos para mantê-la competitiva no mercado. O escopo está dividido em seis etapas, Definição da Organização, a Definição do Escopo e Aplicabilidade, a Definição das restrições da organização, a Definição da equipe, a Definição da estrutura para a continuidade de negócios, o Sumário Executivo e o Mapeamento do Processo. É importante que toda e qualquer definição seja documentada e passe por uma avaliação e aprovação dos responsáveis pelos processos de negócio envolvidos (ISO IEC 27005, 2008). O resultado desta fase é um artefato com o escopo da continuidade de negócios.

3.1.1 Definição da organização

O plano de continuidade de negócios deve levar em conta a situação em que a organização na qual está sendo aplicado se encontra. A análise da organização serve para destacar os elementos aplicáveis na gestão da continuidade de negócios, buscando definir o propósito, o negócio, a missão, os valores e as estratégias da organização. O objetivo desta primeira análise é entender o processo de uma empresa e sua estrutura, auxiliando no entendimento das áreas que serão abordadas e suas funções (ISO IEC 27005, 2008).

Nesta primeira etapa, deve-se registrar o levantamento no Anexo B, 1.1 Definições da organização, conforme figura 8.

Figura 8: Artefato para registro das definições da organização presente na aba escopo dos artefatos

ANEXO B. ARTEFATOS DO PLANO DE CONTINUIDADE DE NEGÓCIOS	
Documento 1. Escopo	
1.1. DEFINIÇÕES DA ORGANIZAÇÃO	
Unidade organizacional	
Propósito da Organização	
Missão	
Negócio	
Valores	
Estratégia	
Organograma	

Deve-se identificar os seguintes pontos:

a) Propósito da organização: Qual é a razão pela qual a organização existe? O propósito define o objetivo da organização e o que ela busca.
b) Missão: A missão é o que a organização acredita e o que ela segue para atingir seu propósito.
c) Negócio: É definido pelo conhecimento de seus usuários, o que a organização faz para cumprir sua missão? O negócio é o processo operacional que a organização realiza para obter o lucro.
d) Valores: São os princípios fundamentais da organização aplicados nas rotinas de negócio. Os valores incluem os recursos humanos, o relacionamento com clientes e fornecedores, a qualidade dos produtos ou serviços prestados pela organização, e outros fatores que influenciam nos processos de negócio da organização.
e) Estratégia: A estratégia da organização determina a direção e o desenvolvimento necessários para que a organização possa se beneficiar das questões em pautas e das principais mudanças planejadas.
f) Organograma: Na definição da organização deve-se levar em conta o organograma e identificar quem tem o poder de decisão e aqueles que influenciam as decisões. São três os níveis destas organizações, nível de tomada de decisão, que estabelece a organização estratégica, nível de liderança, coordenação e gerenciamento, e o nível operacional, referente às áreas de apoio.

As definições podem ser identificadas através de reuniões com os envolvidos, da análise do planejamento estratégico da organização (se permitido) e através de consulta das

políticas e procedimentos da qualidade. A melhor opção seria a realização de reuniões com os envolvidos no processo, sejam eles patrocinadores, gestores de negócio e TI.

3.1.2 Definição do escopo e aplicabilidade do plano de continuidade de negócio

Definir onde será aplicado é o primeiro passo para iniciar o processo de implantação. A escolha da aplicação do plano de continuidade deve partir da organização com base na criticidade dos processos de negócio, quanto mais crítico o processo é para a organização, maior sua prioridade. A definição do escopo deve partir de uma reunião ou levantamento de necessidades com as partes interessadas como patrocinadores, gestores de negócio e TI. A criticidade pode ser apontada por identificação interna, mas também por auditorias externas ou requisitos para certificações de qualidade ISO (BS 25999, 2006).

É importante definir onde inicia o processo de gestão da continuidade e onde este termina. Todas as ações abordadas pelo guia para a criação do plano partirão da definição do escopo. Nesta etapa deve-se definir em conjunto com os gestores do negócio o que o plano irá abordar e o que ele não precisará abordar.

O registro destas definições deve ser realizado no Anexo B, 1.2. Escopo e aplicação.

3.1.3 Identificando as restrições que afetam a organização

No processo de definição do escopo deve-se considerar as diversas restrições que afetam o seu ambiente interno e externo. As restrições são muito importantes para determinar o direcionamento da segurança da informação, são originadas geralmente dentro da própria organização mas podem ser apontadas por agentes externos, como uma auditoria. A solução proposta traz uma sequência de atividades para identificar as restrições envolvidas (ISO IEC 27005, 2008). Através do guia devem ser identificadas restrições como:

a) Restrições de natureza política: Dizem respeito a restrições que envolvem órgãos do governo, como a utilização de nota fiscal eletrônica e SPED, sistema público de escrituração digital.
b) Restrições de natureza estratégica: Restrições abordadas em planejamento estratégico que impactam nos negócios da organização, como o uso de um sistema on-line de pedidos para garantir um maior número de vendas.

c) Restrições territoriais: Restrições referente à localização geográfica da organização. É de suma importância pois pode influenciar na contratação de serviços como serviços de conexão à internet, serviços de manutenção de rede e hardware, entre outros serviços que podem ser críticos na elaboração de um plano de continuidade.
d) Restrições do ambiente econômico e político: As organizações estão envolvidas em meios políticos, deve-se levar em conta a possibilidade de um evento, como greves, interromper as atividades da organização.
e) Restrições estruturais: A estrutura organizacional pode significar uma restrição, por exemplo, empresas multinacionais possuem processos vinculados a diferentes gestões.
f) Restrições funcionais: A organização pode possuir dependência de serviços de TI para cumprir sua missão. Sistemas cuja disponibilidade é necessária cem por cento do tempo em um período de vinte e quatro horas por dia se incluem nestas restrições.
g) Restrições de recursos humanos: A equipe envolvida no processo de continuidade deve ser identificada, bem como suas responsabilidades, qualificações, conscientização, motivação e disponibilidade.
h) Restrições advindas da agenda da organização: Projetos temporários, promoções de mercado, regime alto de horas extra e crises econômicas devem ser levados em consideração na identificação do processo.
i) Restrições relacionadas a métodos e processos: Organizações em geral possuem políticas e códigos de ética e operação. Os planos de continuidade devem levar estas políticas em conta na hora de sua elaboração.
j) Restrições de natureza cultural: A cultura da organização é muito influente na definição de seus processos. Questões culturais como etnia, costumes geográficos, postura e atitude profissional devem ser levados em conta. A implantação de novos processos pode impactar em um choque cultural. Normalmente é a restrição mais difícil de ser tratada.
k) Restrições orçamentárias: A implantação de um plano de continuidade de negócio deve levar em consideração a situação financeira da organização e quanto à mesma está disposta a investir. A aceitação do risco estará sempre se baseando na relação entre custo e beneficio de um controle. Organizações

privadas tendem a avaliar o investimento relacionando o mesmo com o possível prejuízo em caso de ocorrência.

l) Legislações e regulamentações aplicáveis à organização: É necessário identificar os requisitos legais aplicáveis à organização, baseando-se nas leis, decretos, regulamentações específicas à área de atuação da organização ou regulamentos internos e externos. Contratos com fornecedores e clientes também devem ser analisados. Cita-se como exemplo um contrato de fornecimento com um cliente baseado em prazos, a interrupção do processo de entrega pode gerar um prejuízo previsto em contrato ou não.

O registro destas restrições deve ser realizado no Anexo B, 1.3. Restrições que afetam a organização, conforme figura 9. A definição das restrições pode ser amparada através do Anexo C, 1. Restrições organizacionais, este item do anexo descreve os tipos de restrições e o que identificar em cada uma.

Figura 9: Artefato de registro das restrições organizacionais.

1.3. RESTRIÇÕES QUE AFETAM A ORGANIZAÇÃO		
Unidade organizacional		
Restrições	Questões	Sim /Não/ Parcialmente
Restrições de natureza política	O processo a ser abordado possui sistemas e serviços relacionados ao governo?	
Restrições de natureza estratégica	O processo a ser abordado está envolvido na estratégia da organização?	
Restrições territoriais	A organização está localizada em uma área geográfica instável quanto a contratação de link de internet ou contratação de serviços de suporte e manutenção?	
Restrições do ambiente econômico e político	A organização está vinculada à algum sindicato ou órgão responsável por paralizações ou greves? Já houveram ocorrencia de paradas devido à estas questões?	
Restrições estruturais	A organização depende da gestão de um conselho externo que possa influenciar nas decisões do processo de continuidade?	
Restrições funcionais	Há sistemas ou ativos de TI no processo que necessitam estar operantes 24 horas por dia e 7 dias por semana?	
Restrições de recursos humanos	Há uma equipe de TI ou usuários chave que poderão operar o plano de continuidade?	
Restrições advindas da agenda da organizaçã	O processo a ser abordado é um projeto temporário?	
Restrições relacionadas a métodos e process	Há uma política envolvendo a continuidade de negócios do processo a ser abordado?	
Restrições de natureza cultural	A organização possui abertura para implantação de novos processo? A continuidade de negócios faz parte do conhecimento da organização?	
Restrições orçamentárias	A organização está disposta a investir (independente do valor) na continuidade de negócios?	
Legislações e regulamentações aplicáveis	O processo a ser abordado está envolvido em alguma legislação, regulamentação ou contrato que podem colocar em risco a operação?	

3.1.4 Definição dos papéis de responsabilidade

Na solução proposta, todas as atividades do guia possuem identificação das responsabilidades de cada um na realização da atividade. No processo de definição do escopo, deve-se definir quais pessoas fazem parte de cada papel no processo da continuidade de negócios. Esta definição pode ser realizada através de reuniões com os patrocinadores, na identificação dos riscos ou até mesmo durante a definição do tratamento de risco e criação do plano. O ideal é que se tenham definidos os papéis na definição do escopo (Cobit, 2007).

Em empresas de pequeno e médio porte podem ser atribuídos mais de um papel por envolvido, devido às restrições de recursos humanos da organização.

O guia proposto traz ações para identificar quais pessoas farão parte de cada papel. Os papéis da gestão da continuidade de negócios são:

a) Patrocinador (P): Papel responsável por aprovar as decisões da continuidade de negócio. Normalmente é composto pela diretoria e gerência da organização. O patrocinador deve estar a par do andamento da implantação e é responsável, em conjunto com os gestores do processo, definir a aceitação do risco e a aprovação do plano de continuidade.
b) Gestor do processo (GP): É o responsável pelo processo que está sendo aplicado o plano de continuidade de negócios. O gestor do processo não necessariamente é o gerente da área funcional, mas pode ser um usuário-chave que possui domínio sobre o processo e tem liberdade para tomar decisões no mesmo. O gestor do processo é responsável pela aceitação do risco e aprovação do plano de continuidade juntamente com o patrocinador.
c) Gestor da continuidade de negócio (GC): O gestor da continuidade de negócio é responsável por organizar, definir atividades e responsabilidades e mensurar a implantação e gestão da continuidade de negócios, é o principal responsável pela criação do plano de continuidade. Este papel direciona as atividades de gestão de riscos e continuidade de negócios, sendo responsável por fazer o vinculo entre o operacional e a gestão do processo e patrocinadores. O Gestor da continuidade é responsável pela maioria das atividades do guia proposto.
d) TI: A TI é responsável pelos serviços, ativos e tecnologias envolvidas no processo de negócio abordado pelo plano de continuidade de negócios. A TI é responsável por auxiliar os usuários chave e fornecer o garantia da funcionalidade da infraestrutura envolvida no processo, bem como operar as atividades da continuidade de negócio quando necessárias.

e) Usuário-Chave (UC): Papel referente aos usuários envolvidos no processo de negócio abordado pelo plano de continuidade de negócios. O usuário chave é responsável por prover informações necessárias no mapeamento do processo, na identificação de riscos e também na avaliação do plano de continuidade de negócios. Em alguns casos, os usuários chave podem ser responsabilizados por atividades do plano de continuidade em si, desde que possuam a capacitação necessária.

No guia, as responsabilidades estão determinadas especificamente por atividade, baseada na matriz RACI. A tabela 3 representa o resumo das atividades do plano:

Tabela 3: Matriz RACI do modelo de plano de continuidade de negócios baseada no Cobit.

Atividades / Papéis	**P**	**GP**	**GC**	**UC**	**TI**
Determinar o escopo da gestão de continuidade	R	C	A	C	
Mapeamento do Processo		R A	A	C	C
Identificação dos Ativos		C	R	C	C
Análise de Riscos		C	R	C	A
Definições do nível de Risco	I	A	R	C	C
Determinação do Nível de Serviço para a continuidade		C	R	C	A
Elaboração dos planos de continuidade	I	C	R	C	A
Aprovação dos planos de continuidade	R	R	A	C	C
Execução dos planos de continuidade	I	I	R	A	A
Comunicação do processo de elaboração do plano de continuidade	I	I	R	I	A
Administração e manutenção dos planos de continuidade	I	C	R	A	A

A equipe definida deve ser registrada no Anexo B, 1.4 Equipe, conforme a figura 10. No artefato deve-se identificar o nome do usuário, indicar qual papel o usuário possui, qual sua área funcional na organização e quais as formas de contato deste usuário. Um usuário pode estar relacionado em mais de um papel com diferentes responsabilidades.

Figura 10: Artefato para registro da equipe e seus papéis

1.4. EQUIPE							
Usuários	PAPÉIS					Área funcional	Formas de contato
	Patrocinador	Usuário-Chave	Gestor de Processo	TI	Gestor da Continuidade		

Os papéis de TI se dividirão em diversos outros conforme forem elaborados os planos de tratamento do risco. A definição destes papéis no planejamento do escopo é muito importante para economizar tempo nas atividades de analise de riscos e na aceitação do risco.

3.1.5 Definição das restrições que afetam o escopo da continuidade

O guia proposto traz um conjunto de atividades necessárias para identificar as restrições que afetam o escopo (ISO IEC 27005, 2008). As restrições de escopo divergem das restrições da organização pois não necessariamente estão presentes em todos os planos de continuidade, podendo ser específicas de um escopo. Nesta etapa devem ser identificadas restrições como:

a) Restrições técnicas: Referente à infraestrutura de TI. Quais são os sistemas envolvidos no processo? Qual a infraestrutura de hardware, software e rede envolvida no processo? Qual a dependência de serviços de comunicação como internet e telefonia para este processo?
b) Restrições financeiras: Referente ao impacto do processo na organização. Este processo fornece lucro diretamente para a organização? A interrupção deste processo acarreta em prejuízo direto? O quanto aproximado a organização pode investir para garantir a segurança deste processo?
c) Restrições ambientais: Restrições que surgem como consequência do ambiente geográfico e climático da localização da organização. Qual o impacto de fenômenos meteorológicos para este processo?
d) Restrições temporais: Restrições do tempo de implementação de controles para os processos identificados. Longo tempo de espera para a implementação pode invalidar a análise pois os riscos podem sofrer alteração com o tempo. Qual o prazo máximo para a implantação do tratamento de risco para o processo? Quanto tempo o processo pode ficar interrompido?
e) Restrições de recursos humanos: Referente aos usuários e equipe de TI envolvidos no processo a ser abordado. Os usuários envolvidos no processo são capazes de operá-lo com eficiência e segurança? Todos os usuários envolvidos possuem o mesmo nível de conhecimento? A equipe de TI envolvida neste processo é capacitada para fornecer o suporte necessário? Há envolvimento de terceiros no suporte a este processo?

f) Restrições organizacionais: Restrições operacionais como tempo de operação, gestão dos recursos de TI, manutenção, administração do processo, desenvolvimento e relacionamento com terceiros devem ser consideradas.

As restrições de escopo identificadas devem ser registradas no Anexo B, 1.5. Restrições que afetam o escopo da continuidade. A figura 11 representa o registro das restrições no plano de continuidade. O Anexo C 2. Restrições que afetam o escopo, pode ser utilizado para auxiliar na identificação das restrições.

Figura 11: Artefato para registro das restrições que afetam o escopo da continuidade

1.5. RESTRIÇÕES QUE AFETAM O ESCOPO DA CONTINUIDADE		
PLANO DE CONTINUIDADE		
RESTRIÇÕES DE ESCOPO	Resposta	Tipo de resposta
Técnicas		
Quais os sistemas envolvidos no processo		Descrição
Qual a Infra-Estrutura envolvida no processo		Descrição
Dependências dos serviços de comunicação		Descrição
Financeiras		
Processo fornece lucro direto à organização		Sim/Não
A interrupção do processo acarreta em prejuizo direto		Sim/Não
Valor aproximado de investimento para a continuidade		Valor
Ambientais		
Fenômenos meteorológicos a considerar		Descrição
Impacto dos fenômenos meteorológicos		Descrição
Temporais		
Prazo de implantação da continuidade de negócios		Tempo/Dias
Tempo aproximado de parada aceitável do processo		Tempo/Horas
Recursos humanos		
Capacidade da equipe de usuários do processo		Descrição
Nível de conhecimento dos usuários no processo de negócio		Descrição
Capacidade da equipe de TI em fornecer o suporte		Descrição
Organizacionais		
Possui recursos tecnológicos necessários		Sim/Não
Dependência de terceiros na operação		Sim/Não
Dependência de terceiros no suporte e manutenção		Sim/Não

3.1.6 Elaboração e apresentação do sumário executivo

O sumário executivo é uma apresentação dos objetivos do plano de continuidade de negócios (BS 25999, 2006). O sumário aborda todas as definições da aba Escopo.

O primeiro passo é descrever o conceito de continuidade de negócios para entendimento do patrocinador, é sugerida a descrição da continuidade comparada com a atual realidade da organização.

O segundo passo é realizar uma breve descrição do processo que será abordado pelo plano de continuidade de negócios. É importante identificar onde inicia e onde finaliza o escopo.

O terceiro passo é a citar exemplos de riscos que podem acarretar em prejuízo. São exemplos simples e rápidos, apenas para auxiliar os patrocinadores a entenderem o que está sendo proposto.

O quarto passo é descrever o objetivo do plano de continuidade de negócios. O objetivo deve visar apresentar os benefícios da implantação do plano.

O quinto passo identifica as quatro fases da implantação do plano de continuidade de negócios segundo o modelo proposto. No modelo em questão as fases já estão identificadas e descritas conformes seus processos.

O registro do sumário executivo deve ser realizado no Anexo B, 1.6 Sumário executivo. A figura 12 apresenta o modelo proposto para registro do sumário. Para a divulgação para os patrocinadores e gestores pode ser utilizada uma formatação mais clara. Esta formatação fica a critério da organização, ela apenas precisa facilitar o entendimento da continuidade pelos patrocinadores.

Figura 12: Artefato para registro do sumário executivo.

1.6. SUMÁRIO EXECUTIVO		
PLANO DE CONTINUIDADE		
Definição da continuidade de negócios		
Descrição breve do processo a ser abordado		
Exemplos de situação de desastre		
Objetivo da continuidade de negócios		
Fases da Gestão da continuidade de negócios	Definição do Escopo	Na primeira fase é realizado o levantamento do Escopo. O escopo para do levantamento de toda a organização e suas restrições, qual a área de aplicação do plano e define-se a equipe que participará da elaboração do plano de continuidade de negócios.
	Gestão de Riscos	A gestão de riscos compreende a identificação dos riscos que podem afetar o processo definido no escopo. Nesta etapa é mapeado o processo definido, identificado os ativos envolvidos, suas vulnerabilidades, ameaças e consequencias, e então os riscos são avaliados para a elaboração dos planos.
	Elaboração do PCN	A terceira etapa compreende a elaboração das ações de tratamento dos riscos identificados, a definição das cópias de segurança e a elaboração dos planos de resposta a incidente e recuperação de desastres. É nesta fase que o plano de continuidade toma forma e é avaliado.
	Manutenção do PCN	A quarta e última etapa refere-se ao processo de registro de execução, medição e monitoramento, testes, manutenção e revisão preventiva.

3.1.7 Mapeamento do processo

Os processos definidos no escopo precisam estar claros e entendidos pela equipe envolvida na elaboração do plano. Para entender melhor o processo é necessário o

mapeamento do mesmo. Com o mapeamento do processo e a identificação de suas atividades, a identificação de ativos é mais rápida e mais segura.

Para efetuar o mapeamento do processo é sugerido o uso do Business Process Model and Notation (BPMN), Notação e modelo de processo de negócio (BPMN, 2012), que é um conceito de gestão de processos integrada à Tecnologia da Informação com foco na otimização dos resultados através do entendimento e melhorias nos processos de negócio. O BPMN possui conceitos de modelagem de processos que podem ser utilizados para identificar o processo para o plano de continuidade de negócios. Material sobre o BPMN pode ser encontrado no Object Management Group (OMG), através do site http://www.bpmn.org/ e outras bibliografias relacionadas.

Os processos mapeados devem ser registrados no Anexo B, 2.1 Processo. No artefato devem ser registrados uma breve descrição, o responsável pelo processo na organização e a modelagem do processo. Caso o BPMN seja utilizado, o fluxograma deve ser anexado no Anexo B, 2.2 Processo modelado.

3.1.8 Definição do plano de comunicação

A comunicação do processo pode ser realizada de diversas formas como atualização das atividades através de um fluxo por correio eletrônico, reuniões semanais de reporte de atividades ou por algum canal de comunicação que a organização possuir, como portais eletrônicos e sistemas de fluxo de trabalho.

Na solução proposta, o plano de comunicação está implícito no processo, o guia possui um fluxo de trabalho que trata a comunicação com os envolvidos, principalmente nas tomadas de decisão, sendo necessário para a coleta das informações do processo de análise de riscos e definições das ações da continuidade. A disseminação dos resultados pode ser realizada através do envio do próprio modelo do plano preenchido para os envolvidos no processo e reuniões de reporte de atividades.

3.2 ANÁLISE DE RISCOS

A segunda fase da solução proposta é a análise de riscos. A organização deve realizar uma análise dos riscos envolvidos no processo que se deseja implantar o plano de continuidade de negócios. A fase de análise de riscos se inicia com o mapeamento do processo e seus riscos e finaliza com a avaliação qualitativa dos mesmos. O processo de

análise de riscos é pré-requisito indispensável para a implantação de um plano de continuidade de negócios (ISO IEC 27005,2008).

3.2.1 Identificação dos ativos e serviços de TI envolvidos

A identificação dos ativos pode ser realizada através da análise do mapeamento realizado na atividade anterior, em reuniões ou entrevistas com os usuários chave, e pelo acompanhamento dos usuários na execução do processo.

Os ativos devem ser identificados através de análise do processo, de reuniões para discussão do processo com os usuários-chave, e de entrevista com os usuários. Esta análise irá resultar na identificação dos ativos para serem utilizados na atividade de análise de riscos e sua devida criticidade. O registro destes ativos identificados deve ser realizado Anexo B, 3.1. Relação dos ativos de TI envolvidos no processo. A figura 13 apresenta o artefato para registro dos ativos conforme o processo proposto.

Figura 13: Artefato para registro dos ativos.

Documento 3. Ativos							
3.1. RELAÇÃO DOS ATIVOS DE TI ENVOLVIDOS NO PROCESSO							
Ativos							
Ativo	Responsável	Descrição	Classificação	Subtipo	Criticidade	Ativos primários/suporte pertencentes	SLA

A identificação deve considerar todos os ativos que possuem relação com o escopo, seja este direta ou indiretamente. Cada ativo deve possuir um responsável relacionado e sua descrição deve ser realizada da maneira mais detalhada possível.

3.2.1.1 Tipos de ativos

Os ativos podem ser divididos em duas classificações, que representam o tipo majoritário do ativo: o ativo primário, referente aos processos e atividades de negócio e a informação; e ativos de suporte e infraestrutura como hardware, software, rede, recursos humanos, instalações físicas e serviços de TI (NBR ISO IEC 27005, 2008).

Não há um processo específico para cada um dos tipos de ativo, todos deverão ser identificados conforme a análise do processo for realizada. Após a identificação dos ativos,

eles devem ser caracterizados com prioridade baixa, média ou alta conforme as métricas de valoração dos ativos.

Um ativo primário possui diversos ativos de suporte, e um ativo de suporte pode estar associado a diversos ativos primários. No modelo em questão os ativos primários são primeiramente identificados e referenciam os de suporte, identificados na sequencia, envolvidos em seu processo. O registro dos ativos de suporte pode ser feito juntamente com a identificação dos ativos primários, mas necessitam de maior disponibilidade de tempo pois sua quantidade é maior do que os de ativos primários.

3.2.1.2 Identificando os ativos primários

Os ativos primários são os mais críticos para a gestão de risco pois não são ferramentas ou sistemas. Os ativos primários normalmente consistem dos principais processos e informações das atividades incluídas no processo. O levantamento destes ativos ocorre a partir de análise do processo mapeado e de entrevista com os usuários-chave deste processo.

Os ativos primários se dividem em dois subtipos (NBR ISO IEC 27005, 2008):

a) Processos e atividades de negócio: Processos cuja interrupção, mesmo que parcial, tornam impossível cumprir a missão da organização, processos que contem procedimentos secretos ou processos envolvendo tecnologia proprietária, processos que se modificados podem afetar significativamente o cumprimento da missão da organização e processos necessários para que a organização se mantenha em conformidade com requisitos contratuais, legais ou regulatórios. São exemplos: atividade de emissão de nota fiscal eletrônica, implantação de pedido no ERP, Enterprise Resource Management, entre outros.
b) Informação: Informação vital para o cumprimento da missão ou desempenho de negócio de uma organização, informação de caráter pessoal, informação estratégica necessária para o alcance dos objetivos determinados pelo planejamento estratégico, informação de alto custo, cuja coleta possui longo tempo ou alto custo de aquisição. São exemplos: Folha de pagamento, catálogo de desenhos industriais, entre outros.

A identificação dos ativos primários deve considerar as atividades dos usuários dentro do processo e devem ser priorizadas conforme a importância atribuída a elas pelo gestor do processo.

3.2.1.3 Identificando ativos de suporte e infraestrutura

Os ativos de suporte e infraestrutura compreendem equipamentos, sistemas e serviços de TI que podem comprometer os ativos primários através da exploração de sua vulnerabilidade. O levantamento destes ativos ocorre juntamente com a identificação dos ativos primários, através da análise dos processos relacionando cada atividade, ativo primário, com os ativos de suporte envolvidos. Um ativo pode pertencer a outro ativo, de forma hierárquica, por exemplo: um processador é um ativo que pertence a outro ativo, computador.

São diversos tipos de ativos de suporte e infraestrutura, e estes por sua vez se dividem em subtipos (NBR ISO IEC 27005, 2008):

a) Hardware: Compreende os elementos físicos que dão suporte aos processos. Subdivide-se em diversos subtipos:
   - Equipamento de processamento de dados: Equipamento automático de dados incluindo os itens necessários para sua operação independente. Exemplos: softwares de agendamento de tarefas e execução automática.
   - Equipamento móvel: Computadores e dispositivos portáteis como notebooks, tablets, smartphones, coletores de dados e agendas eletrônicas.
   - Equipamento fixo: Computadores utilizados nas instalações da organização. Exemplos: servidores, estações de trabalho, terminais magros e terminais específicos de aplicações.
   - Periféricos de processamento: Equipamentos conectados a um computador através de porta de comunicação ou conexão sem fio para a entrada, transporte ou transmissão de dados. Exemplos: impressoras, unidades de disco removível, leitores de código de barras e periféricos de entrada como mouse e teclado.
   - Mídia de dados: Uma mídia de informações que pode ser conectada a um computador ou rede para armazenamento de dados. A mídia de dados geralmente pode ser utilizada em qualquer tipo de computador. Exemplos: disco flexível, CD-ROM, fita de backup, unidade de disco externa, cartão de memória e unidade de armazenamento flash.
   - Outros tipos de mídia: Mídia estática, não eletrônica, que contem dados. Exemplos: documentos, papel, slides, transparências, fax.

b) Software: Software compreende todos os programas que fazem parte de um sistema de processamento de dados. Subdivide-se em diversos subtipos:
   - Sistema operacional: Compreende os programas que oferecem as operações básicas de um computador e a partir dele outros programas são executados. Seus principais elementos são os serviços de gerenciamento do hardware, gerenciamento de tarefas e os serviços de gerenciamento de usuário. O sistema operacional é encontrado em qualquer tipo de equipamento fixo e móvel. Exemplo: Microsoft Windows, Google Android, Apple Mac OS-X, Linux.
   - Software de serviço, manutenção ou administração: Softwares que servem de complemento para uso e administração do sistema operacional e não ligado diretamente ao usuário. Exemplo: Windows Active Directory, Microsoft WSUS, RedHat Samba, softwares de cópias de segurança, software anti-virus.
   - Software de pacote ou de prateleira: Softwares comercializado como um produto completo com mídia, versão e manutenção. Fornecem serviços para usuários e aplicações mas não é passível de alteração com as aplicações de negócio. Exemplo: Microsoft Office, Adobe Photoshop, Corel Draw.

c) Aplicações de negócio: As aplicações de negócio compreendem os sistemas de informação que a organização utiliza para operar seus processos de negócio. Subdivide-se em dois tipos:
   - Aplicações de negócio padronizadas: Software comercial projetado para fornecer acesso direto as operações de negócio em função de suas áreas de atuação. Normalmente estes tipos de software são a principal ferramenta de trabalho de uma organização, possuindo uma enorme gama de aplicações porem limitadas ao seu conjunto. São ativos que possibilitam sua customização. Exemplo: sistemas ERP, sistemas Customer Relationship Management (CRM), relacionamento com cliente, sistemas de Business Intelligence (BI), Human Capital Management (HCM).
   - Aplicações de negócio específicas: Sistemas desenvolvidos especificamente para aplicações de negócio particulares de uma organização. Existem diversos tipos de software específicos, porém sua atuação limita-se ao que foi implementado. Exemplo: sistema de monitoramento de máquina fabril,

sistema de controle de pressurização em equipamentos industriais, controle de pesagem de matéria prima integrada com balança.

d) Rede: Os ativos de rede compreendem os dispositivos de telecomunicação utilizados para conectar qualquer tipo de ativos de hardware e sistemas de informação. São subdivididos nos seguintes tipos:
   - Meio físico e infraestrutura: Compreendem a rede de comunicação que interligam os diversos computadores e sistemas de uma organização. Identificados pelas características físicas e técnicas e pelos protocolos de comunicação. Exemplos: Rede telefona pública comutada, redes ethernet e gigabit ethernet, linha digital assimétrica para assinante, ADSL, rede Wi-Fi, Bluetooth, FireWire.
   - Pontes (“bridges”) passivas ou ativas: Compreendem os dispositivos intermediários de conexão de rede, responsáveis pelo repasse de trafego de dados, comutação e filtro de rede. Exemplos: pontes, roteadores, hubs, comutadores “switches”, centrais telefônicas automáticas, access points de rede sem fio.
   - Interface de comunicação: Interfaces de redes conectadas as unidades de processamento. Exemplos: adaptadora “ethernet”, adaptador de rede sem fio, serviço de pacotes por rádio.

e) Recursos humanos: Compreende todas as classes de pessoas envolvidas com os sistemas de informação. Subdivide-se nos seguintes tipos:
   - Tomador de decisão: São os recursos humanos responsáveis pelos ativos primários (informação e processos) e os gestores da organização. Exemplo: alta direção, gerentes de área e gerentes de projeto.
   - Usuários: São os recursos humanos que manipulam e executam as atividades do processo de negócio. Possuem a responsabilidade do correto uso dos sistemas de informação e manipulam informações sensíveis de negócio. Possuem acessos referente a suas atividades de negócio nos sistemas de informação. Exemplos: gestores de área específico, analistas de área específica, usuários operadores de sistema.
   - Pessoal de produção/manutenção: Recursos humanos responsáveis pela operação e manutenção dos sistemas de informação, geralmente equipes de TI ou usuários chave com grande conhecimento de sistema. Possuem acesso

especial, com permissões de gerenciamento dos sistemas, para realizarem suas atividades rotineiras. Exemplos: administradores de sistema, analistas de TI, analistas de suporte, Helpdesk, especialistas em segurança.

- Desenvolvedores: responsáveis pelo desenvolvimento dos sistemas aplicativos da organização. Possuem acesso de alto privilégio aos sistemas, incluindo seu código-fonte. Não interferem com os dados de produção. Exemplo: programadores e analistas de aplicações de negócio.

f) Instalações físicas e localidade: Compreendem os lugares onde se encontra o escopo e os meios físicos para operação do processo nele contido. É subdividido em diversos tipos:
   - Ambiente externo: compreende os locais em que as medidas de segurança não podem ser aplicadas. Exemplo: lar das pessoas, instalações de terceiros, áreas urbanas e zonas perigosas.
   - Edificações: Local limitado pelo perímetro externo da organização, compreende a área física onde a organização está localizada. Exemplo: estabelecimentos e prédios.
   - Zona: Referente as áreas físicas delimitadas dentro de uma organização que separam áreas funcionais, processos ou locais específicos. Exemplo: escritórios, pavilhões, área de acesso restrito, área de segurança, centro de processamento de dados.
   - Comunicação: Serviços de telecomunicação e equipamento fornecido pela operadora de telefonia. Exemplos: linha telefônica, PABX, redes internas de telefonia.
   - Serviços de infraestrutura: Serviços e meios necessários para fornecimento de energia elétrica aos equipamentos de tecnologia da informação e seus periférico. Exemplos: fonte de energia de baixa tensão, central de circuitos elétricos, equipamento de prevenção de quedas de energia, serviços de refrigeração.

g) Organização: Compreende a hierarquia da organização e responsabilidades pelas decisões e execuções de tarefas. Subdivide-se em:
   - Autoridades: Organizações que representam autoridade dentro de uma organização, podendo ser legalmente afiliadas ou possuir um caráter externo.

Exemplos: conselho administrativo, sede da organização. Muito comum em organizações filiadas à grupos organizacionais.

- A estrutura da organização: compreendem os diversos ramos e setores da organização. Exemplo: gestão de recursos humanos, gestão de TI, gestão de logística, gestão comercial, gestão financeira.
- Subcontratados / Fornecedores / Fabricantes: Organizações terceiras que fornecem serviços ou recursos para o andamento do processo de negócio. Exemplo: empresa prestadora de serviço terceirizado, empresas de consultoria.

O item 3. Tipos de ativo, presente nas informações complementares pode ser utilizado para auxiliar na identificação dos ativos do processo através da relação de exemplos com cada tipo de ativo.

3.2.1.4 Definindo a criticidade dos ativos

Os ativos identificados devem ser classificados conforme a sua prioridade no processo de negócios. São três tipos de criticidade que podem ser atribuídas: baixa, média e alta (WALLACE, 2004).

a) Baixa: São considerados ativos de criticidade baixa os ativos que não afetam diretamente o processo de negócio. Sua interrupção pode significar perda de desempenho no processo, mas não a sua interrupção, entre outros.
b) Média: Ativos que afetam o processo de negócio. Sua interrupção pode acarretar em perda de desempenho e até interrupção mínima aceitável do processo de negócio pela organização, porem os prejuízos não são graves. São exemplos de consequência média: a interrupção breve nas atividades de negócio, perda de desempenho em atividades críticas do processo, informações não condizentes com a realidade, entre outros.
c) Alta: São ativos de alta criticidade aqueles que afetam diretamente o processo de negócio. Sua interrupção pode acarretar em prejuízo direto ao processo. Sua interrupção não é tolerável. São consequência da interrupção destes ativos prejuízo financeiro, perda de negócios, violação de lei ou de inciso contratual, perigo físico à saúde das pessoas, perda de valor de mercado, entre outros.

É muito importante que os usuários chave, gestores de processo e patrocinadores participem na definição da criticidade dos ativos. A visão da criticidade varia conforme o ponto de vista de cada papel e todos eles devem ser considerados. As restrições da organização e de escopo identificadas na definição do escopo possuem influência direta na criticidade dos ativos e devem ser levadas em consideração. A criticidade definida irá direcionar as ações da gestão de riscos e a prioridade no tratamento dos riscos.

3.2.2 Identificação das ameaças

Para a identificação destas ameaças, o guia propõe a análise do processo, ativo por ativo, iniciando pelos primários. Na sequencia devem ser identificados quais os ativos de suporte envolvidos e quais ameaças possíveis este ativo pode sofrer.

Cada ativo deve possuir uma lista de ameaças independente dos demais, porém uma ameaça pode ser tratada juntamente com outras. É importante que seja identificado o maior número possível de ameaças, mesmo que estas apresentem chances remotas de ocorrência.

Existem diversos tipos de ameaças a ser identificadas: Uma ameaça pode estar relacionada com vários ativos. O guia proposto sugere a identificação dos seguintes tipos de ameaça (NBR ISO IEC 27005, 2008):

a) Dano físico: Fogo, Água, Poluição, Acidente grave, destruição de equipamento ou mídia e poeira, corrosão ou congelamento. Estas ameaças podem ser intencionais, acidentais ou naturais. São comumente encontradas em ativos de hardware.
b) Eventos naturais: Fenômenos climáticos, fenômenos sísmicos, fenômenos vulcânicos, fenômenos meteorológicos e inundações. Estas são ameaças naturais e comumente identificadas nos ativos de hardware, infraestrutura física e instalações prediais.
c) Paralisação de serviços essenciais: Falha do ar condicionado ou sistema de suprimento de água, falha do equipamento de telecomunicação, consideradas ameaças acidentais ou intencionais. Interrupção do suprimento de energia, considerada ameaça acidental, intencional ou natural. São comumente identificadas nos ativos de hardware, infraestrutura e instalações prediais.

d) Distúrbio causado por radiação: Radiação eletromagnética, radiação térmica e pulsos eletromagnéticos. Podem ser acidentais, intencionais ou naturais e possivelmente identificadas nos ativos de hardware, infraestrutura e instalações prediais.
e) Comprometimento da informação: Interceptação de sinais de interferência comprometedores, espionagem a distância, escuta não autorizada, furto de mídia ou documentos, furto de equipamentos, recuperação de mídia reciclada ou descartada, alteração de hardware e determinação da localização são exemplos de ameaças intencionais. Divulgação indevida, dados de fontes não confiáveis e alterações de software podem ser tanto intencionais quanto acidentais. Estas ameaças podem ser identificadas em quase todos os ativos.
f) Falha técnica: Falhas de equipamento, defeitos de equipamentos e defeitos de software são ameaças acidentais. Saturação do sistema de informação e violação das condições de uso do sistema de informação que possibilitam sua manutenção são consideradas ameaças acidentais ou intencionais. São comumente identificadas em ativos de hardware, software, rede e aplicações de negócio.
g) Ações não autorizadas: Uso não autorizado de equipamento, cópia ilegal de software, uso de cópias de software falsificadas ou ilegais, comprometimento dos dados e processamento ilegal de dados. São ameaças intencionais ou acidentes e comumente encontrada nos ativos de software e aplicativos de negócio.
h) Comprometimento de funções: Erro durante o uso, abuso de direitos, forjamento de direitos, repúdio de ações e indisponibilidade de recursos humanos são exemplos de ameaças que podem ser acidentais, intencionais ou naturais. São normalmente identificadas em ativos de software, sistemas de negócio e recursos humanos.
i) Ameaças representadas por seres humanos: As ameaças representadas por seres humanos são diversas e podem ocasionar o maior prejuízo de todas. Elas envolvem crimes digitais, espionagem industriais, entre outras. São ameaças intencionais e associadas a ativos de hardware, software e aplicação de negócio. São elas:
j) Invasores: Invasão, engenharia social, invasão de sistemas e acessos não autorizados ao sistema.
k) Criminoso digital: Crime digital, ato fraudulento, suborno por informação, falsidade ideológica e invasão de sistemas.

l) Terrorista: bomba, guerra de informação, ataque a sistemas, invasão de sistema e alteração do sistema.

m) Espionagem industrial: Violação de informações, furto de informações, engenharia social, invasão de sistema, acesso não autorizado aos sistemas.

n) Pessoal interno: agressão a funcionário, chantagem, interceptação de informação, fraude e furto, suborno por informação, entrada de dados falsificados ou corrompidos, interceptação, código malicioso, venda de informações pessoais, defeitos no sistema, invasão de sistemas, sabotagem e acesso não autorizado aos sistemas.

A origem das ameaças deve ser identificada, podendo ser intencional, acidental ou natural. Existem diversos métodos de identificar as ameaças, podendo ser realizado a partir de análise do processo e dos ativos envolvidos, reuniões e entrevistas com usuários chave, TI e gestores de processo, inspeção física, análise de documentos e através do histórico de ocorrências de desastre na organização.

Toda documentação deste processo deve ser registrada no Anexo B, 4.1 Identificação dos riscos. No artefato devem conter a ameaça relacionada ao ativo pertinente, seu tipo e sua possível origem.

Figura 14: Artefato pra registro dos riscos identificados e analisados

Documento 4. Riscos									
4.1. IDENTIFICAÇÃO DOS RISCOS									
Ativo	Ameaças			Vulnerabilidades	Consequências		Probabilidade	Nível	Observações
	Ameaça	Tipo	Origem		Consequencia	Impacto			

O item 4, Ameaças, presente nas informações complementares, pode auxiliar a identificar as ameaças, sua origem e os ativos comumente relacionados a elas. A figura 14 apresenta o artefato de registro dos riscos, compreendendo toda fase de análise de riscos.

3.2.3 Identificação das vulnerabilidades

Na solução proposta, o guia apresenta uma série de atividades que devem ser executadas para identificar as vulnerabilidades. As vulnerabilidades podem ser identificadas

de diferentes formas conforme a ISO IEC 27005, podendo ser proativas ou reativas. No modelo proposto, as vulnerabilidades devem ser tratadas de forma proativa para evitar problemas futuros, porém, novas vulnerabilidades desconhecidas podem ser identificadas de forma reativa após um desastre.

A equipe envolvida na identificação da vulnerabilidade, geralmente composta por gestor da continuidade, analista de TI e usuário chave, deve trabalhar utilizando dois pontos de vista, interno e externo. A visão interna tende a identificar as vulnerabilidades que podem ser exploradas dentro da organização, por pessoal interno. A visão externa tende a visualizar as possíveis fragilidades oriundas de acesso externo. No processo poderão ser identificadas vulnerabilidades que possuem ou não ameaças, estas ultimas não devem ser desconsideradas mas não requerem a mesma prioridade das que possuem ameaças identificadas. É sugerido que todo o escopo seja percorrido e realizado entrevistas com usuários chaves e operadores de negócio dentro do próprio ambiente deles.

O guia proposto possui atividades de identificação dos seguintes tipos de vulnerabilidade (NBR ISO IEC 27005, 2008):

a) Hardware: Manutenção insuficiente de mídia de armazenamento, ausência de rotina de substituição de equipamentos periódica, ambiente sensível à poeira, umidade e sujeira, sensibilidade a radiação eletromagnética, inexistência de controle eficiente de mudança de configuração, sensibilidade a variações de voltagem, sensibilidade a variações de temperatura, armazenamento não protegido, falta de cuidado durante o descarte, realização de cópias não controladas.
b) Software e aplicações de negócio: Procedimentos de teste de software insuficientes ou inexistentes, falhas conhecidas no software, desassistência da estação de trabalho com usuário conectado, descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados, inexistência de um processo de auditoria, atribuição errônea de direitos de acesso, software amplamente distribuído, utilizar programas com dados inválidos ou de versão antiga, interface de usuário não amigável, inexistência de documentação e ajuda, parametrização incorreta, datas incorretas, inexistência de processo de autenticação de usuários, arquivo com registro de senhas desprotegido ou de passível acesso, gerenciamento de senhas mal realizado, serviços desnecessários habilitados, software novo, não homologado ou imaturo, especificações confusas ou incompletas para desenvolvedores, inexistência de um

controle eficaz de mudança, download e uso não controlado de software, inexistência de cópias de segurança, inexistência de mecanismos de proteção física no prédio, portas e janelas, inexistência de relatórios de gerenciamento.

c) Rede: Inexistência de evidencias que comprovem o envio ou o recebimento de mensagens, linhas de comunicação desprotegidas, tráfego sensível não protegido, junções de cabeamento mal feitas, ponto único de falha, não identificação e não autenticação do emissor e do receptor, arquitetura insegura da rede, transferência de senhas em claro, gerenciamento de rede inadequado, conexões de redes públicas desprotegidas.
d) Recursos humanos: Ausência de recursos humanos, equipe insuficiente, procedimentos de recrutamento inadequados, treinamento insuficiente, uso incorreto de software e hardware, falta de conscientização em segurança, inexistência de mecanismos de monitoramento, trabalho não supervisionado de pessoal terceirizado, inexistência de políticas para uso correto de meios de telecomunicação ou de troca de mensagens.
e) Local e instalações: Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e locais de armazenamento de dados críticos, localização em área suscetível a inundações, instabilidade no fornecimento de energia, inexistência de mecanismos de proteção física no prédio, portas e janelas.
f) Organização: Ausência de políticas de segurança da informação e controle de acessos e alterações, ausência de política de recursos humanos referente ao uso da tecnologia da informação, inexistência de um processo de registro e atendimento de ocorrências, ausência de um plano de continuidade, ausência da gestão de riscos e inexistência de contratos de confidencialidade e acordo de nível de serviço com terceiros.

No que se trata de segurança da informação, são sugeridos alguns métodos proativos de identificação das vulnerabilidades como o uso de ferramentas automatizadas de busca por vulnerabilidades, avaliação e testes de segurança, testes de invasão e análise crítica de código fonte. A política de autenticação para softwares e sistemas também deve ser revisada nesta etapa.

O modelo proposto no presente trabalho sugere o registro das vulnerabilidades no Anexo B, 4.1 Identificação dos riscos, dos artefatos do plano de continuidade, associando-as

aos ativos e ameaças relacionados, futuramente com as consequências e sua aceitação. Para auxiliar na identificação das vulnerabilidades, o item 5, Vulnerabilidades, presente nas informações complementares, pode ser utilizado.

3.2.4 Identificação das consequências e riscos

O guia propõe a identificação das consequências através de entrevistas e reuniões com os usuários chave e equipe de TI. Para identificar as consequências, deve ser realizada a análise da lista de todos os ativos com suas ameaças e vulnerabilidades relacionadas. A partir desta lista, devem-se prever as possíveis consequências de cada ameaça com base em entrevistas com os usuários chave e gestores de processo, histórico de ocorrência na organização e organizações terceiras (NBR ISO IEC 27005, 2008).

São exemplos de consequências:

a) Perda de desempenho ou instabilidade no funcionamento dos sistemas;
b) Condições adversas de operação;
c) Interrupção de operação de negócio;
d) Perda de oportunidade de negócios;
e) Imagem e reputação prejudicadas;
f) Violação de obrigações obrigatórias ou legais;
g) Prejuízo financeiro;
h) Perda de dados ou informações;
i) Prejuízo à vida humana;
j) Perda de competitividade no mercado.

Após a identificação das consequências os gestores de processo e patrocinadores devem avaliar os riscos com suas consequências e determinar a o impacto na organização em baixo, médio ou alto:

a) Baixo: Entende-se por baixo impacto aquele cujo prejuízo financeiro é pequeno ou prejudica a operação de negócio a um nível aceitável.
b) Médio: O médio impacto abrange riscos que ocasionam prejuízo financeiro moderado e não aceitável, ou podem acarretar em perda de oportunidades de negócio ou prejuízo à imagem da organização.

c) Alto: O alto impacto compreendem os riscos cujo prejuízo financeiro é alto, pode prejudicar a organização de forma quase que irreversível no mercado e coloca em risco a vida das pessoas da organização. Este registro influenciará na avaliação final dos riscos, resultado das etapas subsequentes.

As consequências devem estar alinhadas com as restrições da organização e de escopo identificadas na definição do escopo. Os gestores da organização devem definir a criticidade, mas esta pode ser sugerida pelo gestor da continuidade conforme análise realizada.

Todas as consequências devem ser registradas, independente de a organização possuir alguma forma de tratamento já aplicada ou não. É muito importante que o maior número de consequências seja identificado e registrado para facilitar a valoração do risco na etapa subsequente.

Os registros das consequências e seu impacto devem ser realizados no Anexo B, 4.1 Identificação dos riscos. O item 6, Consequências, presente nas informações complementares, pode auxiliar o gestor da continuidade na identificação das consequências e na avaliação das mesmas.

3.2.5 Identificação das probabilidades

No modelo proposto está se utilizando a análise qualitativa para a avaliação do risco. A análise qualitativa é utilizada para medir a probabilidade e para medir o nível do risco através do cruzamento do impacto com a probabilidade (ISO IEC 27001, 2008).

A analise qualitativa foi escolhida perante a quantitativa, pois é mais simples definir os valores de avaliação através de níveis como baixo, médio e alto. Como o nível de gestão da continuidade abordado neste trabalho corresponde a níveis iniciais, a exatidão das probabilidades torna-se mais complexa devido à falta de indicadores concretos. A análise quantitativa torna-se viável quando a gestão da continuidade está em níveis mais elevados, permitindo um controle mais exato das ocorrências.

O guia proposto fornece diversas atividades para identificar as probabilidades. Para medir a probabilidade deve-se analisar a lista de riscos com as vulnerabilidades e as ameaças que podem explorá-las. A fragilidade das vulnerabilidades pode ser identificada a partir de entrevistas com os usuários chave envolvidos no processo e que possuem o conhecimento

necessário e vivência para determinar uma possível probabilidade. Além dos usuários, os analistas de TI também devem ser consultados, pois estes conhecem os ativos de infraestrutura envolvidos e suas vulnerabilidades. O gestor de processo também pode ser fonte de informações para a identificação da probabilidade. A identificação pode ser realizada através de perguntas relacionadas aos riscos. As referências bibliográficas presentes neste trabalho e outros casos reais também podem ser utilizados para identificar probabilidades.

Além da opinião dos envolvidos do processo, deve-se avaliar o histórico de ocorrência do risco na organização, este histórico é bastante influenciador na probabilidade, pois é um fator real. Deve-se firmar uma acordo aceitável entre o tempo de utilização do ativo envolvido e a quantidade de desastres que ocorreram. Esta média é qualitativa, podendo variar conforme a opinião dos envolvidos no processo. O ultimo ponto a ser analisado é o histórico de ocorrência de organizações terceiras e casos reais publicados, para ser usado como um indicador menor para definir a probabilidade.

A probabilidade de um risco deve ser classificada em muito improvável, improvável, possível, provável ou muito provável e/ou presente.

A probabilidade deve ser determinada pelo gestor da continuidade em conjunto com o gestor do processo através de uma média estimada entre a opinião dos usuários, o histórico de ocorrência e com pequena influencia no histórico de outras organizações. A exata estimativa da probabilidade é base para a avaliação do risco.

O registro das probabilidades deve ser realizado no Anexo B, 4.1 Identificação dos ricos.

3.2.6 Avaliação do risco

A avaliação consta em realizar um cruzamento entre a probabilidade de ocorrência de um risco e seu impacto no negócio, baseando-se em análise qualitativa para medir o nível do risco (ISO IEC 27005, 2008).

A análise qualitativa é utilizada pois os dados fornecidos na análise de riscos não possuem a precisão suficiente para uma análise quantitativa. Através da análise qualitativa podemos obter um resultado aproximado favorável ao processo.

O guia proposto apresenta um conjunto de atividades para avaliar os riscos mapeados. Para realizar a avaliação do risco, deve-se utilizar uma comparação entre Impacto e Probabilidade. Para cada probabilidade deve ser atribuído um valor numérico de 1 a 3

conforme a possibilidade de ocorrência. Para cada criticidade de impacto deve ser atribuído um valor numérico de 1 a 3. O nível resultante é a soma dos fatores de probabilidade e impacto. A tabela 4 representa o cruzamento da probabilidade com a criticidade:

Tabela 4: Cruzamento entre a probabilidade de ocorrência e o impacto no negócio

TABELA DE AVALIAÇÃO DO RISCO				
Probabilidade de ocorrência		**Improvável**	**Possível**	**Provável**
Impacto no negócio	**Baixo**	2	3	4
	Médio	3	4	5
	Alto	4	5	6

O resultado da soma representa o nível de risco, quanto maior o nível, mais crítico e mais rapidamente este deve ser tratado. Conforme o valor resultante, o nível de risco pode ser:

a) 2 - Baixo risco: risco pode ser aceito sem tratamento imediato, pode ser desconsiderado ou reavaliado em oportunidades futuras.
b) De 3 e 4 – Médio Risco: risco precisa ser tratado, porém não precisa ser priorizado no momento. Geralmente são tratados no futuro devido a restrições financeiras.
c) De 5 e 6 – Alto risco: risco deve ser tratado o mais breve possível, é o principal alvo de um plano de continuidade de negócios.

Após a estimativa do risco, é essencial que o gestor da continuidade, em conjunto com o gestor do processo, revise o resultado. O registro do nível do risco resultante da avaliação de riscos deve ser realizado no Anexo B, 4.1 Identificação dos riscos.

O item 7, Avaliação do Risco, presente nas informações complementares, pode ser utilizado para auxiliar na avaliação dos riscos.

3.2.7 Revisão da análise de riscos

O processo de análise de riscos tem como artefato resultante um catálogo com os riscos identificados relacionando os ativos, ameaças, vulnerabilidade, consequência, probabilidade e o nível do risco.

Este artefato deve ser revisado e então apresentado juntamente com o escopo para os patrocinadores e gestores de processo para que possam compreender a importância do plano de continuidade de negócios. A apresentação pode ser realizada através de reunião e deve ser realizada de forma simples e objetiva.

Com a compreensão dos patrocinadores e gestores de processo, a elaboração do plano de continuidade tenderá a ser muito mais tranquila. É sugerido o registro em ata desta apresentação para auxiliar nas decisões futuras.

3.3 ELABORAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

A terceira fase da solução proposta é a elaboração do plano de continuidade de negócios. A elaboração do plano tem como base o escopo e a análise de riscos. A elaboração do plano se inicia com a definição do acordo de nível de serviço, SLA, seguido pela elaboração das ações de tratamento dos riscos, da definição do processo de cópia de segurança, da elaboração do plano de resposta a incidentes e pela elaboração do plano de recuperação de desastres.

3.3.1 Definição dos níveis de serviço – SLA

A definição dos níveis de serviço é a primeira etapa para iniciar a elaboração do plano de continuidade. Ela é constituída pela definição dos tempos de interrupção aceitáveis pela organização para cada ativo no processo (COBIT, 2007).

O primeiro passo é a identificação dos ativos e serviços que deverão ser abordados no plano de continuidade com base na análise de riscos. Esta definição é de critério da organização em determinar quais ativos deverão ser abordados pelo plano de continuidade de negócios, não necessariamente todos os ativos precisam ser abordados. É sugerido que os ativos de maior nível de risco sejam tratados primeiramente. Para cada ativo relacionado, deve ser identificada sua criticidade baseada na identificação dos ativos.

O tempo máximo de interrupção aceitável de ser identificado através de opiniões e consultas com os usuários chave e gestores de processo. Além do tempo aceitável, deve ser identificado com a equipe de TI qual o tempo possível de recuperação com base na

capacidade da mesma. O SLA final será um acordo de tempos de recuperação satisfatório para o usuário e para a TI, sendo aprovada pelos gestores de processo. O SLA é definido por ativo, cada ativo possui seu tempo de interrupção aceitável, independente do risco.

Os SLA devem ser registrados no Anexo B, 3.1 Relação dos ativos de TI envolvidos no processo. A figura 15 apresenta o artefato para registro dos SLA no plano.

Figura 15: Registro dos SLA na última coluna do artefato de registro dos ativos.

Documento 3. Ativos

)S ATIVOS DE TI ENVOLVIDOS NO PROCESSO

	Ativos				
	Classificação	Subtipo	Criticidade	Ativos primários/suporte pertencentes	SLA

3.3.2 Elaboração das ações de tratamento do risco

O guia proposto fornece um conjunto de ações para elaborar os planos de tratamento dos riscos identificados na fase de análise de risco (NBR ISO IEC 27005: 2008). Esta etapa inicia com a relação dos ativos, seus riscos, composto por ameaça vulnerabilidade, consequência e nível, que serão tratados para elaborar as ações.

Para cada risco, deve-se elaborar um plano de ação para evitar o risco, reduzir o risco, transferir o risco, aceitar o risco. As ações devem ser elaboradas por risco, porém, uma ação pode tratar mais de um risco. Este plano de ação é um registro breve do que deve ser feito e podem ser: implantação de controles, redundância de sistemas, atividades de revisão manuais, entre outros. As ações devem ser classificadas por tipo de tratamento: evitar, reduzir, transferir ou reter o risco. Para cada ação deve ser identificado o responsável e qual o prazo de implantação da mesma.

As ações propostas podem ser possíveis de aplicação na organização a partir de sua estrutura atual ou podem requerer investimentos. É necessário identificar se a ação precisa ou não de investimento e quanto seria o valor do investimento necessário para realiza-la.

É muito importante identificar ações necessárias para restaurar as cópias de segurança dos ativos envolvidos no processo, porém não é necessário um detalhamento do processo de cópia de segurança nesta etapa, o modelo irá tratar especificamente as cópias de segurança em uma etapa subsequente.

O registro das ações de tratamento deve ser realizado no Anexo B, 5.1 Ações de tratamento. A figura 16 representa o registro das ações no artefato do plano de continuidade.

Figura 16: Artefato para registro das ações de tratamento do risco

Documento 5. Ações de Tratamento											
5.1. AÇÕES DE TRATAMENTO DOS RISCOS											
Plano de continuidade	Ameaça	Vulnerabilidade	Consequência	Ações	Detalhamento	Tipo	Responsável	Requer investimento?	Valor	Aprovação	Justificativa	Prazo de implementação

3.3.3 Aceitação do tratamento do risco

As ações resultantes desta etapa não necessariamente precisam ser aceitas pela organização, desde que a mesma esteja ciente das consequências. O guia propõe um processo de aprovação das ações de tratamento propostas.

As ações devem ser apresentadas para os gestores de processo e patrocinadores avaliarem-nas, seus custos, seu resultado proposto e seu prazo de implementação. Os gestores podem avaliar as ações e aprova-las, reprova-las ou prorroga-las para um futuro. Em caso de rejeição, o motivo da rejeição deve ser registrado. Em caso de prorrogação, um novo prazo de implementação deve ser estabelecido e revisado futuramente.

O resultado da avaliação deve ser registrado no Anexo B, 6.1 Ações de tratamento. O resultado da aceitação das ações de tratamento deve ser comunicado a todos os envolvidos no processo para que fiquem cientes do que irá e não irá ser implementado.

3.3.4 Definição das cópias de segurança

O guia proposto relaciona uma sequencia de atividades específicas para as cópias de segurança devido a sua importância (COBIT, 2007). Este processo deve abordar os ativos que

a organização considera importante, de criticidade média ou alta, independente se já possuem ou não cópias de segurança.

Para iniciar esta etapa, deve-se identificar os métodos de realização de cópias de segurança existentes ou que serão implementados a partir das ações de tratamento. Os métodos podem ser unidades de fita, discos removíveis, servidores de cópias de segurança, cópias na nuvem, armazenamento remoto, entre outros. Estes métodos podem já existir no ambiente ou que serão adquiridos.

Para cada método, identificar os ativos envolvidos como hardware e software, o responsável, qual a ação de validação de seu funcionamento. Também deve-se identificar se o conteúdo das cópias de segurança é formado por dados (arquivos e informações de um servidor ou sistema), por imagem de sistema (imagem ou cópia total de um servidor) ou ambos, e identificar qual a sua posição na ordem de restauração em caso de necessidade. Para cada método deve ser identificado quais os serviços de terceiros envolvidos, como contrato de suporte e garantia de equipamentos.

Os métodos devem ser registrados no Anexo B, 6.1 Métodos de Cópia de Segurança. A figura 17 representa a tabela para o registro das cópias de segurança.

Figura 17: Artefatos para registro dos métodos e ações de cópias de segurança.

Documento 6. Métodos de Cópias de Segurança								
6.1. MÉTODOS DE CÓPIA DE SEGURANÇA								
Método de Backup	Plano de continuidade envolvido	Ativos envolvidos	Responsável	Ações de validação	Dados de Backup	Tipo de backup	Prioridade	Contratos de suporte de terceiros

Documento 7. Cópias de Segurança											
7.1 CÓPIAS DE SEGURANÇA											
Ativo	Possui Backup?	Método de Backup	Periodicidade	Ciclo de vida	Responsável	Ações de validação	Periodicidade da validação	Responsável	Possui armazenamento externo?	Periodicidade do armazenamento externo	Responsável

Após a definição dos métodos de cópias de segurança, devem ser relacionados os ativos envolvidos no processo e se existem processos de geração de cópias de segurança destes ativos. Para os ativos que possuem cópias de segurança, identificar qual o método de cópias de segurança, qual a periodicidade que as cópias de segurança são realizadas, em horas, dias, semanas, meses ou anos, qual o período de armazenamento das mídias (ciclo de cópias de segurança) e quem é o responsável pelas cópias de segurança.

Além da realização das cópias de segurança, deve haver testes de recuperação das mesmas. Devem-se identificar quais ações realizadas para garantir a integridade das cópias de

segurança, quem é o responsável pela validação e qual a periodicidade que a validação deve ser realizada, baseando-se na criticidade do ativo. Segundo o Cobit, é recomendado o armazenamento externo das mídias para segurança em caso de desastres. Deve-se identificar se há armazenamento externo das mídias, qual é a periodicidade do armazenamento externo e quem é o responsável.

Todos os ativos levantados e seus procedimentos de cópias de segurança devem ser registrados Os métodos devem ser registrados no Anexo B, 7.1 Cópias de Segurança. Os procedimentos de cópias de segurança utilizados devem ser apresentados para os gestores e patrocinadores da organização a fim que eles possam se sentir seguros em relação aos seus dados.

3.3.5 Elaboração do plano de resposta a incidentes

O plano de resposta a incidentes deve ser elaborado para uma ameaça referente a um ativo. Devem ser relacionados os ativos, suas ameaças e o SLA de cada ativo.

As ações devem ser tomadas a partir da ocorrência de das ameaças identificadas. A organização deve determinar quais ameaças deverão ser tratadas com base nos níveis dos riscos identificados e da eficiência das ações de tratamento. As ações de tratamento são ações proativas a um risco, os planos de tratamento são ações reativas.

A definição das ações pode ser obtida em conjunto com a área de TI e seus usuários chave. Neste momento não devem ser detalhadas as ações passo a passo, este detalhamento será tratado na etapa subsequente. As ações que serão tomadas variam muito de organização para organização e se baseiam nas restrições apontadas no escopo da continuidade. Estas ações devem levar em consideração o SLA acordado para cada ativo, porém podem possuir um SLA próprio com base na capacidade da equipe em entregar o serviço.

A forma de ativação do plano deve ser identificada para cada ação, estas podem ser através de procedimentos manuais, quando necessitam de intervenção humana, ou de forma automática, quando o sistema consegue realizar os procedimentos de resposta sem a intervenção humana.

Cada ação deve ser identificada em: recuperação, que são ações para restaurar um ativo inoperante; contingência, que representam ações de reativar um serviço em um ambiente paralelo; e de retorno em produção, que são as ações para retornar o uso do ambiente de produção após o uso em contingência. Para cada ação de contingência deve haver uma ação de retorno de produção, estas devem possuir o SLA reestabelecido conforme capacidade da equipe responsável.

Cada ação definida deve possuir um responsável por ativá-la e coordená-la na sua execução. Conforme a BS 25999, deve-se estabelecer um plano de comunicação na ativação dos planos de resposta, definindo quem deverá ser comunicado no momento da ativação e quem deverá ser comunicado após a realização das ações. Em muitos casos pode haver necessidade de suporte a partir de terceiros, esta necessidade deve ser identificada para o acionamento dos terceiros em casos de ativação do plano, registrando o nome e a empresa do contato (BS 25999, 2006).

Todas as ações levantadas devem ser registradas no Anexo B, 8.1 Planos de resposta a incidentes. Este artefato representa o catálogo de ações que devem ser realizadas conforme cada ameaça, conforme figura 18, porém não há detalhamento de cada ação, este detalhamento será compreendido na etapa subsequente, registro do acordo de nível operacional, OLA.

Figura 18: Artefato para registro dos planos de resposta a incidentes.

Documento 8. Plano de Resposta										
8.1. PLANOS DE RESPOSTA A INCIDENTES										
Ação	Ameaça	SLA	Plano de continuidade	Ativação	Tipo	Responsáveis	Quem deve ser comunicado?			OLAs
							Na ocorrência	Após realização	Quem pode ser acionado?	

Os terceiros que relacionados para auxiliar na execução das ações devem ser registrados no item 17, Contatos, dos artefatos do plano de continuidade. É muito importante que a lista de terceiros esteja sempre disponível e contenha o nome do contato, a empresa que este representa, o responsável pelo contato, quais ações estão relacionadas a este contato, o endereço do contato, o telefone fixo e celular, o endereço de correio eletrônico e outras formas de comunicação com este contato. A figura 19 identifica o cadastro dos contatos.

Figura 19: Registro dos contatos na aba contatos do artefato de plano de continuidade.

Documento 17. Contatos								
17.1. CONTATOS								
Contato	Empresa	Responsável	Ações envolvidas	Endereço	Telefone	Celular	E-Mail	Outras formas

3.3.6 Documentação dos controles – Nível de Serviço Operacional - OLA

O nível de serviço operacional, OLA, é um guia para a equipe técnica realizar as ações definidas nos planos de resposta a incidentes, plano de recuperação de desastres e plano de testes. O OLA é um manual de operação e é constituído por um guia de ações que devem ser executadas para atingir o objetivos das ações dos planos. O OLA deve ser detalhado de forma técnica, afim de que os responsáveis pelas ações possam realiza-las sem a necessidade de consultar outra fonte. Cada organização define o OLA da melhor forma aplicável a seu ambiente, podendo ser manuais de instruções com imagens de tela, manuais operacionais dos próprios ativos ou scripts automatizados. A solução proposta compreende um guia de atividades para a elaboração dos OLA na forma de um manual de operações.

Segundo o guia proposto, um OLA deve ser elaborado para cada ação definida nos planos de continuidade. Para cada OLA que será elaborado, deve-se identifica-lo conforme suas ações: plano de resposta a incidentes, plano de recuperação de desastres, testes e revisão, os três últimos serão detalhados nas etapas subsequentes do plano. Esta classificação irá facilitar na visualização dos OLA no momento de ativação.

Para elaborar um OLA, devem ser identificados todos os passos realizados para executar as ações dos planos. Este passo a passo será seguido na ativação dos planos, portanto, quanto maior seu detalhamento, mais simples será sua execução e, em caso de ausência do responsável, outra pessoa da equipe possa executá-lo. Para cada ação do OLA pode-se definir um responsável, que pode ser um executor das atividades diferente do responsável pelo plano, uma pessoa alternativa para a ausência deste ou um terceiro. Em caso de necessidade, registrar os terceiros que podem ser acionados para situações de emergência ou ausência dos responsáveis. Os terceiros devem estar cadastrados na aba de contatos conforme explicado na atividade anterior.

O guia propõe o registro dos OLA no Anexo B, 11.1 Acordos de Nível Operacional – OLA, conforme figura 20, porém, caso a organização ache necessário, pode ser criado um manual de operações com maior detalhamento, imagens de tela e outros recursos de imagem e vídeo. Neste caso, o artefato gerado deve ser anexado no Anexo B, 11.1 Acordos de Nível Operacional – OLA.

Figura 20: Artefato para registro dos OLAs.

Documento 11. OLA					
11.1. ACORDOS DE NÍVEL OPERACIONAL - OLA					
Ação	Tipo	Instruções operacionais	Responsável	Quem pode ser acionado?	Anexos

3.3.7 Revisão do plano de resposta a incidentes

Após o registro dos planos de resposta a incidentes e seus OLAs, a solução proposta sugere a sua revisão e apresentação para os patrocinadores. Nesta etapa deve-se revisar o registro de todas as ações envolvidas no plano de resposta a incidentes referente a sua conformidade, responsáveis definidos e coerência entre as ameaças e ações. Os OLAs também devem ser revisados e validados pela equipe responsável por sua execução, registrando a aprovação na aba OLA do modelo de plano de continuidade.

Os planos de resposta a incidentes devem ser apresentados aos gestores do processo, patrocinadores e usuários chave envolvidos. O objetivo da apresentação é fornecer a segurança para os envolvidos. A divulgação fica a critério da organização, mas é muito importante que seja registrada em ata, identificando pontos importantes que sejam discutidos na apresentação para elaborar planos de manutenção futuros.

3.3.8 Elaboração do plano de recuperação de desastre

O plano de recuperação de desastre é um conjunto de atividades que a organização deve executar para reestabelecer sua operação em caso de ocorrência de um desastre que impossibilite sua operação total. Por ser um conjunto de atividades específica, o plano de recuperação de desastre é tratado de forma diferente dos planos de resposta a incidentes.

Para sua elaboração, foram utilizados conceitos cruzados de todas as referências bibliográficas. O guia proposto apresenta um conjunto de atividades para definir toda a estrutura de ativos necessária para executar a operação de negócio da organização e um conjunto de ações para o reestabelecimento das operações.

3.3.8.1 Definição da estrutura necessária para a recuperação de desastres

Para elaborar um plano de recuperação de desastres é necessário determinar as condições de ativação do plano, quem serão os responsáveis pelas ações e decisões, e quais os ativos necessários para que a organização possa executar suas operações de negócio. O guia proposto apresenta uma sequência de ações para a identificação destes ativos e sua priorização.

O primeiro passo para a elaboração do plano de recuperação de desastres é a definição do desastre que ocasionará a ativação do plano. O desastre pode ser definido pelos gestores e patrocinadores baseado na ocorrência de riscos que resultem na interrupção de uma grande quantidade de ativos. A parada total dos ativos de TI que são necessários para a execução dos processos de negócio é um exemplo bastante utilizado como desastre (WALLACE, 2004).

O plano de recuperação de desastres precisa ter suas condições de ativação bem definidas, como quais as consequências que ocasionariam na necessidade da recuperação de desastres, por exemplo, o incêndio do centro de processamento de dados da organização. Devem ser definidos os responsáveis por acionar e coordenar as ações após a ativação, estes responsáveis não necessariamente precisam ser as mesmas pessoas.

Além destes responsáveis citados, outros responsáveis precisam ser determinados, como quem deverá aprovar as ações do plano, este responsável é acionado quando as ações envolverem alterações nos processos organizacionais e podem apresentar vulnerabilidades. Deve ser determinado um responsável pela aprovação de investimentos e despesas necessárias para executar as ações, este responsável financeiro deverá trabalhar em constante comunicação com o responsável pelas ações e responsável pela aprovação. É necessário determinar quem será o responsável por realizar as aquisições e contratações necessárias, geralmente um funcionário do setor de compras, caso exista.

Da mesma forma que definido nos planos de resposta, o plano de comunicação precisa ser estabelecido. É importante que seja definido quem seve ser comunicado na ativação do plano, nas execuções e na conclusão do plano.

O responsável pelo plano, juntamente com os gestores de processo, patrocinadores e demais responsáveis devem definir um tempo para retorno das operações, um SLA. Este SLA definido é a expectativa da organização baseado na necessidade de retorno e capacidade operacional. O SLA aqui definido será recalculado após a elaboração das ações.

A organização precisa definir um local onde será executado o plano de recuperação de desastres. O local pode variar conforme o desastre ocorrido, em caso de destruição do local de produção deve ser definido um novo local para o reestabelecimento das operações.

Todas estas definições devem ser registradas no Anexo B 9.1 Ativação do plano de recuperação de desastres, conforme figura 21.

Figura 21: Registro da ativação e responsáveis pela recuperação de desastres.

Documento 9. Recuperação de Desastres	
9.1. ATIVAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES	
PLANO DE RECUPERAÇÃO	
Plano de continuidade	
Definição do Desastre	
Responsável pela ativação	
Responsável pelas ações	
Responsável pelas tomadas de Decisão	
Responsável Financeiro	
Responsável pelas aquisições	
Quem deve ser informado	
Prazo Estimado para reestabelecimento das atividades	
Local definido para a continuidade de negócios	
Plano aprovado por	

A solução proposta traz um conjunto de ações para relacionar os ativos de TI, previamente identificados na análise de riscos ou específicos para restauração em novo cenário, como hardware, comunicação, infraestrutura, software, recursos humanos e serviços terceirizados necessários para a organização operar seu processo de negócio. É importante que os todos ativos necessários para operar o negócio como um todo sejam relacionados, não se limitando apenas aos ativos mínimos necessários.

O guia trata a recuperação como um todo, porém a organização pode optar por relacionar apenas os ativos mínimos necessários para o reestabelecimento das operações de negócio.

Para cada ativo deve ser estabelecido o responsável por sua recuperação, este responsável não necessariamente deve ser o responsável pelo ativo em produção.

Para cada ativo, deve ser determinada a prioridade de recuperação em alta, média ou baixa. Estas prioridades podem diferir das previamente identificadas na análise de riscos, pois nesta etapa está sendo definida a prioridade para recuperação em uma ordem para reestabelecimento da operação de negócio como um todo. A prioridade dos ativos deve ser

estabelecida a partir de um consenso entre a equipe de TI, os gestores de processo e usuários chave envolvidos em cada ativo.

Um ativo de alta prioridade de recuperação é um ativo que deve ser recuperado o mais rápido possível, necessário para o reestabelecimento da operação nas condições mínimas. Um ativo de média prioridade de recuperação é um ativo que deve ser recuperado para reestabelecer as operações de negócio, mas que não são urgentes. Um ativo de baixa prioridade de recuperação deve ser recuperado para o retorno em produção após a operação estar reestabelecida.

a) Ativos de Hardware Mínimos necessários

O primeiro tipo de ativos a ser identificado deve ser o Hardware. Deve-se relacionar os ativos de Hardware necessários para manter a operação de negócio funcional, identificando um responsável técnico por administrá-los na ativação do plano de recuperação. Para cada ativo de hardware deve-se identificar a quantidade necessária, a descrição técnica detalhada do hardware para ser adquirido em caso de necessidade, se este ativo possui redundância ou precisará ser adquirido em caso de desastre, o custo da recuperação deste ativo e qual a sua prioridade de recuperação.

Os ativos de hardware necessários podem ser separados em servidores, computadores de usuário, computadores portáteis, impressoras, periféricos como monitores, leitores de código de barras, entre outros, hardware para restauração das cópias de segurança e outros possíveis equipamentos necessários.

Todas as definições devem ser registradas no Anexo B, 9.2.1 Ativos de TI mínimos necessários. A figura 22 representa a tabela para registro dos ativos da estrutura para a continuidade, os demais tipos de ativo seguem este padrão.

Figura 22: Artefato para registro dos ativos de TI necessários para o reestabelecimento da operação de negócio

9.2. ESTRUTURA MÍNIMA PARA CONTINUIDADE DE NEGÓCIOS EM SITUAÇÃO DE RECUPERAÇÃO DE DESASTRE								
9.2.1. Ativos de TI Mínimos Necessários								
Plano de recuperação	Ativo para recuperação	Tipos de Ativos de TI	Quantidade	Descrição Detalhada	Redundante?	Custo aproximado	Prioridade	Responsável

b) Ativos de comunicação mínimos necessários

Os ativos de comunicação necessários para operacionalizar o negócio da organização devem ser identificados. Para cada ativo deve ser identificado um responsável técnico por

administrá-los na ativação do plano de recuperação, a quantidade necessária se aplicável, a descrição técnica para aquisição se necessária, se este ativo possui redundância ou precisará ser adquirido em caso de desastre, o custo da recuperação deste ativo e qual a sua prioridade de recuperação.

Ativos de comunicação que podem ser identificados nesta atividade são comutadores de rede, Switches, a infraestrutura de cabeamento necessária e suas particularidades como conexão, categoria e equipamentos que permitem a comunicação como conversores, roteadores de rede sem fio e outros equipamentos necessários. Os serviços de conexão a internet e telefonia devem ser identificados, detalhando a operadora e velocidade, juntamente com os equipamentos necessários para sua operação como roteadores, centrais e aparelhos telefônicos.

Todas as definições devem ser registradas no Anexo B, 9.2.1 Ativos de TI mínimos necessários.

c) Ativos de infraestrutura necessários

Os ativos de infraestrutura como fornecimento de energia, estrutura predial e outros necessários para a operação devem ser identificados. Nesta atividade deve-se relacionar os ativos de infraestrutura, identificando um responsável técnico por administrá-los na ativação do plano de recuperação. Para cada ativo de infraestrutura deve-se identificar a quantidade necessária se aplicável, a descrição detalhada para aquisição se necessária, se o ativo possui redundância ou precisará ser adquirido em caso de desastre, o custo da recuperação deste ativo e qual a sua prioridade de recuperação.

São possíveis ativos de infraestrutura a serem relacionados nesta atividade: o fornecimento de energia, estrutura predial, ativos de segurança como controle de acesso, câmeras, aparelhos de ar condicionado e estabilizadores de energia.

Todas as definições devem ser registradas no Anexo B, 9.2.1 Ativos de TI mínimos necessários.

d) Ativos de software e sistemas de informação necessários

Os sistemas de informação são essenciais para a operação de negócio da organização. Os ativos de software e sistemas devem ser relacionados, identificando um responsável técnico por administrá-los na ativação do plano de recuperação.

Para cada ativo de software e sistemas de informação deve-se identificar a quantidade necessária se aplicável, a descrição da arquitetura do sistema a fim de facilitar na

elaboração das ações, se este ativo possui redundância ou precisará ser adquirido em caso de desastre, o custo da recuperação deste ativo e qual a sua prioridade de recuperação.

As aplicações de negócio devem ser identificadas e em sua descrição deve constar um resumo de sua arquitetura e funcionamento, relacionando outros ativos que são necessários para o seu funcionamento. É muito importante identificar se há cópias de segurança destas aplicações, seja dos bancos de dados ou dos programas ou instaladores necessários. Quanto aos softwares, é importante identificar se há cópias de segurança das mídias e licenças destes softwares. Os sistemas gerenciados de banco de dados também precisam ser identificados , descrevendo suas características técnicas, quais sistemas o utilizam e se há cópias de segurança tanto das informações dos bancos de dados quanto da sua configuração, das mídias e das licenças para restauração.

Além dos sistemas e software, é importante identificar sistemas de arquivos de rede ou outros arquivos necessários para o processo de negócio, identificando sua localização, ativos envolvidos e existência de cópias de segurança dos mesmos.

É importante definir qual o custo de restauração dos ativos de software e programas caso necessários. Este custo deve incluir serviços de terceiros caso acionados.

Todas as definições devem ser registradas no Anexo B, 9.2.1 Ativos de TI mínimos necessários.

e) Ativos de recursos humanos necessários

As pessoas envolvidas na recuperação de desastres são os ativos mais importantes do processo. É indispensável identificar os recursos humanos necessários para reestabelecer o ambiente tecnológico, identificando a competência necessária, seja esta equipe presente na organização ou não. Para cada competência de recursos humanos identificados devem-se identificar os cargos necessários, a quantidade de pessoas para exercer o cargo, as funções deste cargo, identificar se a organização já possui esta pessoa ou não, se ela deve ser funcionária da organização ou terceira. Cada recurso humano deve ser atribuído uma criticidade desta pessoa no processo, definido em baixo, média e alta através do número de tarefas que esta pessoa irá executar e sua importância.

Todas as definições devem ser registradas no Anexo B, 9.2.2 Ativos de recursos humanos mínimos necessários.

f) Serviços de terceiros necessários

Alguns serviços terceirizados são necessários para a operação da organização, deve-se identificar os serviços de terceiros necessários para operacionalizar o ambiente tecnológico como fornecimento de energia externo, fornecimento de serviços de infraestrutura predial, fornecimento de suporte à servidores, fornecimento de suporte a sistemas, entre outros.

Para cada serviço identificar o terceiro envolvido, a descrição dos serviços prestados, o contato de quem deve ser acionado, o custo aproximado do serviço que será prestado e a necessidade de acionamento do terceiro conforme priorização dos ativos. Os terceiros envolvidos devem ser registrados na aba de contatos do artefato do plano de continuidade.

Todas as definições devem ser registradas no Anexo B, 9.2.3 Serviços de terceiros mínimos necessários.

Após toda a definição da estrutura mínima, é essencial revisar tudo o que foi identificado nesta atividade para garantir que nenhum ativo tenha ficado de fora do levantamento. As definições de estrutura para a recuperação de desastres devem ser apresentadas para os patrocinadores e gestores de processo. É importante que seja registrada em ata para acompanhamento futuro, através dela podem surgir planos de ação para melhorar a estrutura de contingência.

3.3.8.2 Elaboração das ações para recuperação de desastre

A partir da estrutura definida na atividade anterior, o guia propõe uma sequencia de atividades para elaborar um plano de recuperação dos ativos essenciais para a operação de negócio da organização.

Os gestores de processo, a equipe de TI e os usuários chave devem ser envolvidos para a elaboração de um cronograma de atividades para a restauração dos ativos essenciais para o funcionamento das operações de negócio. É muito importante este envolvimento dos usuários para que estes possam compreender os processos de restauração e quando poderão realizar suas atividades de negócio conforme a recuperação for ocorrendo. Este cronograma inicial deve se basear nas prioridades estabelecidas e irá direcionar as ações de recuperação.

Com base nas prioridades estabelecidas na definição dos ativos para a recuperação de desastres, devem-se planejar as ações que devem ser executadas para reestabelecer o ambiente tecnológico. Estas ações devem restaurar os ativos em ordem de prioridade, da alta para a baixa. Para cada ação planejada deve-se calcular um acordo de nível de serviço, SLA, para

definir o tempo necessário para sua execução, que posteriormente irá fazer parte do tempo total de recuperação.

Para cada ação, identificar se é uma reinstalação, comum para hardware, softwares ou serviços de infraestrutura, ou uma recuperação, comum para ações de restauração de cópias de segurança. Cada ação deverá possuir um responsável por sua execução. Este responsável pode ser qualquer pessoa que esteja apta para realizar as tarefas, seja ela funcionária ou terceirizada conforme recursos humanos e serviços de terceiros definidos na atividade anterior.

As ações podem depender de outra ação para poder ser iniciada, esta relação deve ser identificada. Ações independentes de outras poderão ser executadas em paralelo durante a ativação do plano. Para cada ação devem-se identificar quais ativos serão recuperados, caso sejam, após o seu término.

Seguindo o mesmo molde dos planos de resposta a incidentes, deve-se estabelecer quem deve ser comunicado em caso de ocorrência da ação, quem deve ser comunicado após a realização das ações e quem pode ser acionado para prover suporte à realização das ações. Os terceiros acionados devem ser registrados no Anexo B, 17.1 Contatos.

Todas as ações elaboradas nesta atividade devem ser registradas no Anexo B, 10.1 Plano de ações para a recuperação de desastre. A figura 23 representa o artefato para o registro das ações. Para cada ação registrada nesta atividade deve-se registrar um acordo de nível operacional, no Anexo B, 11.1 Acordos de serviço operacional – OLA. As mesmas regras válidas no registro dos OLA na atividade de elaboração dos planos de resposta a incidentes devem ser aplicadas para as ações de recuperação de desastres.

Figura 23: Artefato para registro das ações pertencentes ao plano de recuperação de desastres

Documento 10. Plano de Recuperação												
10.1. PLANO DE AÇÕES PARA A RECUPERAÇÃO DE DESASTRE												
Plano de recuperação	Ação	Nro da Ação	Tipo de ação	SLA	Responsável	Dependente?	Ativos reabilitados	Quem deve ser comunicado			Descrição da ação	OLA
								Na ocorrência	Após realização	Quem pode ser acionado?		

Após o registro das atividades, o tempo de recuperação deve ser recalculado a partir da combinação dos SLA determinados no plano de recuperação de desastres. Este novo SLA deve ser registrado no Anexo B, 9.1 Ativação do plano de recuperação de desastres.

3.3.8.3 Revisão do plano de recuperação de desastres

É importante que todas as ações sejam revisadas para garantir que nenhuma atividade tenha ficado de fora do cronograma de ações. O plano de recuperação de desastres deve ser apresentado aos patrocinadores e gestores de processo para que eles possam compreender a estrutura e o esforço necessários para o reestabelecimento das operações de negócio. Esta apresentação deve ser registrada em ata, através dela podem surgir novas avaliações e aprovações dos planos de tratamento de riscos para evitar o desastre.

Apresentar a estrutura necessária e as ações que devem ser realizadas para executar plano de recuperação de desastres para os patrocinadores e gestores de processo. Esta apresentação pode ser realizada através de reunião ou de envio eletrônico do artefato do plano de continuidade. É importante registrar em ata a apresentação e pontos importantes discutidos na apresentação

Após apresentação, o plano de recuperação deve ser assinado pelo responsável pela continuidade, pelos patrocinadores e gestores do processo validando sua elaboração. Esta validação serve para confirmar o plano, mas não significa que o mesmo será aplicado em produção ainda.

3.3.9 Revisão e aprovação do plano de continuidade de negócios

Segundo o guia proposto, até esta etapa foram gerados o escopo da continuidade, o resultado da análise de riscos, os acordos de nível de serviço, as ações de tratamento, os planos de resposta a incidentes, os procedimentos de cópia de segurança, o plano de recuperação de desastre e os acordos de nível operacional. É sugerida a revisão de consistência entre todos os registros do plano antes de prosseguir para a aprovação.

O plano de continuidade gerado deve ser distribuído para os patrocinadores e gestores de processo. Estes devem realizar a leitura e avaliação do plano de continuidade elaborado. O gestor da continuidade deve orientar os gestores e patrocinadores a avaliarem a consistência das informações e a possível eficiência da recuperação de desastre em situações reais, quanto mais detalhistas nessa avaliação, melhor será o resultado. O resultado da avaliação deve ser aprovado, reprovado ou revisar. Em caso de reprovação, os avaliadores devem registrar o que não está de acordo e causou a reprovação. Em caso de necessidade de revisão, os avaliadores devem apontar o que precisa ser revisado. Conforme as necessidades

de revisão, deve ser criado um plano de revisão, abordado nas etapas subsequentes, para corrigir o que foi apontado, após a manutenção realizada, o processo de avaliação deve ser retomado.

O gestor da continuidade precisa recolher o parecer de todos os avaliadores e registrar no Anexo B, 12.1 Aprovação do plano de continuidade de negócios. A figura 24 apresenta o artefato sugerido para este registro. Caso seja conveniente, podem ser feitas observações no Anexo B, 12.2 Observações adicionais do gestor da continuidade, referente a aprovação do plano para auxiliar o gestor da continuidade no futuro.

Figura 24: Artefato para registro da aprovação do plano de continuidade de negócios

Documento 12. Avaliação							
12.1. APROVAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS							
Plano de continuidade	Aprovador	Papel	Parecer	Etapa			Observações
				Definição do escopo	Análise de riscos	Plano de continuidade	

Quando todos os avaliadores realizarem a aprovação do plano, pode-se efetivamente considerá-lo finalizado e aprovado, a partir disto pode ser aplicado em produção e utilizado conforme as ocorrências demandarem. A próxima fase trata a execução, monitoramento e controle da continuidade de negócios.

3.4 EXECUÇÃO, MONITORAMENTO E CONTROLE DA CONTINUIDADE DE NEGÓCIOS

Para uma gestão correta da continuidade não basta elaborar o plano de continuidade, este deve ser administrado, mantido, testado e melhorado. A solução proposta se baseia nos conceitos da BS 25999, Itil e Cobit para montar um plano de execução, monitoramento e controle da gestão da continuidade. O guia apresenta um conjunto de atividades para realizar a distribuição e armazenamento do plano, criar e manter os indicadores de desempenho, manter um processo de registro de ocorrência de ameaças, criar e registrar um plano de testes e elaborar e manter um processo de manutenção e melhoria contínua do plano de continuidade de negócios.

3.4.1 Distribuição do plano de continuidade

O plano de continuidade é um documento crítico para a organização e por isso deve ser armazenado de forma segura e divulgado na organização.

O plano deve ser disseminado entre os envolvidos nas atividades, estes devem estar cientes de todos os ativos, ricos e ações a serem realizadas em caso de ocorrência de alguma ameaça. É sugerido a utilização de ferramentas de armazenamento e publicação gerenciáveis como sistemas de colaboração, sistemas de gestão eletrônica de documentos, servidores de arquivos e bibliotecas de documentos físicos.

Todos os responsáveis por atividades devem possuir acesso ao plano e precisam estar cientes de suas responsabilidades e momento de ativação de seus planos, esta certificação pode ser obtida através de reunião registrada em ata, confirmações por correio eletrônico ou aprovações eletrônicas (Cobit, 2007).

Por se tratar de um documento crítico para a organização, o plano de continuidade deve ser identificado como um ativo da análise de risco, incluso nas rotinas de cópias de segurança e tratado através de ações de tratamento de riscos que envolvem este ativo. O plano precisa ter cópias impressas e digitais armazenadas em local a prova de fogo e em locais remoto, caso possível, estas medidas visam garantir que o plano esteja disponível sempre que for necessária sua ativação.

3.4.2 Registro de ocorrências

Conforme o ITIL, todo e qualquer serviço de TI realizado deve possuir o devido registro a fim de gerar condições para a medição e desempenho do plano de continuidade elaborado. Este registro deve ser algo simples e que forneça condições para a organização administrar a utilização dos planos (ITIL, 2007).

O modelo proposto sugere a utilização de um artefato contendo informações das ocorrências e da efetividade dos planos. A organização pode optar por utilizar ferramentas de gerenciamento de serviço caso seja conveniente.

Para os planos de resposta a incidentes, o guia proposto sugere o registro no Anexo B, 13.1 Registro de ocorrências de incidentes, conforme figura 25. Neste artefato devem ser registradas cada ameaça que ocorrer, identificada por um número sequencial e a data de sua ocorrência. Para cada ocorrência, deve-se registrar se houve interrupção do funcionamento do

ativo ou serviço de TI, quais as ações realizadas, quem foram os responsáveis por sua execução e se o plano de resposta a incidentes foi eficiente na solução ou não. Deve-se registrar também o SLA acordado e tempo de realização da tarefa, este registro servirá para alimentar os indicadores de desempenho. Caso haja algum custo de aquisição, manutenção ou de serviço envolvido na ação, este deve ser registrado.

Figura 25: Artefato para registro de ocorrências de incidentes

Documento 13. Registro de Ocorrências										
13.1. REGISTRO DE OCORRÊNCIAS DE INCIDENTES										
Número da Ocorrência	Data	Ameaça	Interrupção de ativos?	Ação realizada	Ação realizada (caso não prevista)	Utilização do plano na solução	SLA acordado	Tempo realizado	Custo da solução	Responsável

O plano de recuperação de desastres deve ser registrado de forma semelhante aos de resposta, porém registrado no Anexo B, 13.2 Registro de recuperação de desastres, conforme figura 26.

Figura 26: Artefato para registro de recuperação de desastres

13.2. REGISTRO DE RECUPERAÇÃO DE DESASTRES									
Desastre	Data de início	Data de solução	Desastre (descrição)	Utilizado plano na solução?	Plano de recuperação utilizado?	Eficiência do plano	SLA acordado	Tempo realizado	Responsável

Para cada ativação do plano de recuperação de desastres deve-se registrar um número sequencial, a data de ocorrência e a data do reestabelecimento das operações de negócio. O desastre ocorrido deve ser descrito com detalhes, relatando como aconteceu, descrevendo um resumo do que foi realizado para sua recuperação e o que não ocorreu de acordo, caso aplicável. O responsável pela execução das ações do plano deve ser registrado juntamente com o parecer da efetividade do plano na recuperação. Ações não contempladas no plano devem ser registradas nos detalhes. Deve-se registrar também o SLA acordado e tempo de realização da tarefa, este registro servirá para alimentar os indicadores de desempenho. Caso haja algum custo de aquisição, manutenção ou de serviço envolvido na ação, este deve ser registrado.

Os resultados de ocorrências registrados devem ser enviados aos patrocinadores e gestores de processo conforme a organização achar conveniente. Estes resultados são fontes para os indicadores de desempenho tratados na etapa subsequente. É importante que os planos que não estiverem em conformidade sejam revisados através de uma ação de manutenção.

3.4.3 Medição e monitoramento

Os planos de continuidade precisam ser medidos para obter-se a segurança de seu funcionamento, para isso o Cobit sugere algumas métricas para a avaliação da eficiência dos planos (Cobit, 2007). O modelo proposto apresenta alguns indicadores e as atividades para elaborá-los e medi-los.

São indicadores sugeridos no guia: a quantidade de horas perdidas por usuários devido à inoperância não planejada dos sistemas, a porcentagem de incidentes atendidos e solucionados pelos planos de resposta a incidentes, a porcentagem de incidentes atendidos e solucionados dentro do prazo do SLA, a quantidade de ativos cobertos pelo plano de continuidade de negócios, o percentual de testes realizados com sucesso, sem necessidade de correção e a frequência de interrupção de serviços nos sistemas críticos.

Para elaborar os indicadores, na ordem proposta acima deve-se:

a) Determinar uma quantidade mínima aceitável de horas perdidas por usuários devido à inoperância não planejada dos sistemas. Esta quantidade deve levar em consideração a expectativa de recuperação da organização e a sua capacidade de resolução, já definidas nos SLAs de cada plano de resposta a incidentes. A fonte destes dados é o tempo efetivo de solução registrado no registro de ocorrências;
b) Determinar uma porcentagem de incidentes atendidos pelos planos de resposta a incidentes. Este indicador visa identificar às ameaças que foram recuperadas pelos planos de resposta a incidentes, a efetividade dos planos está registrada no registro de ocorrências e serve como fonte para este indicador;
c) Determinar uma porcentagem de incidentes atendidos e solucionados dentro do prazo do SLA. Este indicador serve para medir a eficiência de atendimento dentro dos SLAs estabelecidos nas ações. A organização deve estabelecer uma meta para que os planos sejam executados em tempo possível. A meta não necessariamente precisa ser cem por cento do SLA, ela pode variar conforme as

condições de organização para organização. Os tempos efetivos registrados no registro de ocorrências servem como base para este identificador;

d) Definir uma quantidade possível de ativos cobertos pelo plano de continuidade de negócios. A meta deste indicador deve ser o número de ativos mapeados na análise de risco, qualquer outro ativo identificado não coberto pelos planos ocasionará um impacto negativo neste indicador. Este indicador serve para medir a abrangência do plano de continuidade. Os dados deste indicador podem ser obtidos através dos resultados das ocorrências, onde são identificados ativos que não estavam cobertos pelos planos de resposta ou recuperação;
e) Definir um percentual de testes realizados com sucesso, sem necessidade de correção. Este indicador serve para medir a eficiência dos testes. A meta deve ser estabelecida conforme a quantidade de testes realizados. Os dados para este indicador são provenientes dos registros dos testes;
f) Definir uma meta mínima de interrupção de serviços nos sistemas críticos. Este indicador serve para avaliar a eficiência das ações de tratamento com objetivo de evitar o risco. A meta deste indicador deve ser estabelecida com base na criticidade dos ativos e determinada em conjunto dos gestores de processo. Qualquer ocorrência que represente a parada de um ativo crítico causa impacto negativo neste indicador, conforme identificado no registro de ocorrências;
g) Criar indicador com número máximo de desastres ocorridos. Este indicador serve para medir as ações de tratamento para evitar desastres. Este indicador deve contemplar a não ocorrência de desastre, pois estes não devem ocorrer. O registro de desastres serve como fonte de dados para este indicador;
h) Criar indicador de sucesso na recuperação de desastres através do plano de recuperação caso ocorra um desastre. Este indicador deve ser considerado somente na ocorrência de desastres e deve possuir como meta um valor positivo.

A organização pode precisar criar outros indicadores que possam ser úteis para medir a eficiência do plano de continuidade, esta decisão fica a cargo da organização.

Os indicadores devem ter seus períodos de avaliação definidos conforme período que a organização deseja medir, o guia propõe um acompanhamento mensal dos resultados, mas cada indicador pode ter uma periodicidade de avaliação independente.

Os indicadores devem ser registrados no Anexo B, 14.1 Indicadores de desempenho da continuidade. A figura 27 ilustra o artefato de registro dos indicadores de desempenho.

Após cada período de avaliação, o resultado dos indicadores deve ser registrado na aba de indicadores e então comunicado para os patrocinadores e gestores de processo envolvidos.

Figura 27: Artefato para registro dos indicadores propostos pelo modelo de plano de continuidade

Documento 14. Indicadores												
14.1. INDICADORES DE DESEMPENHO DA CONTINUIDADE												
Indicador de performance	Mês 1		Mês 2		Mês 3		Mês 4		Mês 5		Mês 6	
	Meta	Realizado	Meta	Realizado	Meta	Realizado	Meta	Realizado	Meta	Realizado	Meta	Realizado
Quantidade de horas perdidas por usuários devido à inoperância não planejada dos sistemas												
Porcentagem de incidentes atendidos e solucionados pelos planos de resposta a incidentes												
Porcentagem de incidentes atendidos e solucionados dentro do prazo do SLA												
Quantidade de ativos cobertos pelo plano de continuidade de negócios												
Percentual de testes realizados com sucesso, sem necessidade de correção												
Frequencia de interrupção de serviços nos sistemas críticos												
Desastres ocorridos												
Sucesso na recuperação de desastres através do plano												
Outros												

3.4.4 Simulações e Testes do processo

Os planos de continuidade podem ser validados operacionalmente pelos seus responsáveis, mas somente através da sua execução que pode ser confirmada sua eficiência. O guia proposto sugere atividades para a elaboração de um plano de testes e dos registros de suas simulações. Os testes são uma forma de se garantir que os planos funcionaram nas situações que precisarem ser ativados.

3.4.4.1 Definição do plano de testes

Para realização dos testes, primeiramente precisa-se definir quais serão os testes e seus objetivos. Os testes são elaborados para testar ações do plano de continuidade.

Segundo o modelo, deve-se iniciar definindo os tipos de plano de testes a serem realizados como testes de desempenho, simulação de queda de energia, simulações em ambiente de produção, simulações em ambiente de protótipo, entre outros possíveis tipos que a organização definir. Estes planos de testes servem para facilitar na classificação dos testes.

Para cada plano de teste, definir qual será a ação de teste e identificar quais planos serão abrangidos neste teste. A ação deve ser detalhada através do registro de um OLA, no item 9 dos artefatos, do tipo teste, é essencial que as ações de teste sejam descritas da melhor

maneira possível para facilitar na execução dos testes. Para cada teste devem-se estabelecer os objetivos do teste, são exemplos de objetivos a identificação de ameaças, validação de alterações, identificação de vulnerabilidades, garantia de segurança, entre outros objetivos que podem ser definidos pela organização.

Os testes podem ter sua complexidade variada conforme suas ações e envolvimento de pessoas. A complexidade do teste deve ser classificada em baixa, média ou alta. Baixa complexidade refere-se a testes que podem ser realizados rapidamente sem envolvimento de mais de uma pessoa, média são testes que requerem mais de uma pessoa para executar e podem demorar um tempo moderado, alto são testes que envolvem muitas pessoas, geralmente quase ou todos os envolvidos, e levam diversos dias para sua realização.

Seguindo o modelo, uma frequência de realização de testes deve ser estabelecida em um período aceitável pela organização. Estes períodos refletem nos indicadores propostos. Para cada teste deve-se definir um responsável por realizar, acompanhar ou coordenar os testes. Este será responsável por informar os resultados dos testes.

Um plano de testes para recuperação de desastre deve ser elaborado com cautela. A complexidade de uma simulação deste tipo é muito alta e o OLA deve ser elaborado o mais semelhante possível com as ações do plano. A organização pode dividir o teste de recuperação de desastres em diversos testes menores para minimizar a complexidade.

Todos os testes definidos nesta etapa devem ser registrados no Anexo B, 15.1 Plano de testes. A figura 28 representa o artefato para cadastro do plano de testes e o registro de sua realização.

Figura 28: Artefato para registro do plano de testes, de ocorrência de testes e de testes para recuperação de desastres

Documento 15. Testes											
15.1. PLANO DE TESTES											
PLANO DE TESTES			Ações de teste	Planos testados		Objetivo	Complexidade	Periodicidade de realização		Responsável	OLA
15.2. REGISTRO DE REALIZAÇÃO DE TESTES E SIMULAÇÕES											
Data de início	Data de Término	Tipo de teste	Teste realizado	Resultados	Responsável	Planos testados	Possível testar SLA?	Possível testar SLA?	SLA acordado	Tempo realizado	Necessidades de revisão

3.4.4.2 Registro dos testes e simulações

Para cada teste realizado, deve ser registrado todo seu procedimento no Anexo B, 15.2 Registro de realização de testes e simulações, a fim de se ter acompanhamento e garantia do funcionamento dos planos.

Quando um teste é realizado, é necessário registrar um número sequencial do teste, a data de início e término do mesmo. Registrar qual foi o teste realizado e o resultado dos testes, podendo ser positivo ou negativo, neste ultimo caso, registrar as inconsistências. O responsável pelo teste deve ser registrado.

O teste tem objetivos definido, para cada plano de teste registrado deve ser registrado se este atingiu o objetivo proposto. Na sequência, deve-se registrar se pelo teste foi possível testar os tempos acordados no SLA, mas somente caso as condições de teste forem mais parecidas possíveis com as reais, o SLA acordado dos planos testados e o tempo efetivo do teste. Um teste pode não suprir o efeito desejado, neste caso é necessário registrar as necessidades de alteração, revisão ou correção dos planos de ação testados.

Quando se trata de testes do plano de recuperação de desastres o plano de teste precisa ser mais cauteloso. Para os planos de recuperação de desastres utiliza-se o mesmo Anexo B, 15.2 Registro de realização de testes e simulações, para registro dos testes. Conforme realizado um teste de recuperação, registrar o número do teste, sua data de início e do término. Devem-se registrar quais foram os resultados dos testes de recuperação de desastres da maneira mais detalhada possível. Os demais registros seguem o mesmo padrão dos testes de planos de resposta e ações de tratamento.

O resultado dos testes deve ser divulgado para os patrocinadores e gestores conforme período estabelecido nos indicadores elaborados que compreendem os testes.

3.4.5 Atualização e Melhoria contínua do processo

O guia proposto apresenta um conjunto de ações para elaborar um plano de revisão periódico e o registro de ações de revisão para a manutenção e melhoria do plano.

3.4.5.1 Revisão, manutenção e melhoria contínua do plano de continuidade

Para realizar a manutenção do plano de continuidade deve ser estabelecido um processo de revisão de todas as suas etapas, desde o escopo até os processos de teste. O guia proposto apresenta um conjunto de ações para organizar estas ações. Um plano de revisão é um conjunto de ações para realizar as atividades do guia novamente a fim de identificar alterações. Todos os planos de revisão devem ser elaborados e registrados no Anexo B, 16.1 Revisão e manutenção do plano de continuidade de negócios, para cada uma das etapas do processo de revisão.

Uma revisão deve ser criada com um objetivo, cada plano de revisão deve apresentar um ou mais objetivos definidos pela organização. Estes objetivos podem ser identificar mudanças no ambiente, garantir a conformidade, encontrar erros, propor melhorias, entre outros. Um plano pode possuir mais de um objetivo. Caso haja alguma etapa diferente do plano proposto elaborada pela organização, ou a mesma deseja dividir as etapas do plano em etapas menores, devem ser registradas e tratadas da mesma forma que as demais.

Para cada etapa do plano, registrar qual será a periodicidade de revisão. As revisões poderão ser realizadas fora do cronograma previsto caso haja uma necessidade oriunda de testes, alterações de avaliação, falhas detectadas na execução dos planos, entre outras. Cada plano deve possuir um responsável por executar a revisão e um responsável por aprovar a revisão.

As revisões devem seguir os mesmos passos realizados na elaboração do plano de continuidade, seguindo o guia proposto. Podem surgir necessidades de alteração no processo padrão para realizar a revisão. Caso seja necessário deve-se registrar um OLA Anexo B, 11.1 Acordos de nível Operacional - OLA, identificando as novas ações que deverão ser realizadas na revisão.

A figura 29 ilustra a planilha de plano de manutenção e seu registro de revisões, presente no artefato do plano de continuidade de negócios.

Figura 29: Planilha de registro do plano de manutenção e registro de realização das revisões

Documento 16. Manutenção

16.1. REVISÃO E MANUTENÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

Plano de Continuidade	Etapas do Plano	Objetivos	Frequência de revisão	Responsável pela atividade	Responsável pela aprovação
	Definição de escopo				
	Mapeamento do Processo				
	Identificação de Ativos				
	Análise de riscos				
	SLAs				
	Ações de tratamento de riscos				
	Cópias de Segurança				
	Plano de resposta a incidentes				
	Plano de recuperação de desastres				
	OLAs				
	Distribuição e armazenamento do plano de				
	Indicadores				
	Testes				
	Outros...				

16.2. REGISTRO DE REVISÕES

Plano de continuidade	Data da Revisão	Responsável	Motivo da revisão	Revisão programada	Revisão realizada	Alterações realizadas no plano	Aprovação

Após seu registro, os planos de revisão devem ser divulgados para os patrocinadores, gestores de processo, responsáveis pelas revisões e responsáveis pela aprovação das revisões.

3.4.5.2 Registro das Revisões

Conforme o modelo proposto, toda e qualquer ação realizada deve possuir um registro. As revisões do plano de continuidade também necessitam de registro. Para este registro, o guia propõe o registro no Anexo B, 16.2 Registro das revisões.

O guia propõe um conjunto de atividades para realizar os registros de cada revisão realizada. Quando uma revisão é realizada, seu resultado deve ser registrado, identificando-a com um número sequencial para acompanhamento, a data do término da revisão e o responsável por realiza-la. O motivo da revisão deve ser registrado, este motivo pode ser por revisão periódica ou por demanda oriunda de testes ou manutenção reativa. Após a ocorrência, é necessário registrar qual foi a revisão realizada e quais as alterações que devem ser realizadas no plano. É muito importante que seja detalhado o que deve ser alterado da maneira mais clara possível.

As revisões propõem mudanças no plano de continuidade, antes de registrar qualquer alteração no plano de continuidade deve-se realizar uma cópia da versão anterior e armazená-la em ambiente seguro. As alterações no plano de continuidade devem ser realizadas pelo responsável pela continuidade. O responsável pela aprovação da revisão deve aprova-la após a realização das alterações.

O resultado das revisões deve ser divulgado conforme a organização definir. Esta divulgação pode ser eletrônica em um período mensal ou após cada revisão, o critério de divulgação fica a cargo da organização conforme indicadores existentes.

3.5 CONSIDERAÇÕES DO CAPÍTULO

Esta proposta tem como objetivo apresentar um guia e modelo para a elaboração de um plano de continuidade de negócios em uma empresa de pequeno a médio porte, procurando ser flexível para que a organização possa adaptá-la as suas necessidades.

A proposta baseia-se no estudo de diversas referências bibliográficas e traz um refinamento do que pode ser aplicado em uma empresa de pequeno a médio porte. A NBR ISO IEC 27005 foi utilizada principalmente nas fases de definição do escopo e a análise de riscos, a norma possui foco na gestão de riscos e diversos conceitos da mesma podem ser utilizados para a elaboração do escopo. A norma, em conjunto com a NBR ISO IEC 27002 foi utilizada para elaborar as ações de tratamento do risco. Por se tratarem de normas técnicas, ambas focam em processos e definições de escopo, essenciais para estas fases.

Para a fase de elaboração do plano de continuidade de negócios foram utilizados conceitos do COBIT e do ITIL como SLA, OLA, cópias de segurança e os planos de resposta a incidentes. A BS 25999 e a NBR ISO IEC 27005 foram referência para a elaboração do plano de recuperação de desastres, pois tratam a recuperação de desastres de maneira específica na continuidade.

As bibliotecas ITIL e COBIT prezam a gestão do serviço de TI como foco de seus livros, sendo referência para a definição dos processos de testes e medição e monitoramento. Todas as referências bibliográficas tratam o processo de revisão e manutenção, o que permitiu a elaboração de um plano de revisões bastante amplo.

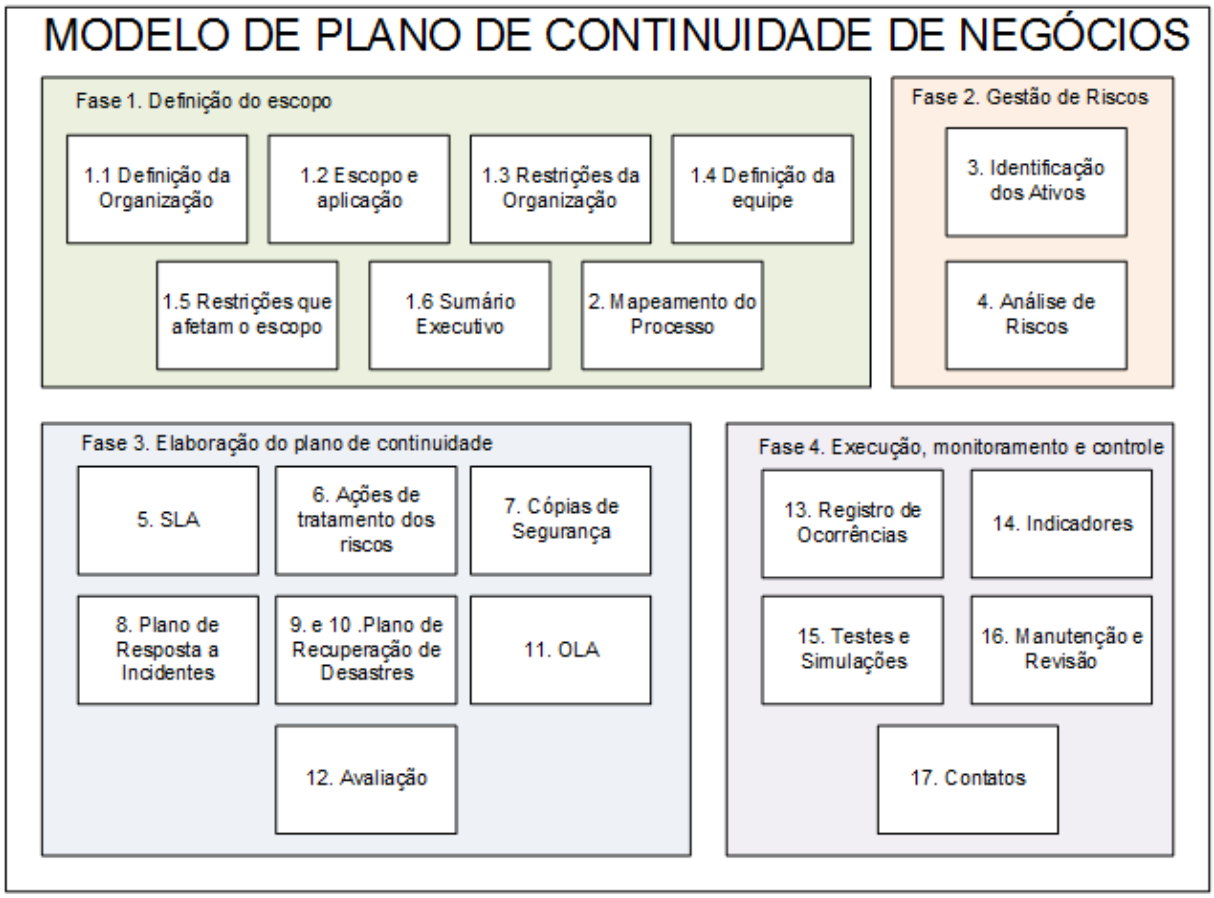
Todas as referências tratam a continuidade de negócios de uma maneira semelhante porem com detalhes específicos. A solução proposta é uma compilação das particularidades de cada referência para elaborar um modelo aplicável à realidade das indústrias de pequeno e médio porte.

O plano de continuidade pode ser alterado pelo gestor da continuidade conforme a necessidade da empresa visto que cada uma possui suas características específicas. A solução proposta não apresenta muitos exemplos de ações e planos a serem realizados, pois cada uma varia de organização para organização. Como a solução proposta foca na elaboração dos

planos, a etapa de execução e registro acaba sendo pouco abordada, a gestão do plano de continuidade será abordada em trabalhos futuros.

Cada fase do modelo proposto é formada por um conjunto de artefatos. A relação entre as fases e seus artefatos está ilustrada na figura 30. A figura ilustra quais itens do Anexo B, Artefatos do plano de continuidade de negócios, deverão ser elaborados em cada uma das fases.

Figura 30: Relação entre as fases e artefatos do plano de continuidade de negócios



4 FERRAMENTA, APLICAÇÃO E AVALIAÇÃO DO MODELO DE PLANO DE CONTINUIDADE DE NEGÓCIOS

O capítulo a seguir refere-se à aplicação do modelo de plano de continuidade de negócios elaborado no capítulo anterior. O capítulo se divide em duas partes: desenvolvimento do sistema PCN, que compreende a disponibilização do modelo elaborado em uma ferramenta de colaboração, e o estudo de caso da aplicação em uma empresa de médio porte, que compreende a elaboração de um plano de continuidade de negócios utilizando o modelo proposto.

No desenvolvimento do sistema PCN, estão detalhados os requisitos utilizados para definir a ferramenta a ser utilizada, a ferramenta utilizada, o desenvolvimento da aplicação, a descrição do sistema PCN e seus recursos disponíveis, as alterações realizadas na proposta e a disponibilização do sistema.

No estudo de caso está detalhada a aplicação do sistema PCN para elaborar um plano de continuidade de negócios contemplando as quatro fases da proposta: a definição do escopo da continuidade, a gestão de riscos, a elaboração do plano de continuidade e a execução, monitoramento e controle da continuidade.

Com a aplicação do modelo é possível avaliar sua eficiência.

4.1 DESENVOLVIMENTO DO SISTEMA PCN

O Plano de Continuidade de negócios deve estar disponível de maneira interativa para que o gestor da continuidade e os demais membros da equipe possam ter acesso simples e intuitivo do plano de continuidade. O desenvolvimento consta em disponibilizar o modelo, seu guia, artefatos e informações complementares, em um sistema colaborativo.

Para o desenvolvimento foram analisadas algumas ferramentas disponíveis ao NUSIS, tendo como premissas o custo acessível e a facilidade em disponibilizar o sistema no tempo proposto. Atendendo estas premissas, foi definido que deveria ser utilizada uma ferramenta de colaboração que permitisse desenvolver um sistema baseado em listas, que correspondem aos artefatos elaborados na proposta, para a construção do modelo sem a necessidade do conhecimento em alguma linguagem de programação. Uma ferramenta de colaboração é um sistema que permite a comunicação entre diversos colaboradores de forma on-line e permite o compartilhamento de conteúdo (Microsoft, 2010).

Com base nestas definições iniciais, uma série de requisitos foi definida para selecionar uma ferramenta.

4.1.1 Requisitos necessários

Um requisito define uma função ou característica de um sistema que especificam resultados particulares, fazendo parte da arquitetura do sistema ou proporcionando uma melhor utilização do mesmo (SOMMERVILLE, 2007).

A ferramenta adotada deve atender uma série de requisitos:

a) O produto da ferramenta deve ser um portal disponível em ambiente Web;
b) A ferramenta deve possuir uma infraestrutura de portal já elaborada, eliminando a necessidade de construir todo o sistema;
c) A ferramenta deve permitir o desenvolvimento do PCN sem a necessidade de intervenção de programadores;
d) A ferramenta deve estar presente nos ativos do NUSIS ou ser distribuída de forma livre;
e) A ferramenta precisa permitir que sejam criadas tabelas para representar cada um dos artefatos descritos no modelo, permitindo o relacionamento entre elas. Por exemplo, uma tabela de riscos que tenha como chave estrangeira os ativos e responsáveis previamente cadastrados em outras tabelas;
f) A ferramenta deve permitir a criação de páginas personalizadas para facilitar a navegação e disponibilizar a informação necessária para a criação dos planos pelo usuário. O anexo A, Guia para elaboração do plano de continuidade, deve estar disponibilizado no produto gerado pela ferramenta;
g) O portal a ser criado deve permitir que o usuário registre um ou mais planos de continuidade, percorrendo as quatro fases: definição do escopo, gestão de riscos, elaboração do plano de continuidade e manutenção do plano de continuidade. O produto final deve permitir que o administrador possa personaliza-lo.
h) A ferramenta precisa possuir um controle de acessos com permissões de segurança bem definidas. A integração com o Microsoft Active Directory (AD) é uma maneira rápida e segura de gerenciar os usuários do sistema;
i) O produto gerado pela ferramenta precisa facilitar a visualização do usuários. A ferramenta precisa facilitar a estratificação de dados e relatórios;

4.1.2 Ferramenta adotada - Microsoft Sharepoint 2010 Foundation

O Microsoft Sharepoint é uma plataforma de colaboração que permite que seus usuários criem, editem e montem portais colaborativos. A ferramenta é muito utilizada no mercado para gestão de conteúdo, colaboração e gestão integrada de documentos. O Sharepoint trabalha com um conceito de listas, onde estas listas são tabelas criadas pelo usuário e tem como objetivo montar um cadastro específico para determinado fim, como por exemplo, uma lista de ativos. O Microsoft Sharepoint 2010 Foundation é a versão básica integrada ao ambiente Microsoft, não sendo necessária a aquisição de licenças de uso desde que a empresa tenha adquirido ao menos uma licença do Windows Server 2008 Release 2 (R2) (Microsoft, 2010).

A versão Foundation possui algumas limitações se comparadas com as versões comercializadas do Sharepoint, porém atende os requisitos especificados neste trabalho. O desenvolvimento de customizações no Sharepoint se baseia na linguagem de programação .NET, porém não é necessário o conhecimento pois a ferramenta permite a criação do sistema através de seus próprios recursos. O banco de dados utilizado pelo Sharepoint é o Microsoft SQL Server, podendo ser adotada sua versão livre, Express. O NUSIS, devido à parceria da Universidade de Caxias do Sul com a Microsoft, possui o Microsoft Sharepoint Foundation disponível para uso.

4.1.3 Desenvolvimento da Aplicação

O Modelo de plano de continuidade é um portal colaborativo em ambiente Web. Seu funcionamento depende de uma infraestrutura de ferramentas Microsoft para disponibilização formada por um servidor de sistema operacional Microsoft Windows Server 2012 R2, com as seguintes aplicações instaladas: Microsoft Sharepoint Foundation 2010, serviço de publicação Internet Information Services (IIS) para disponibilizar o sistema na Web e um sistema gerenciador de banco de dados Microsoft SQL Server 2012 para armazenar o banco de dados da aplicação. Por padrão, na instalação do Microsoft Sharepoint Foundation 2010 todos estes serviços são instalados e configurados automaticamente. O Sharepoint é uma ferramenta integrada com o serviço Microsoft Active Directory, gestor de usuários do Windows, e permite que a gestão de usuários seja realizada pelo administrador da rede Windows da empresa (Microsoft, 2010).

a) Estrutura do sistema

O desenvolvimento do modelo é realizado utilizando recursos próprios do Sharepoint, o administrador do sistema pode criar e editar sites conforme a necessidade de negócio da aplicação. O Sharepoint possui recursos para a criação de listas, que são tabelas definidas pelo administrador para servirem como um formulário de cadastro. Cada artefato apresentado no modelo foi criado no formato de uma lista. O guia para a elaboração do plano de continuidade de negócios foi disponibilizado no Sharepoint através de uma lista de tarefas com descrição da atividade e a matriz RACI. Cada atividade do guia foi cadastrada manualmente na lista criada.

As listas criadas possuem uma coluna chave primária, que é referenciada por outras listas através de chaves estrangeiras. Estes relacionamentos e suas cardinalidades estão representados através de um diagrama entidade e relacionamento (ER), na notação Chen de banco de dados. Na representação a chave primária não foi representada através da forma elíptica devido a restrições de espaço na figura, porém está destacada sobre cada uma das entidades do diagrama ER. Para melhor organização da representação das relações o diagrama ER foi dividido em quatro partes, conforme as fases do guia elaborado. As figuras 31, 32, 33 e 34 representam o diagrama ER do sistema PCN, separados respectivamente por fase. As cores representam cada fase e diferenciam quais listas pertencem a cada fase.

Figura 31: Representação dos artefatos da fase 1. Definição do escopo através de diagrama ER da notação Chen de Banco de Dados

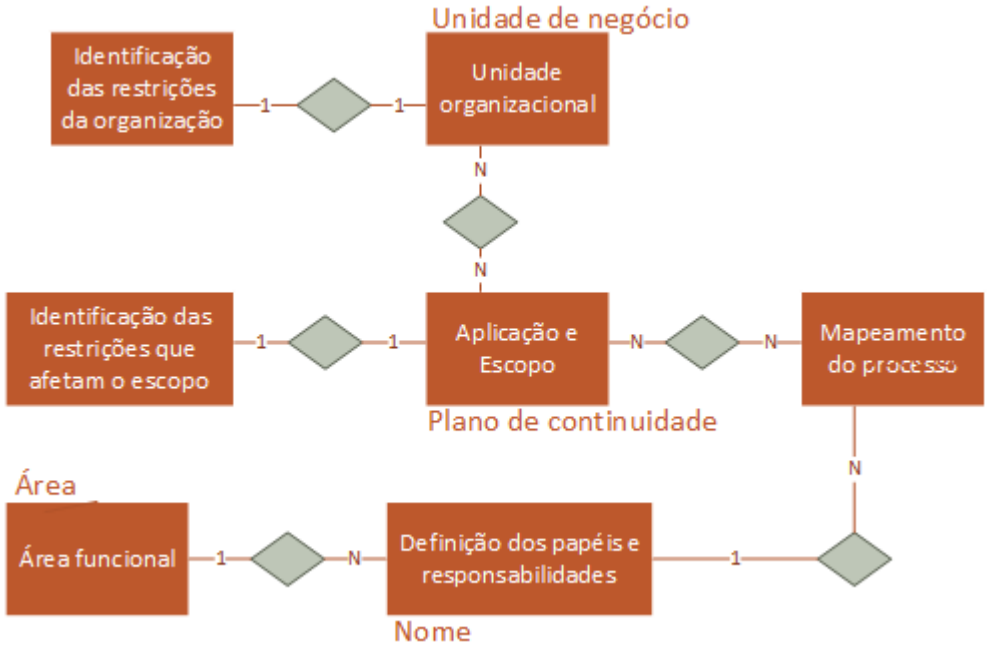


Figura 32: Representação dos artefatos da fase 2. Gestão de riscos através de diagrama ER da notação Chen de Banco de Dados

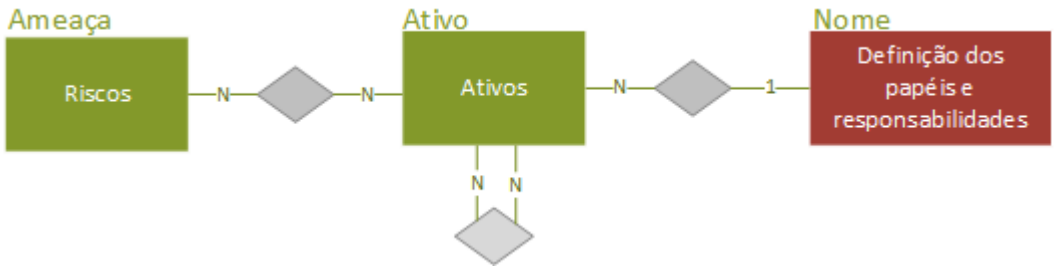


Figura 33: Representação dos artefatos da fase 3. Elaboração do Plano de continuidade de negócios através de diagrama ER da notação Chen de Banco de Dados

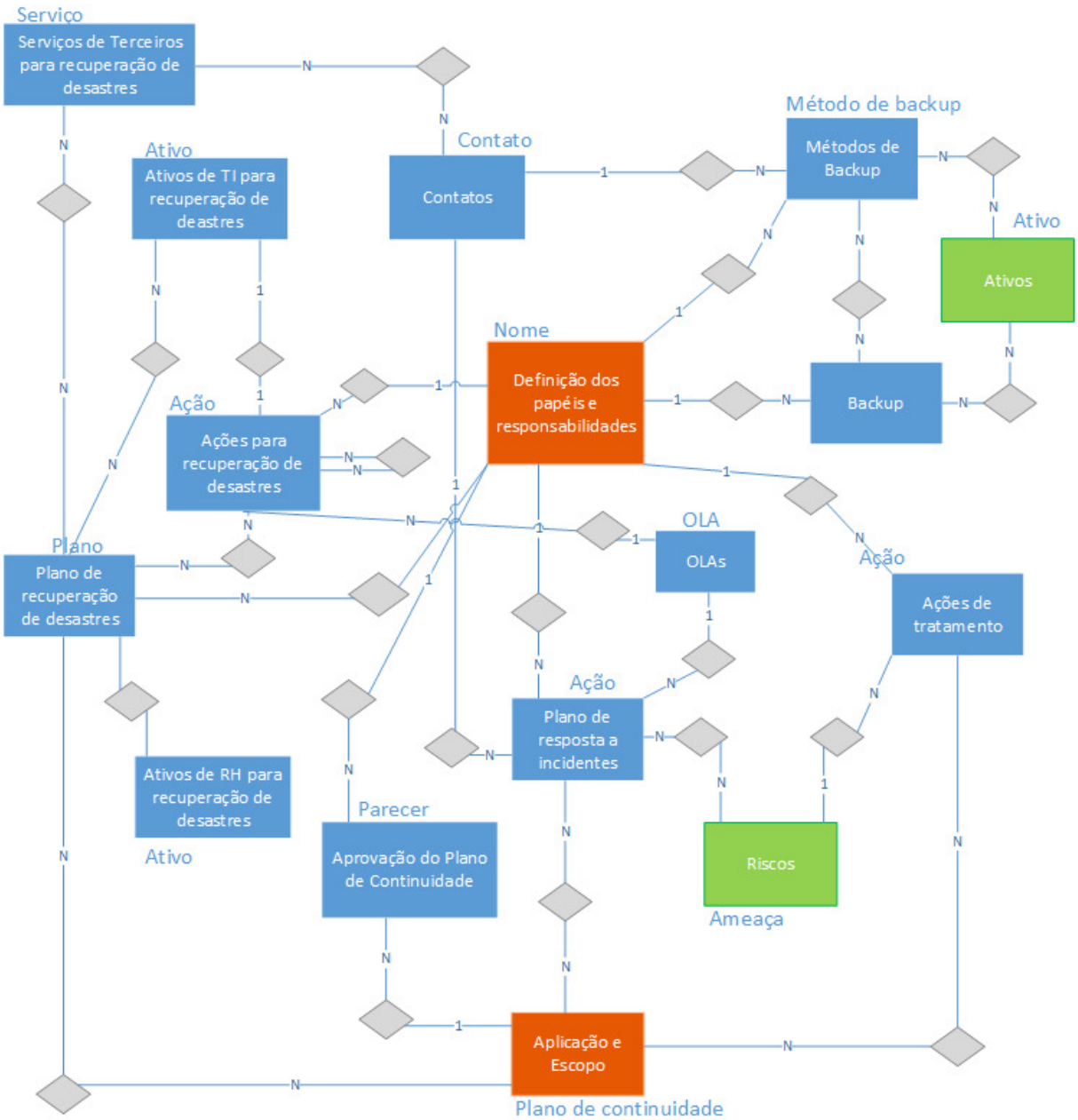
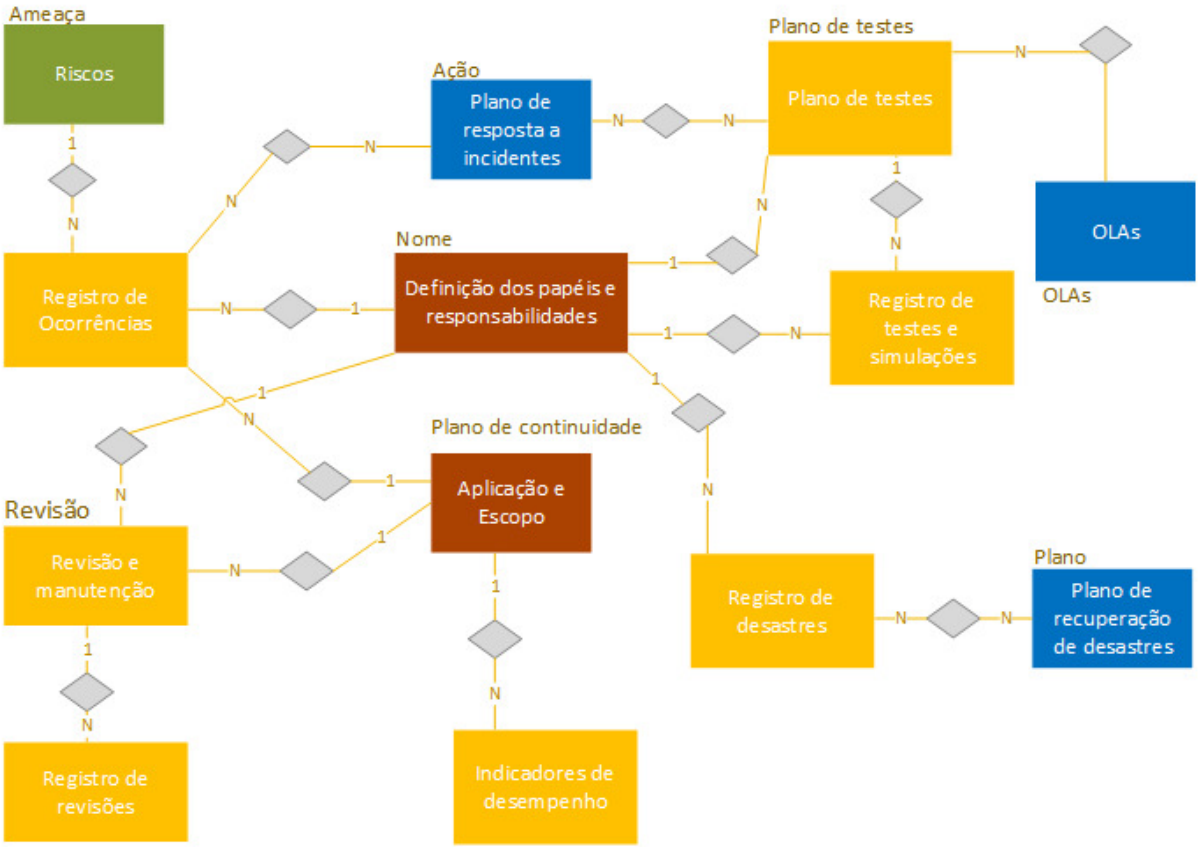


Figura 34: Representação dos artefatos da fase 4. Execução, monitoramento e controle da continuidade de negócios através de diagrama ER da notação Chen de Banco de Dados



b) Segurança no uso do sistema

Por ser uma ferramenta Microsoft, o Sharepoint possui integração nativa com o sistema operacional Windows. Os usuários do sistema PCN são criados no Windows, podendo ser usuários locais do servidor em que o Sharepoint está instalado ou usuário de um domínio gerenciado pelo Microsoft AD, Active Directory, esta definição fica a cargo do administrador do sistema.

No sistema PCN foram utilizados os grupos de segurança padrão do Sharepoint para acesso ao sistema: O grupo de Administradores possui permissão para editar o sistema, suas listas e estrutura, conforme a necessidade, o grupo de Colaboradores compreende o gestor da continuidade, que pode preencher e editar as listas, e o grupo de Visitantes, que corresponde aos demais integrantes da equipe, que podem apenas visualizar o que está sendo criado. O administrador do sistema deve vincular os usuários nos grupos conforme a definição da equipe.

4.1.4 Descrição do sistema PCN

Para possibilitar seu uso contínuo em uma organização foi criado um cadastro de Empresa e Planos de Continuidade na fase de definição do escopo, permitindo que o sistema seja utilizado por diferentes unidades organizacionais e possam ser registrados mais de um plano de continuidade.

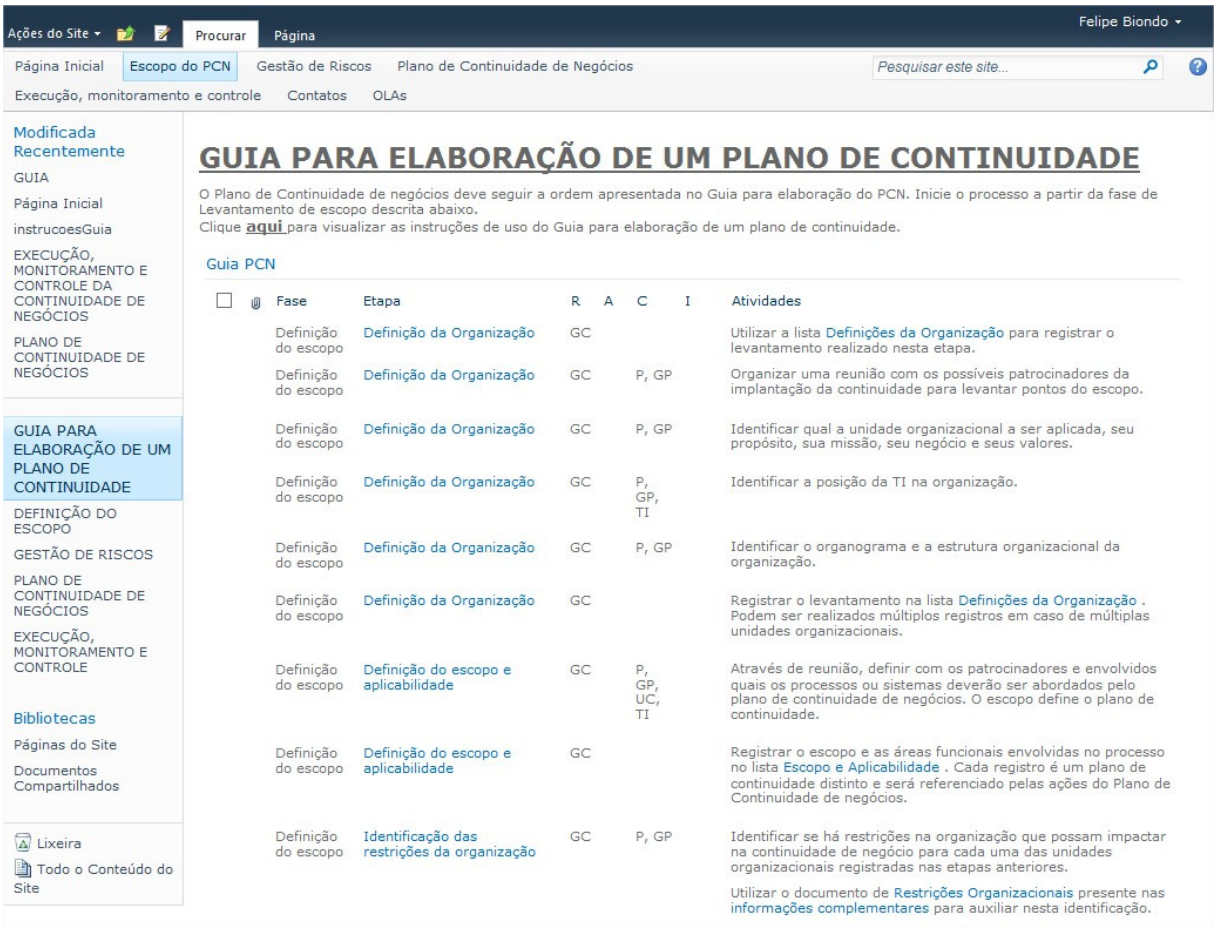
O sistema PCN é apresentado através de uma página inicial contendo o diagrama das fases do guia e o índice com links para cada atividade. A navegação no Guia pode ser realizada através do menu esquerdo da tela, neste menu estão listadas cada uma das fases do guia, que direcionam às atividades correspondentes do guia. A barra de Menus superior permite a navegação do usuário aos artefatos gerados em cada fase do guia. O menu lateral direito possui um resumo rápido dos planos de continuidade cadastrados, acesso aos artefatos do plano e um índice referente as informações complementares. A página inicial do PCN está ilustrada na figura 35.

Figura 35: Tela de abertura do sistema PCN

a) Utilizando o guia no PCN

O guia para elaboração do plano de continuidade de negócios pode ser encontrado ao clicar na fase desejada no menu lateral esquerdo. O guia disponibilizado no sistema PCN é uma lista de itens que representam cada uma das atividades propostas pelo modelo. A lista de atividades é identificada por fase, etapa, matriz RACI, atividades e Status de acompanhamento conforme a figura 36. As atividades descritas no guia referenciam listas para registro ou informações complementares conforme surgem as necessidades de interação. A atividade possui um vínculo de acesso para as listas ou informações complementares na descrição da atividade, simplificando a navegação.

Figura 36: Guia para elaboração de um plano de continuidade representado no sistema PCN



Uma atividade pode ser visualizada clicando no nome da Etapa da atividade. O sistema PCN permite o filtro das atividades por fase e etapa, bem como exibir somente as atividades não iniciadas ou em andamento. Estes filtros podem ser aplicados clicando nas colunas que se deseja filtrar.

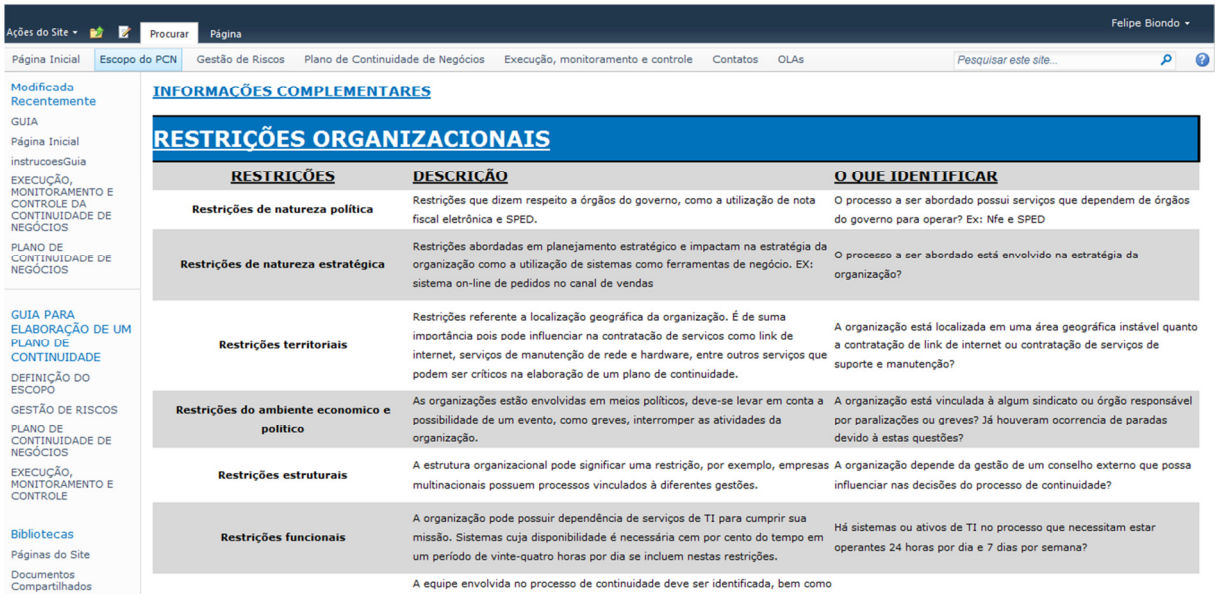
O menu lateral esquerdo permite uma rápida navegação entre as fases e etapas, apresentando somente os itens referentes a fase acessada. Na exibição do guia pode-se acompanhar em qual etapa o usuário está conforme exibido na linha de acompanhamento, logo abaixo da barra de links superior.

O guia sofreu alterações ao ser implementado no PCN para melhor se adaptar ao ambiente disponibilizado no sistema. Estas alterações incluem mudanças de termos, simplificação de atividades e instruções de referência a um plano de continuidade, devido ao sistema permitir um cadastro de mais de um plano de continuidade.

b) Informações complementares

As informações complementares para consulta, presentes no Anexo C, Informações complementares, foram disponibilizadas em páginas exclusivas que podem ser acessadas na página inicial ou pelos links diretos referenciados nas atividades do guia. A figura 37 exibe uma página de informações complementares no sistema PCN.

Figura 37: Informações complementares referente a restrições organizacionais no sistema PCN



c) Iniciando o uso do sistema

Seguindo as atividades definidas no guia, o processo deve ser iniciado pelo Escopo e Aplicação. O sistema PCN permite que sejam cadastradas mais de uma unidade organizacional e que diversos planos de continuidade sejam criados. Estas definições são registradas nas primeiras atividades do guia, e o escopo do plano que determina seu registro

no sistema. Este cadastro de escopo será referenciado nas diversas ações que serão elaboradas e registradas ao longo do guia no sistema PCN.

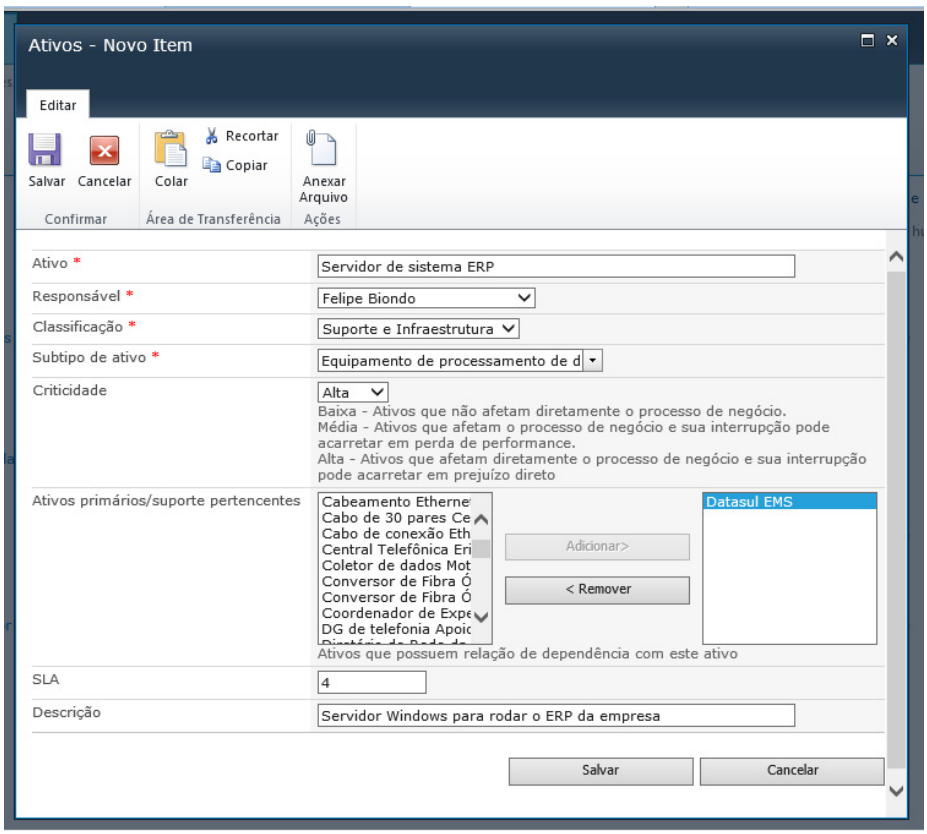
O sistema possui um cadastro de áreas funcionais com áreas comuns já existentes no sistema, mas que pode ser alterado pelo usuário conforme a definição de cada organização. O vínculo para o cadastro de áreas funcionais está disponibilizado na página inicial do sistema e será utilizado na definição do escopo e de equipe.

d) Registrando as atividades do guia

O sistema PCN possui um conjunto de listas, que representam os artefatos elaborados no modelo, para os diversos registros do plano de continuidade. Cada lista possui atributos próprios conforme o modelo elaborado.

Para registrar uma atividade o usuário deve acessar a lista referente à etapa do guia e então adicionar um novo item da lista que está sendo trabalhada. Ao adicionar um novo item é necessário o preenchimento do formulário de cadastro que é exibido em tela. Os campos identificados com um asterisco são de preenchimento obrigatório. Cada lista de registros possui campos específicos, podendo haver campos com chave estrangeira. A inclusão de um item é confirmada pelo botão Salvar disponível no formulário. A figura 38 apresenta o cadastro de um ativo no sistema PCN.

Figura 38: Formulário para registro de ativos no sistema PCN



Os itens registrados em uma lista podem ser editados conforme a necessidade do usuário, para isso o usuário deve selecionar o item desejado e clicar em editar.

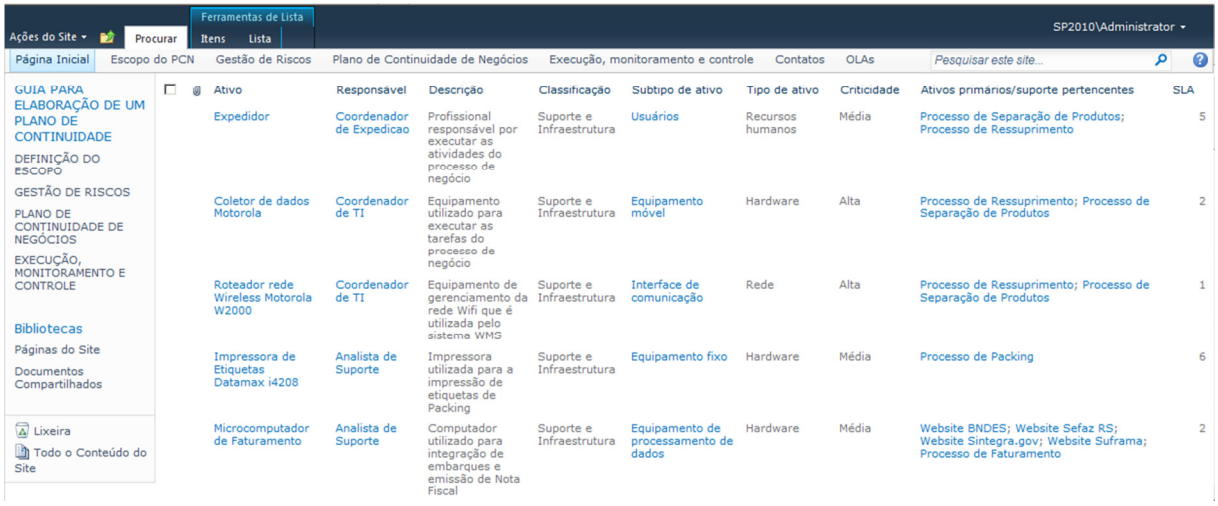
Todas as atividades do guia seguem o mesmo padrão para registro. A partir da terceira fase, Elaboração do plano de continuidade de negócios, é necessário referenciar o plano de continuidade ou de recuperação de desastres nos registros.

e) Visualizando o plano de continuidade

O plano de continuidade pode ser visualizado através dos vínculos da barra superior do sistema. O plano é dividido pelas suas quatro fases e os contatos separadamente. Para visualizar o plano basta acessar a fase desejada na barra superior e as listas de etapas desta fase serão exibidas em tela.

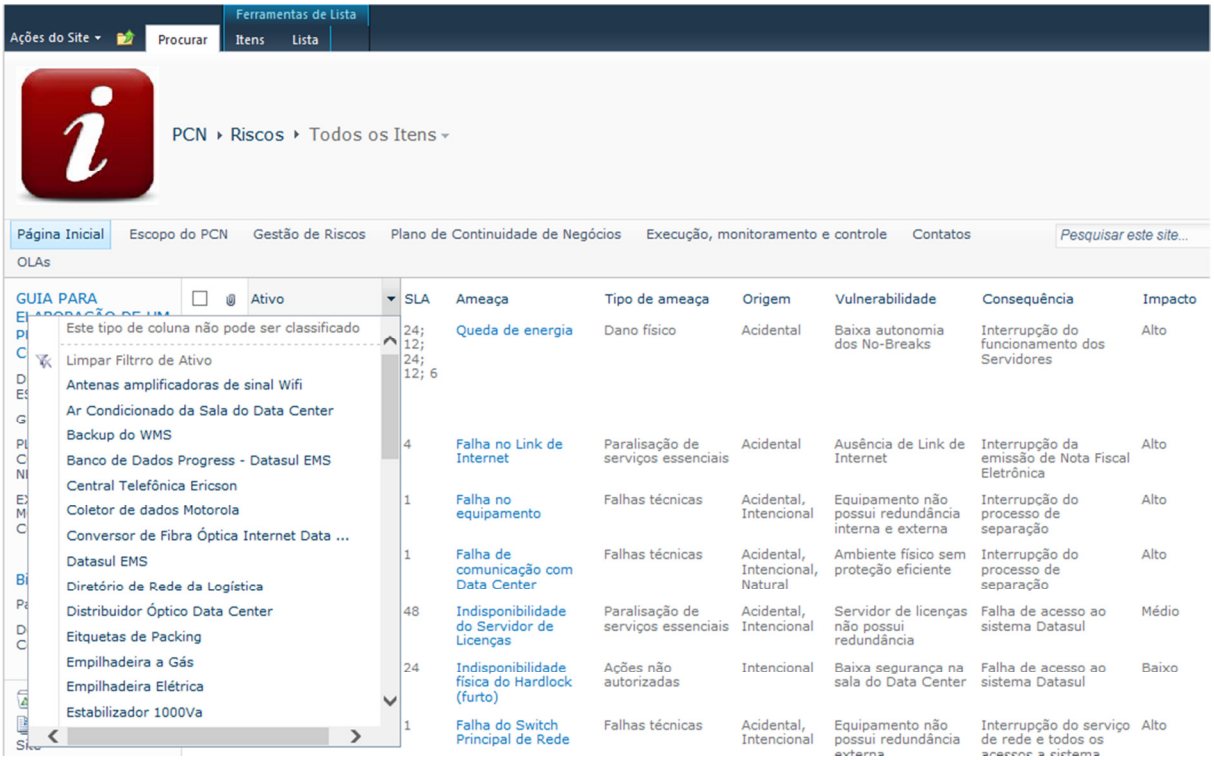
É possível visualizar somente uma etapa, e aplicar diversos filtros de visualização em seus itens, selecionando o título da etapa na exibição. Os itens da etapa em questão podem ser visualizados na lista correspondente no sistema. A figura 39 representa uma lista de ativos cadastrada no sistema PCN.

Figura 39: Recorte de uma lista de ativos no sistema PCN



É possível refinar a exibição das listas do plano de continuidade alterando sua ordenação ou aplicando filtros de busca. Para ordenar por uma coluna, basta clicar no título da coluna na tela da lista. Para refinar a visualização, o usuário deve clicar na caixa ao lado do título da coluna e especificar o filtro, conforme demonstrado na figura 40.

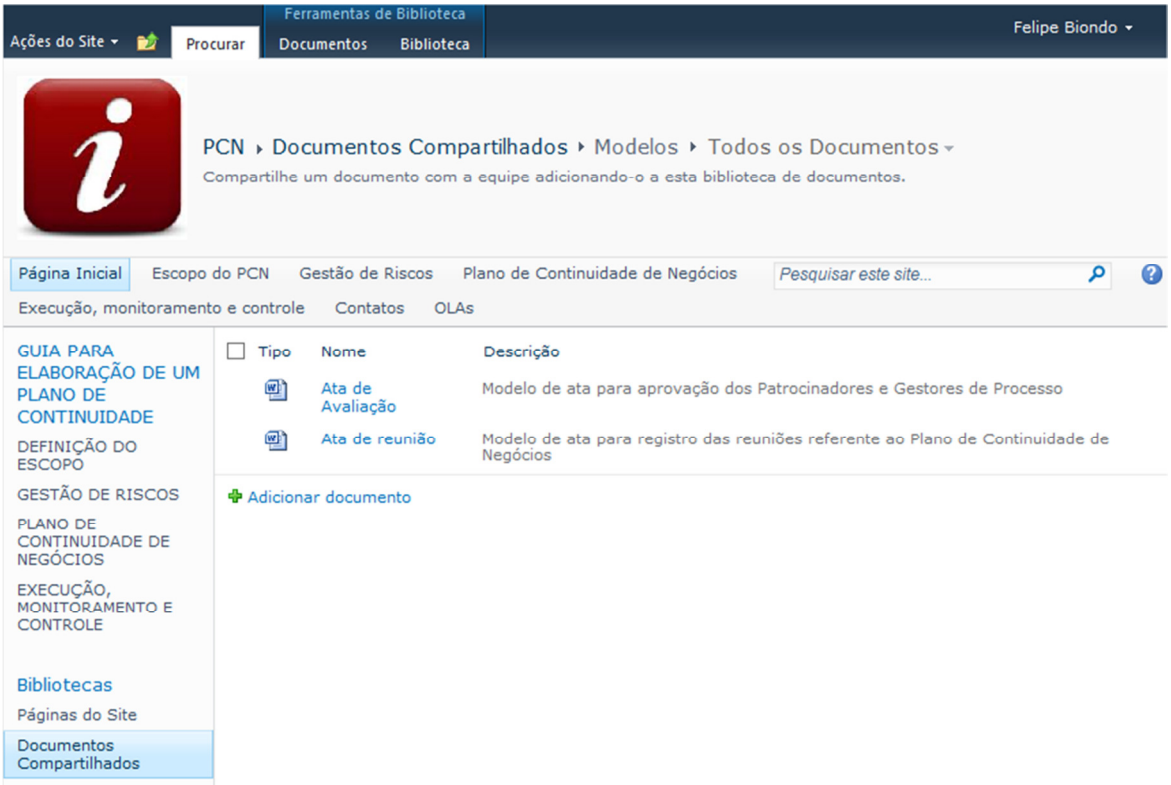
Figura 40: Refinando a exibição da lista de riscos através de filtros no sistema PCN.



f) Biblioteca de Documentos

Para auxiliar o usuário no registro de atividades e manter os registros formais da aplicação o sistema PCN disponibiliza uma biblioteca de documentos com modelos de atas de reunião e de coleta de assinatura dos gestores e patrocinadores. A biblioteca de documentos é um recurso disponível no Sharepoint, sua utilização é referenciada no guia para elaboração do plano de continuidade através de vínculo direto nas atividades que seja necessário o seu uso. A figura 41 representa dois modelos de ata disponibilizados na biblioteca de documentos.

Figura 41: Modelos disponibilizados na biblioteca de documentos no sistema PCN



Além de disponibilizar os modelos para acesso do usuário, a biblioteca de documentos permite que o usuário disponibilize os documentos preenchidos no sistema, facilitando assim a gestão dos documentos de aprovação do plano de continuidade e garantindo sua segurança.

4.1.5 Alterações realizadas

Para o desenvolvimento do sistema PCN foram realizadas algumas alterações nos artefatos. Estas alterações referem-se a adições ou remoções de colunas nos artefatos, alterações de instruções no guia, para tornar o guia mais adaptável ao sistema.

O guia para elaboração do plano de continuidade sofreu alterações em sua estrutura. A nomenclatura geral do guia foi alterada, onde o guia se referia a artefatos, agora está referenciando a lista que deve ser utilizada. Pelo fato do sistema trabalhar com diversos planos de continuidade, foram adicionadas instruções no guia para referenciar qual plano de continuidade de negócio a ação criada pertence. Foram simplificadas algumas ações, pois o software por si só já torna o cadastro intuitivo para o usuário. Com a adição da biblioteca de

documentos no sistema PCN, foram adicionadas instruções para utilizar modelos e armazenar os documentos gerados na biblioteca.

Os artefatos para registro do guia também sofreram alterações para se adequarem melhor ao sistema PCN. A principal alteração realizada se deve ao fato do sistema trabalhar com diversos planos, tornando necessário criar uma coluna com chave estrangeira referenciando a quais planos cada ação do plano pertence. Alguns artefatos foram remodelados e simplificados para tornarem o desenvolvimento e a usabilidade do usuário mais simples, como um cadastro único de ativos de suporte para a recuperação de desastres. Um dos recursos do Sharepoint é a possibilidade de adicionar arquivos como Anexo aos registros, tornando o plano de continuidade mais rico em informações.

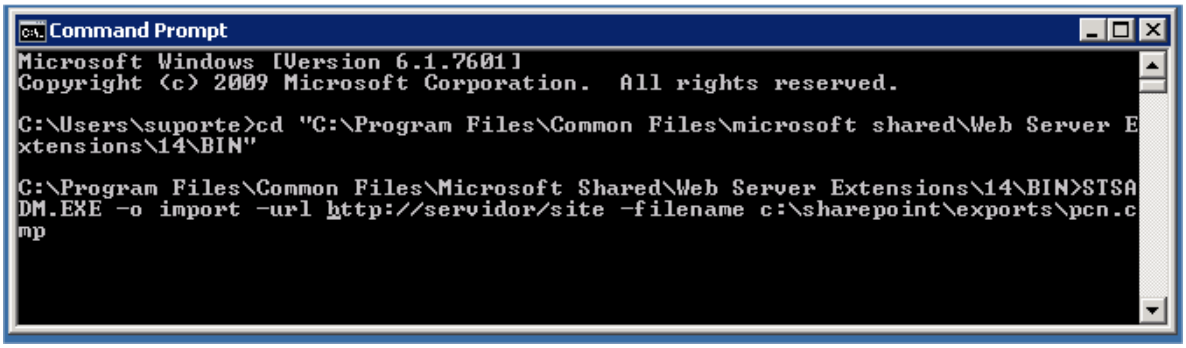
4.1.6 Disponibilização do sistema

O sistema PCN é um subsite do Sharepoint. Um subsite do Sharepoint é um conjunto de páginas e listas que possui administração e segurança independente, porém pode herdar as configurações de sites superiores. Para disponibilizar o sistema PCN para uso, é necessário importa-lo dentro de uma instalação existente no Microsoft Sharepoint Foundation 2010. O Sharepoint Foundation permite que seja exportado um subsite através de sua ferramenta de administração central, realizando uma cópia de segurança do sistema e todo seu conteúdo (Microsoft, 2010).

A importação do sistema PCN no Sharepoint pode ser realizada utilizando a ferramenta Stsadm, disponível em servidores com o Microsoft Sharepoint 2010 instalado. O Stsadm é um recurso do Sharepoint Foundation 2010 que permite a administração de sites através de linha de comando e manipulação de arquivos e procedimentos.

Para utilizar o Stsadm deve-se, no terminal de comando do Windows, acessar o diretório onde estão os arquivos executáveis do Sharepoint e utilizar o comando Stsadm –o import para importar um subsite. Adiciona-se o parâmetro –url para indicar qual o sítio do Sharepoint a importar o sistema, e -filename para indicar o arquivo do sistema a ser importado. A figura 42 apresenta os comandos de importação do Sistema PCN em ambiente do Sharepoint Foundation 2010 através do recurso Stsadm.

Figura 42: Utilização do Stsadm para importar o sistema PCN em ambiente Sharepoint Foundation 2010



4.2 APLICAÇÃO DO MODELO DE PLANO DE CONTINUIDADE DE NEGÓCIOS

Para a validação do modelo de plano de continuidade de negócios é necessária sua aplicação em um ambiente real, gerando um caso de uso passível de avaliação. O modelo para elaboração de um plano de continuidade de negócios foi aplicado em uma indústria de médio porte na cidade de Caxias do Sul. O tempo de aplicação do modelo foi de três meses, sendo o primeiro mês utilizado para desenvolver e disponibilizar o sistema no Sharepoint da empresa e os demais para aplica-lo na organização. O guia foi aplicado de forma sequencial e as alterações foram realizadas no modelo conforme a necessidade de adequação.

O plano de continuidade elaborado na aplicação do modelo está disponível no Anexo D, Plano de continuidade de negócios. O anexo é dividido em itens que representam os artefatos criados no Anexo B, Artefatos do plano de continuidade. Por questões de sigilo, no Anexo D foram utilizados nomes, endereços e números de telefone fictícios para a representação dos membros da equipe e contatos.

O escopo da aplicação na empresa abrange as três primeiras fases do guia por completo: definição do escopo, gestão de riscos e elaboração do plano de continuidade de negócios. A quarta fase: execução, monitoramento e controle do plano de continuidade, não pôde ser finalizada devido ao tempo disponível, sendo definidos alguns planos de teste, planos de revisão e os indicadores da continuidade. A aplicação do modelo foi iniciada pela definição da empresa.

4.2.1 Definição do escopo da continuidade

A primeira fase do modelo é a definição do escopo da continuidade de negócio, nesta fase foram definidas a empresa que será aplicada, o escopo do processo da aplicação, as restrições da organização, a equipe que será envolvida na elaboração e execução do plano, as restrições que podem afetar o escopo, o sumário executivo do escopo e o mapeamento do processo definido em escopo.

a) Definição da empresa

A empresa aplicada é uma empresa fabricante de materiais de fricção e componentes para freio com matriz em Caxias do Sul, Rio Grande do Sul. A empresa conta com uma unidade comercial em São Paulo e uma unidade de montagem e centro de distribuição em Santa Catarina. Com mais de 250 funcionários, a empresa é um dos grandes nomes do mercado de fricção.

A empresa possui um processo produtivo parcialmente automatizado, estruturado a partir de um sistema ERP e diversos outros sistemas satélites. A fabricação do material de fricção passa por um processo de mistura, prensagem, tratamento térmico, beneficiamento e usinagem, embalagem e então armazenamento. As áreas de apoio ao processo, como planejamento e controle de produção, Engenharia, Qualidade e Segurança do trabalho, atuam diretamente na melhoria do processo. O departamento de vendas é responsável pela prospecção de novos clientes e emissão de pedidos. O setor de expedição e logística é quem realiza a separação dos produtos e seu faturamento, bem como a negociação com fornecedores de fretes.

A equipe de TI da empresa é formada por dois colaboradores, sendo um coordenador e um analista de suporte. A TI possui como princípio a aquisição de software e contratos de suporte de mais alto nível com terceiros. A continuidade de negócios é um conceito novo para a empresa, porém esta tem consciência da importância da mesma, possuindo políticas de segurança da informação e processos de cópias de segurança auditadas anualmente pela auditoria de certificação ISO 9001 e pela auditoria financeira e fiscal.

O registro da organização pode ser encontrado no anexo D, 1.1. Definição da organização.

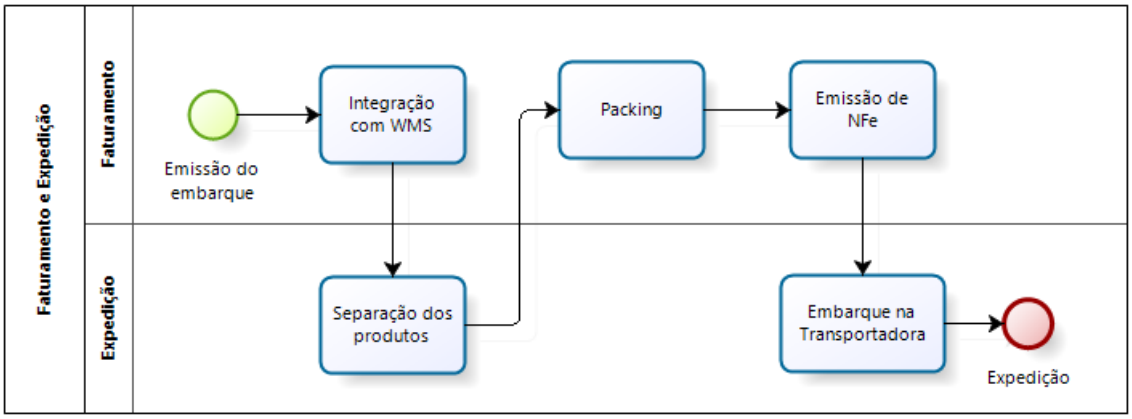
b) Definição do escopo da aplicação

Em conjunto com os patrocinadores, foi definido que o plano de continuidade deve ser aplicado em uma área ou processo de alto valor agregado e de alto risco. Como a empresa possui duas unidades, foi definido aplicar o PCN apenas na unidade de Caxias do Sul por ser a maior unidade e a mais dependente dos serviços de TI.

Após levantamento de diversos processos críticos, o processo de faturamento para o mercado nacional, denominado Faturamento e Expedição, foi definido como escopo de aplicação do plano. A decisão de elaborar o plano por processo foi definida devido a empresa trabalhar fortemente com gestão de processo e pela integração de diversas áreas no mesmo. A empresa entende que não bastaria garantir a continuidade de uma única área apenas visto que os processos críticos envolvem a integração de diversas áreas, tornando o plano de continuidade menos eficiente.

O processo de faturamento segue um fluxo iniciado pela emissão do embarque, seguido pela integração do embarque, separação dos produtos, processo de empacotamento packing, faturamento e emissão de nota fiscal, embarque no transportador e expedição. O processo está resumido na Figura 43. O fluxo do processo é mais complexo do que o descrito nesta etapa, e será detalhado na etapa de mapeamento do processo.

Figura 43: Processo resumido de Faturamento e Expedição



O departamento de Faturamento é formado por um Gerente de Logística, um Coordenador de expedição, dois Faturistas e cinco separadores. O setor responde diretamente ao Diretor Financeiro. A equipe está dimensionada para atender as demandas mensais, porém, nos últimos dois dias do mês a demanda é excessiva e demanda regime de horas extras e colaboração de funcionários de outras áreas para atender a demanda sem prejuízo. Neste

período, qualquer interrupção no processo pode ser crucial para o atingimento das metas de faturamento.

A empresa entende a importância da continuidade de negócios para este processo pois sua interrupção pode afetar diretamente seu resultado financeiro. O processo é bastante crítico pois corresponde a sessenta por cento do faturamento da empresa e diversos ativos de TI estão presentes no processo, tais como:

a) Roteadores e antenas para rede sem fios;
b) Coletores de dados para acesso ao sistema;
c) Micro computadores para faturamento;
d) Sistema ERP e módulo WMS para separação.

A aplicação do plano de continuidade visa garantir ações para que este processo esteja sempre em funcionamento, e se recupere o mais rápido possível em caso de falhas. O registro do escopo está presente no Anexo D, 1.2. Definição do escopo e aplicabilidade.

c) Identificação das restrições da organização

Em conjunto com os patrocinadores, foi identificada a existência de diversas restrições. A organização possui restrições de natureza política como a dependência de órgãos do governo para emissão de Nota Fiscal Eletrônica, restrições de natureza estratégica, pois o processo de faturamento é extremamente crítico ao resultado, restrições políticas devido à forte atuação do Sindicato dos Metalúrgicos de Caxias do Sul, restrições funcionais, pois o processo depende dos ativos de TI para operar.

Há também restrições de pessoal para operar os planos de continuidade devido a estrutura de TI ser pequena, dependendo de terceiros para algumas atividades. Não há uma política de continuidade de negócios abordada na gestão de processos da organização se tratando de ativos de TI, porém a empresa tem consciência do prejuízo que ela pode vir a ter em situação de desastre. O orçamento da empresa é restrito quando o assunto é aquisição de ferramentas de tecnologia da informação, sendo muitas de suas aquisições realizadas de forma reativa. Esta restrição se reflete na quantidade de planos de resposta a incidentes em comparação com ações de tratamento de riscos.

As restrições da organização estão identificadas no Anexo D, 1.3. Restrições da organização.

d) Definição dos papéis e responsabilidades

Os papéis e responsabilidades foram atribuídos a todos os usuários que possuem envolvimento direto no processo definido no escopo ou que possuem alguma relação com as ações do plano a serem realizadas na fase 3 do modelo. A equipe é formada por colaboradores da gestão da empresa, expedição, faturamento, manutenção e TI. O coordenador de TI, que assume o papel de gestor da continuidade, foi responsabilizado por gerenciar a aplicação do modelo, utilizar o sistema PCN e realizar os registros no mesmo. A equipe para a continuidade de negócios foi definida conforme a Tabela 5. A equipe envolvida está registrada no Anexo D, 1.4. Definição dos papéis e responsabilidades.

Tabela 5: Equipe definida para elaborar e operar o plano de Continuidade

Usuários	**PAPÉIS**				
	Patrocinador	**Usuário-Chave**	**Gestor de Processo**	**TI**	**Gestor da Continuidade**
Coordenador de Ti				X	X
Analista de Suporte				X	
Coordenador da Expedição		X	X		
Gerente de Logística	X		X		
Diretor Financeiro	X				
Faturista		X			
Expedidor 1		X			
Expedidor 2		X			
Expedidor 3		X			
Expedidor 4		X			
Expedidor 5		X			
Coordenadora Comercial		X	X		
Coordenadora de Segurança do Trabalho			X		
Gerente Industrial			X		
Analista Fiscal		X			
Coordenadora de Controladoria		X	X		
Gerente de Desenvolvimento de Produto			X		
Coordenador de Manutenção		X	X		

e) Definição das restrições que afetam o escopo

A etapa subsequente à definição da equipe é a definição das restrições de escopo. Foram identificadas diversas restrições de escopo em reunião com os gestores de processo, de maneira não detalhada: Sistemas utilizados no processo, infraestrutura envolvida para operar os sistemas, dependência da conexão com internet para emissão de notas fiscais, dependência do processo para o resultado da empresa, acarretando prejuízo direto em caso de interrupção, fenômenos meteorológicos podem prejudicar o processo em baixa escala.

A equipe que opera o processo é bastante enxuta, porém há redundância das funções operacionais, sendo seu coordenador o responsável por gerir o conhecimento e organizar a equipe, três expedidores possuem conhecimento para gerir o processo na ausência do líder, enquanto os demais possuem um nível de conhecimento semelhante. A área de TI é formada por apenas dois colaboradores, sendo um Coordenador responsável pelo suporte avançado aos sistemas e um analista de suporte que realiza as tarefas operacionais do suporte a infraestrutura.

O processo é bastante automatizado e os recursos de TI são suficientes para que o processo seja operado corretamente. Não há dependência de terceiros na operação, porém a manutenção e suporte aos ativos do processo envolvem contratos com terceiros. Foi definido um prazo de 60 dias para a elaboração do plano de continuidade, sendo um investimento extremamente restrito para ações de tratamento de forma proativa.

As restrições que afetam o escopo encontram-se Anexo D, 1.5. Restrições que afetam o escopo da continuidade.

f) Sumário Executivo

Após as demais etapas de definição do escopo, as informações foram reunidas e apresentadas de forma informal aos gestores de processo e patrocinadores. Na apresentação foi buscado informar os patrocinadores das consequências da interrupção dos serviços de TI, de casos de desastres que ocorreram em outras empresas da região e das vantagens de se ter um plano de continuidade. A implantação do plano de continuidade foi aprovada e foi definido que toda e qualquer ação de tratamento possível, independente do seu custo, será passada para a validação dos patrocinadores e devidamente aplicadas conforme a liberação de recursos financeiros pela empresa.

O sumário executivo elaborado na empresa está presente no anexo D, 1.6. Sumário executivo.

g) Mapeamento do processo

Para o mapeamento do processo foi utilizada a abordagem BPMN conforme sugerido no modelo. Para realizar o mapeamento foram reunidos os usuários chave juntamente com o gestor do processo para identificar todas as etapas do processo. O processo de expedição da empresa possui como entrada o recebimento de pedidos da área de vendas e estende-se a separação do produto até o faturamento e expedição do mesmo. Utiliza-se um sistema WMS, módulo do ERP, para a gestão do armazém. O processo listado na definição do escopo foi amplamente detalhado nesta etapa.

A expedição dos produtos para clientes inicia-se com a liberação dos pedidos pela área de vendas, o faturista monta um embarque no sistema para enviar ao cliente e o integra ao WMS. Com o embarque integrado, o expedidor imprime as etiquetas de packing(empacotamento) e então inicia a separação do embarque item à item com o coletor de dados. O separador realiza o picking (separação) dos produtos conforme a necessidade, caso um produto não esteja mais disponível em um endereço de separação, o sistema cria uma tarefa de ressuprimento da área de picking, sub-processo do processo de faturamento, para reabastecer a separação. Após a separação de todo o embarque, o packing é gerado automaticamente e o faturista libera o embarque para faturamento e emissão da nota fiscal. Com a nota fiscal emitida, o expedidor carrega o embarque para a transportadora e o processo é concluído.

O processo de faturamento e o sub-processo de ressuprimento estão representados no anexo D, 2.1. Mapeamento do processo.

h) Plano de comunicação

A comunicação entre os membros da equipe foi realizada principalmente através de reuniões. Em horários pré-agendados, o gestor da continuidade realizava as tarefas do guia em conjunto com os demais envolvidos, sempre fornecendo os retornos conforme as atividades do guia sugeriam. Decisões foram registradas a partir de envio de correio eletrônico entre o gestor da continuidade e os patrocinadores. As bibliotecas de documentos foram pouco usadas pois foram disponibilizadas no sistema PCN após o término da implantação.

4.2.2 Gestão de riscos

A gestão de riscos é crucial para a elaboração do plano de continuidade, pois a partir dela que são fundamentadas as ações a serem elaboradas. A identificação dos ativos procurou relacionar o maior número de ativos, não se limitando apenas aos ativos de hardware e software. A gestão de riscos buscou atingir todos os ativos de criticidade média e alta.

a) Identificação dos ativos

Para a identificação dos ativos, foram realizadas diversas reuniões com o gestor do processo, com os usuários e com a equipe de TI para identificar o maior número possível de ativos. Ao identificar um ativo, discutia-se com os membros da equipe da continuidade qual era sua importância e qual seria o tempo mínimo aceitável de parada do mesmo para definir sua criticidade.

Percorrendo o processo, puderam-se identificar ativos de suporte e sua relação com ativos primários. Cada ativo de suporte possui relacionamento com no mínimo um ativo primário, e pode ser um conjunto de diversos outros ativos de suporte, por exemplo: o datacenter é formado por diversos servidores e equipamentos de infraestrutura.

Como principais ativos primários foram identificados: processo de separação, processo de faturamento, processo de emissão de nota fiscal eletrônica, conhecimento estratégico, entre outros.

Como principais ativos de suporte foram relacionados: servidores, sistema ERP e banco de dados, coletores de dados móveis, computadores, impressoras, empilhadeiras, separadores, faturistas, depósito, prateleiras, documentos, entre outros. Foram identificados também ativos utilizados nos processos de cópias de segurança da empresa. A figura 44 apresenta um recorte de alguns ativos de suportes registrados no sistema PCN.

Figura 44: Recorte do registro de ativos no sistema PCN da empresa

Ativo	Responsável	Descrição	Classificação	Subtipo de ativo	Tipo de ativo	Criticidade	Ativos primários/suporte pertencentes	SLA
Expedidor	Coordenador de Expedicao	Profissional responsável por executar as atividades do processo de negócio	Suporte e Infraestrutura	Usuários	Recursos humanos	Média	Processo de Separação de Produtos; Processo de Ressuprimento	5
Coletor de dados Motorola	Coordenador de TI	Equipamento utilizado para executar as tarefas do processo de negócio	Suporte e Infraestrutura	Equipamento móvel	Hardware	Alta	Processo de Ressuprimento; Processo de Separação de Produtos	2
Roteador rede Wireless Motorola W2000	Coordenador de TI	Equipamento de gerenciamento da rede Wifi que é utilizada pelo sistema WMS	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Ressuprimento; Processo de Separação de Produtos	1
Impressora de Etiquetas Datamax i4208	Analista de Suporte	Impressora utilizada para a impressão de etiquetas de Packing	Suporte e Infraestrutura	Equipamento fixo	Hardware	Média	Processo de Packing	6
Microcomputador de Faturamento	Analista de Suporte	Computador utilizado para integração de embarques e emissão de Nota Fiscal	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Média	Website BNDES; Website Sefaz RS; Website Sintegra.gov; Website Suframa; Processo de Faturamento	2

Diversos ativos identificados já possuem ações de tratamento para reduzir riscos, por exemplo: coletores de dados já possuem redundância, sendo quatro unidades utilizadas diariamente e duas unidades mantidas em espera para caso algum apresente defeito. Os ativos foram devidamente registrados no sistema e disponibilizados para acompanhamento dos diversos membros da equipe.

Os ativos identificados podem ser encontrados no Anexo D, 3.1. Ativos.

b) Análise de riscos

A partir da identificação dos ativos, foi realizado um extenso trabalho de análise de riscos. Seguiu-se a mesma linha da identificação dos ativos, percorrendo a lista de ativos em conjunto com os usuários-chave, usuários de TI e gestores de processo. Os ativos de TI de alta criticidade foram os primeiros a serem avaliados e foram foco da atividade.

A análise de riscos tornou-se bastante extensa pois em um único ativo de suporte, como um computador de faturamento, foram identificados mais de dez possíveis ameaças: falha de disco rígido, falha de memória, falha de processador, falha em adaptador de rede ethernet, falha em placa mãe, ameaça de vírus, dano do sistema operacional, queima de fonte, problema com cliente do sistema ERP, falha em periféricos, entre outros. Visto que as ameaças exploram vulnerabilidades e possuem consequências semelhantes, em conjunto com os gestores de processo optou-se por simplificar as ameaças em uma única: falha de equipamento.

Cada risco identificado foi avaliado quanto a seu impacto no processo. A probabilidade de ocorrência foi identificada com base em histórico de ocorrências internas,

parcialmente registrada no sistema de atendimento de TI da empresa, ocorrências em outras empresas da região e segmento, e nas condições físicas e lógicas dos ativos. Com as informações de impacto e probabilidade, o nível do risco pode ser calculado e devidamente registrado para cada risco identificado. A figura 45 representa alguns riscos identificados e registrados no sistema PCN.

Figura 45: Riscos identificados e registrados no sistema PCN da empresa.

Ativo	SLA	Ameaça↓	Tipo de ameaça	Origem	Vulnerabilidade	Consequência	Impacto	Probabilidade	Nível
Banco de Dados Progress - Datasul EMS	1	Usuário trancado no EMS	Paralisação de serviços essenciais	Acidental	Usuários do sistema só podem estar logados uma unica vez	Impossibilidade de entrar no sistema com o usuário	Alto	Média	Médio
Datasul EMS	1	Sistema sem licenças disponiveis	Comprometimento de funções	Acidental, Intencional	Sistema possui limite de 30 licenças de acesso	Impossibilidade de acessar o sistema	Alto	Baixa	Médio
Fibra Óptica Apoio > Data Center	2	Rompimento de fibra óptica externa	Dano físico	Acidental, Intencional, Natural	Fibra óptica muito sensível	Interrupção da conexão de rede com o Data Center	Alto	Baixa	Médio
Distribuidor Óptico Data Center	2	Rompimento de fibra interna	Dano físico	Acidental, Intencional	Fibra óptica muito sensível	Interrupção da conexão de rede	Alto	Baixa	Médio
HP Data Protector	48	Restauração de backup com falhas	Falhas técnicas	Acidental	Frequência de teste de restauração muito baixa	Possibilidade de não conseguir restaurar o backup quando necessário	Alto	Baixa	Médio
Servidor Físico de Licenças Datasul - FMSBK07	48	Reinicialização do servidor de Licenças	Comprometimento de funções	Acidental, Intencional	Servidor físico não consegue reestabelecer a operação automaticamente	Interrupção de novo Login no sistema EMS	Alto	Baixa	Médio
Microcomputador de Faturamento	2	Queima de Fonte de Alimentação	Dano físico	Acidental, Intencional	Computador com fonte única	Interrupção do uso do computador	Médio	Média	Baixo

Os riscos identificados estão presentes no Anexo D, 4.1. Riscos.

c) Revisão da análise de riscos

Os riscos identificados foram revisados pelo gestor da continuidade, gestor de processo e um dos patrocinadores. Diversos riscos já possuem alguma forma de controle, o que simplificou a etapa subsequente. Durante a revisão foram identificados alguns riscos que não haviam sido relacionados e então devidamente registrados.

4.2.3 Elaboração do plano de continuidade de negócios

Com a gestão de riscos executada e revisada, pôde ser iniciada a elaboração do plano de continuidade propriamente dito. As ações foram coordenadas pelo gestor da continuidade juntamente com os demais papéis, conforme sugerido no guia.

a) Definição dos SLA

A elaboração do plano de continuidade é iniciada pela definição dos SLA. Cada ativo identificado na análise de riscos teve seu SLA definido pelo gestor da continuidade em conjunto com os gestores de processo e pela equipe de TI. Os SLA foram determinados com base na importância de cada ativo para o processo e em quanto tempo a empresa poderia operar sem aquele ativo, considerando as quantidades. Neste momento não é considerada a capacidade de atendimento da equipe de TI, reavaliado na elaboração dos planos de resposta a incidentes.

Os SLA podem ser encontrados no registro de ativos, presente no Anexo D, 3.1. Ativos.

b) Elaboração das ações de tratamento

Com base nos riscos identificados, as ações de tratamento foram elaboradas. Conforme sugerido no guia, foram primeiro analisados os riscos com maior nível, porém como diversos riscos já possuíam controles elaborados, estes logo foram registrados como ações de tratamento já realizadas. Dentre os riscos de maior impacto, dividiu-se a equipe em duas para acelerar o processo. O gestor de processo, juntamente com os usuários chave, foi responsável por elaborar ações para ativos não diretamente envolvidos com a TI da empresa. O gestor da continuidade e a equipe de TI se responsabilizaram por elaborar as ações dos ativos específicos de TI e do Datacenter da empresa.

Pelo gestor do processo, foram elaboradas ações como: contingência de colaboradores por função, adquirir coletores reservas, manter baterias reservas para coletores, operar com empilhadeiras acima da capacidade mínima, entre outras. Pela equipe de TI foram elaboradas ações como redundância de servidores, redundância de serviços críticos Microsoft, ativação de controle de inatividade de usuários no ERP, entre outras. Foram levantadas também ações para transferência de riscos, como a migração de serviços para datacenter de terceiros.

Houveram riscos que foram aceitos pelo gestor de processo e pelos patrocinadores, porém serão tratados de forma reativa nas ações de tratamento. Ações de tratamento que requerem investimento estão sob análise dos patrocinadores e permanecem não executadas até sua liberação. A figura 46 representa algumas das ações de tratamento elaboradas e registradas no sistema PCN.

Figura 46: Ações de tratamento elaboradas e registradas no sistema PCN

Plano de Continuidade	Ameaça	Vulnerabilidade	Consequência	Ação	Tipo de tratamento	Responsável	Requer investimento?	Valor↓	Aprovado?
Faturamento e Expedição	Sistema sem licenças disponiveis	Sistema possui limite de 30 licenças de acesso	Impossibilidade de acessar o sistema	Aquisição de novas licenças FULL no EMS2	Reduzir risco	Coordenador de TI	Sim	R$ 50.000,00	Não
Faturamento e Expedição	Falha em ambas controladoras do Storage	Storage depende das controladoras para funcionamento	Interrupção total do ambiente de TI da empresa e possibilidade de corrupção na base de dados.	Aquisição de novo Storage mais moderno e com maior capacidade	Reduzir risco	Coordenador de TI	Sim	R$ 45.000,00	Sim
Faturamento e Expedição	Falha no Servidor de Virtualização	Estrutura de TI dependente de Hardware Físico	Interrupção do acesso a rede e todos seus sistemas	Aquisição de novos servidores de virtualização	Reduzir risco	Coordenador de TI	Sim	R$ 30.000,00	Sim
Faturamento e Expedição	Interrupção acidental dos servidores virtuais	Servidores administrados pelo Xen Center podem ser desligados por quem tem acesso a Console	Interrupção de servidores e serviços de rede/sistemas	Aquisição do XenServer Standard	Reduzir risco	Coordenador de TI	Sim	R$ 15.000,00	Não
Faturamento e Expedição	Falha no servidor de E-mail	Servidor único interno para gerenciamento e hospedagem de E-mail	Interrupção no envio e recebimento de E-mail	Disponibilização do Serviço de E-mail na Nuvem	Transferi risco	Coordenador de TI	Sim	R$ 12.000,00	Não
Faturamento e Expedição	Falha no Switch SAN	Switches estão em atividade por mais de 3 anos.	Interrupção na comunicação entre Storage e Servidores. Interrupção dos processos de negócio.	Aquisição de novos Switches para rede SAN	Reduzir risco	Coordenador de TI	Sim	R$ 12.000,00	Sim

As ações de tratamento elaboradas, independentemente de sua aprovação, estão presentes no Anexo D, 5.1 Ações de tratamento dos riscos.

c) Cópias de Segurança

A empresa possui uma cultura de realizar cópias de segurança dos ativos importantes para o negócio, o que facilitou a identificação dos métodos e processos desta etapa.

A organização possui ferramentas para efetuar as cópias de segurança, bem como a cultura de armazenamento seguro de mídias para recuperação. Foram identificados ferramentas como o software HP Data Protector para realizar as tarefas de cópia de segurança, a unidade de fita Linear Tape-Open (LTO), Dell Power Vault 4 para gravar as cópias de segurança em mídias de fita LTO, e o servidor de cópias em disco HP ML110. Os métodos de cópia de segurança estão relacionados no Anexo D, 6.1. Métodos de cópias de segurança.

Com o levantamento das ferramentas utilizadas para realizar as cópias de segurança, foram analisados todos os ativos pela equipe de TI e verificado se estes já possuem alguma rotina de arquivamento ou se era necessária sua elaboração. Ativos críticos como a cópia da base de dados do sistema ERP, arquivos de rede e programas de uso do ERP já estavam contemplados em rotinas de cópias de segurança diária em mídias de fita LTO. A rotina diária em fita é validada semanalmente através da recuperação de dados armazenados ao selecionar uma amostragem dos arquivos e então é testada a sua restauração. Esta rotina, principal rotina de cópias de segurança da empresa, é realizada diariamente e suas mídias são armazenadas em

um cofre à prova de fogo no setor financeiro da empresa e uma mídia é semanalmente armazenada pelo diretor administrativo da empresa em ambiente externo.

Os servidores da empresa também possuem uma rotina de cópias de segurança com objetivo de simplificar o plano de recuperação de desastres. Mensalmente o sistema operacional de virtualização armazena uma cópia, em tempo real de execução, do servidor virtual por completo. Esta rotina permite que o servidor seja completamente recuperado de maneira rápida em caso de sinistros no ambiente de virtualização. Pela complexidade do processo, não são realizados testes frequentes de validação destas cópias, porém foi sugerida uma rotina semestral de validação. A figura 47 representa um recorte de algumas das cópias de segurança registradas no sistema PCN. As cópias de segurança estão presente no Anexo D, 7.1. Cópias de segurança.

Figura 47: Recorte do registro de Cópias de segurança no sistema PCN

Ativo	Possui backup?	Método de backup	Periodicidade	Ciclo de vida	Responsável	Ações de validação	Periodicidade de validação
Datasul EMS	Sim	Diário Datasul em Disco	2 vezes ao dia	1 dia	Coordenador de TI	Restauração do backup da base em ambiente de protótipo.	Semanal
Datasul EMS	Sim	Diário em Fita	Diário	Semanal	Coordenador de TI	Restauração do backup da fita em área de restore	Mensal
Infra Estrutura de Virutalização	Sim	Semanal de VMs	Semanal	Único	Coordenador de TI	Restaurar uma VM no ambiente de produção através do backup realizado	Nunca realizada
Microsoft Active Directory - Servidor Virtual VMSAD05 e VMSAD19	Sim	Diário em Fita	Diário	Semanal	Coordenador de TI	Verificar se o backup foi realizado através do Data Protector	Mensal
Diretório de Rede da Logística	Sim	Diário em Fita	Diário	Semanal	Coordenador de TI	Restauração dos arquivos em diretório temporário de rede	Mensal

d) Elaboração do plano de resposta a incidentes

Com as principais rotinas de cópias de segurança identificadas e devidamente registradas, a aplicação pode prosseguir à elaboração das ações de resposta a incidentes. Esta etapa tornou-se a mais importante do plano devido à restrição de recursos financeiros para implementar as ações de tratamento propostas. Parte dos planos de resposta foram elaboradas para responder as ameaças com menor custo possível, possuindo um tempo aceitável, acordado pelos patrocinadores, para sua execução.

Para elaborar o plano de resposta a incidentes, o processo foi dividido em duas partes: riscos envolvendo ativos de contato direto dos usuários como coletores, computadores

e o sistema ERP, e os riscos envolvendo ativos de infraestrutura como servidores, link de acesso à internet e banco de dados. O primeiro grupo de ativos teve suas ações elaboradas pela equipe de TI juntamente com o gestor do processo e seus usuários-chave, enquanto o segundo grupo teve as ações elaboradas exclusivamente pela equipe de TI.

Para os ativos de uso direto pelos usuários foram elaboradas ações como: configurar emergencialmente o coletor de dados em caso de falha de inicialização, trocar peça de hardware danificada, alterar de servidor utilizado para a conexão dos coletores, derrubar usuários trancados no sistema ERP, formatar computador com sistema operacional corrompido, entre outros.

Para os ativos de infraestrutura do datacenter foram elaboradas ações como: restaurar cópia de segurança de arquivos perdidos, ativar servidores virtuais críticos em único servidor físico, reativar banco de dados após queda, acionar suporte do fabricante de hardware em caso de falhas, ativar contingência de nota fiscal eletrônica, entre outros.

Na elaboração do plano de resposta foram abordados os principais ativos do processo. Por opção da empresa, nem todos os ativos tiveram planos de resposta elaborados. Os planos elaborados foram validados pela área de TI e pelo gestor do processo. A figura 48 representa um recorte de alguns dos planos de resposta a incidentes que foram elaborados durante a aplicação do sistema PCN.

Figura 48: Recorte de planos de resposta a incidentes registrados no sistema PCN

Ação	Observações	Ameaça	SLA	Plano de continuidade	Ativação	Tipo de ação	Responsáveis	Quem deve ser acionado na ocorrência?
Conserto do ar condicionado	Acionar a MAeli para consertar o ar condicionado.	Falha no Ar Condicionado	48	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI
Acionar terceiro responsável para conserto	Chamar fornecedor para reparar o No-Break. Transferir a carga para o no -break secundário (somente FMSBK07 não possui redundância automática)	Falha no No-Break primário do Data Center	12	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI
Abrir as janelas do Data Center	Abrir as janelas para ventilar o Data Center	Falha no Ar Condicionado	1	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Analista de Suporte
Configurar Data/Hora no coletor	Reconfigurar manualmente as configurações de Data/Hora do coletor para pertmir acesso ao TS.	Coletor não acessa o sistema após troca de bateria	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte
Forçar reinicilização através da tecla F1 fisicamente	Forçar a inicilização apertando a tecla F1	Reinicialização do servidor de Licenças	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte

Nem todos os riscos tiveram ações de tratamento ou planos de resposta elaborados, isto se deve à variação das ameaças e na complexidade de identifica-las. Cita-se como exemplo um erro de processo no sistema ERP. Como os erros podem ser variados e não foram todos identificados, foi elaborado um plano de resposta único para acionar o suporte do ERP

em caso de qualquer erro de sistema que possa ocorrer. Esta ação foi aprovada pelo gestor do processo.

Os planos de resposta a incidentes estão presentes no Anexo D, 8.1. Planos de resposta a incidentes.

Os contatos de terceiros que podem auxiliar nas ações do plano de continuidade também foram levantados e registrados ao longo da execução do plano. Os contatos estão relacionados no Anexo D, 17.1 Contatos.

e) Recuperação de desastres

A empresa já possui ações para recuperação, porém não há um registro formal das atividades necessárias para restaurar a sua operação de faturamento em caso de desastre. A elaboração do plano de recuperação de desastres foi considerada um dos principais ganhos pelos gestores de processo e patrocinadores.

- Ativação do plano de recuperação de desastres

O processo de faturamento da empresa depende dos sistemas de informação para operar. Pensando nesta dependência, foi determinado que o desastre seria a parada total do datacenter da empresa e os demais ativos exclusivos de TI, tendo seus equipamentos e dados danificados. Esta definição de desastre abrange incêndios, falhas em hardware ou outros possíveis sinistros identificados na análise de riscos que afetariam o datacenter da empresa. O plano de recuperação foi nomeado Recuperação Emergencial, priorizando a recuperação mais rápida possível, simplificando o processo e recuperando apenas os ativos cruciais para o funcionamento. O processo será retomado sem a recuperação do sistema automatizado por coletores, WMS, visto que este retardaria a recuperação, sacrificando parcialmente a segurança e robustez no processo. Por se tratar de um plano de TI, não foram considerados desastres que afetam ativos de negócio como estoque e o armazém. As definições foram realizadas pelo gestor da continuidade, gestores de processo e patrocinadores.

Com o desastre definido, foi estabelecido que a recuperação deverá ocorrer no interior da própria expedição, onde ocorre o processo de faturamento, em uma sala exclusiva para a instalação do Hardware e realização dos serviços de recuperação. Cabe ao Coordenador de TI, gestor da continuidade na empresa, a responsabilidade pela ativação e pela realização das ações do plano de recuperação de desastres. O Diretor Financeiro, patrocinador da continuidade, é o responsável financeiro e pelas tomadas de decisões em caso de alteração no decorrer do plano de recuperação. O Gerente de Logística, outro patrocinador, é responsável pelas aquisições, negociações e locações dos ativos que serão recuperados. A aprovação do

plano de recuperação de desastres fica por conta do Diretor Financeiro, patrocinador. O SLA definido para a recuperação foi de 80 horas corridas, devido a dependência de equipamentos e serviços de terceiros.

As definições de ativação do plano de recuperação de desastres estão presentes no Anexo D, 9.1 Ativação da recuperação de desastres.

- Ativos de TI para a recuperação de desastres

Com a diretiva de recuperar o ambiente o mais rapidamente possível, simplificando o processo, os ativos para recuperação divergem dos ativos presentes na empresa atualmente. A empresa conta com diversos servidores, equipamento de armazenamento de dados, sistema automatizado com coletores, entre outros. Para a recuperação devem ser adquiridos ou, na medida do possível, locados uma quantidade inferior de ativos, permitindo que o processo de faturamento seja executado, porém sacrificando parcialmente sua robustez e segurança. O levantamento foi realizado em reuniões com toda a equipe da continuidade.

Para que a recuperação de desastres ocorra com sucesso, é necessária a restauração das cópias de segurança já existentes na empresa, como a cópia do sistema ERP, a cópia dos servidores virtuais, as cópias de atualização dos servidores virtuais, a cópia do servidor de arquivos, e as demais cópias de segurança identificadas na aplicação.

O hardware de recuperação definido representa uma estrutura simplificada da atual TI da empresa. Para a recuperação serão necessários ativos como: Servidor para restauração das cópias de segurança, unidade de Fita para restaurar as cópias de segurança, Link de acesso a internet, servidor para hospedagem de máquinas virtuais, fornecimento de energia, servidor virtual Microsoft Active Directory recuperado, servidor virtual para banco de dados do ERP, servidor virtual de aplicação ERP recuperado, sistema para emissão de nota fiscal eletrônica, chave de licenças do ERP, computador para faturamento, impressora de notas fiscais, entre outros. A figura 49 apresenta um recorte de alguns dos ativos de TI identificados e registrados para a recuperação de desastres no sistema PCN.

Os ativos de TI para a recuperação estão presentes no Anexo D, 9.2.1 Ativos de TI para a recuperação de desastres.

Figura 49: Recorte de ativos de TI necessários para a recuperação de desastres registrados no sistema PCN

Plano de recuperação de desastres	Ativo para recuperação	Tipo de ativo	Quantidade	Descrição detalhada	Possui redundância?	Custo aproximado	Prioridade
Recuperação emergencial	Rack de servidores	Meio físico e infraestrutura	1	Rack de 42U com 2 unidades de distribuição de energia estabilizada. Marca independe.	Não	R$ 5.000,00	Baixa
Recuperação emergencial	Switch Camada 2	Interface de comunicação	1	Switch Core de Rede Camada 3	Não	R$ 5.000,00	Alta
Recuperação emergencial	Servidor para virtualização de serviços críticos do negócio	Equipamento de processamento de dados	1	Servidor para hospedagem dos demais servidores Virtuais. Sistema operacional Xen Server (Free Edition) , 2 Processadores Xeon Quad Core, 48 Gb de Memória, 6 portas de Rede (4 On Board, 2 Off Board), 8 discos de 600 Gb SAS 15k HotPlug.	Não	R$ 25.000,00	Alta
Recuperação emergencial	Sala para servidores	Edificações	1	Sala para instalação dos Servidores	Não		Média

– Ativos de recursos humanos para a recuperação de desastres

Para recuperação foi definido um conjunto de pessoas que são necessárias para recuperar e executar o processo após este estar recuperado. São colaboradores necessários: faturistas, expedidores, um coordenador de equipe de expedição e um analista de suporte para eventualmente apoiar os demais. Além destes profissionais, foi identificada a necessidade de um analista de manutenção eletricista para fornecer energia elétrica à expedição, um especialista em infraestrutura e hardware para auxiliar na reconstrução do ambiente tecnológico e um especialista no ERP da empresa, para reconstruir o ambiente de sistema da empresa.

Os ativos de recursos humanos estão presentes no Anexo D, 9.2.2 Ativos de RH para a recuperação de desastres.

– Serviços de terceiros necessários para a recuperação de desastres

Devido à equipe de TI e manutenção da empresa ser restrita, é necessária a contratação de profissionais terceirizados especialistas para executar algumas ações do plano de recuperação. Estes profissionais foram registrados nos contatos do sistema PCN e devem ser acionados assim que a recuperação for iniciada.

São necessários os serviços de terceiros para o fornecimento de energia elétrica, sendo este um fornecedor parceiro da empresa. Para a restauração da infraestrutura de TI da empresa há um terceiro contratado para executar serviços de suporte, foram identificados dois profissionais deste fornecedor para fornecer serviço de suporte na recuperação das cópias de segurança e reconstituição do ambiente de TI. O último serviço de terceiros necessário é o de suporte à tecnologia do ERP da empresa, sendo crucial para a reinstalação do banco de dados

e restauração das cópias de segurança do sistema ERP. A figura 50 representa os serviços de terceiros identificados para a recuperação de desastres.

Figura 50: Recorte do registro de serviços de terceiros para a recuperação de desastres

Plano de recuperação	Serviço	Descrição detalhada	Custo aproximado	Necessidade de acionamento	Contato	Contat:Empresa	Responsável interno
Recuperação emergencial	Restauração da infraestrutura de TI	Profissional com alto nível de conhecimento em ambiente de Infraestrutura (Storage, Servers e SAN). Responsável por reestabelecer o funcionamento da estrutura de TI. A Gruppen possui equipe especializada para atender esta demanda.		Alta	Consultor Storage; Consultor Linux	SuporteTI; SporteTI	Coordenador de TI
Recuperação emergencial	Restauração do ambiente Datasul	Profissional especialista em Ambiente Progress e Datasul para reinstalar os bancos de Dados e colocar o Sistema operante no ar.		Alta	Consultor Progress; Consultor Banco	SuporteERP; SuporteERP	Coordenador de TI
Recuperação emergencial	Restauração do fornecimento de Energia	Empresa fornecedora de Energia à Infraestrutura da empresa.		Alta	Eletricista Eletro; Eletricista EnergiSA	Eletro SA; Energi SA	Coordenador de Manutencao
Recuperação emergencial	Restauração dos serviços Microsoft	PRofissional capacitado para restaurar e reconfigurar os serviços de TI Microsoft como Active Directory e SQL Server		Alta	Consultor Microsoft; Consultor Storage	SuporteTI; SuporteTI	Coordenador de TI

Os serviços de terceiros relacionados estão presentes no Anexo D, 9.2.3 Serviços de terceiros para a recuperação de desastres.

– Ações para a recuperação desastres

Com os ativos e responsáveis definidos, foi elaborado o plano de recuperação propriamente dito. As ações foram elaboradas pelo gestor da continuidade em conjunto com a equipe de TI para recuperar a infraestrutura de TI o mais rápido possível.

A recuperação de desastre se inicia a partir de uma definição e organização do local onde será reinstalada a estrutura de TI. Com esta definição, os responsáveis pelas ações e aquisições devem providenciar os ativos de hardware para iniciar as atividades de restauração. A empresa pode tanto adquirir os equipamentos quanto aluga-los dos fornecedores parceiros, a decisão terá como base o prazo de entrega de cada opção. Em paralelo à aquisição, o fornecimento de energia deve ser estabelecido no local pela equipe de manutenção.

As primeiras ações do plano de recuperação de desastres contemplam a instalação de servidor e demais periféricos para realizar a restauração das cópias de segurança da empresa. Um servidor para hospedagem dos servidores virtuais deve ser instalado, juntamente com o reestabelecimento de acesso à Internet. Esta é a infraestrutura básica necessária para a recuperação. As ações necessitam de terceiros para serem executadas de maneira a atender prazo e qualidade.

Com a infraestrutura básica recuperada, pode-se iniciar a restauração do sistema ERP da empresa, acesso à rede, sistema de nota fiscal eletrônica, computadores para faturamento, entre outros através de restauração das cópias de segurança. Após restauração do ambiente de TI, o processo pode ser validado pela equipe de faturamento e então reestabelecido em produção.

A figura 51. representa algumas das ações do plano de recuperação de desastre elaborada na empresa.

Figura 51: Ações do plano de recuperação de desastres

Plano de recuperação	Ação	Descrição da ação	Nº Ação	Tipo de ação	SLA	Responsável	Dependente de ação	Ativos para recuperação habilitados
Recuperação emergencial	Adqurir computador para uso no faturamento	Adqurir computador com fornecedores parceiros. O micro pode ser "Locado" para emergência.	55	Reinstalação	1	Coordenador de TI		
Recuperação emergencial	Adquirir unidade de fita LTO-4	Adquirir (ou Locar) unidade de Fita LTO -4 para realizar a restauração dos Backups em fita	60	Reinstalação	8	Coordenador de TI		
Recuperação emergencial	Instalar e configurar servidor para recuperação	Instalar o Microsft Windows Server 2008 R2 , configurar o servidor com acesso a Internet e instalar o HP Data Protector	70	Reinstalação	8	Coordenador de TI	Aquisição de Servidor para Restauração dos Backups; Estabelecer e organizar local para instalação dos equipamentos de TI	Servidor para restauração dos Backups
Recuperação emergencial	Instalar e configurar a unidade de Fita no servidor de backup	Realizar instalação da unidade de Fita no servidor de backup. Esta atividade pode ser feita pelos técnicos da Suporte TI, previsto	80	Reinstalação	4	Coordenador de TI	Instalar e configurar servidor para recuperação; Adquirir unidade de fita LTO-4	Unidade de Fita Dell LTO-4

As ações para recuperação de desastre estão relacionadas no Anexo D, 10.1 Ações para recuperação de desastres.

f) Implementação dos OLAs

As atividades registradas no plano de continuidade de negócios são, em parte, compreendidas pela equipe de TI, o que reduz a necessidade em elaborar os OLAs para cada atividade. Porém, quando se trata de continuidade de negócios, não deve-se depender do conhecimento individual dos integrantes da equipe.

Os OLAs serão elaborados pela equipe da continuidade conforme a necessidade e disponibilidade para sua elaboração. A equipe TI possui manuais de diversas operações e estes estarão sendo convertidos em novos OLAs. O primeiro documento OLA elaborado é referente ao plano de resposta “Derrubar usuários trancados no ERP”. O OLA pode ser encontrado no Anexo D, 11.1 Acordos de nível operacional – OLA.

g) Avaliação do plano de continuidade de negócios

Tendo o plano de continuidade elaborado e revisado pelo gestor da continuidade, foi realizada uma apresentação do plano para os gestores de processo, equipe de TI e patrocinadores. O acesso ao plano foi liberado para que os gestores de processo e patrocinadores pudessem acessá-lo e validá-lo. Após um tempo determinado, a aprovação do plano foi obtida pelo gestor da continuidade, pelo gestor do processo e pelos patrocinadores. Devido a restrições orçamentárias, nem todas as ações de tratamento foram aprovadas, no entanto estão planejadas para execução conforme decorrer do segundo semestre deste ano. A aprovação do plano foi registrada em ata e armazenada na biblioteca de documentos do sistema PCN.

O registro da aprovação do plano de continuidade está presente no Anexo D, 12.1 Aprovação do plano de continuidade de negócios.

4.2.4 Execução, monitoramento e controle da continuidade

A quarta fase, execução, monitoramento e controle da continuidade teve como foco a disponibilização do plano e a elaboração dos indicadores da continuidade, planos de teste e planos de revisão. Devido ao tempo disponível para o estudo de caso não puderam ser registradas ocorrências e acompanhar o funcionamento do plano em execução.

a) Disponibilização do plano de continuidade de negócios

O plano de continuidade de negócios está disponibilizado no Sharepoint da empresa e seu acesso é liberado aos membros da equipe da continuidade. O sistema Microsoft Sharepoint Foundation 2010 possui rotina de cópias de segurança e é tratado como um ativo crítico do processo de negócio. Além de estar armazenada nos servidores, uma cópia do plano de continuidade foi impressa e armazenada em local seguro, a prova de fogo. Outra cópia do plano foi impressa e armazenada na residência do gestor da continuidade, bem como o arquivo utilizado na impressão.

b) Medição e monitoramento do plano de continuidade

Pensando no menor tempo de interrupção possível e no melhor aproveitamento do plano de continuidade, foram adotados os indicadores sugeridos no modelo pois estes se encaixam perfeitamente no que a empresa deseja medir. As metas forma definidas de maneira

otimista, baseando-se em ocorrências do passado e na expectativa da empresa com o plano de continuidade. A interrupção deve ser a mínima possível, sendo 10 horas o máximo aceitável de parada parcial do processo, porém a interrupção total não é tolerada. O desempenho da continuidade pode ser medido pelo uso dos planos dentro dos SLA acordado. O plano de continuidade tem como objetivo abranger todos os ativos possíveis envolvidos no processo. As ações de tratamento foram elaboradas para evitar desastres, sendo avaliadas pela sua eficiência em evitar tal risco. Em caso de desastres, a empresa avalia a eficiência da recuperação através do plano de recuperação de desastres. As metas foram determinadas com base nos índices de qualidade da empresa, auditados anualmente pela auditoria de certificação ISO 9001.

Os indicadores serão avaliados mensalmente e se tornarão parte das metas de desempenho da equipe de TI da empresa. A tabela 6 representa os indicadores adotados e suas metas. Os indicadores também estão presente no anexo D, 14.1 Indicadores da continuidade de negócios.

Tabela 6: Indicadores do plano de continuidade elaborados pela empresa

Indicador	**Meta**
Quantidade de horas perdidas por usuários devido à inoperância não planejada dos sistemas	10 horas
Porcentagem de incidentes atendidos e solucionados pelos planos de resposta a incidentes	95%
Porcentagem de incidentes atendidos e solucionados dentro do prazo do SLA	95%
Porcentagem de ativos cobertos pelo plano de continuidade de negócios	100%
Frequência de interrupção de serviços nos sistemas críticos	Nunca
Desastres ocorridos	0
Sucesso na recuperação de desastres através da utilização do plano	Sim

c) Simulações e testes

Para garantir a segurança proporcionada pelo plano de continuidade, está sendo elaborada uma lista de testes para validar as ações do plano de continuidade, porém devido ao tempo disponibilizado a lista não foi finalizada. Os testes foram elaborados conforme sugerido no modelo, sendo definido o que deve ser testado, qual ação será realizada para efetuar o teste, qual o objetivo e o que deve ser analisado, a complexidade do teste, a periodicidade que deverá ser realizado o teste, o responsável pelo teste. Os OLA para o plano de testes estão em elaboração pela equipe da continuidade.

Foram testes elaborados pela empresa: teste de desempenho dos servidores com ar condicionado desativado, teste de reativação dos servidores virtuais em único servidor físico, teste de envio de nota fiscal em ambiente de contingência nacional, troca de servidor de

acesso remoto dos coletores, entre outros. Os planos de testes estão em constante evolução e deverão fazer parte dos indicadores em uma próxima revisão do plano de continuidade.

O primeiro teste elaborado consiste em avaliar o desempenho dos servidores virtuais operando com 50% da capacidade de processamento, com único servidor físico operando. O teste deve ser realizado através do desligamento de um dos servidores físicos e transferir os servidores virtuais para o servidor que foi mantido ligado. O teste pode ser avaliado pelo tempo de realização da transferência dos servidores e pelo desempenho do ambiente nestas condições. Os testes estão presentes no anexo D, 15.1 Plano de testes.

d) Revisão, atualização e melhoria contínua do plano de continuidade

Devido ao processo de faturamento da empresa sofrer alterações, o plano de continuidade também necessita de manutenção. Pensando nesta situação, foram determinadas revisões por fases e etapas do plano.

Os integrantes da equipe envolvida será revisada mensalmente com base na rotatividade na empresa. A análise de ativos e riscos será realizada bimestralmente, seguindo as mesmas atividades do guia conforme o levantamento inicial. Trimestralmente deverão ser revisadas as ações de tratamento e os planos de resposta a incidentes a fim de atender novos riscos ou aperfeiçoar seus controles já existentes. O processo será revisado semestralmente ou conforme alterações forem realizadas por demanda externa. O plano de recuperação de desastres deverá ser revisado anualmente. Os OLAs serão revisados conforme alterações nos demais processos.

O plano de revisão está presente no Anexo D, 16.1 Revisão e manutenção do plano de continuidade.

4.3 CONSIDERAÇÕES E AVALIAÇÃO DO PLANO DE CONTINUIDADE

O plano de continuidade é um documento de extrema importância para a empresa pois está ligado diretamente com um de seus processos mais importantes, o faturamento. A elaboração do primeiro plano de continuidade representa uma mudança na maneira que a empresa visualiza seus processos, focando não apenas no resultado imediato, mas também em fatores que possam prejudicar este resultado e ações para garantir o melhor resultado possível. O plano de continuidade elaborado é o primeiro passo para que a empresa adote a

continuidade em sua estratégia e, nos próximos anos, passe a elaborar planos para outros processos críticos ao seu resultado.

Durante a aplicação do modelo na empresa foram encontradas algumas dificuldades. Na análise de riscos existe uma grande quantidade de vulnerabilidades para o mesmo ativo, sendo necessário simplificar estes riscos, tornando a análise menos variada, porém abordando quase todas as ameaças possíveis. Os planos de resposta a incidentes também foram elaborados de maneira mais simples, pensando na usabilidade do plano em caso de incidentes. Um plano envolvendo riscos e ações muito complexas poderia acarretar a não utilização do plano pelo gestor da continuidade. O ambiente de TI da empresa já possui certa maturidade e complexidade em sua organização, o que tornou a análise de riscos extensa, porem devido à esta complexidade, já existem algumas ações de tratamento dos riscos que foram apenas transcritas para o plano de continuidade.

Nem todas as ações de tratamento desejadas foram aprovadas, principalmente devido a restrições financeiras da organização. Com o plano em execução e tendo seu resultado visível para a empresa, é possível que um número maior de ações de tratamento sejam implementadas, pois tratar os riscos de forma proativa é mais seguro do que trata-los reativamente. O objetivo é que, nas próximas revisões do plano de continuidade, sejam elaboradas e aprovadas mais ações de tratamento do que planos de resposta a incidentes.

Para a avaliação do plano de continuidade gerado, foi elaborado um questionário a ser respondido pelos patrocinadores. O questionário foi elaborado com base no questionário de nivelamento do gerenciamento da continuidade de serviços do ITIL. O ITIL apresenta um conjunto de recursos para classificar as organizações em níveis de maturidade da continuidade de serviços (ITIL, 2008).

O questionário de avaliação é um conjunto de perguntas com possibilidade de resposta Sim, Parcialmente ou Não, possuindo pesos de avaliação 2, 1 e 0 respectivamente. Este questionário foi encaminhado para o diretor administrativo e financeiro, principal patrocinador da continuidade, durante a aprovação do plano de continuidade e, com resultado de 81% de aprovação, pode comprovar a satisfação da empresa com plano elaborado. A empresa considera este resultado satisfatório pois todos os itens do questionário que não foram atendidos se devem a restrições impostas pela própria empresa, de natureza financeira ou estratégica, mas que poderão ser atendidos conforme novos planos de continuidade sejam elaborados.

O questionário de avaliação e suas respostas estão presente no Anexo E. Questionário de avaliação do plano de continuidade de negócios.

4.4 CONSIDERAÇÕES FINAIS

Durante a aplicação do modelo elaborado, diversas questões foram levantadas e validadas na prática. A aplicação permitiu que o modelo fosse adaptado no sistema PCN para garantir uma melhor usabilidade aos usuários. A principal alteração sofrida no modelo foi a possibilidade de registrar diversos planos de continuidade de negócios, permitindo que o modelo seja aplicado em diferentes cenários dentro de uma organização. No plano de recuperação de desastres foram alteradas algumas instruções do guia e artefatos para permitir que o usuário identifique ativos que ainda não existem na organização e somente serão necessários em caso de recuperação de desastres. Nas ações de tratamento, planos de resposta e ações de recuperação foram acrescentadas colunas para descrever estas ações, facilitando seu entendimento reduzindo a necessidade de acesso aos OLAs em sua execução.

Por ter sido adotado o Microsoft Sharepoint Foundation 2010, não foi necessário desenvolver a estrutura do sistema desde o princípio, a ferramenta já possui uma infraestrutura própria e recursos para o desenvolvimento. O Sharepoint possui alguns recursos adicionais que facilitaram a usabilidade como a integração com o ambiente Microsoft de forma nativa, a edição simplificada de páginas e a possibilidade de criar uma biblioteca de documentos e listas para registro sem a necessidade de conhecimento em uma linguagem de programação específica. Estes recursos tornam a usabilidade do Sharepoint viável para a disponibilização do modelo de plano de continuidade elaborado neste trabalho.

A ferramenta adotada também possui limitações. O relacionamento entre as listas criadas permite a exibição apenas da chave estrangeira, dificultando a visualização do usuário. Há também dificuldades em gerar relatórios do plano de continuidade por completo, forçando o usuário a exportar artefato por artefato do plano para disponibilizar o plano no formato de arquivo. Outra limitação da ferramenta é a dependência do ambiente Microsoft, necessitando a aquisição de no mínimo uma licença do sistema operacional Windows Server 2008 r2.

A aplicação do modelo, com as devidas alterações, possibilitou a criação de um plano de continuidade para a empresa aplicada, atingindo seu objetivo principal. Após a elaboração do primeiro plano de continuidade de negócios, o gestor da continuidade não terá tanta necessidade de recorrer ao o guia, pois o uso do sistema é intuitivo e já existem ativos e riscos identificados que podem ser aproveitados, reduzindo o tempo de elaboração.

O modelo permite a elaboração de um plano de continuidade eficiente, porém ainda é necessário avaliá-lo através de uma série de critérios. Para elaboração dos critérios, foi

utilizado o questionário de nivelamento da continuidade de serviços do ITIL. O ITIL possui recursos para medir o nível de maturidade dos serviços de TI (ITIL, 2008).

Os critérios utilizados foram elaborados a partir das questões do nível iniciante, do nível repetitivo, do nível definido e algumas do nível gerenciado do ITIL, conforme as questões fossem aplicáveis ao modelo (ITSFM, 2013). O resultado positivo permite que o modelo seja utilizado em organizações que estejam nestes níveis. O questionário utilizado e suas respostas estão descritos na tabela 7.

Tabela 7: Critérios de avaliação do modelo segundo o ITIL v3

Avaliação do modelo de plano de continuidade segundo o ITIL	
Critérios	**Atende?**
O modelo permite a definição de um ou mais escopos para elaboração dos planos de continuidade?	Sim
O modelo permite a definição das restrições que podem vir afetar a implantação do plano de continuidade?	Sim
O modelo possui um plano de comunicação bem definido?	Não
O modelo possui atividades de gestão de riscos?	Sim
O modelo permite que seja registrada uma análise de impacto dos riscos?	Sim
O modelo permite a criação de planos de testes?	Sim
O modelo define responsabilidades para as ações de elaboração do plano?	Sim
O modelo define responsabilidades para cada ação registrada no plano?	Sim
O modelo permite um controle de atividades já executadas na elaboração do plano?	Não
O modelo possui um conjunto de atividades para elaborar ações para tratamento dos riscos?	Sim
O modelo possui um conjunto de atividades para elaborar ações de resposta a riscos ocorridos?	Sim
O modelo possui um conjunto de atividades para elaborar um plano de recuperação de desastres?	Sim
O modelo permite um controle de execução de ações a serem executadas durante a recuperação de desastres?	Não
O modelo permite criar uma sequencia de ações, com relacionamento entre elas e definições das tomadas de decisão a serem realizadas?	Não
O modelo permite a criação de diversos planos de continuidade e de recuperação?	Sim
O modelo possui um procedimento formal para acionar a recuperação de desastres?	Sim
O modelo permite definir as responsabilidades para situações de crise?	Sim
O modelo permite o relacionamento das atividades com a capacidade da equipe que vai executá-lo?	Não
O modelo possui relacionamento com contratos com terceiros?	Sim
O modelo sugere uma análise cíclica da análise de risco?	Sim
O modelo exige uma formalização para alterações no plano de continuidade?	Sim
Existe um procedimento formal para testes e revisões dos planos de continuidade?	Sim
O modelo foi elaborado seguindo critérios de padrões de qualidade (ISO) reconhecidos?	Sim
O modelo sugere a elaboração de instruções operacionais para a execução das ações elaboradas?	Sim

Avaliação do modelo de plano de continuidade segundo o ITIL	
O modelo está disponibilizado em uma ferramenta para a gestão da continuidade?	Sim
Os artefatos gerados pelo modelo está disponibilizado em uma ferramenta para a gestão da continuidade?	Sim
Os artefatos gerados pelo modelo fornece informação sobre o processo e vulnerabilidades no plano de continuidade?	Sim
Os artefatos gerados pelo modelo fornece informação sobre opções de planos de continuidade?	Sim
Os artefatos gerados pelo modelo fornece informação sobre as alterações dos planos de continuidade?	Sim
Os artefatos gerados pelo modelo fornece informação sobre a realização de testes e revisões dos planos de continuidade?	Sim
Os artefatos gerados pelo modelo fornece informação sobre riscos e ações de tratamento destes riscos?	Sim
Os artefatos gerados pelo modelo fornece informação sobre a eficiência do plano de continuidade?	Sim

Nem todos os critérios puderam ser atendidos, porém estes podem ser abordados em trabalhos futuros. O plano de comunicação proposto no modelo é simplificado, sugerindo algumas ações mas fica a critério do gestor da continuidade que irá aplica-lo. Pelo fato do modelo permitir que diversos planos sejam criados de forma simultânea, não há uma forma de acompanhar as atividades do guia conforme estas são executadas. O modelo tem como foco o planejamento e elaboração do plano de continuidade, o acompanhamento da execução também é de critério do gestor da continuidade, bem como o registro das tomadas de decisão. O modelo sugere a indicação de um responsável para cada atividade a ser realizadas na execução do plano, porém limita a um único colaborador.

Com base no resultado da avaliação do modelo através do ITIL, que atingiu 84% dos critérios, junto com a satisfação da organização com o plano de continuidade de negócios elaborado, pode-se concluir que o modelo é aplicável em organizações cuja gestão da continuidade de serviços seja de nível inexiste, inicial, repetitivo e definido.

5 CONCLUSÃO

O modelo elaborado no presente trabalho compreende uma compilação das diversas normas que tratam a continuidade de negócios e as refinam em uma única referência, baseada em autores e traduzida em uma linguagem simplificada para facilitar na elaboração de um plano de continuidade. A partir deste estudo foi elaborada uma proposta de solução e esta foi disponibilizada através de uma ferramenta de colaboração e aplicada em uma empresa de médio porte.

O resultado do trabalho é um modelo para a elaboração de um plano de continuidade de negócios eficiente, robusto e aplicável em diversos cenários. A continuidade de negócios precisa estar incorporada nos princípios da organização. Os planos de continuidade variam de organização para organização, o modelo compreende uma forma genérica de elaboração de um plano de continuidade de negócios.

As referências bibliográficas utilizadas no trabalho contribuíram tanto para a elaboração do guia e dos artefatos, quanto para a definição da medição e monitoramento e para a avaliação do modelo elaborado. Para a avaliação do modelo foi utilizado o questionário de nivelamento da maturidade dos serviços de TI presente no ITIL como base.

O modelo foi desenvolvido e disponibilizado através do Microsoft Sharepoint Foundation 2010 e disponibilizado no ambiente do NUSIS para uso. Com a transposição do modelo de artefatos para um sistema, alterações foram realizadas a fim de melhorar o uso para o usuário. Por se tratar de um subsite do Sharepoint, o sistema é aplicável em empresas que possuem ambiente Microsoft, devido à dependência do sistema operacional Windows, com a versão Foundation do Sharepoint. O Sharepoint atendeu as expectativas ao permitir que o sistema PCN pudesse ser implementado e utilizado para a elaboração do plano de continuidade.

A partir do estudo de caso da aplicação do modelo em uma empresa de médio porte da cidade de Caxias do Sul foi possível validar sua eficiência. A aplicação do modelo permitiu que fosse criado um plano de continuidade para um processo crítico da empresa. A partir da aplicação, a empresa possui condições de elaborar novos planos de continuidade conforme surgir a necessidade. O plano de continuidade elaborado foi aprovado pela empresa e providencia uma segurança maior aos patrocinadores que o processo do escopo sofrerá a menor interrupção possível, e, caso necessite, permita a recuperação do processo o mais rápido possível.

O modelo de plano de continuidade de negócios foi elaborado para ser aplicado em indústrias em que a continuidade de negócios está em nível “inexistente” ou “inicial”, cuja continuidade de negócios não é tratada ou é pouco conhecida nas organizações. A partir do modelo, a organização aplicada tem condições de elaborar um plano de continuidade para garantir a operação do negócio respondendo a incidentes de forma segura, garantindo maior segurança contra os possíveis riscos através do mapeamento e tratamento destes riscos, e recuperando sua operação de negócios em situações de desastre, de forma organizada e segura a partir dos planos de recuperação de desastre.

A expectativa foi atingida de forma positiva, e, com base nos resultados obtidos através do estudo de caso da aplicação em uma empresa, e da avaliação do modelo utilizando o questionário de maturidade do ITIL, pode-se concluir que o modelo é completo e pode ser aplicado também em organizações de nível “repetitivo” e até mesmo “definido”.

O presente trabalho tem como propósito tornar-se uma referência para as indústrias de pequeno e médio porte na elaboração de seus planos de continuidade de negócios, que ainda é uma área que precisa ser amadurecida no Brasil. O modelo proposto é completo e permite que seja aplicado em diferentes cenários.

Como trabalhos futuros, diversas melhorias podem ser implementadas no modelo como o aperfeiçoamento do modelo para atender os critérios não atingidos no questionário de avaliação, e incrementando-o para atingir todos os níveis de maturidade do ITIL e COBIT.

As fases de medição e monitoramento, aprimorando os processos de simulação e de revisão do plano de continuidade, que apenas complementam o modelo atual, também podem ser trabalhadas para otimizar o gerenciamento da continuidade.

O sistema também pode ser aperfeiçoado através da disponibilização do mesmo em novas versões do Microsoft Sharepoint, utilizando novos recursos e melhorando o guia conforme este for sendo aplicado. O anexo C, de informações complementares poderia ser complementado como um manual de apoio na elaboração, abrangendo também a fase de elaboração do plano de continuidade, abrangendo exemplos reais de ações a serem aplicadas.

REFERÊNCIAS BIBLIOGRÁFICAS

APM Group Ltd, **ITIL v3**: Information Technology Infrastructure Library, Buckinghamshire, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, **ABNT ISO/IEC 17799:2005**, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, **ABNT ISO/IEC 27001:2005**, Tecnologia da informação – Técnicas de segurança – Sistemas de Gestão de Segurança de Informação, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, **ABNT ISO/IEC 27005:2005**, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, **ABNT ISO/IEC 27005:2008**, Tecnologia da informação – Técnicas de segurança –Gestão de Riscos de segurança da informação , 2008.

BRITISH STANDARDS INSTITUE. **BS 25999-1**: Code of Practice for Business Continuity Management. London, 2006.

CANTOR FITZGERALD, CANTOR FAMILIES MEMORIAL, 2001. Disponível em <http://www.cantorfamilies.com/cantor/jsp/index.jsp > Acesso em: 29 Jul 2012.

CARTLIDGE, ALISON; LILLYCROP, MARK. **The IT Infrastructure Library**: An Introductory Overview of ITIL - Version 3. Wokingham, United Kingdom: IT Service Management Forum, 2007.

CHIAVENATO, Idalberto. **Introdução Geral da Administração**. 8 ed. São Paulo: Campus, 2011.

CONVERGÊNCIA DIGITAL, EMPRESAS INVESTEM POUCO EM CONTINUIDADE DE NEGÓCIOS, 2011. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=26940&sid=5> Acesso em: 25 Ago 2012.

IT GOVERNANCE INSTITUTE, **CobIT 4.1**: Control Objectives for Information and Related Technology, Illinois, 2007.

ITSMF. **Itil Service Management Self Assetment**, 2012. Disponível em <http://www.itsmf.com/trans/sa.asp> Acesso em: 30 abr. 2013.

MAGALHÃES, I. L.; PINHEIRO W.B. **Gerenciamento de Serviços de TI na prática**: Uma abordagem com base no ITIL. PortoAlegre: Novatec, 2007.

MICROSOFT. **Introdução ao Sharepoint Foundation 2010**, 2010. Disponível em: <http://office.microsoft.com/pt-br/sharepoint-foundation-help/introducao-ao-sharepoint-foundation-2010-HA010370686.aspx?CTT=3> Acesso em: 29 mar. 2013.

MICROSOFT. **O que é o Sharepoint?**, 2010. Disponível em: <http://office.microsoft.com/pt-br/sharepoint-foundation-help/o-que-e-o-sharepoint-HA010378184.aspx> Acesso em: 29 mar. 2013.

NOW! DIGITAL, METADE DAS COMPANHIAS NO BRASIL NÃO TEM PLANO DE RECUPERAÇÃO DE DESASTRES, 2011. Disponível em: <http://cio.uol.com.br/noticias/2011/12/23/metade-das-companhias-no-brasil-nao-tem-plano-de-recuperacao-de-desastres/> Acesso em: 25 Ago 2012.

OBJECT MANAGEMENT GROUP, BUSINESS PROCESS MODEL AND NOTATION, 2012. Disponível em: < http://www.bpmn.org/ >. Acesso em: 19 Set 2012.

PMBOK, A. **Guide to the Project Management Body of Knowledge**, Third Edition, PMI, USA, 2004.

SOMMERVILLE, I. **Engenharia de Software**. 8 ed. Editora: Addison-Wesley,2007.

WALLACE, Michael; WEBBER, Lawrence. **The Disaster Recovery Handbook**: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets¸ 2 ed. AMACOM Div American Mgmt Assn, 2004.

ANEXO A – Guia para elaboração de um plano de continuidade de negócios

ANEXO A. GUIA PARA A CRIAÇÃO DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS						
Fase	**Etapa**	**Papéis**				**Atividades**
		R	**A**	**C**	**I**	
Definição do escopo	Definição da Organização	GC				Utilizar a lista Definições da Organização para registrar o levantamento realizado nesta etapa.
		GC		P , GP		Organizar uma reunião com os possíveis patrocinadores da implantação da continuidade para levantar pontos do escopo.
		GC		P , GP		Identificar qual a unidade organizacional a ser aplicada, seu propósito, sua missão, seu negócio e seus valores.
		GC		P , GP , TI		Identificar a posição da TI na organização.
		GC		P , GP		Identificar o organograma e a estrutura organizacional da organização.
		GC				Registrar o levantamento na lista Definições da Organização . Podem ser realizados múltiplos registros em caso de múltiplas unidades organizacionais.
	Definição do escopo e aplicabilidade	GC		P , GP , UC , TI		Através de reunião, definir com os patrocinadores e envolvidos quais os processos ou sistemas deverão ser abordados pelo plano de continuidade de negócios. O escopo define o plano de continuidade.
		GC				Registrar o escopo e as áreas funcionais envolvidas no processo no lista Escopo e Aplicabilidade . Cada registro é um plano de continuidade distinto e será referenciado pelas ações do Plano de Continuidade de negócios.
	Identificação das restrições da organização	GC		P , GP		Identificar se há restrições na organização que possam impactar na continuidade de negócio para cada uma das unidades organizacionais registradas nas etapas anteriores. Utilizar o documento de Restrições Organizacionais presente nas informações complementares para auxiliar nesta identificação.
		GC		P		Organizar uma reunião com os possíveis patrocinadores da implantação.
		GC				Registrar o levantamento na lista Restrições da Organização por unidade organizacional e seguir as instruções presentes para auxiliar no processo de identificação.
	Definição dos papéis e responsabilidades	GC		P , GP		Realizar reunião com os patrocinadores e gestores do processo para identificar a equipe.
		GC			P , GP , UC	Identificar a equipe que participará da elaboração do plano de continuidade de negócios, com sua área funcional e formas de contato.
		GC				Registrar os membros da equipe na lista Equipe , relacionando com suas devidas áreas funcionais e responsabilidades.
	Identificação das restrições que afetam o escopo da continuidade	GC				Identificar se há restrições na organização que possam impactar no escopo dos planos de continuidade de negócio.
		GC		GP , UC , TI		Organizar uma reunião com os possíveis participantes da implantação.
		GC				Utilizar o documento Restrições de Escopo, das informações complementares para auxiliar na identificação.
		GC				Registrar as restrições levantadas na lista Restrições de Escopo para cada plano de continuidade de negócios.
	Sumário executivo	G				Identificar o plano de continuidade e descrever em um parágrafo rápido alguns conceitos de continuidade de negócios.
		GC				Descrever brevemente o processo a ser abordado pela continuidade de negócios.
		GC				Citar exemplos de situações de risco que podem acarretar em possível prejuízo.
		GC				Descrever os objetivos da elaboração do plano de continuidade de negócios.
		GC				Registrar o sumário executivo na lista Sumário Executivo para cada plano de continuidade registrado.
		GC			P , GP , UC , TI	Apresentar o sumário executivo para os demais envolvidos no processo através de reunião de reporte de atividades ou por envio de link para o sumário através de correio eletrônico (ferramenta disponibilizada ao visualizar o sumário no sistema) Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
	Mapeamento do processo	GP	GC	UC , TI		Identificar e registrar o processo que está sendo tratado, a quais planos de continuidade ele pertence, e seu responsável na lista Processo .
		GP	GC			Utilizar alguma abordagem técnica para realizar o mapeamento do processo. Abordagem sugerida: BPMN
		GC			P , GP	Registrar o mapeamento do processo na lista Processo .
		GC				Utilizar a lista Ativos para registrar a identificação dos ativos. Utilizar o documento Tipos de Ativo, incluso nas informações complementares para auxiliar na identificação.
		GC		UC , TI		Analisar o mapeamento do processo realizado na atividade anterior.
		GC		UC , TI		Reunir-se com os usuários-chave e TI para a identificação dos ativos primários no processo
		GC	UC	TI		Definir quais as atividades do processo e as informações geradas e identificá-las como ativos primários.
		GC	TI	UC		Realizar entrevista com os usuarios chave e equipe de TI para identificação dos ativos de suporte.

Gestão de riscos	Identificação dos ativos	GC	TI	UC		Identificar qual o hardware envolvido no processo de negócio e sua relação com os ativos primários.
		GC	TI	UC		Identificar quais os softwares envolvidos no processo de negócio e sua relação com os ativos primários.
		GC	TI	UC		Identificar as aplicações de negócio envolvidas no processo e sua relação com os ativos primários.
		GC	TI	UC		Identificar a estrutura de rede envolvida no processo e sua relação com os ativos primários.
		GC	TI	UC		Identificar os recursos humanos envolvidos no processo e sua relação com os ativos primários.
		GC	TI	UC		Identificar as instalações fisicas e localidades envolvidas no processo e sua relação com os ativos primários.
		GC	TI	UC		Identificar outros ativos que pertencem ou possuem relação de dependência com o ativo. Esta relação simplificará a análise de riscos.
		GC		P , GP , UC , TI		Definir um responsável para cada ativo.. Definir a criticidade dos ativos em baixa, média ou alta em conjunto com os demais envolvidos.
		GC				Registrar os ativos primários e de suporte na lista Ativos . O campo SLA deve ser deixado em branco para preenchimento posterior.
	Identificação das ameaças	GC				Utilizar a lista Riscos para registrar o processo completo de análise de riscos. Utilizar o documento Ameaças, incluso nas informações complementares para auxiliar na identificação.
		GC		UC , TI		Analisar o mapeamento do processo realizado na atividade anterior.
		GC		GP , UC , TI		Analisar os ativos primários em conjunto com os usuarios chave, TI e gestores de processo.
		GC	TI	UC		Realizar a identificação das ameaças individualmente por ativo de suporte.
		GC		UC , TI		Realizar entrevista com os usuarios chave e equipe de TI para identificação das ameaças.
		GC	TI	UC		Realizar inspeção física nos ativos envolvidos no processo.
		GC	TI	UC		Identificar as ameaças referentes à dano físico dos ativos envolvidos.
		GC	TI	UC		Identificar as possíveis ameaças resultantes de eventos naturais e meteorologicos .
		GC	TI	UC		Identificar possiveis ameaças aos serviços de infra estrutura básica como fornecimento de energia.
		GC	TI	UC		Identificar possíveis danos provenientes de radiação.
		GC	TI	UC		Identificar possíveis comprometimentos à informação como violações de segurança, alterações indevidas e furto de informação e hardware.
		GC	TI	UC		Identificar as possíveis falhas técnicas dos ativos de suporte, principalmente dos sistemas de informaçao e hardware envolvido.
		GC	TI	UC		Identificar possíveis ações não autorizadas como uso ilegal de software e acesso indevido ao código fonte das aplicações de negócio.
		GC	TI	UC		Identificar possíveis falhas no uso dos sistemas de informação, hardware e software que possa comprometer os ativos primários.
		GC	TI	UC		Identificar possíveis falhas de segurança e humanas que poderão resultar em comprometimento do processo como invasões, hackers ou furto de informação confidencial.
		GC	TI	UC		Definir a origem das ameças em acidental, intencional ou natural
		GC			P , GP	Registrar as ameaças na lista de Riscos conforme relacionamento com os ativos. Utilizar sempre o maior ativo da estrutura hierárquica quando a ameaça afetar diversos ativos semelhantes, desde que esta seja aplicável a todos.
	Identificação das vulnerabilidades	GC	TI			Analisar os ativos e suas ameaças relacionadas e realizar um primeiro esboço das vulnerabilidades possíveis.
		GC	TI	UC		Percorrer todo o processo de negócio para identificar possíveis vulnerabilidades. Utilizar o documento Vulnerabilidades presente nas informações complementarespara auxiliar na identificação.
		GC		UC , TI		Realizar entevistas com os usuários-chave e TI para a identificação de vulnerabilidades.
		GC				Utilizar o item 5, Vulnerabilidades, incluso nas informações complementares para auxiliar na identificação.
		GC	TI	UC		Identificar vulnerabilidades baseando-se nas ameaças identificadas de hardware, software e aplicações de negócio.
		GC	TI	UC		Identificar vulnerabilidades baseando-se nas ameaças identificadas de rede e instalações físicas.
		GC	TI	GP		Identificar vulnerabilidades na equipe e recursos humanos envolvidos.
		GC	TI	GP		Identificar vulnerabilidades na estrutura organizacional baseando-se nas possíveis ameaças de segurança.
		GC	TI			Utilizar ferramentas de teste de segurança e de invasão.
		GC	TI			Revisar a política de autenticação dos sistemas e softwares envolvidos.
		GC				Registrar as vulnerabilidades identificadas na lista Riscos para cada ameaça previamente cadastrada, relacionando com os ativos identificados.
		GC	TI			Analisar a lista de ativos, ameaças e vulnerabilidade e realizar o primeiro esboço das consequencias possíveis.

	Identificação das consequências	GC		GP , UC , TI		Realizar entevistas com os usuários-chave e TI para a identificação das consequências
		GC				Utilizar o documento Consequencias, incluso nas informações complementares para auxiliar na identificação.
		GC		GP , UC , TI		Identificar consequencias como prejuízo financeiro, perda de oportunidade de negócios, interrupção de operação de negócio, risco à saude humana, perda de competitividade, danos à imagem da organização e perda de dados ou informações.
		GC	GP	P		Classificiar o impacto consequência em baixo, médio ou alto conforme definição da organização baseando-se nas restrições de escopo.
		GC				Registrar as consequencias dos riscos na lista Riscos para cada ameaça previamente identificada.
	Identificação das probabilidades	GC				Analisar a lista de riscos para definição das probabilidades.
		GC	TI	GP , UC		Realizar entrevistas com os usuários-chave e TI para identificação das probabilidades baseadas na projeção dos usuários.
		GC		TI	GP , UC	Identificar a fragilidade das vulnerabilidades com base no histórico de ocorrência na organização ou organizações terceiras.
		GC	GP			Classificar a probabilidade do risco em baixa (improvável), média(possível), alta(presente ou provável) conforme análise realizada com os envolvidos no processo
		GC		GP		Registrar a probabilidade classificada dos riscos na lista Riscos para cada ameaça previamente identificada.
	Avaliação dos riscos	GC				Analisar a lista de riscos e probabilidades para avaliar os riscos.
		GC		GP		Pontuar o impacto no negócio e dos riscos em 1, 2 e 3 para baixa , média, e alta respectivamente.
		GC				Pontuar a probabilidade dos riscos em 1, 2 e 3 para baixa, média e alta respectivamente.
		GC				Utilizar a tabela de Avaliação presente nas informações complementares para auxiliar no cálculo da estimativa de risco.
		GC				Realizar a soma das criticidades para determinar a avaliação do risco em baixo risco (2 e 3), médio risco (4 e 5) ou alto risco (6).
		GC				Realizar a revisão dos níveis de risco com o gestor de processo.
		GC				Registrar a nível do risco em baixo, médio ou alto conforme resultado da avaliação na lista Riscos para cada ameaça previamente identificada.
	Revisão da Análise de Riscos	GC		GP , UC , TI		Revisar o registro dos ativos e dos riscos envolvidos na análise de riscos e retornar para as etapas de análise caso algo não estar claro.
		GC			P , GP , UC	Apresentar o escopo da continuidade e análise de risco para os patrocinadores e gestores de processo. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
		GC			P , GP	É importante registrar em ata a apresentação e pontos importantes discutidos na apresentação.
	Definição do SLA	GC				Utilizar a lista Ativos para registrar o resultado desta atividade.
		GC		GP , TI		Identificar os ativos e serviços que deverão ser abordados no plano de continuidade e sua criticidade com base na análise de riscos. Esta definição fica a critério da organização.
		GC				Através de reunião, definir com os usuários chave e gestores de processo qual o tempo mínimo de interrupção aceitável para cada ativo.
		GC	TI			Através de entrevista com a equipe de TI, definir qual seria o tempo possível de atender e solucionar a interrupção nas condições atuais.
		GC	GP			Em conjunto com os gestores de processo, definir um tempo aceitável de atendimento.
		GC				Registrar na lista Ativos os acordos de nível de serviço definidos nos seus respectivos ativos que serão abordados pelo plano de continuidade.
	Elaboração das ações de tratamento do risco	GC				Utilizar a lista Ações de tratamento para orientar esta atividade.
		GC				Identificar o risco, por ameaça, que será tratado para elaborar as ações. Vincular esta ameaça em um ou mais planos de continuidade.
		GC	TI	GP , UC		Para cada risco, elaborar um plano de ação para evitar o risco, reduzir o risco, transferir o risco, aceitar o risco.
		GC				Identificar ações necessárias para restaurar as cópias de segurança dos ativos envolvidos no processo. (Será aprofundada nas etapas subsequentes)
		GC	TI			Identificar qual é o tipo do tratamento do risco: evitar risco, reduzir risco, transferir risco ou reter o risco.
		GC		UC , TI		Identificar se as ações são possíveis de aplicação na situação atual ou necessitam de investimento
		GC		UC , TI		Identificar o valor do investimento para execução das ações que deverão ser tomadas.
		GC		GP		Identificar o responsável por elaborar e operar o plano para cada ação.
		GC		TI		Identificar o prazo de implantação do controle sugerido no plano de ação baseando-se na urgência e no prazo possível de ativação.
		GC				Registrar as ações identificadas nesta etapa na lista Ações de tratamento.
		GC			P , GP	Apresentar os planos de ação para os gestores de processo e patrocinadores.

	Aceitação das ações de tratamento	GC	P , GP		UC , TI	Coletar a aprovação, rejeição ou prorrogação do plano de ação com os patrocinadores e gestores de processo. Registrar o motivo da rejeição e um novo prazo de implantação em caso de prorrogação. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
		GC				Registrar os planos de ação, seu custo, responsável e a posição de aprovação na lista Ações de tratamento .
		GC			UC , TI	Comunicar os envolvidos no processo do resultado da aprovação dos controles propostos para elaboração dos planos de continuidade de negócios.
	Definição das cópias de segurança	GC				Utilizar a lista Métodos de cópias de segurança para orientar e registrar a primeira parte desta atividade
		GC	TI			Identificar os métodos de realização de cópias de segurança presentes no ambiente ou que serão adquiridos como unidades de fita, discos removíveis, servidores de backup, backup na nuvem, entre outros.
		GC	TI			Identificar em quais planos de continuidade este método é utilizado. Identificar os ativos envolvidos como hardware e software, o responsável, qual a ação de validação do backup de cada método identificado.
		GC	TI			Identificar se o conteudo do backup é formado por dados (arquivos e informações de um servidor ou sistema), por imagem de sistema (ghost ou cópia total de um servidor) ou ambos.
		GC	TI			Identificar qual é a prioridade de restauração daquele método em caso de necessidade.
		GC	TI			Identificar os serviços de terceiros relacionado a cada método de backup. (garantias, contratos de suporte)
		GC				Registrar os métodos de backup na lista Métodos de Cópia de Segurança .
		GC				Utilizar a lista Cópias de Segurança para orientar e registrar a segunda parte desta atividade.
		GC	TI			Identificar os ativos envolvidos no processo e se há cópia de segurança destes ativos.
		GC	TI			Caso positivo, identificar qual o método de backup, qual a periodicidade que o backup é realizado, qual o período de armazenamento das mídias(ciclo de backup) e quem é o responsável pelo backup.
		GC	TI			Caso negativo e se a organização desejar, deverá ser gerada uma ação de tratamento de risco para realizar cópias de segurança deste ativo.
		GC	TI			Identificar as ações realizadas para garantir a integridade dos backups realizados, quem é o responsável pela validação e qual a periodicidade que esta validação deve ser realizada conforme criticidade do ativo.
		GC	TI			Identificar se as mídias externas, caso utilizadas, possuem armazenamento remoto à organização. (ao menos uma unidade)
		GC	TI			Identificar qual a periodicidade do armazenamento externo das mídias, caso exista
		GC	TI	P , GP		Identificar o responsável pelo armazenamento externo das mídias.
		GC				Registrar os ativos levantados e seu procedimento de cópias de segurança na lista Cópias de Segurança .
		GC	TI		P , GP , TI	Apresentar para os patrocinadores e gestores de processo quais são os procedimentos de cópias de segurança que estarão sendo utilizados para garantir a continuidade. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
	Elaboração do plano de resposta a incidentes	GC				Utilizar a lista Plano de Resposta a Incidentes para orientar e registrar esta atividade.
		GC		GP , UC , TI		Relacionar os ativos, seus SLA definidos e as possíveis ameaças resultantes da análise de risco e das ações de tratamento que desejam ser elaborados os planos de resposta.
		GC	TI			Planejar as ações que deverão ser tomadas a partir da ocorrência de uma ameaça. Estas ações podem ser procedimentos manuais, quando necessitam da intervenção humana, ou automáticas, quando o sistema consegue se adaptar sozinho à situações de emergência.
		GC	TI			Identificar se as ações definidas são de recuperação, contingência (reabilitar o serviço em um ambiente paralelo) ou retorno em produção (retorno em produção após uso em contingência).
		GC	TI			Identificar as ações de retorno de produção para cada ação de contingência, o SLA deve ser reestabelecido pela equipe Responsável pela ação.
		GC		GP , UC , TI		Identificar os responsáveis por cada ação.
		GC		GP , UC , TI		Identificar quem deve ser comunicado em caso de ocorrência, quem deve ser comunidado após a realização das ações e quem pode ser acionado para prover suporte à realização das ações.
		GC				Registrar todos os contatos que podem ser acionados em caso de ameaças na lista Contatos do menu Listas.

		GC				Os SLA podem ser revisados conforme a elaboração do plano e consequentemente alterados. Caso ocorra alteração em um SLA, alterar na lista Ativos. Os SLA dos planos de resposta a incidente podem ser atribuídos por ação, levando em conta os SLA originais dos ativos, mas de forma independente baseando-se na capacidade de entrega do serviço pela equipe. Um risco pode possuir diferentes ações com diferentes SLAs.
		GC				Registrar as informações identificadas nesta atividade na lista Plano de Resposta a Incidentes . Cada ação deve estar relacionada a um ou mais plano de continuidade.
	Implementação da documentação e controles (OLAs)	GC				Utilizar a lista OLAs para orientar e executar esta tarefa
		GC	TI			Para cada ameaça com ação definida no plano de resposta a incidentes, criar um novo OLA para detalhar o processo que deve ser realizado para realizar o procedimento.
		GC	TI			Identifique o tipo de OLA entre plano de resposta, recuperação de desastres ou testes (estes três ultimos serão detalhados no futuro) para facilitar na classificação dos OLAs.
		GC	TI	GP , UC		Identificar o passo-a-passo que deve ser realizado para operar o plano de resposta a indidentes . Este passo-a-passo deverá ser seguido em caso de ativação dos planos de resposta a incidentes e recuperação de desastres.
		GC	TI	GP , UC		Detalhar o processo da melhor maneira possível para que o responsável possa executá-lo facilmente, ou, na ausencia deste, ser realizado por outro operador capacitado.
		GC	TI	GP , UC		Caso necessário, monte um manual do processo utilizando-se de print screens e outros recursos de imagem ou video. Anexe os arquivos resultantes no campo Instruções Operacionais do OLA.
		GC		GP , UC , TI		Para cada ação do OLA pode-se definir um responsável, caso este se altere, ou terceiros que podem ser acionados em caso de emergência.
		GC				Registre os OLAs definidos na lista OLAs e anexe os artefatos ou documentos(manuais) gerados em ferramentas externas no modelo. Os OLAs devem ser associados nos planos de resposta a indicentes, ações para recuperação de desastre ou plano de testes .
	Revisão do plano de resposta a incidentes	GC		GP , UC , TI		Revisar o registro de todas as ações envolvidas no plano de resposta a incidentes referente a sua conformidade, responsáveis definidos e coerencia entre as ameaças e ações.
		GC		GP , UC , TI		Revisar os registros dos OLAs e validá-los operacionalmente, coletando a aprovação de quem realizou a validação.
		GC			P , GP	Apresentar os planos de resposta a incidentes aos gestores, patrocinadores e demais usuários envolvidos, garantindo de que todos possam se sentir seguros quanto aos incidentes. Esta apresentação pode ser realizada através de reunião ou por envio dos planos através de correio eletrônico.
		GC			P , GP	É importante registrar em ata a apresentação e pontos importantes discutidos na apresentação. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
Elaboração do plano de continuidade		GC				Utilizar a lista Ativação do plano de Recuperação de desastres, para orientar e registrar a primeira parte desta tarefa.
		GC		P , GP , TI		Nomear o plano de recuperação de desastres que será elaborado e identificar o desastre que pode acioná-lo. Identificar a qual plano de continuidade este plano de recuperação pertence.
		GC		P , GP , TI		Determinar quem será o responsável por ativar o plano e por coordenar as ações de continuidade. Podem ser pessoas diferentes.
		GC		P , GP , TI		Determinar quem será o responsável por aprovar as ações de continuidade.
		GC		P , GP		Determinar quem será o responsável pela autorização de investimentos necessários para a operação do plano.
		GC		P , GP		Determinar quem será o responsável pelas aquisições necessárias. (geralmente algum usuário do setor de compras)
		GC		P , GP , TI		Definir quem deve ser informado quanto à ativação do plano de recuperação de desastres.
		GC		P , GP , TI		Definir um prazo desejado possível para o retorno das atividades. Este prazo será recalculado após a elaboração do plano.
		GC		P , GP , TI		Definir o local que será utilizado para a execução do plano de recuperação de desastres. É importante que o local definido possui o menor número de vulnerabilidades possíveis
		GC				Registrar todas as definições na lista Ativação do plano de recuperação de desastres.
		GC				Utilizar a lista Ativos de TI para a recuperação de desastres para orientar e registrar a segunda parte desta atividade.

	Definição do plano de recuperação de desastres	GC		GP , UC		Relacionar os ativos primários e secundários necessários para manter a operação de negócio funcional, identificando um responsável técnico por administrá-los na ativação do plano de recuperação. Estes ativos não necessariamente necessitam ser os mesmos identificados na gestão de riscos.
		GC	TI			Para cada ativo relacionado deve-se identificar a quantidade necessária, a descrição técnica do mesmo, se este ativo possui redundância ou precisará ser adquirido em caso de desastre, o custo da recuperação deste ativo e qual a sua prioridade de recuperação em escala qualitativa (alta, média ou baixa).
		GC	TI			Relacionar os servidores envolvidos, detalhando sua configuração de hardware, sistema operacional e outras particularidades essenciais para a aquisiçao de um novo servidor caso necessário.
		GC		GP , UC		Identificar os ativos de comunicação necessários para manter a operação de negócio funcional, identificando um responsável técnico por administrá-los na ativação do plano de recuperação.
		GC	TI	GP , UC		Identificar os ativos de infraestrutura necessários para manter a operação de negócio funcional, identificando um responsável técnico por administrá-los na ativação do plano de recuperação.
		GC	TI	GP , UC		Identificar os ativos de software e sistemas de informação necessários para manter a operação de negócio funcional, identificando um responsável técnico por administrá-los na ativação do plano de recuperação.
		GC	TI	GP		Registrar todos os ativos relacionados na lista Ativos de TI para a recuperação de desastres. Identificar seu responsável e em quais planos de recuperação de desastres estes ativos serão necessários.
		GC				Utilizar a lista Ativos de recursos humanos para a continuidade de negócios para orientar e registrar esta atividade.
		GC		GP , UC , TI		Identificar os recursos humanos necessários para operacionalizar o ambiente tecnológico por cargo e função. Relacionar estes recursos aos planos de recuperação aos quais se fazem necessário.
		GC	TI	GP , UC		Para cada recurso humano identificado deve-se identificar o cargo necessário, a quantidade de pessoas para exercer o cargo, as funções deste cargo, identificar se a organização já possui esta pessoa, se ela é funcionária da orgnaização ou terceira e a criticidade desta pessoa no processo, definido em baixo, média e alta, através do número de tarefas que esta pessoa irá executar.
		GC				Registrar os ativos de RH relacionados na lista Ativos de recursos humanos para a continuidade de negócios . Relacionar um responsável por estes recursos.
		GC	TI	GP		Utilizar a lista Serviços de terceiros para a recuperação de desastres para dar continuidade a esta atividade.
		GC	TI	GP , UC		Identificar os serviços de terceiros necessários para operacionalizar o ambiente tecnológico como fornecimento de energia externo, fornecimento de serviços de infraestrutura predial, fornecimento de suporte à servidores, fornecimento de suporte a sistemas, entre outros. Identificar os planos de recuperação nos quais estes serviços são necessários.
		GC	TI	GP , UC		Para cada serviço identificar o terceiro envolvido, a descrição dos serviços prestados, o contato de quem deve ser acionado, o custo aproximado do serviço que será prestado e a necessidade de acionamento do terceiro em baixa, média e alta
		GC				Registrar todos os serviços de terceiros identificados na lista Serviços de terceiros para a recuperação de desastres . Definir um responsável na organização para acionar este serviço.
		GC				Registrar todos os contatos que podem ser acionados em caso de ameaças na lista Contatos presente no menu de Listas.
		GC				Revisar toda a estrutura identificada nesta atividade para garantir que nenhum ativo tenha ficado de fora do levantamento.
		GC			P , GP	Apresentar a estrutura necessária para operacionalizar o plano de recuperação de desastres para os patrocinadores e gestores de processo. Esta apresentação pode ser realizada através de reunião ou de envio eletrônico dos artefatos do plano de continuidade.
		GC				Utilizar a lista Plano de recuperação de desastres para orientar e registrar esta atividade.
		GC		GP , UC , TI		Elaborar com os gestores de processo, TI e usuários chave o cronograma de ações necessárias para reestabelecer a operação de negócio em caso de desastre.
		GC	TI	GP , UC		Planejar as ações que devem ser executadas para reestabelecer o ambiente tecnológico a partir das prioridades definidas na atividade anterior. As ações devem restaurar os ativos em ordem de prioridade, da alta para a baixa. Os ativos de alta prioridade são os ativos emergenciais que devem ser restaurado para iniciar as operações o mais rapido possível, a média indica ativos que são necessários para um bom desempenho e a prioridade baixa é referente aos ativos necessários para o reestabelecimento total do ambiente em produção.

	Elaboração do plano de recuperação de desastres	GC	TI	GP		Para cada ação planejada, registrá-la e recalcular o seu SLA para definir o tempo necessário para sua execução. Identificar quais os planos de recuperação que aquela ação pertence. É sugerido descrever a ação da maneira mais detalhada possível para facilitar seu uso em caso de ativação.
		GC	TI			Identificar se a ação é uma reinstalação, comum para hardware, softwares ou serviços de infraestrutura, ou uma recuperação, comum para ações de restauração de cópias de segurança.
		GC	TI	GP		Identificar o responsável pela execução da ação. Este responsável pode ser qualquer pessoa que esteja apta para realizar as tarefas, seja ela funcionária ou terceirizada conforme definido na atividade anterior.
		GC	TI			Identificar se a ação é dependente de outra ação para ser executada. Ações independentes poderão ser executadas em paralelo.
		GC	TI			Identificar quais ativos serão recuperados, caso sejam, após o término da ação.
		GC		GP , UC , TI		Identificar quem deve ser comunicado em caso de ocorrência, quem deve ser comunidado após a realização das ações e quem pode ser acionado para prover suporte à realização das ações.
		GC				Registrar as informações identificadas nesta atividade na lista Plano de Recuperação de desastres .
		GC	TI			Após o registro das atividades, o tempo de recuperação deve ser recalculado a partir da combinação dos SLAs determinados no plano de recuperação de desastres. Este novo SLA deve ser registrado na lista Ativação do plano de Recuperação de Desastres .
		GC	TI	GP , UC		Para cada ação registrada nesta atividade podee-se registrar um OLA, vinculando-o à ação. Os OLAs podem ser cadastrados na lista OLAs, do menu de listas. As mesmas regras válidas no registro dos OLAs na atividade realizada anteriormente devem ser aplicadas para as ações de recuperação de desastres.
	Revisão do plano de recuperação de desastres	GC		GP , UC , TI		Revisar toda a estrutura identificada nesta atividade para garantir que nenhum ativo tenha ficado de fora do levantamento.
		GC		GP , UC , TI		Revisar todas as ações necessárias para executar o plano de recuperação de desastres para garantir que nenhuma atividade tenha ficado de fora do cronograma de ações.
		GC			P , GP	Apresentar a estrutura necessária e as ações que devem ser realizadas para executar plano de recuperação de desastres para os patrocinadores e gestores de processo. Esta apresentação pode ser realizada através de reunião ou de envio eletrônico dos artefatos do plano de continuidade. É importante registrar em ata a apresentação e pontos importantes discutidos na apresentação. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
		GC	TI	GP		Após apresentação, a Ata referente à apresentação do plano de recuperação deve ser assinada pelo responsável pela continuidade, pelos patrocinadores e gestores do processo validando sua elaboração.
	Revisão e aprovação do Plano de continuidade	GC				Utilizara lista Aprovação do plano de continuidade de negócios para orientar e registrar esta atividade.
		GC			P , GP	Entregar uma cópia (ou forma de acesso digital) de todos os artefatos do plano de continuidade de negócios para os patrocinadores e gestores de processo realizarem a leitura e avaliação do plano de continuidade gerado.
		GC			P , GP	Orientar os gestores e patrocinadores a avaliarem a consistencia das informações e a possível eficiência da recuperação de desastre em situações reais. Quanto mais detalhista essa avaliação, melhor será o resultado. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
		GC	P , GP			Os gestores devem registrar a avaliação do plano como aprovado, reprovado ou revisar. É necessário sugerido registrar um parecer subjetivo da aprovação do aprovador.
		GC	P , GP			Em caso de reprovação, os avaliadores devem registrar o que não está de acordo e causou a reprovação.
		GC				Em caso de necessidade de revisão, os avaliadores devem apontar o que precisa ser revisado.
		GC				Conforme necessidade de revisão, devem ser revisados os pontos levantados pelos avaliadores para então gerar uma ação de manutenção. Após a manutenção realizada, o processo de avaliação deve ser retomado.
		GC				Recolher os resultados da avaliação de todos os avaliadores e registrar na lista Aprovação do plano de continuidade de negócios, identificando qual o plano de continuidade que está sendo aprovado.
		GC				Caso necessário, registrar observações pertinentes à aprovação.
		GC			P , GP , TI	Quando todos os avaliadores aprovarem o plano, pode-se efetivamente considerá-lo aplicado em produção, podendo ser utilizado conforme as ocorrências demandarem.

	Divulgação, distribuição e armazenamento do plano de continuidade	GC			P , GP , UC , TI	Disseminar o plano de continuidade gerado entre todos os envolvidos nas atividades. O importante é que todos os ativos, riscos e planos sejam de conhecimento de todos.
		GC				Utilizar canais de armazenamento e publicação gerenciáveis como sistemas colaborativos, gestão eletronica de documentos ou servidores de arquivos, para o armazenamento seguro do plano.
		GC			P , GP , UC , TI	Certificar de que todos os envolvidos no plano de continuidade em geral estejam cientes de suas responsabilidades. Esta certificação pode ser obtida através de reunião registrada em ata ou aprovações eletrônicas.
		GC				Incluir o plano de continuidade nos ativos que devem ser tratados na análise de risco.
		GC				Incluir o plano de continuidade nas rotinas de cópias de segurança inclusas no mesmo.
		GC				Armazenar uma cópia impressa e digital do plano em local a prova de fogo, e, caso possível, em local remoto para garantir de que o plano estará disponível quando for necessário.
	Registro de ocorrências	GC				Utilizar a lista Registro de Ocorrências para orientar e registrar a primeira para desta atividade.
		GC	TI			Registrar na lista Registro de Ocorrências cada ameaça que ocorrer registrando a data de ocorrência.
		GC	TI			Para cada ocorrência registrar quais as ações realizadas e quem foram os responsáveis por executá-las. Caso a ação realizada não estiver descrita em um plano, descreva a mesma no campo Ações não previstas.
		GC	TI			Para cada ocorrência, identificar se houve parada ou não do ativo ou serviço de TI.
		GC	TI			Para cada ação, registrar se o plano de tratamento de risco foi eficiente na solução ou não.
		GC	TI			Para cada ação registrar o tempo de atendimento realizado.
		GC	TI			Para cada ação, registrar se houve algum custo de manutenção ou aquisição envolvido. Registrar quem foi o responsável por executar a ação.
		GC	TI			Para o registro da ativação do plano de recuperação de desastres, registrar na lista Registro de Desastres a data de ocorrência e a data de recuperação da operação de negócio.
		GC	TI			Descrever com detalhes o desastre, o que ocorreu e outras observações que forem necessárias para auxiliar nos relatórios futuros.
		GC	TI			Registrar o responsável pela execução do plano de recuperação.
		GC	TI			Registrar qual plano de recuperação utilizado e se foi eficiente na solução ou se houveram ações não contempladas em sua execução.
		GC	TI			Registrar o SLA acordado e qual o tempo efetivo da recuperação dos desastres.
		GC	TI			Registrar o custo total de aquisições e manutenção envolvidos na recuperação.
		GC				Enviar os resultados registrados para os patrocinadores e gestores conforme for conveniente para a organização.
	Medição e monitoramento do plano de continuidade	GC				Utilizar a lista Indicadores de Desempenho da Continuidade para orientar e registrar os indicadores.
		GC				Todas as metas dos indicadores deverão ser registrados nas colunas Meta MÊS da lista de Indicadores para cada mês.
		GC		GP , TI		Determinar uma quantidade mínima aceitável estimada de horas perdidas por usuários devido à inoperância não planejada dos sistemas.
		GC		GP , TI		Determinar uma porcentagem de incidentes atendidos pelos planos de resposta a incidentes.
		GC		GP , TI		Determinar uma porcentagem de incidentes atendidos e solucionados dentro do prazo do SLA.
		GC		TI		Definir uma quantidade possível de ativos cobertos pelo plano de continuidade de negócios.
		GC		TI		Definir um percentual de testes realizados com sucesso, sem necessidade de correção.
		GC		GP , TI		Definir uma meta mínima de interrupção de serviços nos sistemas críticos.
		GC		TI		Criar indicador com número máximo de desastres ocorridos. Por padrão a meta deste indicador deve ser 0 pois não devem ocorrer desastres.
		GC		TI		Criar indicador de sucesso na recuperação de desastres através do plano de recuperação caso ocorra um desastre, este indicador deve ser acionado somente se houverem desastres.
		GC		GP , TI		Criar outros indicadores que possam ser úteis para medir a eficiência do plano de continuidade. Estes indicadores propostos são sugestões, sendo de liberdade da organização adotá-los ou não.
		GC				Os indicadores devem ser definidos conforme período que a organização deseja medir, no padrão do modelo é sugerido mês a mês, mas cada indicador pode ter uma periodicidade independente.
		GC				Registrar os indicadores na lista Indicadores de Desempenho da Continuidade , dos artefatos do plano de continuidade.

Execução, monitoramento e controle		GC				A cada período de avaliação, devem-se registrar o resultado dos indicadores na lista Indicadores de desempenho da continuidade .
		GC			P , GP , UC , TI	Comunicar os envolvidos o resultado dos indicadores após cada período de avaliação.
	Simulações e testes	GC				Utilizar a lista Plano de Testes para orientar e registrar esta atividade.
		GC		GP , TI		Definir possíveis tipos de testes a serem realizados como Simulação, Teste de desempenho, simulação de falha, Teste em protótipo, teste em produção. Este tipo serve para organizar os planos de testee a serem realizados.
		GC		TI		Descrever qual a ação de teste que deverá ser realizada. O detalhamento desta ação deverá ser registrada na aba de OLAs.
		GC		TI		Descrever quais planos de resposta a incidentes que serão testados neste teste. Caso não haja um plano de resposta, descrever na ação.
		GC		GP , TI		Registrar qual o objetivo do teste realizado como verificar problemas, testar novas vulnerabilidades, garantir a segurança, entre outros objetivos que podem ser definidos pela organização.
		GC			TI	Definir a complexidade do teste em baixa, média ou alta. Baixa complexidade refere-se a testes que podem ser realizados rapidamente sem envolvimento de mais de uma pessoa, média são testes que requerem mais de uma pessoa para executar e podem demorar um tempo moderado, alto são testes que envolvem muitas pessoas, geralmente quase ou todos os envolvidos, e levam diversos dias para sua realização
		GC		GP , TI		Definir qual a frequência de realização dos testes conforme período aceitável pela organização.
		GC				Definir um responsável por realizar, acompanhar ou coordenar os testes. Este será responsável por informar os resultados dos testes.
		GC				Registrar o levantamento na lista Plano de testes.
	Registro de testes e simulações	GC				Realizar os testes conforme programação estabelecida. Para cada teste realizado, deve ser registrado todo seu procedimento na lista Registro de testes e simulações , a fim de se ter acompanhamento e garantia do funcionamento dos planos.
		GC	UC , TI			Registrar as datas de início e término do teste realizado. Identificar qual o tipo do teste.
		GC	UC , TI			Registrar qual foi o teste realizado e o resultado dos testes, podendo ser positivo ou negativo. Em caso negativo, registrar as inconsistências.
		GC	UC			Registrar quem foi o responsável pelo teste e se o plano de teste criado atingiu o objetivo proposto.
		GC	UC			Registrar se pelo teste foi possível testar os tempos acordados no SLA (caso as condições de teste forem mais parecidas possíveis com as reais), o SLA acordado dos planos testados e o tempo efetivo do teste.
		GC	UC			Registrar as necessidades de alteração, revisão ou correção dos planos de ação testados.
		GC	UC			Para os planos de recuperação de desastres deve-se continuar utilizando a lista Registro de testes e simulações. Registrar sua data de início e do término.
		GC	UC , TI			Registrar quais foram os resultados dos testes de recuperação de desastres da maneira mais detalhada possível.
		GC	UC , TI			Registrar quem foi o responsável pelo teste e se o plano de teste criado atingiu o objetivo proposto.
		GC	UC , TI			Registrar se pelo teste foi possível testar os tempos acordados no SLA (caso as condições de teste forem mais parecidas possíveis com as reais), o SLA acordado dos planos testados e o tempo efetivo do teste.
		GC	UC , TI			Registrar as necessidades de alteração, revisão ou correção do plano de recuperação de desastre. Caso haja necessidade, encaminhar para o responsável pelo plano gerar uma necessidade de revisão do plano testado.
		GC			P , GP	Comunicar o resultados dos testes para os patrocinadores e gestores de processo quando for conveniente para a organização. Deve ser estabelecida uma periodicidade de comunicação dos resultados.
	Revisão, atualização e melhoria contínua do plano	GC				Utilizar a lista Revisão e Manutenção para orientar e registrar esta atividade.
		GC	GP , TI			Definir qual o escopo da revisão e a qual plano este escopo pertence. Definir qual é o objetivo da revisão de cada uma das etapas do plano de continuidade, ou escopo definido. Estes objetivos devem ser definidos pela organização. Exemplos: identificar mudanças no ambiente, garantir a conformidade, encontrar error, propor melhorias, entre outros.
		GC	GP , TI			Caso haja alguma etapa diferente do plano proposto elaborada pela organização, ou a mesma deseja dividir as etapas do plano em sub etapas, devem ser registradas e tratadas da mesma forma que as demais.
		GC		GP , TI		Para cada etapa do plano, identificar qual será a periodicidade de revisão. As revisões poderão ser realizadas fora do periodo previsto caso haja uma necessidade oriunda de testes realizados.
		GC		GP , TI		Identificar quem é o responsável por executar a revisão e quem é o responsável por aprovar a revisão.
		GC				Registrar as definições na tabela Revisão e manutenção .

		GC	TI			As revisões seguem as etapas descritas neste guia. Porém, o processo de revisão pode ser determinado pela organização da maneira que melhor é aplicável.
		GC			P , GP	Divulgar o plano de manutenção para os patrocinadores e gestores de processo. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.
	Registro das revisões	GC				Utilizar a lista Registro de Revisões para orientar e registrar o processo de revisões .
		GC	UC , TI			Quando uma revisão é realizada, o seu resultado e alterações devem ser registrados na lista Registro de Revisões. Deve-se identificar o plano que foi revisado.
		GC				Antes de registrar as alterações em algum outro artefato do plano de continuidade, garantir uma cópia da versão atual em ambiente seguro.
		GC	UC , TI			Para cada revisão realizada registrar a data da revisão (término) e o responsável que realizou a revisão.
		GC	UC , TI			Registrar se o motivo da revisão foi por revisão periódica, por demanda oriunda de testes ou manutenção reativa.
		GC	UC , TI			Registrar qual foi a revisão programada realizada e descrever um breve resumoi. Caso a revisão realizada não estiver no cadastro prévio, deve-se resumir a ação realizada no campo Revisão realizada apenas. Descrever quais as alterações que devem ser realizadas no plano. É muito importante que seja detalhado o que deve ser alterado da maneira mais clara possível.
		GC				Alterar nos artefatos do plano de continuidade as alterações que forem necessárias.
		GC				Registrar a aprovação do responsável pela aprovação da revisão realizada.
		GC				Divulgar os resultados das manutenções para os patrocinadores, gestores de processo, TI e usuários chave envolvidos no processo revisado. Pode-se utilizar os modelos de atas presentes na Biblioteca de Documentos do sistema para auxiliar neste registro. Os documentos preenchidos podem ser anexados no diretório Registros.

ANEXO B – Artefatos do plano de continuidade de negócios

ANEXO B. ARTEFATOS DO PLANO DE CONTINUIDADE DE NEGÓCIOS

Documento 1. Escopo

1.1. DEFINIÇÕES DA ORGANIZAÇÃO	
Unidade organizacional	
Propósito da Organização	
Missão	
Negócio	
Valores	
Estratégia	
Organograma	

1.2 . ESCOPO E APLICAÇÃO	
Plano de continuidade	
Escopo	
Áreas funcionais envolvidas	

1.3. RESTRIÇÕES QUE AFETAM A ORGANIZAÇÃO		
Unidade organizacional		
Restrições	**Questões**	**Sim / Não / Parcialmente**
Restrições de natureza política	O processo a ser abordado possui sistemas e serviços relacionados ao governo?	
Restrições de natureza estratégica	O processo a ser abordado está envolvido na estratégia da organização?	
Restrições territoriais	A organização está localizada em uma área geográfica instável quanto a contratação de link de	
Restrições do ambiente econômico e político	A organização está vinculada à algum sindicato ou órgão responsável por paralizações ou greves? Já	
Restrições estruturais	A organização depende da gestão de um conselho externo que possa influenciar nas decisões do processo de continuidade?	
Restrições funcionais	Há sistemas ou ativos de TI no processo que necessitam estar operantes 24 horas por dia e 7 dias por semana?	
Restrições de recursos humanos	Há uma equipe de TI ou usuários chave que poderão operar o plano de continuidade?	
Restrições advindas da agenda da organização	O processo a ser abordado é um projeto temporário?	
Restrições relacionadas a métodos e processos	Há uma política envolvendo a continuidade de negócios do processo a ser abordado?	
Restrições de natureza cultural	A organização possui abertura para implantação de novos processo? A continuidade de negócios faz	
Restrições orçamentárias	A organização está disposta a investir (independente do valor) na continuidade de negócios?	
Legislações e regulamentações aplicáveis	O processo a ser abordado está envolvido em alguma legislação, regulamentação ou contrato que	

1.4. EQUIPE							
Usuários	PAPÉIS					Área funcional	Formas de contato
	Patrocinador	Usuário-Chave	Gestor de Processo	TI	Gestor da Continuidade		

1.5. RESTRIÇÕES QUE AFETAM O ESCOPO DA CONTINUIDADE		
PLANO DE CONTINUIDADE		
RESTRIÇÕES DE ESCOPO	Resposta	Tipo de resposta
Técnicas		
Quais os sistemas envolvidos no processo		Descrição
Qual a Infra-Estrutura envolvida no processo		Descrição
Dependências dos serviços de comunicação		Descrição
Financeiras		
Processo fornece lucro direto à organização		Sim/Não
A interrupção do processo acarreta em prejuizo direto		Sim/Não
Valor aproximado de investimento para a continuidade		Valor
Ambientais		
Fenômenos meteorológicos a considerar		Descrição
Impacto dos fenômenos meteorológicos		Descrição
Temporais		
Prazo de implantação da continuidade de negócios		Tempo/Dias
Tempo aproximado de parada aceitável do processo		Tempo/Horas
Recursos humanos		
Capacidade da equipe de usuários do processo		Descrição
Nível de conhecimento dos usuários no processo de negócio		Descrição
Capacidade da equipe de TI em fornecer o suporte		Descrição
Organizacionais		
Possui recursos tecnológicos necessários		Sim/Não
Dependência de terceiros na operação		Sim/Não
Dependência de terceiros no suporte e manutenção		Sim/Não

1.6. SUMÁRIO EXECUTIVO		
PLANO DE CONTINUIDADE		
Definição da continuidade de negócios		
Descrição breve do processo a ser abordado		
Exemplos de situação de desastre		
Objetivo da continuidade de negócios		
Fases da Gestão da continuidade de negócios	Definição do Escopo	Na primeira fase é realizado o levantamento do Escopo. O escopo para do levantamento de toda a organização e suas restrições, qual a área de aplicação do plano e define-se a equipe que participará da elaboração do plano de continuidade de negócios.
	Gestão de Riscos	A gestão de riscos compreende a identificação dos riscos que podem afetar o processo definido no escopo. Nesta etapa é mapeado o processo definido, identificado os ativos envolvidos, suas vulnerabilidades, ameaças e consequencias, e então os riscos são avaliados para a elaboração dos planos.
	Elaboração do PCN	A terceira etapa compreende a elaboração das ações de tratamento dos riscos identificados, a definição das cópias de segurança e a elaboração dos planos de resposta a incidente e recuperação de desastres. É nesta fase que o plano de continuidade toma forma e é avaliado.
	Manutenção do PCN	A quarta e última etapa refere-se ao processo de registro de execução, medição e monitoramento, testes, manutenção e revisão preventiva.

Documento 2. Processo

2.1. PROCESSO	
Descrição do processo	
Plano de Continuidade	
Responsável pelo processo	

2.2. PROCESSO MODELADO
Anexar o mapeamento realizado

Documento 3. Ativos

3.1. RELAÇÃO DOS ATIVOS DE TI ENVOLVIDOS NO PROCESSO

Ativos							
Ativo	Responsável	Descrição	Classificação	Subtipo	Criticidade	Ativos primários/suporte	SLA

Documento 4. Riscos

4.1. IDENTIFICAÇÃO DOS RISCOS

Ativo	Ameaças			Vulnerabilidades	Consequências		Probabilidade	Nível	Observações
	Ameaça	Tipo	Origem		Consequencia	Impacto			

Documento 5. Ações de Tratamento

5.1. AÇÕES DE TRATAMENTO DOS RISCOS

Plano de continuidade	Ameaça	Vulnerabilidade	Consequência	Ações	Detalhamento	Tipo	Responsável	Requer investimento?	Valor	Aprovação	Justificativa	Prazo de implementação

Documento 6. Métodos de Cópias de Segurança

6.1. MÉTODOS DE CÓPIA DE SEGURANÇA

Método de Backup	Plano de continuidade envolvido	Ativos envolvidos	Responsável	Ações de validação	Dados de Backup	Tipo de backup	Prioridade	Contratos de suporte de terceiros

Documento 7. Cópias de Segurança

7.1 CÓPIAS DE SEGURANÇA

Ativo	Possui Backup?	Método de Backup	Periodicidade	Ciclo de vida	Responsável	Ações de validação	Periodicidade da validação	Responsável	Possui armazenamento externo?	Periodicidade do armazenamento externo	Responsável

Documento 8. Plano de Resposta

8.1. PLANOS DE RESPOSTA A INCIDENTES

Ação	Ameaça	SLA	Plano de continuidade	Ativação	Tipo	Responsáveis	Quem deve ser comunicado?			OLAs
							Na ocorrência	Após realização	Quem pode ser acionado?	

Documento 9. Recuperação de Desastres

9.1. ATIVAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES

Plano de recuperação	
Plano de continuidade	
Definição do desastre	
Responsável pela ativação	
Responsável pelas ações	
Responsável pelas tomadas de decisão	
Responsável financeiro	
Responsável pelas aquisições	
Quem deve ser informado	
Prazo Estimado para reestabelecimento das atividades	
Local definido para a continuidade de negócios	
Plano aprovado por	

9.2. ESTRUTURA MÍNIMA PARA CONTINUIDADE DE NEGÓCIOS EM SITUAÇÃO DE RECUPERAÇÃO DE DESASTRE

9.2.1. Ativos de TI Mínimos Necessários

Plano de recuperação	Ativo para recuperação	Tipos de Ativos de TI	Quantidade	Descrição	Redundante?	Custo aproximado	Prioridade	Responsável

9.2.2. Ativos de Recursos Humanos mínimo necessários para a recuperação de desastre

Plano de recuperação	Profissional necessário	Descrição Detalhada	Quantidade	Presente?	Interno/Externo?	Criticidade	Responsável

9.2.3. Serviços de terceiros mínimos necessários

Plano de recuperação	Serviços	Descrição detalhada	Custo aproximado	Necessidade de acionamento	Contato	Empresa	Responsável

Documento 10. Plano de Recuperação

10.1. PLANO DE AÇÕES PARA A RECUPERAÇÃO DE DESASTRE

Plano de recuperação	Ação	Nro da Ação	Tipo de ação	SLA	Responsável	Dependente?	Ativos reabilitados	Quem deve ser comunicado			Descrição da ação	OLA
								Na ocorrência	Após realização	Quem pode ser acionado?		

Documento 11. OLA

11.1. ACORDOS DE NÍVEL OPERACIONAL - OLA

Ação	Tipo	Instruções operacionais	Responsável	Quem pode ser acionado?	Anexos

Documento 12. Avaliação

12.1. APROVAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

Plano de continuidade	Aprovador	Papel	Parecer	Etapa			Observações
				Definição do escopo	Análise de riscos	Plano de continuidade	

Documento 13. Registro de Ocorrências

13.1. REGISTRO DE OCORRÊNCIAS DE INCIDENTES

Número da Ocorrência	Data	Ameaça	Interrupção de ativos?	Ação realizada	Ação realizada (caso não prevista)	Utilização do plano na solução	SLA acordado	Tempo realizado	Custo da solução	Responsável

13.2. REGISTRO DE RECUPERAÇÃO DE DESASTRES

Desastre	Data de início	Data de solução	Desastre (descrição)	Utilizado plano na solução?	Plano de recuperação utilizado?	Eficiência do plano	SLA acordado	Tempo realizado	Responsável

Documento 14. Indicadores

14.1. INDICADORES DE DESEMPENHO DA CONTINUIDADE

Indicador de performance	Mês 1		Mês 2		Mês 3		Mês X ...	
	Meta	Realizado	Meta	Realizado	Meta	Realizado	Meta	Realizado
Quantidade de horas perdidas por usuários devido à inoperância não planejada dos sistemas								
Porcentagem de incidentes atendidos e solucionados pelos planos de resposta a incidentes								
Porcentagem de incidentes atendidos e solucionados dentro do prazo do SLA								
Quantidade de ativos cobertos pelo plano de continuidade de negócios								
Percentual de testes realizados com sucesso, sem necessidade de correção								
Frequencia de interrupção de serviços nos sistemas críticos								
Desastres ocorridos								
Sucesso na recuperação de desastres através do plano								
Outros								

Documento 15. Testes

15.1. PLANO DE TESTES

Plano de Testes	Ações de teste	Planos testados	Objetivo	Complexidade	Periodicidade de realização	Responsável	OLA

15.2. REGISTRO DE REALIZAÇÃO DE TESTES E SIMULAÇÕES

Data de início	Data de Término	Tipo de teste	Teste realizado	Resultados	Responsável	Planos testados	Possível testar SLA?	Possível testar SLA?	SLA acordado	Tempo realizado	Necessidades de revisão

Documento 16. Manutenção

16.1. REVISÃO E MANUTENÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

Plano de Continuidade	Etapas do Plano	Objetivos	Frequência de revisão	Responsável pela atividade	Responsável pela aprovação
	Definição de escopo				
	Mapeamento do Processo				
	Identificação de Ativos				
	Análise de riscos				
	SLAs				
	Ações de tratamento de riscos				
	Cópias de Segurança				
	Plano de resposta a incidentes				
	Plano de recuperação de desastres				
	OLAs				
	Distribuição e armazenamento do plano de continuidade				
	Indicadores				
	Testes				
	Outros...				

16.2. REGISTRO DE REVISÕES

Plano de continuidade	Data da Revisão	Responsável	Motivo da revisão	Revisão programada	Revisão realizada	Alterações realizadas no plano	Aprovação

Documento 17. Contatos

17.1. CONTATOS

Contato	Empresa	Responsável	Ações envolvidas	Endereço	Telefone	Celular	E-Mail	Outras

ANEXO C – Informações complementares

ANEXO C. INFORMAÇÕES COMPLEMENTARES

1. RESTRIÇÕES ORGANIZACIONAIS

RESTRIÇÕES	DESCRIÇÃO	O QUE IDENTIFICAR
Restrições de natureza política	Restrições que dizem respeito a órgãos do governo, como a utilização de nota fiscal eletrônica e SPED.	O processo a ser abordado possui serviços que dependem de órgãos do governo para operar? Ex: Nfe e SPED
Restrições de natureza estratégica	Restrições abordadas em planejamento estratégico e impactam na estratégia da organização como a utilização de sistemas como ferramentas de negócio. EX: sistema on-line de pedidos no canal de vendas	O processo a ser abordado está envolvido na estratégia da organização?
Restrições territoriais	Restrições referente a localização geográfica da organização. É de suma importância pois pode influenciar na contratação de serviços como link de internet, serviços de manutenção de rede e hardware, entre outros serviços que podem ser críticos na elaboração de um plano de continuidade.	A organização está localizada em uma área geográfica instável quanto a contratação de link de internet ou contratação de serviços de suporte e manutenção?
Restrições do ambiente economico e político	As organizações estão envolvidas em meios políticos, deve-se levar em conta a possibilidade de um evento, como greves, interromper as atividades da organização.	A organização está vinculada à algum sindicato ou órgão responsável por paralizações ou greves? Já houveram ocorrencia de paradas devido à estas questões?
Restrições estruturais	A estrutura organizacional pode significar uma restrição, por exemplo, empresas multinacionais possuem processos vinculados à diferentes gestões.	A organização depende da gestão de um conselho externo que possa influenciar nas decisões do processo de continuidade?
Restrições funcionais	A organização pode possuir dependência de serviços de TI para cumprir sua missão. Sistemas cuja disponibilidade é necessária cem por cento do tempo em um período de vinte-quatro horas por dia se incluem nestas restrições.	Há sistemas ou ativos de TI no processo que necessitam estar operantes 24 horas por dia e 7 dias por semana?
Restrições de recursos humanos	A equipe envolvida no processo de continuidade deve ser identificada, bem como suas responsabilidades, qualificações, conscientização, motivação e disponibilidade. O processo de continuidade de negócios é extremamente dependente das pessoas envolvidos no mesmo.	Há uma equipe de TI ou usuários chave que poderão operar o plano de continuidade?
Restrições da agenda da organização	Projetos temporários, promoções de mercado, regime alto de horas extra e crises econômicas devem ser levados em consideração na identificação do processo. Um projeto temporário pode requerer muito esforço e criticidade alta em sua implantação, sendo necessário um plano específico para ele.	O processo a ser abordado é um projeto temporário?
Restrições relacionadas a métodos e processos	Organizações em geral possuem políticas e códigos de ética e operação. Os planos de continuidade devem levar estas políticas em conta na hora de sua elaboração.	Há uma política envolvendo a continuidade de negócios do processo a ser abordado?

Restrições de natureza cultural	A cultura da organização é muito influente na definição de seus processos. Questões culturais como etnia, costumes geográficos, postura e atitude profissional devem ser levados em conta. A implantação de novos processos pode impactar em um choque cultural. Normalmente é a restrição mais difícil de ser tratada.	A organização possui abertura para implantação de novos processo? A continuidade de negócios faz parte do conhecimento da organização?
Restrições orçamentárias	A implantação de um plano de continuidade de negócio deve levar em consideração a situação financeira da organização e quanto a mesma está disposta a investir. A aceitação do risco estará sempre se baseando na relação entre custo e beneficio de um controle. Organizações privadas tendem a avaliar o investimento relacionando o mesmo com o possível prejuízo em caso de ocorrência.	A organização está disposta a investir (independente do valor) na continuidade de negócios?
Legislações e regulamentações aplicáveis	**:** É necessário identificar os requisitos legais aplicáveis a organização, baseando-se nas leis, decretos, regulamentações específicas a área de atuação da organização ou regulamentos internos e externos. Contratos com fornecedores e clientes também devem ser analisados. Cita-se como exemplo um contrato de fornecimento com um cliente baseado em prazos, a interrupção do processo de entrega pode gerar um prejuízo previsto em contrato ou não.	O processo a ser abordado está envolvido em alguma legislação, regulamentação ou contrato que podem colocar em risco a operação?

ITEM 2. RESTRIÇÕES QUE AFETAM O ESCOPO		
RESTRIÇÕES	**DESCRIÇÃO**	**O QUE IDENTIFICAR**
Restrições técnicas	Referente à infraestrutura de TI, seus sistemas, hardware e a dependencia dos serviços para o processo.	Quais são os sistemas envolvidos no processo? Qual a infraestrutura de hardware, software e rede envolvida no processo? Qual a dependência de serviços de comunicação como internet e telefonia para este processo?
Restrições financeiras	Referente ao impacto do processo na organização.	Este processo fornece lucro diretamente para a organização? A interrupção deste processo acarreta em prejuízo direto? O quanto aproximado a organização pode investir para garantir a segurança deste processo?
Restrições ambientais	Restrições que surgem como consequência do ambiente geográfico e climático da localização da organização.	Qual o impacto de fenômenos meteorológicos para este processe? Quais fenomenos meteorológicos devem ser considerados?
Restrições temporais	Restrições do tempo de implementação de controles para os processos identificados. Longo tempo de espera para a implementação pode invalidar a análise pois os riscos podem sofrer alteração com o tempo.	Qual o prazo máximo para a implantação do tratamento de risco para o processo? Quanto tempo o processo pode ficar interrompido?
Restrições de recursos humanos	Referente aos usuários e equipe de TI envolvidos no processo a ser abordado.	Os usuários envolvidos no processo são capazes de operá-lo com eficiência e segurança? Todos os usuários envolvidos possuem o mesmo nível de conhecimento? A equipe de TI envolvida neste processo é capacitada para fornecer o suporte necessário?
Restrições organizacionais	Restrições operacionais como tempo de operação, gestão dos recursos de TI, manutenção, administração do processo, desenvolvimento e relacionamento com terceiros devem ser consideradas.	A organização possui todos os recursos tecnológicos necessários? A organização depende de terceiros para operar o processo? A organização depende de terceiros para realizar suporte e manutenção do processo?

ITEM 3. TIPOS DE ATIVOS

Ativos Primários

Tipos	Descrição	Exemplos
Processos e atividades de negócio	Processos cuja interrupção, mesmo que parcial, torna impossível cumprir a missão da organização, processos que contem procedimentos secretos ou processos envolvendo tecnologia proprietária, processos que se modificados podem afetar significativamente o cumprimento da missão da organização e processos necessários para que a organização se mantenha em conformidade com requisitos contratuais, legais ou regulatórios.	Implantação de pedido de venda, geração e impressão de ordem de produção, reporte e apontamento de produção, faturamento de nota fiscal, emissão de nota fiscal eletrônica, calculo de folha de pagamento, cotação e aprovação de solicitações de compra, pagamento de boletos em website do banco, etc.
Informação	Informação vital para o cumprimento da missão ou desempenho de negócio de uma organização, informação de caráter pessoal, informação estratégica necessária para o alcance dos objetivos determinados pelo planejamento estratégico, informação de alto custo, cuja coleta possui longo tempo ou	Ata de reunião de gerencia e direção, planejamento estratégico, folha de pagamento, segredo industrial, etc.

Ativos de suporte e infraestrutura

Tipos	Subtipos	Descrição	Exemplos
Hardware	Equipamento de processamento de dados	Equipamento automático de dados incluindo os itens necessários para sua operação independente.	softwares de agendamento de tarefas e execução automática.
	Equipamento móvel	Computadores e dispositivos portáteis	notebooks, tablets, smartphones, coletores de dados e agendas eletrônicas.
	Equipamento fixo	Computadores utilizados nas instalações da organização	servidores, estações de trabalho, terminais magros e terminais específicos de aplicações.
	Periféricos de processamento	Equipamentos conectados a um computador através de porta de comunicação ou conexão sem fio para a entrada, transporte ou transmissão de dados.	impressoras, unidades de disco removível, leitores de código de barras e periféricos de entrada como mouse e teclado.
	Mídia de dados	Uma mídia de informações que pode ser conectada a um computador ou rede para armazenamento de dados. A mídia de dados geralmente pode ser utilizada em qualquer tipo de computador.	disco flexível, CD-ROM, fita de backup, unidade de disco externa, cartão de memória e unidade de armazenamento flash
	Outros tipos de mídia	Mídia estática, não eletrônica, que contem dados	documentos, papel, slides, transparências, fax

Software	Sistema operacional	Compreende os programas que oferecem as operações básicas de um computador e a partir dele outros programas são executados. Seus principais elementos são os serviços de gerenciamento do hardware, gerenciamento de tarefas e os serviços de gerenciamento de usuário. O sistema operacional é encontrado em qualquer tipo de equipamento fixo e móvel.	Microsoft Windows, Google Android, Apple Mac OS-X, Linux
	Software de serviço, manutenção ou administração	Softwares que servem de complemento para uso e administração do sistema operacional e não ligado diretamente ao usuário	Windows Active Directory, Microsoft WSUS, RedHat Samba, softwares de cópias de segurança e anti-virus
	Software de pacote ou de prateleira	: Softwares comercializado como um produto completo com mídia, versão e manutenção. Fornecem serviços para usuários e aplicações mas não é passível de alteração com as aplicações de negócio	Microsoft Office, Adobe Photoshop, Corel Draw
Aplicações de negócio	Aplicações de negócio padronizadas	Software comercial projetado para fornecer acesso direto as operações de negócio em função de suas áreas de atuação. Normalmente estes tipos de software são a principal ferramenta de trabalho de uma organização, possuindo uma enorme gama de aplicações porem limitadas ao seu conjunto. Passível de customização	sistemas ERP, sistema de gestão empresarial, sistemas CRM, relacionamento com cliente, sistemas de BI, inteligência de negócio, HCM, gestão do capital humano
	Aplicações de negócio específicas	Sistemas desenvolvidos especificamente para aplicações de negócio particulares de uma organização. Existem diversos tipos de software específicos, porém sua atuação limita-se ao que foi implementado	sistema de monitoramento de máquina fabril, sistema de controle de pressurização em equipamentos industriais, controle de pesagem de matéria prima integrada com balança
Rede	Meio físico e infraestrutura	Compreendem a rede de comunicação que interligam os diversos computadores e sistemas de uma organização. Identificados pelas características físicas e técnicas e pelos protocolos de comunicação.	Rede telefona pública comutada, redes ethernet e gigabit ethernet, linha digital assimétrica para assinante, ADSL, rede Wi-Fi, Bluetooth, Firewire.
	Pontes (“relays”) passivas ou ativas	Compreendem os dispositivos intermediários de conexão de rede, responsáveis pelo repasse de trafego de dados, comutação e filtro de rede	pontes, roteadores, hubs, comutadores “switches”, centrais telefônicas automáticas, access points de rede sem fio

	Interface de comunicação	Interfaces de redes conectadas as unidades de processamento.	adaptadora “ethernet”, adaptador de rede sem fio, serviço de pacotes por rádio GPRS
Recursos Humanos	Tomador de decisão	São os recursos humanos responsáveis pelos ativos primários (informação e processos) e os gestores da organização	alta direção, gerentes de área e gerentes de projeto.
	Usuários	São os recursos humanos que manipulam e executam as atividades do processo de negócio. Possuem a responsabilidade do correto uso dos sistemas de informação e manipulam informações sensíveis de negócio. Possuem acessos referente a suas atividades de negócio nos sistemas de informação.	gestores de área específico, analistas de área específica, usuários operadores de sistema
	Pessoal de produção/manutenção	Recursos humanos responsáveis pela operação e manutenção dos sistemas de informação, geralmente equipes de TI ou usuários chave com grande conhecimento de sistema. Possuem acesso especial, com permissões de gerenciamento dos sistemas, para realizarem suas atividades rotineiras	administradores de sistema, analistas de TI, analistas de suporte, Helpdesk, especialistas em segurança.
	Desenvolvedores	responsáveis pelo desenvolvimento dos sistemas aplicativos da organização. Possuem acesso de alto privilégio aos sistemas, incluindo seu código-fonte. Não interferem com os dados de produção	programadores e analistas de aplicações de negócio.
Instalações físicas e localidade	Ambiente externo	compreende os locais em que as medidas de segurança não podem ser aplicadas.	lar das pessoas, instalações de terceiros, áreas urbanas e zonas perigosas
	Edificações	Local limitado pelo perímetro externo da organização, compreende a área física onde a organização está localizada	estabelecimentos e prédios
	Zona	Referente as áreas físicas delimitadas dentro de uma organização que separam áreas funcionais, processos ou locais específicos	escritórios, pavilhões, área de acesso restrito, área de segurança, centro de processamento de dados
	Comunicação	Serviços de telecomunicação e equipamento fornecido pela operadora de telefonia.	linha telefônica, PABX, redes internas de telefonia
	Serviços de infraestrutura	Serviços e meios necessários para fornecimento de energia elétrica aos equipamentos de tecnologia da informação e seus periférico	fonte de energia de baixa tensão, central de circuitos elétricos, equipamento de prevenção de quedas de energia, serviços de refrigeração.

Tabela de criticidade dos ativos		
Criticidade	**Descrição**	**Consequencias de interrupção**
Baixa	Ativos que não afetam diretamente o processo de negócio. Sua interrupção pode significar perda de performance no processo mas não a sua parada.	Perda de performance de processo, inacuracidade na execução de atividades
Média	Ativos que afetam o processo de negócio. Sua interrupção pode acarretar em perda de performance e até parada minima do processo de negócio, porem os prejuizos não são graves.	Interrupção curta nas atividades de negócio, perda de performance em atividades críticas do processo, informações não condizentes com a realidade
Alta	Ativos que afetam diretamente o processo de negócio. Sua interrupção pode acarretar em prejuizo direto ao processo, perda de credibilidade com clientes, perda de oportunidades de negócios. Sua interrupção não é tolerável.	prejuizo financeiro, perda de negócios, violação de lei ou de inciso contratual, perigo físico à saude das pessoas, perda de valor de mercado

ITEM 4. AMEAÇAS			
EXEMPLO DE AMEAÇAS TÍPICAS			
Tipos	**Ameaças**	**Origem**	**Ativos de possível identificação**
Dano Físico	Fogo	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
	Água	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
	Poluição	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
	Destruição de equipamento ou mídia	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
	Poeira, corrosão, congelamento	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
Eventos Naturais	Fenômeno climático	Natural	Hardware, Infraesturtura e Instalações físicas
	Fenômeno sísmico	Natural	Hardware, Infraesturtura e Instalações físicas
	Fenômeno vulcânico	Natural	Hardware, Infraesturtura e Instalações físicas
	Fenômeno meteorológico	Natural	Hardware, Infraesturtura e Instalações físicas
	Inundação	Natural	Hardware, Infraesturtura e Instalações físicas
Paralisação de serviços essenciais	Falha do ar condicionado ou do sistema de suprimento de água	Acidental, Intencional	Hardware, Infraesturtura e Instalações físicas
	Interrupção do suprimento de energia	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
	Falha do sistema de telecomunicação	Acidental, Intencional	Hardware, Infraesturtura e Instalações físicas
Distúrbio causado por radiação	Radiação eletromagnética	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
	Radiação térmica	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
	Pulsos eletromagnéticos	Acidental, Intencional, Natural	Hardware, Infraesturtura e Instalações físicas
Comprometimento da informação	Interceptação de sinais de interferencia comprometedores	Intencional	Hardware, Software, Aplicações de negócio Recursos Humanos
	Espionagem à distância	Intencional	Hardware, Software, Aplicações de negócio Recursos Humanos
	Escuta não autorizada	Intencional	Hardware, Software, Aplicações de negócio Recursos Humanos
	Furto de mídia ou documentos	Intencional	Hardware, Instalações Físicas e Recursos Humanos
	Furto de equipamentos	Intencional	Hardware, Instalações Físicas e Recursos Humanos
	Recuperação de mídia reciclada ou descartada	Intencional	Hardware, Instalações Físicas e Recursos Humanos
	Divulgação indevida	Acidental, Intencional	Recursos Humanos
	Dados de fontes não confiáveis	Acidental, Intencional	Recursos Humanos
	Alteração do hardware	Intencional	Hardware, Instalações Físicas e Recursos Humanos
	Alteração do software	Acidental, Intencional	Software, Aplicações de negócio, Instalações Físicas e Recursos Humanos
	Determinação da localização	Intencional	Hardware, Infraesturtura e Instalações físicas
	Falha de equipamento	Acidental	Hardware, Infraestrutura
	Defeito de equipamento	Acidental	Hardware, Infraestrutura

Falhas técnicas	Saturação do sistema de informação	Acidental, Intencional	Hardware, Infraestrutura
	Defeito de software	Acidental	Software
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	Acidental, Intencional	Hardware, Software, Aplicações de negócio Recursos Humanos
Ações não autorizadas	Uso não autorizado de equipamento	Intencional	Hardware, Instalações Físicas e Recursos Humanos
	Cópia ilegal de software	Intencional	Software, Recursos Humanos
	Uso de cópias de software falsificadas ou ilegais	Acidental, Intencional	Software, Recursos Humanos
	Comprometimento dos dados	Intencional	Software, Aplicações de negócio, Recursos Humanos
	Processamento ilegal de dados	Intencional	Software, Aplicações de negócio, Recursos Humanos
Comprometimento de funções	Erro durante o uso	Acidental	Software, Aplicações de negócio, Recursos Humanos
	Abuso de direitos	Acidental, Intencional	Software, Aplicações de negócio, Recursos Humanos
	Forjamento de direitos	Intencional	Software, Aplicações de negócio, Recursos Humanos
	Repúdio de ações	Intencional	Software, Aplicações de negócio, Recursos Humanos
	Indisponibilidade de recursos humanos	Acidental, Intencional, Natural	Recursos Humanos
Ameaças humanas	Hacking, Cracking	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Invasão de sistemas	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Acesso não autorizado a sistemas	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Destruição de informações	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Falsidade ideológica	Intencional	Recursos Humanos
	Bomba/Terrorismo	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Furto de informação	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Uso impróprio de recurso computacional	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Interceptação	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Código malicioso (virus, cavalo de tróia, etc)	Intencional	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas

ITEM 5. VULNERABILIDADES		
EXEMPLO DE AMEAÇAS TÍPICAS		
Tipos de ameaças	**Exemplos de vulnerabilidades**	**Ameaças relacionadas**
Hardware	Manutenção insuficiente de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Ausencia de rotina de substituição de equipamentos periódica	Destruição de equipamento ou mídia
	Ambiente sensível à poeira, umidade, sujeira	Poeira, corrosão, congelamento
	Sensibilidade a radiação eletromagnética	Radiação eletromagnética
	Inexistência de controle eficiente de mudança de configuração	Erro durante o uso
	Sensibilidade a variações de voltagem	interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Armazenamento não protegido	Furto de mídia, dados ou documentos
	Falta de cuidado durante o descarte	
	Realização de cópias não controladas	
Software	Procedimentos de teste de software insuficientes ou inexistentes	Abuso de direitos
	Falhas conhecidas no software	
	Deixar estação de trabalho desasistida e com usuário conectado	
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimenos apropriados de remoção dos dados	
	Inexistencia de um processo de auditoria	
	Atribuição errônea de direitos de acesso	
	Software amplamente distribuido	Comprometimento dos dados
	Utilizar programas com dados inválidos ou de versão antiga	
	Interface de usuário não amigável	Erro durante o uso
	Inexistencia de documentação e ajuda	
	Parametrização incorreta	
	Datas incorretas	
	Inexistencia de processo de autenticação de usuarios	Forjamento de Direitos
	Arquivo com registro de senhas desportegido ou de passível acesso	
	Gerenciamento de senhas mal feito	
	Serviços desnecessários habilitados	Processamento ilegal de dados
	Software novo, não homologado ou imaturo	Defeito de software
	Especificações confusas ou incompletas para desenvolvedores	
	Inexistencia de um controle eficaz de mudança	

	Download e uso não controlado de software	Alteração do software
	Inexistencia de cópias de segurança	
	Inexistencia de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia, dados ou documentos
	Inexistencia de relatórios de gerenciamento	Uso não autorizado de equipamento
Rede	Inexistencia de evidencias que comprovem o envio ou o recebimento de mensagens	Repúdio de ações
	Linhas de comunicação desprotegidas	Escuta não autorizada
	Tráfego sensível não protegido	
	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	
	Não identificação e não autenticação do emissor e do receptor	Forjamento de direitos
	Arquitetura insegura da rede	Espionagem à distância
	Transferência de senhas em claro	
	Gerenciamento de rede inadequado	Saturação do sistema de informação
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Recursos humanos	Ausência de recursos humanos, equipe insuficiente	Indisponibilidade de recursos humanos
	Procedimentos de recrutamento inadequados	Destruição de equipamento ou mídia
	Treinamento insuficiente	Erro durante o uso
	Uso incorreto de software e hardware	
	Falta de conscientização em segurança	
	Inexistência de mecanismos de monitoramento	Processamento ilegal de dados
	Trabalho não supervisionado de pessoal terceirizado	Furto de mídia, dados ou documentos
	Inexistência de políticas para uso correto de meios de telecomunicação ou de troca de mensagens	Uso não autorizado de equipamento, Furto de mídia, dados ou documentos
Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e locais de armazenamento de dados críticos	Destruição de equipamento ou mídia
	Localização em área suscetível a inundações	Inundação
	Instabilidade no fornecimento de energia	interrupção do suprimento de energia
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamentos
	Inexistencia de um procedimento formal para o registro e exclusão de usuários	Abuso de direitos
	Inexistência de processo formal para a análise crítica dos direitos de acesso(supervisão)	
	Contratos com clientes e/ou terceiros sem firmamento de termo de confidencialidade quando trata-se de informação crítica	

Organização	Inexistência de procedimento de monitoramento das instalações de processamento de informações	Abuso de direitos
	Inexistência de auditorias periódicas	
	Inexistência de procedimentos de identificação, análise e avaliação de riscos	
	Inexistência de relatório de falhas de auditoria em serviços de segurança	
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	SLA inexistente	
	Inexistência de procedimento de controle de mudanças	
	Inexistência de um procedimento formal para a gestão da segurança da informação	Comprometimento dos dados
	Inexistencia de um procedimento formal para a autorização das publicação de informações de domínio público	Dados de fontes não confiáveis
	Atribuição inadequada de responsabilidades	Repúdio de ações
	Inexistencia de um plano de continuidade	Falha de equipamento
	Inexistência de política de uso de correspondencia eletrônica (E-mail)	Erro durante o uso
	Inexistência de procedimentos para a instalação de software em sistemas operacionais	
	Ausência de registros de auditoria de administradores e operadores - LOGs	
	Inexistência de procedimentos para a manipulação de informações reservadas e confidenciais	
	Ausência das responsabilidades ligadas à delegação de cargos e funções	
	Inexistência de contratos de confidencialidade com funcionários	Processamento ilegal de dados
	Inexistência de um processo disciplinar em situações de desastre	Furto de equipamentos
	Inexistência de uma política formal sobre o uso de computadores móveis	
	Inexistência de controle sobre ativos externos à dependência da orgnaização	
	Inexistência de política de mesas e telas limpas	Furto de mídia, dados ou documentos
	Inexistência de autorização para as instalações de processamento de informações	
	Inexistência de mecanismos de controle de violações de segurança	
	Inexistência de análises críticas periódicas por parte da direção	Uso não autorizado de equipamento
	Inexistência de procedimentos para o relato de fragilidades ligadas à segurança	
	Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual da organização	

ITEM 6. CONSEQUENCIAS		
EXEMPLOS DE CONSEQUENCIAS		
CONSEQUENCIAS	**Ameaças comuns**	**Tipo de ativos comuns**
Perda de desempenho ou instabilidade no funcionamento dos sistemas	Falha do Ar condicionado	Infraestrutura
	Alteração de hardware ou software	Hardware, Software
	Falha ou defeito de equipamento	Hardware
	Saturação do sistema de informação	Aplicação de Negócio
	Defeito de software	Software
	Erro durante o uso	Aplicação de Negócio, Hardware, Software
	Invasão de sistemas	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Uso impróprio de recurso computacional	Recursos Humanos, Software, Hardware, Aplicações de negócio
	Código malicioso (virus, cavalo de tróia, etc)	Recursos Humanos, Software, Hardware
Condições adversas de operação	Falha do Ar condicionado	Infraestrutura
	Alteração de hardware ou software	Hardware, Software
	Falha ou defeito de equipamento	Hardware
	Invasão de sistemas	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Código malicioso (virus, cavalo de tróia, etc)	Recursos Humanos, Software, Hardware
Interrupção de operação de negócio	Falha ou defeito de equipamento	Hardware
	Invasão de sistemas	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Saturação do sistema de informação	Aplicação de Negócio
	Destruição de informações	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Danos Físicos	Hardware, Infraesturtura e Instalações físicas
	Interrupção do suprimento de energia	Hardware, Infraesturtura e Instalações físicas
Perda de oportunidade de negócios	Falha ou defeito de equipamento	Hardware , Software
	Destruição de informações	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Furto de informação	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Divulgação indevida	Recursos Humanos
	Falha do sistema de telecomunicação	Hardware, Infraesturtura e Instalações físicas
	Destruição de informações	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas

Imagem e reputação prejudicadas	Furto de informação	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Divulgação indevida	Recursos Humanos
	Forjamento de direitos	Software, Aplicações de negócio, Recursos Humanos
	Falsidade ideológica	Recursos Humanos
Violação de medidas obrigatórias ou legais	Uso não autorizado de equipamento	Hardware, Instalações Físicas e Recursos Humanos
	Cópia ilegal de software	Software, Recursos Humanos
	Uso de cópias de software falsificadas ou ilegais	Software, Recursos Humanos
	Comprometimento dos dados	Software, Aplicações de negócio, Recursos Humanos
	Processamento ilegal de dados	Software, Aplicações de negócio, Recursos Humanos
Prejuízo financeiro	Destruição de informações	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Furto de informação	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Falha de equipamento	Hardware, Infraestrutura
	Danos Físicos	Hardware, Infraesturtura e Instalações físicas
	Paralisação de serviços essenciais	Hardware, Infraesturtura e Instalações físicas
	Invasão de sistemas	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Uso impróprio de recurso computacional	Recursos Humanos, Software, Hardware, Aplicações de negócio
	Furto de equipamentos	Hardware, Instalações Físicas e Recursos Humanos
Perda de dados ou informações	Destruição de informações	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Furto de informação	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Falha de equipamento	Hardware, Infraestrutura
	Danos Físicos	Hardware, Infraesturtura e Instalações físicas
	Invasão de sistemas	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
Prejuízo à vida humana	Danos Físicos	Hardware, Infraesturtura e Instalações físicas
	Paralisação de serviços essenciais	Hardware, Infraesturtura e Instalações físicas
	Eventos Naturais	Hardware, Infraesturtura e Instalações físicas
Perda de competitividade no mercado	Destruição de informações	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Furto de informação	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas
	Invasão de sistemas	Hardware, Software, Aplicações de negócio, Recursos Humanos, Instalações Físicas

	Divulgação indevida	Recursos Humanos
	Forjamento de direitos	Software, Aplicações de negócio, Recursos Humanos
	Falsidade ideológica	Recursos Humanos
	Uso impróprio de recurso computacional	Recursos Humanos, Software, Hardware, Aplicações de negócio

IMPACTO DAS CONSEQUÊNCIAS	
Nível	**Descrição**
Baixo	Prejuízo financeiro é pequeno ou prejudica a operação de negócio a um nível aceitável
Médio	Ocasionam prejuízo financeiro moderado e não aceitável, podem acarretar em perda de oportunidades de negócio ou prejuízo à imagem da organização
Alto	Prejuízo financeiro é alto, pode prejudicar a organização de forma quase que irreversível, ocasiona perda de desempenho no mercado ou coloca em risco a vida das pessoas da organização.

ITEM 7. AVALIAÇÃO DO RISCO

TABELA DE AVALIAÇÃO DO RISCO

Probabilidade de ocorrência		Improvável	Possível	Provável
Impacto no negócio	Baixo	2	3	4
	Médio	3	4	5
	Alto	4	5	6

TABELA DE NÍVEIS DO RISCO

Pontuação	Níveis de Risco	
2	Baixo Risco	Risco pode ser aceitável sem tratamento imediato
3 e 4	Médio Risco	Risco precisa ser tratado, porém pode seguir em segundo plano
5 e 6	Alto Risco	Risco deve ser tratado o mais rápido possível

ANEXO D – Plano de continuidade de negócios

Item 1.1. DEFINIÇÃO DA ORGANIZAÇÃO					
Unidade de Negócio	**Missão**	**Negócio**	**Valores**	**Estratégia de TI**	**Organograma**
Empresa S.A.	Desenvolver, produzir e comercializar soluções completas aos nossos clientes em freios e componentes.	Solução em controle de movimentos	Qualidade, eficiência, excelência em processos e gestão de pessoas	A TI da empresa responde diretamente ao Diretor Financeiro e está alinhada com os processos de negócio da empresa. A TI tem como política a aquisição de sistemas e terceirização de serviços de TI, mantendo uma equipe reduzida para gerir estes	Organograma Empresa Simplificado v04-2013.pdf

Item 1.2. DEFINIÇÃO DO ESCOPO E APLICABILIDADE			
Plano de Continuidade	**Áreas funcionais envolvidas**	**Escopo**	**Unidade de negócio**
Faturamento e Expedição	Logística, TI, Vendas, Controladoria	Faturamento e Expedição	Empresa S.A.

Item 1.3. RESTRIÇÕES DA ORGANIZAÇÃO													
Unidade organizacional	**Restrições de Natureza Política**	**Restrições de natureza estratégica**	**Restrições territoriais**	**Restrições do ambiente econômico e político**	**Restrições estruturais**	**Restrições funcionais**	**Restrições de recursos humanos**	**Restrições relacionadas a métodos e processos**	**Restrições de natureza cultural**	**Restrições orçamentárias**	**Legislações e regulamentações aplicáveis**	**Restrições da agenda da organização**	**Observações**
Empresa S.A.	Sim	Sim	Não	Sim	Não	Sim	Sim	Parcialmente	Não	Parcialmente	Não	Não	A contingência de operações sempre foi colocada em segundo plano pela organização.

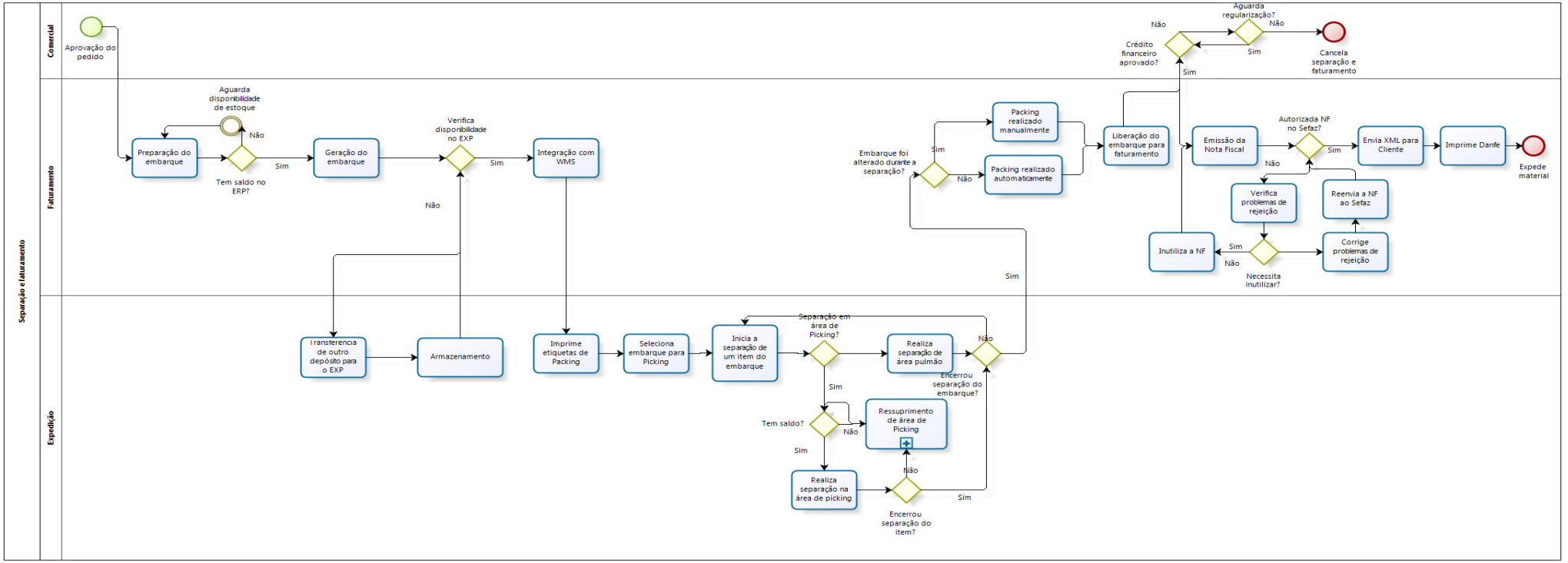
Item 1.4. DEFINIÇÃO DOS PAPÉIS E RESPONSABILIDADES			
Nome do usuário	**Papéis**	**Área Funcional**	**Formas de contato**
Coordenador de TI	TI, Gestor da Continuidade	TI	Celular: 54 9999 9999 skype: coordenador.ti E-mail pessoal: coordenador.ti@hotmail.com
Analista de Suporte	TI	TI	Plantão: 54 9999 9999 Skype: analista.suporte
Coordenador de Expedição	Gestor de Processo	Logística	Celular: 54 9999 9999
Gerente de Logística	Gestor de Processo, Patrocinador	Logística	Celular: 54 9999 9999
Diretor financeiro	Patrocinador	Financeiro	Celular: 54 9999 9999
Expedidor I	Usuário-Chave	Logística	
Expedidor II	Usuário-Chave	Logística	
Expedidor III	Usuário-Chave	Logística	
Faturista	Usuário-Chave	Logística	
Expedidor IV	Usuário-Chave	Logística	
Coordenadora de Vendas	Usuário-Chave, Gestor de Processo	Vendas	Celular: 54 9999 9999
Coordenador de Manutenção	Usuário-Chave	Manutenção	Celular: 54 9999 9999
Gerente Industrial	Gestor de Processo	Produção	Celular: 54 9999 9999
Coordenadora de Segurança do Trabalho	Gestor de Processo	SESMT	
Coordenadora de Controladoria	Gestor de Processo	Controladoria	Celular: 54 9999 9999
Analista Fiscal	Usuário-Chave	Controladoria	
Gerente de Engenharia	Gestor de Processo	Engenharia de Produto	Celular: 54 9999 9999

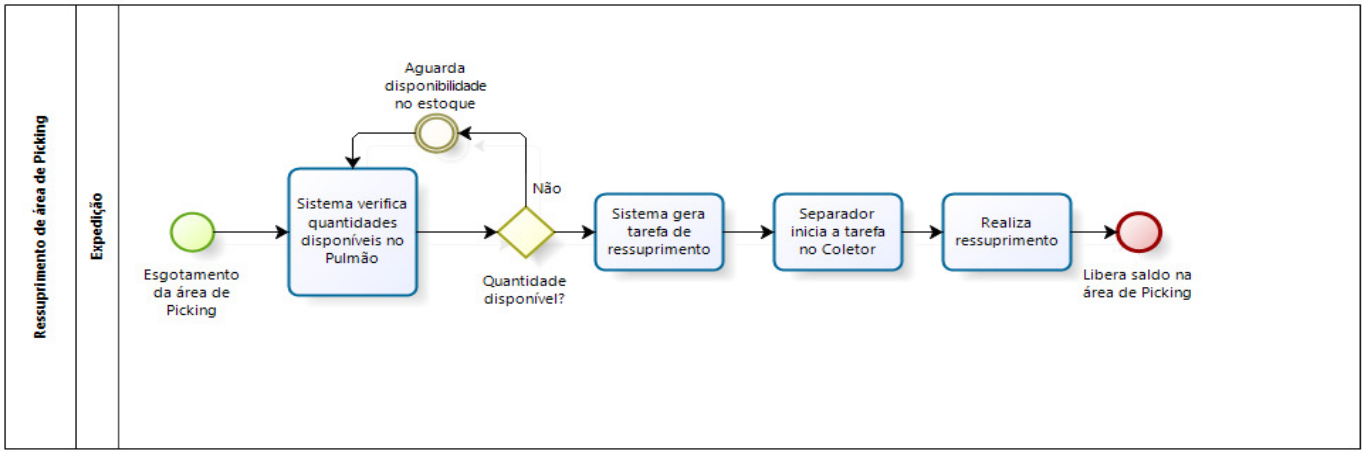
Item 1.5. RESTRIÇÕES QUE AFETAM O ESCOPO DA CONTINUIDADE							
Plano de Continuidade	**Quais os sistemas envolvidos no processo?**	**Qual a infra-estrutura envolvida no processo?**	**Qual a dependência dos serviços de comunicação?**	**Processo do escopo fornece lucro direto à organização?**	**A interrupção do processo acarreta em prejuízo direto?**	**Valor aproximado de investimento para a continuidade**	**Fenômenos meteorológicos a considerar**
Faturamento e Expedição	Datasul EMS2 (ERP logística), WMS, Datasul EMS5 (ERP Contábil), CRM (Vendas)	Link de Internet Telecom SA (10 Mbps), Rede Wi-Fi específica para a expedição, Rede cabeada 100 mbps, Microcomputadores de uso da equipe, Coletores de dados Motorola Symbol, Telefonia Fixa, Telefonia Móvel	Internet utilizada para emissão de NFe, Telefonia para comunicação com transportadoras	SIM	SIM		Fortes chuvas prejudicam o processo de separação e embarque pela limitação de espaço.
Prazo estimado para a implantação da continuidade de negócios	**Tempo aceitável de parada do processo**	**Capacidade da equipe de usuários do processo**	**Nível de conhecimento dos usuários no processo de negócio**	**Capacidade da equipe de TI em fornecer o suporte**	**Possui recursos tecnológicos necessários?**	**Dependência de terceiros na operação?**	**Dependência de terceiros no suporte e manutenção?**
60	2	são 5 separadores, 2 faturistas e 1 coordenador de área. A TI possui 2 funcionários para suporte e apoio.	O coordenador do processo possui um conhecimento forte do processo geral da Empresa. Dos separadores, 3 são capacitados tecnicamente para operar o sistema WMS e gerí-lo.	O Coordenador de TI pode fornecer suporte de alto nível, nos processos de negócio dentro dos sistemas. O analista de suporte pode fornecer suporte de tencologia e infra-estrutura no processo.	SIM	NÃO	SIM

Item 1.6. SUMÁRIO EXECUTIVO				
Plano de continuidade	**Descrição breve do processo a ser abordado**	**Definição da continuidade de negócios**	**Exemplos de situação de desastre**	**Objetivo da continuidade de negócios**
Faturamento e Expedição	O processo de Faturamento para mercado nacional compreende desde a entrada dos produtos na expedição até a emissão de Nota fiscal, passando pela gestão do sistema WMS Totvs.	O plano de continuidade de negócios é um conjunto de ações e ferramentas para manter o processo de faturamento (WMS) em funcionamento 100% do tempo, e em caso de falha, recuperá-lo o mais rápido possível.	A interrupção do faturamento pode ocorrer a partir de falhas na infraestrutura de TI. Os coletores de dados dependem da rede Wi-Fi instalada na expedição, caso a rede Wifi parar de funcionar, o faturamento estará impedido de ser realizado.	Manter o processo de faturamento e gestão do armazem operacional o maior tempo possível.

Item 2.1. MAPEAMENTO DO PROCESSO				
Processo	**Planos de continuidade envolvidos**	**Descrição do processo**	**Responsável pelo processo**	**Processo modelado**
Faturamento e Expedição	Faturamento e Expedição	O processo de expedição da empresa compreende desde o lançamentode produtos em estoque controlado (EXP), a separação do produto até o faturamento e expedição do mesmo. Utiliza-se o sistema WMS para a gestão do armazem. Se divide em Armazenamento, Separação e Expedição. O processo inicia no recebimento do produto pronto liberado pela produção, sendo realizada a transferência do depósito TMP(fabrica) para o depósito EXP(expedição). A etapa seguinte compreende o armazenamento dos produtos na expedição, sendo totalmente controlado por coletor e código de barras. A segunda parte do processo compreende a expedição dos produtos para clientes. Após a emissão dos pedidos, o faturista monta um embarque no sistema para enviar ao cliente e o integra ao WMS. Com o embarque integrado, o expedidor imprime as etiquetas de "Packing" e então inicia a separação do embarque item a item com o coletor de dados. O separador realiza o "picking" dos produtos conforme a necessidade, caso um produto não esteja mais disponível em um Box de separação, o sistema cria uma tarefa de ressuprimento da área de picking para reabastecer a separação. Após a separação de todo o embarque, o Packing é gerado automaticamente e o faturista libera o embarque para faturamento e emissão da nota fiscal. Com a nota fiscal emitida, o expedidor carrega o embarque para a transportadora e o processo é concluído.	Coordenador de Expedição	PROCESSO WMS.bpm

Item 2.1. MAPEAMENTO DO PROCESSO





Item 3.1. ATIVOS								
Ativo	Responsável	Descrição	Classificação	Subtipo de ativo	Tipo de ativo	Criticidade	Ativos primários/suporte pertencentes	SLA
Expedidor	Coordenador de Expedição	Profissional responsável por executar as atividades do processo de negócio	Suporte e Infraestrutura	Usuários	Recursos humanos	Média	Processo de Separação de Produtos; Processo de Ressuprimento	5
Coletor de dados Motorola	Coordenador de TI	Equipamento utilizado para executar as tarefas do processo de negócio	Suporte e Infraestrutura	Equipamento móvel	Hardware	Alta	Processo de Ressuprimento; Processo de Separação de Produtos	2
Roteador rede Wireless Motorola W2000	Coordenador de TI	Equipamento de gerenciamento da rede Wifi que é utilizada pelo sistema WMS	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Ressuprimento; Processo de Separação de Produtos	1
Impressora de Etiquetas Datamax i4208	Analista de Suporte	Impressora utilizada para a impressão de etiquetas de Packing	Suporte e Infraestrutura	Equipamento fixo	Hardware	Média	Processo de Packing	6
Microcomputador de Faturamento	Analista de Suporte	Computador utilizado para integração de embarques e emissão de Nota Fiscal	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Média	Website BNDES; Website Sefaz RS; Website Sintegra.gov; Website Suframa; Processo de Faturamento	2
Telefone	Coordenador de TI	Telefone utilizado para comunicação interna e externa	Suporte e Infraestrutura	Interface de comunicação	Rede	Baixa		6
Central Telefônica Ericson	Coordenador de TI	Equipamento responsável por gerenciar e executar a telefonia da empresa	Suporte e Infraestrutura	Interface de comunicação	Rede	Média	Telefone; Cabo de 30 pares Central > Apoio	6
Rede da Sala da Expedição	Coordenador de TI	Conexão de rede para os micros da sala da expedição	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Alta	Processo de Faturamento	4
Impressora Laser Samsung Scx5835	Coordenador de TI	Impressora para impressão de Notas Fiscais e demais documentos	Suporte e Infraestrutura	Equipamento fixo	Hardware	Baixa	Processo de Emissão de Nota Fiscal	8
Switch Gerenciável 3com (Apoio)	Coordenador de TI	Switch responsável pela conexão de Rede dos ativos da Expedição com o Data Center Empresa	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Rede da Sala da Expedição; Roteador rede Wireless Motorola W2000	2
Fibra Óptica Apoio > Data Center	Coordenador de TI	Cabo de fibra óptica interligando o Switch da Rede Apoio (expedição) com o Switch Core no Data Center	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Faturamento	2
Switch Core de Rede 3com 4200G	Coordenador de TI	Switch Responsável por gerenciar toda a rede da Empresa	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Faturamento	1
Distribuidor Óptico Data Center	Coordenador de TI	Distirbuidor do cabeamento de Fibra Óptica, receptor de todos os Racks da empresa	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Faturamento	2
Firewall Sonic Wall	Coordenador de TI	Firewall de rede e controlador do acesso a Internet	Suporte e Infraestrutura	Equipamento fixo	Hardware	Média	Processo de Emissão de Nota Fiscal; Link de Internet Telecom SA 10 Mbps	4
Conversor de Fibra Óptica Internet Data Center	Coordenador de TI	Conversor de Fibra Optica para Ethernet que liga o Firewall com a Fibra Óptica do link de internet	Suporte e Infraestrutura	Interface de comunicação	Rede	Média	Processo de Emissão de Nota Fiscal	4
Distribuidor Óptico Administrativo	Coordenador de TI	Distribuidor Óptico que distribui as fibras no Rack do administrativo. Redes da área de Vendas, Administrativo e Link de Internet	Suporte e Infraestrutura	Interface de comunicação	Rede	Média	Processo de Emissão de Nota Fiscal	2
Fibra Óptica Comercial > Data Center	Coordenador de TI	Fibra Óptica que liga a rede do Administrativo e Comercial com o Data Center	Suporte e Infraestrutura	Interface de comunicação	Rede	Média		4
Fibra Óptica Link Internet > Data Center	Coordenador de TI	Cabo de fibra óptica que liga o Link de Internet (que está no administrativo) com o Data Center	Suporte e Infraestrutura	Interface de comunicação	Rede	Média	Processo de Emissão de Nota Fiscal; Link de Internet Telecom SA 10 Mbps; Conversor de Fibra Óptica Internet Administrativo; Conversor de Fibra Óptica Internet Data Center	4
Cabeamento Ethernet para Link de Internet	Coordenador de TI	Cabeamento de rede para conexão dos equipamentos do Link de Internet	Suporte e Infraestrutura	Interface de comunicação	Rede	Média		4
Conversor de Fibra Óptica Internet Administrativo	Coordenador de TI	Conversor de Ethernet para a Fibra Óptica que liga o Link de Internet com o Data Center	Suporte e Infraestrutura	Interface de comunicação	Rede	Baixa	Processo de Emissão de Nota Fiscal	4
Roteador de Internet	Coordenador de TI	Roteador da operadora Telecom SA responsável pelo link de internet	Suporte e Infraestrutura	Equipamento fixo	Hardware	Média	Processo de Emissão de Nota Fiscal	6
Receptor de Link Telecom SA	Coordenador de TI	Modem da operadora Telecom SA que recebe a conexão de Internet e Telefonia	Suporte e Infraestrutura	Equipamento fixo	Hardware	Média	Processo de Emissão de Nota Fiscal	6
DG de telefonia Apoio	Coordenador de TI	Distribuidor de Telefonia instalado na sala de Apoio, distribui os ramais para a Expedição.	Suporte e Infraestrutura	Interface de comunicação	Rede	Baixa	Cabo de 30 pares Central > Apoio	8
Cabo de 30 pares Central > Apoio	Coordenador de TI	Cabo de telefonia que interliga a Central Telefonica com o DG da sala de apoio	Suporte e Infraestrutura	Interface de comunicação	Rede	Baixa		8
Switch Gigabit 3com (CTT)	Coordenador de TI	Switch responsavel por gerenciar a rede do CTT, utilizada pela equipe de TI e Egenharia	Suporte e Infraestrutura	Interface de comunicação	Rede	Baixa		8
Cabo de conexão Ethernet CTT > Data Center	Coordenador de TI	Cabo Ethernet Cat6 que liga o Switch do CTT com o Switch do Data Center	Suporte e Infraestrutura	Interface de comunicação	Rede	Baixa		8

Notebook TI	Coordenador de TI	Notebook do coordenador de TI	Suporte e Infraestrutura	Equipamento móvel	Hardware	Média		6
Notebook Gerência	Coordenador de TI	Notebook do Gerente de Logística	Suporte e Infraestrutura	Equipamento móvel	Hardware	Baixa		48
Rack de comunicação Apoio	Coordenador de TI	Rack de armazenamento dos equipamentos de Rede da sala de Apoio	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Baixa	Fibra Óptica Apoio > Data Center; Switch Gerenciável 3com (Apoio); Roteador rede Wireless Motorola W2000; Rede da Sala da Expedição	12
Rack de telefonia Administrativo	Coordenador de TI	Rack para armazenamento dos equipamentos de Internet da operadora e demais switches da área de Vendas e Administrativo	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Baixa	Cabeamento Ethernet para Link de Internet; Conversor de Fibra Óptica Internet Administrativo; Distribuidor Óptico Administrativo; Receptor de Link Telecom SA; Roteador de Internet; Switch Gerenciável 3com (Adm); Processo de Emissão de Nota Fiscal	12
Rack de telefonia CTT	Coordenador de TI	Rack para armazenamento dos equipamentos da rede do CTT	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Baixa	Switch Gigabit 3com (CTT)	12
Rack de Servidores do Data Center	Coordenador de TI	Rack de armazenamento com fonte de alimentação, de todos os servidores e demais ativos presentes no Data Center da empresa	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Média	Cabeamento Ethernet para SAN no Data Center; Conversor de Fibra Óptica Internet Data Center; Distribuidor Óptico Data Center; SERVERPROG - Servidor HP DL 380 p/ Banco de Dados; Firewall Sonic Wall; Processo de Faturamento; Servidor de Backup em Disco - BKPSERVER26; Servidor Dell Power Edge R610 - HOST1 e HOST2; Servidor Físico de Licenças Datasul - BKPSERVER07; Storage de Dados Dell MD3000i; Switch Core de Rede 3com 4200G; Switch SAN Dell 5424; Unidade de Fital Dell LTO-4	1
No-Break Primário para Data Center	Coordenador de TI	NoBreak responsável por estabilizar a energia elétrica do Data Center e mantê-lo na ausência de energia externa.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Alta	Processo de Faturamento	1
No-Break secundário para Data Center	Coordenador de TI	No Break reserva para Data Center. Também utilizado como no-break geral do CTT.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Média	Processo de Faturamento	6
Energia Elétrica Externa	Coordenador de Manutenção	Fornecimento de energia elétrica externa pela RGE.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Baixa	Processo de Faturamento;#94	3
Sala da Expedição	Gerente de Logística	Sala de trabalho da expedição. Compreende também os móveis nela contidos como mesas e cadeiras.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Média	Rede da Sala da Expedição; Microcomputador de Faturamento; Telefone; Impressora de Etiquetas Datamax i4208; Impressora Laser Samsung Scx5835	24
Sala do Data Center	Coordenador de TI	Sala segura para armazenamento dos Servidores da empresa. A Sala possui Ar Condicionado e Controle de Acesso	Suporte e Infraestrutura	Edificações	Instalações físicas e localidade	Média	Rack de Servidores do Data Center; Ar Condicionado da Sala do Data Center	12
Sala dos No-Breaks	Gerente de Engenharia	Sala para armazenamento dos No-Breaks do CTT, que sustentam o Data Center. A Sala possui ar condicionado.	Suporte e Infraestrutura	Edificações	Instalações físicas e localidade	Média	No-Break Primário para Data Center; No-Break secundário para Data Center; Rack de telefonia CTT; Ar Condicionado da Sala dos No-Breaks	24
Ar Condicionado da Sala dos No-Breaks	Coordenador de TI	Ar Condicionado para esfriar os NoBreaks que sustentam o Data Center. Aumenta a vida útil dos equipamentos.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Baixa		72
Ar Condicionado da Sala do Data Center	Coordenador de TI	Ar Condicionado para refrigeramento dos Servidores da Empresa. Crítico para manter os equipamentos em funcionamento.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Alta		12
Switch SAN Dell 5424	Coordenador de TI	Switch utilizado para conectar os Servidores Físicos no Storage de Dados da empresa	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Faturamento; Cabeamento Ethernet para SAN no Data Center	2

Storage de Dados Dell MD3000i	Coordenador de TI	Storage de armazenamento de dados de toda a empresa. Extremamente crítico.	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Alta	Processo de Faturamento; DNS Linux - Servidor Virtual DNSLINUX; Microsoft Active Directory - Servidor Virtual ADVIRTUAL05 e ADVIRTUAL19; Microsoft Exchange 2010 - Servidor Virtual EXCHANGE2010; Microsoft File Server - Servidor Virtual SERVER18; Microsoft Share Point - Servidor Virtual SP2010; SQL Server 2012 - Servidor Virtual SQLDB2012; Totvs TSS NFe - Servidor Virtual NFETSS; ERP14 - Servidor virtual de aplicações ERP; SERVERTS - Servidor virtual para acesso TS dos coletores de dados; Xen Server; Banco de Dados Progress - Datasul EMS	1
Servidor Dell Power Edge R610 - HOST1 e HOST2	Coordenador de TI	Servidores Físicos para processamento do ambiente Virtual da empresa.	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Alta	Xen Server; Processo de Faturamento	4
Cabeamento Ethernet para SAN no Data Center	Coordenador de TI	Cabeamento Ethernet Categoria 6 para utilização da Rede SAN entre Storage e Servidores	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Faturamento	2
SERVERPROG - Servidor HP DL 380 p/ Banco de Dados	Coordenador de TI	Servidor Linux CentOS de banco de dados Progress para rodar o ERP da empresa	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Alta	Banco de Dados Progress - Datasul EMS; Processo de Faturamento	1
ERP14 - Servidor virtual de aplicações ERP	Coordenador de TI	Servidor virtual onde estão armazenados os programas do ERP Datasul EMS e WMS	Suporte e Infraestrutura	Aplicações de negócio específicas	Aplicações de negócio	Alta	Datasul EMS; Processo de Faturamento	2
SERVERTS - Servidor virtual para acesso TS dos coletores de dados	Coordenador de TI	Servidor virtual Windows utilizado para rodar o sistema nos coletores de dados através de TS	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Alta	WMS; Processo de Separação de Produtos	2
Microsoft Active Directory - Servidor Virtual ADVIRTUAL05 e ADVIRTUAL19	Coordenador de TI	Servidor Windows responsável pelo gerenciamento dos usuários e da rede Microsoft na empresa.	Suporte e Infraestrutura	Software de serviço, manutenção ou administração	Software	Alta	Processo de Faturamento	4
Microsoft File Server - Servidor Virtual SERVER18	Coordenador de TI	Servidor para armazenamento de documentos e arquivos do processo	Suporte e Infraestrutura	Mídia de dados	Hardware	Média	IT0032 - Processo de Expedição; Plano de Continuidade de Negócios; Diretório de Rede da Logística	12
Link de Internet Telecom SA 10 Mbps	Coordenador de TI	Link de Internet da operadora Telecom SA com velocidade de 10 Mbps. Necessário para a emissão de NFe	Suporte e Infraestrutura	Serviços de infraestrutura	Instalações físicas e localidade	Alta	Processo de Emissão de Nota Fiscal	4
Totvs TSS NFe - Servidor Virtual NFETSS	Coordenador de TI	Servidor que roda o sistema TSS da Totvs, responsável pelo envio e autorização da Nota Fiscal Eletrônica	Primário	Aplicações de negócio específicas	Aplicações de negócio	Alta	Totvs TSS NFe - Sistema de emissão de Nota Fiscal Eletrônica; Processo de Emissão de Nota Fiscal	4
Datasul EMS	Coordenador de TI	Sistema ERP Datasul EMS206 , utilizado para operar todo o processo de negócio	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Alta	WMS; Processo de Faturamento	1
WMS	Coordenador de TI	Módulo WMS para gestão do armazem, pertencente ao ERP Totvs Datasul EMS	Suporte e Infraestrutura	Aplicações de negócio específicas	Aplicações de negócio	Alta	Processo de Separação de Produtos; Processo de Ressuprimento; Processo de Packing	2
Servidor Físico de Licenças Datasul - BKPSERVER07	Coordenador de TI	Servidor que roda o Servidor de Licenças Datasul EMS e o Data Protector	Suporte e Infraestrutura	Software de serviço, manutenção ou administração	Software	Média	Hardlock de Licenças Datasul; Data Protector; License Server Datasul; Unidade de Fital Dell LTO-4; Processo de Faturamento	48
Hardlock de Licenças Datasul	Coordenador de TI	Hardlock que controla as licenças do ERP Datasul EMS e todo ambiente Totvs. NEcessita estar conectado no servidor de licenças.	Suporte e Infraestrutura	Equipamento móvel	Hardware	Média	Processo de Faturamento	24
HP Data Protector	Coordenador de TI	Software de Backup HP Data Protector. Roda o Backup do ambiente e está instalado no Servidor BKPSERVER07.	Suporte e Infraestrutura	Software de serviço, manutenção ou administração	Software	Média	Backup do WMS	48
Unidade de Fital Dell LTO-4	Coordenador de TI	Unidade de fita LTO-4 para backup. Gerenciada pelo HP Data Protector	Suporte e Infraestrutura	Equipamento fixo	Hardware	Média	Backup do WMS	48
Mídias de Backup LTO-4	Coordenador de TI	Mídia de fita LTO4 (800gb) para armazenamento do Backup diário. São armazenadas no Cofra e uma cópia é mantida com o CFO.	Suporte e Infraestrutura	Mídia de dados	Hardware	Alta	Backup do WMS	24
Servidor de Backup em Disco - BKPSERVER26	Coordenador de TI	Servidor onde o Data Protector armazena o Backup em Disco das Máquinas Virtuais e dos dados da empresa. Está instalado no setor Administrativo.	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Média	Backup do WMS	24
Switch Gerenciável 3com (Adm)	Coordenador de TI	Switch que gerencia a rede do Administrativo.	Suporte e Infraestrutura	Interface de comunicação	Rede	Média		12
DNS Linux - Servidor Virtual DNSLINUX	Coordenador de TI	Servidor de DNS externo Linux CentOS para comunicação com endereos externos.	Suporte e Infraestrutura	Serviços de infraestrutura	Instalações físicas e localidade	Média	Processo de Emissão de Nota Fiscal	12
Xen Server	Coordenador de TI	Software para gerenciamento dos servidores Virtuais.	Suporte e Infraestrutura	Software de serviço, manutenção ou administração	Software	Média	Processo de Faturamento	24

Microsoft Exchange 2010 - Servidor Virtual EXCHANGE2010	Coordenador de TI	Servidor de Emails interno para comunicação com fornecedores e clientes	Suporte e Infraestrutura	Software de serviço, manutenção ou administração	Software	Média	Processo de Emissão de Nota Fiscal	12
Empilhadeira Elétrica	Coordenador de Expedição	Empilhadeira para realizar armazenamento, separação de pulmão e ressuprimento.	Suporte e Infraestrutura	Equipamento móvel	Hardware	Alta	Processo de Separação de Produtos; Processo de Ressuprimento	8
Empilhadeira a Gás	Coordenador de Expedição	Empilhadeira a gás utilizada para carregar os produtos faturados nos caminhões das transportadoras. Não pode ser utilizada no interior da expedição.	Suporte e Infraestrutura	Equipamento móvel	Hardware	Média	Processo de Separação de Produtos; Processo de Ressuprimento	8
Website Sintegra.gov	Coordenador de TI	Website http://www.sintegra.gov.br utilizado para validação de clientes quanto a CNPJ, endereço e IE	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Média	Processo de Emissão de Nota Fiscal	24
Website Sefaz RS	Coordenador de TI	Website https://www.sefaz.rs.gov.br/NFE/NFE-COM.aspx - utilizado para Consulta de NF-e completa e Carta de Correção;	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Média	Processo de Emissão de Nota Fiscal	4
Website BNDES	Coordenador de TI	Website https://www.cartaobndes.gov.br/cartaobndes/ - Implantação de pedidos no BNDES;	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Média	Processo de Emissão de Nota Fiscal	12
Website Suframa	Coordenador de TI	Website https://servicos.suframa.gov.br/servicos/ - Consulta de situação cadastral na SUFRAMA e realização do PIN;	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Média	Processo de Emissão de Nota Fiscal	4
Estabilizador 1000Va	Coordenador de TI	Estabilizador para ligar as impressoras na rede de energia 220v.	Suporte e Infraestrutura	Equipamento móvel	Hardware	Baixa	Processo de Emissão de Nota Fiscal	12
Eitquetas de Packing	Coordenador de Expedição	Etiquetas para identificar os produtos separados na transportadora.	Suporte e Infraestrutura	Outros tipos de mídia	Hardware	Baixa	Processo de Packing	8
Paleteira manual	Coordenador de Expedição	Equipamento para realizar separação em área de picking	Suporte e Infraestrutura	Equipamento móvel	Hardware	Média	Processo de Separação de Produtos	24
Embaladora Strech	Coordenador de Expedição	Maquina utilizada para embalar os pallets com os produtos separados antes de serem embarcados.	Suporte e Infraestrutura	Equipamento fixo	Hardware	Média	Processo de Separação de Produtos; Plástico Strech	4
Faturista	Coordenador de Expedição	Funcionário responsável pela geração dos embarques e faturamento dos produtos separados.	Primário	Usuários	Recursos humanos	Alta	Processo de Faturamento	1
Armazem	Coordenador de Expedição	Estrutura física para armazenamento dos produtos em estoque.	Primário	Edificações	Instalações físicas e localidade	Alta	Processo de Faturamento; DG de telefonia Apoio; Embaladora Strech; Empilhadeira a Gás; Empilhadeira Elétrica; No-Break da Área de Apoio; Paleteira manual; Pallets de separação; Plástico Strech; Prateleiras Endereçadas; Rack de comunicação Apoio; Sala da Expedição	1
Prateleiras Endereçadas	Coordenador de Expedição	PRateleiras enderaçadas para armazenamento dos produtos em estoque dentro do armazem. Essencial para o processo atual.	Suporte e Infraestrutura	Edificações	Instalações físicas e localidade	Alta		4
Coordenador de Expedição	Gerente de Logística	Pessoa responsável pela gestão da expedição e seus funcionários. Direciona os objetivos do setor.	Primário	Usuários	Recursos humanos	Média		12
Analista de Suporte	Coordenador de TI	Equipe de TI para fornecer suporte e manutenção no sistema.	Suporte e Infraestrutura	Usuários	Recursos humanos	Baixa		48
Gerente de Logística	Diretor Financeiro	Gerente responsável pela tomada de decisão	Primário	Tomador de decisão	Recursos humanos	Baixa		48
Pallets de separação	Coordenador de Expedição	Pallet necessário para alocar os produtos separados durante o processo de separação.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Alta	Expedidor	1
Transportador	Coordenador de Expedição	Transportador contratado para a expedição do produto	Suporte e Infraestrutura	Serviços de infraestrutura	Instalações físicas e localidade	Baixa		24
Plástico Strech	Coordenador de Expedição	Plastico utilizado para organizar os pallets no caminhão.	Suporte e Infraestrutura	Meio físico e infraestrutura	Rede	Média		24
Processo de Separação de Produtos	Coordenador de Expedição	Processo base de separação de produtos conforme embarques liberados	Primário	Processos e atividades de negócio	Primário	Alta	Processo de Packing; Processo de Ressuprimento	1
Ressuprimento de área de picking	Coordenador de Expedição	Sub-Processo de ressuprimento de área de picking, necessário para a realimentação das áreas de separação.	Primário	Processos e atividades de negócio	Primário	Alta	Processo de Separação de Produtos	1
IT0032 - Processo de Expedição	Coordenador de Expedição	IT que descreve o processo de Expedição nos padrões da gestão da qualidade	Suporte e Infraestrutura	Outros tipos de mídia	Hardware	Baixa	Processo de Faturamento	24
Plano de Continuidade de Negócios	Coordenador de TI	Plano de continuidade de negócios disponibilizado no Microsoft Share Point	Suporte e Infraestrutura	Aplicações de negócio específicas	Aplicações de negócio	Baixa	Microsoft Share Point - Servidor Virtual SP2010; SQL Server 2012 - Servidor Virtual SQLDB2012	4
Microsoft Share Point - Servidor Virtual SP2010	Coordenador de TI	Servidor Sharepoint para disponibilização do plano de continuidade de negócios	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Média	Plano de Continuidade de Negócios	48

Microsoft Office	Coordenador de TI	Pacote Office para edição de documentos e impressão	Suporte e Infraestrutura	Software de pacote ou de prateleira	Software	Média	Processo de Faturamento	12
SQL Server 2012 - Servidor Virtual SQLDB2012	Coordenador de TI	Banco de dados Microsoft SQL Server 2012 utilizado pelo SharePoint.	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Baixa		24
Microsoft EOpen	Coordenador de TI	Website com acesso às licenças Microsoft e Downloads das mídias dos produtos Microsoft.	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Baixa		
Arquivo de Senhas de Acesso aos sistemas de administração	Coordenador de TI	Documento contendo as senhas de acesso administrativo ao ambiente tecnológico da empresa	Suporte e Infraestrutura	Outros tipos de mídia	Hardware	Média		4
No-Break da Área de Apoio	Coordenador de Manutenção	No Break responsável por estabilizar a rede elétrica 110v da Expedição	Suporte e Infraestrutura	Equipamento fixo	Hardware	Alta	Processo de Faturamento	2
Totvs TSS NFe - Sistema de emissão de Nota Fiscal Eletrônica	Coordenador de TI	Sistema Datasul para envio de nota fiscal eletrônica e autorização na SEFAZ	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Alta	Processo de Emissão de Nota Fiscal	2
Processo de Faturamento	Coordenador de Expedição	Processo de geração do embarque, separação e emissão de nota fiscal.	Primário	Processos e atividades de negócio	Primário	Alta	Processo de Emissão de Nota Fiscal; Processo de Ressuprimento; Processo de Separação de Produtos	1
Processo de Emissão de Nota Fiscal	Coordenador de Expedição	Processo de emissão de Nota Fiscal Eletrônica após separação.	Primário	Processos e atividades de negócio	Primário	Alta		2
Processo de Ressuprimento	Coordenador de Expedição	Processo de ressuprimento da área de picking, essencial para a separação	Primário	Processos e atividades de negócio	Primário	Alta		4
Processo de Packing	Coordenador de Expedição	Processo de emissão de etiquetas de Packing, pertencente ao processo de separação.	Primário	Processos e atividades de negócio	Primário	Média		8
Banco de Dados Progress - Datasul EMS	Coordenador de TI	Banco de dados utilizado pelo ERP da empresa	Suporte e Infraestrutura	Aplicações de negócio específicas	Aplicações de negócio	Alta	Processo de Faturamento	1
Infra Estrutura de Virutalização	Coordenador de TI	Estrutura para executar os processos de TI para o negócio da empresa	Suporte e Infraestrutura	Equipamento de processamento de dados	Hardware	Alta	Storage de Dados Dell MD3000i; Switch SAN Dell 5424; Servidor Dell Power Edge R610 - HOST1 e HOST2; Processo de Faturamento	1
Diretório de Rede da Logística	Coordenador de TI	Documentos e ativos relacionados a Expedição	Suporte e Infraestrutura	Outros tipos de mídia	Hardware	Média	Processo de Faturamento	12
License Server Datasul	Coordenador de TI	Servidor de licenciamento EMS , necessário para Login no sistema.	Suporte e Infraestrutura	Aplicações de negócio padronizadas	Aplicações de negócio	Média	Processo de Faturamento	8
Backup do WMS	Coordenador de TI	Backup do banco de dados e arquivos relacionados ao WMS	Suporte e Infraestrutura	Mídia de dados	Hardware	Média		24
Equipe de Expedição	Coordenador de Expedição	Equipe para operação do processo de negócio	Suporte e Infraestrutura	Usuários	Recursos humanos	Alta	Expedidor; Faturista; Coordenador de Expedição; Analista de Suporte; Gerente de Logística	1
Gestão do ambiente de TI	Coordenador de TI	PRocesso de gerenciamento das operações de TI relacionadas ao processo WMS	Primário	Informação	Primário	Média	Arquivo de Senhas de Acesso aos sistemas de administração; Analista de Suporte; Backup do WMS	12
Antenas amplificadoras de sinal Wifi	Coordenador de TI	Antenas replicadoras de sinal Wireless. São 4 antenas que abrangem todo o armazém.	Suporte e Infraestrutura	Interface de comunicação	Rede	Alta	Processo de Separação de Produtos	8

Item 4.1. RISCOS									
Ativo	**SLA**	**Ameaça**	**Tipo de ameaça**	**Origem**	**Vulnerabilidade**	**Consequência**	**Impacto**	**Probabilidade**	**Nível**
Sala da Expedição; Sala do Data Center; Sala dos No-Breaks; Rack de telefonia Administrativo; Central Telefônica Ericson	24; 12; 24; 12; 60	Queda de energia	Dano físico	Acidental	Baixa autonomia dos No-Breaks	Interrupção do funcionamento dos Servidores	Alto	Média	Médio
Link de Internet Telecom SA 10 Mbps	40;	Falha no Link de Internet	Paralisação de serviços essenciais	Acidental	Ausência de Link de Internet	Interrupção da emissão de Nota Fiscal Eletrônica	Alto	Baixa	Médio
Roteador rede Wireless Motorola W2000	10;	Falha no equipamento	Falhas técnicas	Acidental; Intencional	Equipamento não possui redundância interna e externa	Interrupção do processo de separação	Alto	Baixa	Médio
Roteador rede Wireless Motorola W2000	10;	Falha de comunicação com Data Center	Falhas técnicas	Acidental; Intencional; Natural	Ambiente físico sem proteção eficiente	Interrupção do processo de separação	Alto	Baixa	Médio
Servidor Físico de Licenças Datasul - BKPSERVER07	48;	Indisponibilidade do Servidor de Licenças	Paralisação de serviços essenciais	Acidental; Intencional	Servidor de licenças não possui redundância	Falha de acesso ao sistema Datasul	Médio	Média	Médio
Hardlock de Licenças Datasul	24;	Indisponibilidade física do Hardlock (furto)	Ações não autorizadas	Intencional	Baixa segurança na sala do Data Center	Falha de acesso ao sistema Datasul	Baixo	Baixa	Baixo
Switch Core de Rede 3com 4200G	10;	Falha do Switch Principal de Rede	Falhas técnicas	Acidental; Intencional	Equipamento não possui redundância externa	Interrupção do serviço de rede e todos os acessos a sistema.	Alto	Baixa	Médio
Central Telefônica Ericson	60;	Falha na Central Telefônica	Falhas técnicas	Acidental; Intencional; Natural	Central telefônica muito antiga e com pouca segurança	Parada do serviço de telefonia da empresa	Baixo	Média	Baixo
Coletor de dados Motorola	20;	Falha no coletor de dados	Dano físico	Acidental; Intencional	Coletores de dados são resistentes mas suscetíveis a falha	Interrupção do processo de separação	Alto	Média	Alto
Coletor de dados Motorola	20;	Coletor não acessa o sistema após troca de bateria	Paralisação de serviços essenciais	Acidental	Coletor de dados não salva as conexões com o sistema	Impossibilidade de acessar o sistema pelo coletor	Alto	Média	Médio
Coletor de dados Motorola	20;	Falta de bateria no coletor	Paralisação de serviços essenciais	Acidental; Intencional	Coletor de dados depende da bateria de LiOn para funcionamento	Interrupção do processo de separação	Alto	Baixa	Médio
Microcomputador de Faturamento	20;	Queima de Fonte de Alimentação	Dano físico	Acidental; Intencional	Computador com fonte única	Interrupção do uso do computador	Médio	Média	Baixo
Microcomputador de Faturamento	20;	Falha no Sistema operacional	Falhas técnicas	Acidental; Intencional	Sistema operacional Windows apresenta problemas com o tempo de uso e atualizações	Interrupção ou retardo do uso do computador	Médio	Média	Médio
No-Break da Área de Apoio	20;	Falha no No-Break da Área de Apoio	Falhas técnicas	Acidental; Intencional; Natural	Único No-Break responsável pela rede da área de Expedição	Interrupção do processo de separação	Alto	Baixa	Médio
No-Break Primário para Data Center	10;	Falha no No-Break primário do Data Center	Falhas técnicas	Acidental; Intencional	Equipamento vulnerável a falhas, acesso irrestrito ao no-break	Interrupção do fornecimento de energia ao Data Center, forçando o uso dos equipamentos em meia carga. Interrompe o funcionamento do Servidor de Licenças.	Alto	Baixa	Médio
No-Break secundário para Data Center	60;	Falha no No-Break secundário do Data Center	Falhas técnicas	Acidental; Intencional	Equipamento vulnerável a falhas, acesso irrestrito ao no-break	Interrupção do fornecimento de energia ao CTT e ao Data Center, interrompendo o funcionamento dos micros do CTT.	Alto	Baixa	Médio
Firewall Sonic Wall	40;	Falha no Firewall	Falhas técnicas	Acidental; Intencional	Appliance sucetivel a falhas	Interrupção da conexão com a Internet, impedindo o processo de emissão de NFe	Alto	Baixa	Médio
Switch SAN Dell 5424	20;	Falha no Switch SAN	Falhas técnicas	Acidental; Intencional	Switches estão em atividade por mais de 3 anos.	Interrupção na comunicação entre Storage e Servidores. Interrupção dos processos de negócio.	Alto	Baixa	Médio
Distribuidor Óptico Data Center	20;	Rompimento de fibra interna	Dano físico	Acidental; Intencional	Fibra óptica muito sensível	Interrupção da conexão de rede	Alto	Baixa	Médio
Fibra Óptica Apoio > Data Center	20;	Rompimento de fibra óptica externa	Dano físico	Acidental; Intencional; Natural	Fibra óptica muito sensível	Interrupção da conexão de rede com o Data Center	Alto	Baixa	Médio
Conversor de Fibra Óptica Internet Data Center	40;	Falha no conversor de fibra óptica	Dano físico	Acidental; Intencional	Conversor de fibra é frágil e facilmente danificado	Interrupção da conexão com a Internet, impedindo o processo de emissão de NFe	Alto	Baixa	Médio
Impressora Laser Samsung Scx5835	80;	Falha na impressora de NFe	Dano físico	Acidental; Intencional	Impressora de uso continuo suscetivel a problemas	Interrupção na impressão de NFe	Médio	Média	Médio
Impressora de Etiquetas Datamax i4208	60;	Falha na impressora de etiquetas	Falhas técnicas	Acidental; Intencional	Impressora de uso continuo suscetivel a problemas elétricos ou trancamento do Ribbon	Interrupção da emissão de etiquetas de Packing	Médio	Média	Médio

Totvs TSS NFe - Servidor Virtual NFETSS	40;	Falha no sistema de NFe	Dano físico	Acidental; Intencional	Servidor de NFe suscetível a falhas	Interrupção do processo de emissão de Nota Fiscal	Alto	Baixa	Médio
Servidor Físico de Licenças Datasul - BKPSERVER07	48;	Reinicialização do servidor de Licenças	Comprometimento de funções	Acidental; Intencional	Servidor físico não consegue reestabelecer a operação automaticamente	Interrupção de novo Login no sistema EMS	Alto	Baixa	Médio
Expedidor; Faturista	50; 10;	Indisponibilidade de pessoal	Eventos naturais	Acidental; Intencional; Natural	Dependência de pessoas no processo	Retardo ou paralisação do processo	Alto	Baixa	Médio
SERVERPROG - Servidor HP DL 380 p/ Banco de Dados	10;	Espaço insuficiente de armazenamento em disco	Paralisação de serviços essenciais	Acidental	Espaço limitado em disco rígido	Interrupção do funcionamento do Sistema ERP da empresa	Alto	Baixa	Médio
Coletor de dados Motorola	20;	Estravio do coletor de dados	Ameaças humanos	Acidental; Intencional	Coletores são pequenos e fáceis de serem perdidos	Redução da operação e necessidade de aquisição de equipamentos	Médio	Média	Médio
Ar Condicionado da Sala do Data Center	12;	Falha no Ar Condicionado	Dano físico	Acidental; Intencional; Natural	Ar condicionado vulnerável a falhas técnicas	Super aquecimento e aumento da possibilidade de parada dos equipamentos do Data Center	Médio	Baixa	Médio
Pallets de separação	10;	Falta de Pallets para separação	Comprometimento de funções	Acidental; Intencional; Natural	Necessida da separação em Pallets individuais	Interrupção parcial do processo de separação	Alto	Baixa	Médio
Datasul EMS	10;	Erros no sistema EMS	Falhas técnicas	Acidental; Intencional	Sistema sujeito a falhas de programação ou tecnologia	Interrupção ou retardo dos processos de negócio	Alto	Média	Médio
Eitquetas de Packing	80;	Falta de etiquetas de packing	Comprometimento de funções	Acidental; Intencional	Necessidade de impressão de etiquetas para identificação de produtos	Aumento na margem de erro no transporte e entrega ao cliente	Médio	Baixa	Médio
Diretório de Rede da Logística	12;	Espaço insuficiente de armazenamento na rede	Comprometimento de funções	Acidental; Intencional	Espaço limitado em disco rígido	Impossibilidade de gravação ou alteração de arquivos na rede	Médio	Baixa	Baixo
Backup do WMS	24;	Falha no processo de Backup	Comprometimento da informação	Acidental; Intencional	Alto tráfego de dados em um curto espaço de tempo	Inutilização do backup diário	Alto	Baixa	Médio
Banco de Dados Progress - Datasul EMS	10;	Usuário trancado no EMS	Paralisação de serviços essenciais	Acidental	Usuários do sistema só podem estar logados uma unica vez	Impossibilidade de entrar no sistema com o usuário	Alto	Média	Médio
Datasul EMS	10;	Sistema sem licenças disponiveis	Comprometimento de funções	Acidental; Intencional	Sistema possui limite de 30 licenças de acesso	Impossibilidade de acessar o sistema	Alto	Baixa	Médio
Totvs TSS NFe - Sistema de emissão de Nota Fiscal Eletrônica	20;	Nota fiscal rejeitada na SEFAZ	Paralisação de serviços essenciais	Acidental; Intencional	Possibilidade de erros em cadastro ou na emissão de nota fiscal	Rejeição de notas fiscais impedindo faturamento	Alto	Média	Médio
Estabilizador 1000Va	12;	Queima de estabilizador	Dano físico	Acidental; Intencional; Natural	Estabilizador vulnerável a instabilidade da rede, tempo e exposto a contato humano	Parada do fornecimento de energia as impressoras	Alto	Baixa	Médio
Empilhadeira Elétrica	80;	Esgotamento de bateria da empilhadeira	Paralisação de serviços essenciais	Natural	Empilahdeira elétrica depende de bateria	Interrupção do processo de separação	Médio	Baixa	Médio
Empilhadeira a Gás	80;	Falta de gás na empilhadeira	Comprometimento de funções	Natural	Empilhadeira a gás depende de combustível	Redução de desempenho no processo de faturamento	Médio	Baixa	Médio
Impressora Laser Samsung Scx5835	80;	Falta de Tonner	Paralisação de serviços essenciais	Natural	Impressora depende de Tonner para imprimir	Interrupção na impressão de NFe	Médio	Baixa	Médio
Microsoft Active Directory - Servidor Virtual ADVIRTUAL05 e ADVIRTUAL19	40;	Falha no Active Directory	Falhas técnicas	Acidental; Intencional	Servidores de Active Directory são sujeitos a falhar	Interrupção do acesso a rede e todos seus sistemas	Alto	Baixa	Médio
ERP14 - Servidor virtual de aplicações ERP	20;	Falha no servidor Datasul ERP14	Falhas técnicas	Acidental	Servidor Windows sujeito a falhas	Impossibilidade de acessar o sistema EMS	Alto	Baixa	Médio
Storage de Dados Dell MD3000i	10;	Falha em controladora/fonte do Storage de Dados	Dano físico	Acidental; Intencional; Natural	Cada controladora do Storage possui uma unica fonte de alimentação	Redução do processamento no Storage	Médio	Baixa	Médio
Storage de Dados Dell MD3000i	10;	Falha em ambas controladoras do Storage	Dano físico	Acidental	Storage depende das controladoras para funcionamento	Interrupção total do ambiente de TI da empresa e possibilidade de corrupção na base de dados.	Alto	Baixa	Médio
Storage de Dados Dell MD3000i	10;	Corrupção da base de dados do Storage	Falhas técnicas	Acidental; Intencional	Base de dados vulnerável a danos em caso de desligamento acidental do Storage	Corrupção da base de dados das VM, impossibilitando sua recuperação normal	Alto	Média	Alto
Servidor Dell Power Edge R610 - HOST1 e HOST2	40;	Falha no Servidor de Virtualização	Falhas técnicas	Acidental	Estrutura de TI dependente de Hardware Físico	Interrupção do acesso a rede e todos seus sistemas	Alto	Baixa	Médio
SERVERTS - Servidor virtual para acesso TS dos coletores de dados	20;	Falha no servidor de TS	Falhas técnicas	Acidental; Intencional	Dependência de único servidor para acesso a TS pelos coletores	Impossibilidade de acessar o sistema pelo coletor	Alto	Média	Médio
Unidade de Fital Dell LTO-4; Mídias de Backup LTO-4	48; 24;	Falha na unidade de Fita	Falhas técnicas	Acidental	Backup diário ocorre somente em fita	Backup diário não realizado	Alto	Média	Alto
Xen Server	24;	Interrupção acidental dos servidores virtuais	Paralisação de serviços essenciais	Acidental; Intencional	Servidores administrados pelo Xen Center podem ser desligados por quem tem acesso a Console	Interrupção de servidores e serviços de rede/sistemas	Alto	Média	Alto

Banco de Dados Progress - Datasul EMS	10;	Interrupção acidental do banco de dados	Ameaças humanos	Acidental; Intencional	Os scripts de manutenção do banco de dados Progress permitem que os bancos sejam derrubados	Impossibilidade de acessar o sistema	Alto	Média	Médio
Link de Internet Telecom SA 10 Mbps	40;	Invasão virtual de terceiros	Ações não autorizadas	Intencional	Acesso a internet traz consigo a possibilidade de invasão	Danos ao ambiente da empresa	Alto	Média	Alto
HP Data Protector	48;	Restauração de backup com falhas	Falhas técnicas	Acidental	Frequência de teste de restauração muito baixa	Possibilidade de não conseguir restaurar o backup quando necessário	Alto	Baixa	Médio
Storage de Dados Dell MD3000i	10;	Falha geral do Storage	Dano físico	Acidental	Término da garantia do Hardware atual	Dificuldade no reparo do Hardware em caso de falha	Alto	Média	Alto
Banco de Dados Progress - Datasul EMS	10;	Parada do banco de dados Progress	Falhas técnicas	Acidental; Intencional	Servidor antigo e vulnerável a falha de sistema	Impossibilidade de acessar o sistema	Alto	Baixa	Médio
Servidor Dell Power Edge R610 - HOST1 e HOST2	40;	Falha parcial em servidor de virtualização	Dano físico	Acidental; Intencional; Natural	Estrutura de TI dependente de Hardware Físico	Queda de desempenho dos sistemas de rede	Médio	Baixa	Médio
Microsoft Exchange 2010 - Servidor Virtual EXCHANGE2010	12;	Falha no servidor de E-mail	Falhas técnicas	Acidental	Servidor único interno para gerenciamento e hospedagem de E-mail	Interrupção no envio e recebimento de E-mail	Médio	Baixa	Médio
Microsoft Exchange 2010 - Servidor Virtual EXCHANGE2010	12;	Base do Exchange corrompida	Falhas técnicas	Acidental; Intencional	Base de dados sujeita a falha após ocorrência de falhas	Perda total do serviço e base de E-mail	Alto	Baixa	Médio
Banco de Dados Progress - Datasul EMS	10;	Corrompimento da base de dados do EMS	Dano físico	Acidental	Fragilidade da base em caso de muitas falhas consecutivas	Perda total do banco de dados	Alto	Baixa	Alto
Roteador rede Wireless Motorola W2000	10;	Desconfiguração da rede Wireless	Paralisação de serviços essenciais	Acidental	Existência de único equipamento para gerenciar a rede Wireless	Interrupção do processo de separação	Alto	Baixa	Alto
Antenas amplificadoras de sinal Wifi	80;	Falha nas antenas WiFi	Dano físico	Acidental; Intencional; Natural	Antenas vulneráveis a falhas	Interrupção parcial da rede Wifi	Médio	Baixa	Médio
Sala dos No-Breaks	24;	Alteração não autorizada nos NoBreaks	Ações não autorizadas	Acidental; Intencional	Acesso irrestrito à sala dos NoBreaks	Interrupção no fornecimento de energia ao DataCenter	Alto	Média	Alto
Microcomputador de Faturamento; Infra Estrutura de Virutalização	20; 10;	Ameaça de Virus	Comprometimento da informação	Acidental; Intencional	Sistema operacional Windows vulnerável a Virus	Danos no sistema operacional	Médio	Média	Médio
Sala do Data Center	12;	Incêndio	Dano físico	Acidental; Intencional	Sala do Data Center não possui sistema anti-incêndio	Interrupção total da infraestrutura de TI e dano permanente nos equipamentos	Alto	Baixa	Médio

Item 5.1. AÇÕES DE TRATAMENTO DOS RISCOS											
Plano de Continuidade	Ameaça	Vulnerabilidade	Consequência	Ação	Tipo de tratamento	Responsável	Requer investimento?	Valor	Aprovado?	Justificativa	Prazo de implementação
Faturamento e Expedição	Falha no Link de Internet	Ausência de Link de Internet	Interrupção da emissão de Nota Fiscal Eletrônica	Cotnratação de redundância	Contingência	Coordenador de TI	SIM	R$ 200,00	NÃO		1
Faturamento e Expedição	Estravio do coletor de dados	Coletores são pequenos e fáceis de serem perdidos	Redução da operação e necessidade de aquisição de equipamentos	Controle e revista	Evitar risco	Coordenadora Sesmt	NÃO		NÃO	É necessário revistar funcionários que possuem acesso aos equipamentos do processo para evitar que estes sejam estraviados.	
Faturamento e Expedição	Falha na Central Telefônica	Central telefônica muito antiga e com pouca segurança	Parada do serviço de telefonia da empresa	Utilização de telefonia Móvel	Transferi risco	Coordenador de Expedição	NÃO		SIM	Usar celular para chamar a transportadora	
Faturamento e Expedição	Queda de energia	Baixa autonomia dos No-Breaks	Interrupção do funcionamento dos Servidores	Utilização de 2 no Breaks na alimentação do Datacenter	Reduzir risco	Coordenador de TI	SIM		SIM	Controle já existente na empresa	0
Faturamento e Expedição	Falha no coletor de dados	Coletores de dados são resistentes mas suscetíveis a falha	Interrupção do processo de separação	Possuir 2 coletores de reserva	Reduzir risco	Gerente de Logística	SIM	R$ 4.500,00	SIM	Aprovado pela gerência devido a dependência dos coletores no processo.	15
Faturamento e Expedição	Falha no Active Directory	Servidores de Active Directory são sujeitos a falhar	Interrupção do acesso a rede e todos seus sistemas	Redundância de AD	Reduzir risco	Coordenador de TI	NÃO		SIM	Ação de tratamento já existente na organização	0
Faturamento e Expedição	Invasão virtual de terceiros	Acesso a internet traz consigo a possibilidade de invasão	Danos ao ambiente da empresa	Instalação de Firewall	Evitar risco	Coordenador de TI	NÃO		SIM	Controle já existente na empresa	0
Faturamento e Expedição	Falta de bateria no coletor	Coletor de dados depende da bateria de LiOn para funcionamento	Interrupção do processo de separação	Possuir baterias para reserva	Evitar risco	Coordenador de Expedição	SIM	R$ 2.000,00	SIM	Baterias adquiridas para evitar risco.	10
Faturamento e Expedição	Esgotamento de bateria da empilhadeira	Empilahdeira elétrica depende de bateria	Interrupção do processo de separação	Carregar a bateria da empilhadeira sempre que parada	Reduzir risco	Coordenador de Expedição	NÃO		SIM	Controle pode ser aplicado imediatamente, sem custos	0
Faturamento e Expedição	Indisponibilidade do Servidor de Licenças	Servidor de licenças não possui redundância	Falha de acesso ao sistema Datasul	Trocar servidor de Licenças para um que possua redundância interna	Reduzir risco	Coordenador de TI	NÃO	R$ 5.000,00	NÃO		
Faturamento e Expedição	Falha no Servidor de Virtualização	Estrutura de TI dependente de Hardware Físico	Interrupção do acesso a rede e todos seus sistemas	Trabalhar com 2 hosts de virtualização	Reduzir risco	Coordenador de TI	NÃO		SIM	Tratamento já implementado na empresa.	0
Faturamento e Expedição	Falha do Switch Principal de Rede	Equipamento não possui redundância externa	Interrupção do serviço de rede e todos os acessos a sistema.	Adquirir mais um Switch para trabalhar parelalemente	Reduzir risco	Coordenador de TI	SIM	R$ 10.000,00	NÃO	Aguardando aprovação devido a alto investimento.	
Faturamento e Expedição	Falha em ambas controladoras do Storage	Storage depende das controladoras para funcionamento	Interrupção total do ambiente de TI da empresa e possibilidade de corrupção na base de dados.	Aquisição de novo Storage mais moderno e com maior capacidade	Reduzir risco	Coordenador de TI	SIM	R$ 45.000,00	SIM	Aquisição necessária devido à garantia expirada do Storage.	35
Faturamento e Expedição	Falha no Switch SAN	Switches estão em atividade por mais de 3 anos.	Interrupção na comunicação entre Storage e Servidores. Interrupção dos processos de negócio.	Trabalhar com 2 switches SAN em paralelo	Reduzir risco	Coordenador de TI	NÃO		SIM	Tratamento já existente na Empresa	0
Faturamento e Expedição	Usuário trancado no EMS	Usuários do sistema só podem estar logados uma unica vez	Impossibilidade de entrar no sistema com o usuário	Utilização de TimeOut	Reduzir risco	Coordenador de TI	NÃO		SIM	Tratamento já existente na empresa.	0
Faturamento e Expedição	Falha no Ar Condicionado	Ar condicionado vulnerável a falhas técnicas	Super aquecimento e aumento da possibilidade de parada dos equipamentos do Data Center	Adquirir um segundo ar condicionado para o Data Center	Reduzir risco	Diretor Financeiro	SIM	R$ 5.000,00	NÃO	Aguardando aprovação devido ao custo elevado.	
Faturamento e Expedição	Interrupção acidental dos servidores virtuais	Servidores administrados pelo Xen Center podem ser desligados por quem tem acesso a Console	Interrupção de servidores e serviços de rede/sistemas	Aquisição do XenServer Standard	Reduzir risco	Coordenador de TI	SIM	R$ 15.000,00	NÃO	Aguardo aprovação devido ao alto investimento.	

Faturamento e Expedição	Falha no servidor de TS	Dependência de único servidor para acesso a TS pelos coletores	Impossibilidade de acessar o sistema pelo coletor	Criar novo servidor para TS	Reduzir risco	Coordenador de TI	NÃO		SIM	Necessário para garantir a continuidade de negócios	60
Faturamento e Expedição	Falha nas antenas WiFi	Antenas vulneráveis a falhas	Interrupção parcial da rede Wifi	Adquirir e manter uma antena de reserva	Reduzir risco	Coordenador de TI	SIM	R$ 1.500,00	NÃO	Aguardando aprovação para investimento devido a valor	60
Faturamento e Expedição	Alteração não autorizada nos NoBreaks	Acesso irrestrito à sala dos NoBreaks	Interrupção no fornecimento de energia ao DataCenter	Controlar acesso na sala dos No-Breaks	Reduzir risco	Gerente de Engenharia	NÃO		NÃO	Aguardando posição da gerência do prédio para esvaziar a sala e trancá-la.	60
Faturamento e Expedição	Ameaça de Virus	Sistema operacional Windows vulnerável a Virus	Danos no sistema operacional	Utilizar anti Virus na Rede e mantê-lo atualizado	Reduzir risco	Coordenador de TI	NÃO		SIM	Tratamento já existente na empresa.	0
Faturamento e Expedição	Incêndio	Sala do Data Center não possui sistema anti-incêndio	Interrupção total da infraestrutura de TI e dano permanente nos equipamentos	Aceitar risco e utilizar plano de recuperação de desastres	Aceitar risco	Coordenador de TI	NÃO		SIM	Definido em conjunto com a direção da organização	30

Item 6.1. MÉTODOS DE CÓPIAS DE SEGURANÇA								
Método de backup	**Plano de continuidade envolvido**	**Ativos envolvidos**	**Responsável**	**Ações de validação**	**Dados de backup**	**Tipo de backup**	**Prioridade**	**Contrato de suporte com terceiros**
Diário em Fita	Faturamento e Expedição	Unidade de Fital Dell LTO-4; HP Data Protector	Coordenador de TI	Sistema envia relatório diário com o resultado do Job de Backup	Dados e Imagem	Completo	Alta	SUPORTE TI SA
Semanal em disco	Faturamento e Expedição	Servidor de Backup em Disco - BKPSERVER26; HP Data Protector	Coordenador de TI	Servidor envia relatório de sucesso após job realizado	Dados e Imagem	Completo	Alta	SUPORTE TI SA
Semanal de VMs	Faturamento e Expedição	HP Data Protector; Servidor de Backup em Disco - BKPSERVER26	Coordenador de TI	Verifricar Backups das VMs realizadas no diretório descrito no Job	Imagem	Completo	Alta	SUPORTE TI SA
Diário Datasul em Disco	Faturamento e Expedição	Banco de Dados Progress - Datasul EMS; SERVERPROG - Servidor HP DL 380 p/ Banco de Dados	Coordenador de TI	Verificar no diretório descrito no Job se o backup foi gerado.	Dados	Completo	Alta	SUPORTE TI SA
Diário SQL em disco	Faturamento e Expedição	SQL Server 2012 - Servidor Virtual SQLDB2012	Coordenador de TI	Servidor envia Logs de realziação do backup após realizar Job.	Dados	Completo	Média	SUPORTE TI SA

Item 7.1. CÓPIAS DE SEGURANÇA											
Ativo	**Possui backup?**	**Método de backup**	**Periodicidade**	**Ciclo de vida**	**Responsável**	**Ações de validação**	**Periodicidade de validação**	**Responsável pela validação**	**Possui armazenamento externo?**	**Periodicidade do armazenamento externo**	**Responsável pelo armazenamento externo**
Datasul EMS	SIM	Diário Datasul em Disco	2 vezes ao dia	1 dia	Coordenador de TI	Restauração do backup da base em ambiente de protótipo.	Semanal	Coordenador de TI	NÃO		
Datasul EMS	SIM	Diário em Fita	Diário	Semanal	Coordenador de TI	Restauração do backup da fita em área de restore	Mensal	Coordenador de TI	SIM	Semanal	Diretor Financeiro
Infra Estrutura de Virutalização	SIM	Semanal de VMs	Semanal	Único	Coordenador de TI	Restaurar uma VM no ambiente de produção através do backup realizado	Nunca realizada	Coordenador de TI	NÃO		
Microsoft Active Directory - Servidor Virtual ADVIRTUAL05 e ADVIRTUAL19	SIM	Diário em Fita	Diário	Semanal	Coordenador de TI	Verificar se o backup foi realizado através do Data Protector	Mensal	Coordenador de TI	SIM	Semanal	Diretor Financeiro
Diretório de Rede da Logística	SIM	Diário em Fita	Diário	Semanal	Coordenador de TI	Restauração dos arquivos em diretório temporário de rede	Mensal	Coordenador de TI	SIM	Semanal	Diretor Financeiro
Arquivo de Senhas de Acesso aos sistemas de administração	SIM	Diário em Fita	Diário	Semanal	Coordenador de TI	Restaurar arquivo em ambiente de testes.	Mensal	Coordenador de TI	SIM	Semanal	Diretor Financeiro
Servidor Dell Power Edge R610 - HOST1 e HOST2	SIM	Semanal em disco	Semanal	Único	Coordenador de TI	Verificar se os arquivos de backup forma gerados no diretório do Job de Backup.	Mensal	Coordenador de TI	NÃO		
Microsoft Share Point - Servidor Virtual SP2010	SIM	Diário SQL em disco; Diário em Fita	Diário	Semanal	Coordenador de TI	Verificação dos Logs de sistema e arquivos de backup gerados nos diretórios.	Mensal	Coordenador de TI	SIM	Semanal	Diretor Financeiro
ERP14 - Servidor virtual de aplicações ERP	SIM	Diário em Fita	Semanal	Semanal	Coordenador de TI	Restauração dos arquivos em área de protótipo	Mensal	Coordenador de TI	SIM	Semanal	Diretor Financeiro
SERVERTS - Servidor virtual para acesso TS dos coletores de dados	SIM	Semanal de VMs	Mensal	Mensal	Coordenador de TI	Verificação da geração do arquivo de Backup no servidor destino.	Trimestral	Coordenador de TI	NÃO		
IT0032 - Processo de Expedição	SIM	Diário em Fita	Diário	Semanal	Coordenador de TI	Restauração do arquivo em área de protótipo	Mensal	Coordenador de TI	SIM	Semanal	Diretor Financeiro
Totvs TSS NFe - Sistema de emissão de Nota Fiscal Eletrônica	SIM	Diário em Fita	Diário	Semanal	Coordenador de TI	Restauração do banco em ambiente de protótipo	Trimestral	Coordenador de TI	SIM	Semanal	Diretor Financeiro

Item 8.1. PLANO DE RESPOSTA A INCIDENTES											
Ação	**Descrição**	**Ameaça**	**SLA**	**Plano de continuidade**	**Ativação**	**Tipo de ação**	**Responsáveis**	**Quem deve ser acionado na ocorrência?**	**Quem deve ser comunicado após realização?**	**Quem pode ser acionado ?**	**OLA**
Conserto do ar condicionado	Acionar a Maeli para consertar o ar condicionado.	Falha no Ar Condicionado	48	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI		
Acionar terceiro responsável para conserto	Chamar fornecedor para reparar o No-Break. Transferir a carga para o no-break secundário (somente BKPSERVER07 não possui redundância automática)	Falha no No-Break primário do Data Center	12	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI		
Abrir as janelas do Data Center	Abrir as janelas para ventilar o Data Center	Falha no Ar Condicionado	1	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Analista de Suporte	Coordenador de TI		
Configurar Data/Hora no coletor	Reconfigurar manualmente as configurações de Data/Hora do coletor para pertmir acesso ao TS.	Coletor não acessa o sistema após troca de bateria	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de Expedição		
Forçar reinicilização através da tecla F1 fisicamente	Forçar a inicilização apertando a tecla F1	Reinicialização do servidor de Licenças	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI		
Abertura de chamado na Operadora	Acionar o suporte da Telecom SA para consertar o Link inoperante.	Falha no Link de Internet	4	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Suporte Telecom SA; Gerente Telecom SA	
Ativar emissão de NF em contingência	Ativar a contingência de NF caso o link não retorne em 4 horas.	Falha no Link de Internet; Falha no sistema de Nfe	4	Faturamento e Expedição	Manual	Contingência		Analista Fiscal	Coordenador de Expedição		
Derrubar usuario trancado	Derrubar usuário através de script do banco de dados	Usuário trancado no EMS	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de Expedição		
Trocar estabilizador	Trocar estabilizador por outro funcional	Queima de estabilizador	4		Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de Expedição		
Incrementar disco na máquina Virtual SERVER18	Aumentar o espaço em disco na máquina virtual	Espaço insuficiente de armazenamento na rede	2	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI		
Limpeza de arquivos desnecessários	Realizar limpeza de disco como resposta imediata	Espaço insuficiente de armazenamento na rede	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI		
Reiniciar servidor do TSS Totvs	Forçar a reinicialização dos serviços através da reinicialização do sistema.	Falha no sistema de Nfe	4	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Analista Fiscal		
Reinstalar o sistema TSS em novo ambiente	Reinstalar o TSS com suporte da TOTVS	Falha no sistema de Nfe	12	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Analista Fiscal	Consultor NFe	
Iniciar manualmente os bancos de dados Progress	Reiniciar os bancos para retornar o funcionamento do sistema	Interrupção acidental do banco de dados; Parada do banco de dados Progress	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Progress	
Transferência do core de rede para Switch SAN	Colocar um dos switches SAN para fazer o papel de Core até o conserto/troca do principal.	Falha do Switch Principal de Rede	12	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux	
Instalação de novo Core de Rede	Adquirir, Instalar e configurar um novo Switch para ser Core de Rede. Acionar terceiros para auxiliar na tarefa.	Falha do Switch Principal de Rede	144	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux	
Reparar cabeamento rompido	Acionar o terceiro para reparar o cabeamento/fibra danificado	Rompimento de fibra interna; Rompimento de fibra óptica externa	4		Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Manutentor de Rede	
Adquirir novo coletor de dados	Comprar novo coletor e colocá-lo no ambiente de produção.	Estravio do coletor de dados	48	Faturamento e Expedição	Manual	Recuperação	Gerente de Logística	Coordenador de TI	Gerente de Logística		

Instalar impressora de contingência	Instalar a impressora reserva no lugar da danificada	Falha na impressora de etiquetas	1	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Analista de Suporte	Coordenador de Expedição	
Manutenção da impressora de etiquetas	Acionar a manutenção da Barras para consertar a impressora	Falha na impressora de etiquetas	48	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Barras
Acionar consultoria e suporte Totvs	Entrar em contato com os consultores da Totvs para correçao do problema emergencial	Erros no sistema EMS	4		Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor WMS; Programador WMS
Correção de problema na infraestrutura de comunicação	Acionar prestadores de serviço para diagnosticar e solucionar os problemas.	Falha de comunicação com Data Center	4	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Consultor Linux; Manutentor de Rede
Acionar a garantia do Storage	Acionar a DELL para trocar a controladora danificada. Caso seja apenas uma controladora não requer outra ação. Caso ambas as controladoras estejam danificadas, requer outra ação.	Falha em controladora/fonte do Storage de Dados; Falha em ambas controladoras do Storage	8	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Linux; Dell Suporte
Acionar a garantia dos servidores	Acionar a garantia da Dell para realizar a manutenção nos servidores.	Falha parcial em servidor de virtualização	12	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Dell Suporte
Restauração de ambiente em novo Storage	Restauração do ambiente em um Storage emprestado pela SuporteTI. Característica de Desastre, será tratado de maneira detalhada na recuperação de Desastres.	Falha geral do Storage	72	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Storage
Aguardar liberação de licenças	Em primeira instância, aguarda-se a liberação de licenças	Sistema sem licenças disponiveis	1	Faturamento e Expedição	Automática	Recuperação	Coordenador de Expedição	Analista de Suporte	Coordenador de TI	
Verificar usuários trancados no sistema e derrubá-los	Verificar se há usuários presos no sistema e derrubá-los para liberar licenças.	Sistema sem licenças disponiveis	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	
Corrigir falhas no backup para o próximo job	Verificar o motivo da falha, verificar o ponto com problemas e corrigí-lo. Somente será aplicado no próximo Job executado.	Restauração de backup com falhas; Falha no processo de Backup	24	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Consultor Linux
Encaminhar para correção do setor Fiscal	Encaminhar para a área fiscal verificar os erros de emissão e corrigí-los. Em caso de necessidade o fiscal pode acionar a TI ou um consultor Totvs.	Nota fiscal rejeitada na SEFAZ	4	Faturamento e Expedição	Manual	Recuperação	Coordenadora de Controladoria	Analista Fiscal	Faturista	Consultor NFe
Substituição da fonte do computador	Consertar a peça danificada no fornecedor	Queima de Fonte de Alimentação	8	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	PC Suporte Ltda
Configurar micro de contingência para uso de faturista	Configurar micro de outro usuário para uso do faturamento	Queima de Fonte de Alimentação	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de Expedição	
Comunicar manutenção para reestabelecer o fornecimento de energia	Acionar a manutenção para reestabelecer o fornecimento de energia.	Queda de energia	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI; Coordenador de Manutenção	Coordenador de Manutenção	Coordenador de TI	
Desligar DataCenter	Desligar o Data Center para evitar falhas nos equipamentos de Hardware	Queda de energia	2	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Linux
Utilizar impressora de outra área para impressão imediata	Utilizar impressora de outra área para realizar as impressões enquanto a impressora está em manutenção.	Falha na impressora de Nfe	1	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Analista de Suporte	Coordenador de Expedição	
Reparar impressora de NFe com problemas	Acionar suporte para reparar a impressora com defeito	Falha na impressora de Nfe	8	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Analista de Suporte	Coordenador de TI	Suporte Print

Acionar suporte para manutenção do firewall	Acionar suporte contratado para realizar manutenção no equipamento de Firewall	Falha no Firewall	8	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Consultor Firewall; Suporte Firewall
Bloquear acesso externo à rede	Identificar causa da invasão e realizar bloqueio retroativo	Invasão virtual de terceiros	8	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Firewall; Suporte Firewall
Solicitar Tonner no almoxarifado interno	Solicitar tonner no almoxarifado interno da empresa.	Falta de Tonner	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de Expedição	Analista de Suporte	Coordenador de Expedição	
Solicitar Tonner no fornecedor	Na ausência de Tonner no almoxarifado interno deve ser solicitado no fornecedor.	Falta de Tonner	4	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de Expedição	Suporte Print
Ativar a chave de emergência do EMS	Ativar a chave de emergência para o sistema poder operar sem o uso do License server. Deve-se acionar a Totvs após isto para corrigir o LS.	Indisponibilidade do Servidor de Licenças	2	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Coordenador de TI	Coordenador de TI	
Corrigir problemas com License Server	Realizar manutenção no servidor de licenças para corrigir problemas e então recolocá-lo no ar.	Indisponibilidade do Servidor de Licenças	48	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Banco;TOTVS Suporte
Direcionar TS para outro servidor temporário	Direcionar o TS manualmente nos coletores para outro servidor disponível.	Falha no servidor de TS	2	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Coordenador de TI	Coordenador de Expedição	
Restaurar servidor de TS	Restaurar ou criar novo servidor para TS e redirecionar os coletores de volta para este.	Falha no servidor de TS	24	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Linux;
Restaurar servidor de Programas Datasul	Reinstalar servidor de programas e restaurar backups e configurações. Utilizar suporte da Totvs e SuporteTI para auxiliar na restauração.	Falha no servidor Datasul ERP14	24	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Banco; Consultor Linux
Acionar suporte de Tecnologia Totvs para manutenção	Acionar suporte Totvs para tentar corrigir o problema no Banco de Dados.	Parada do banco de dados Progress	4	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Diretor Financeiro	Consultor Progress; Consultor Banco
Restaurar banco de dados em ambiente de contingência virtual	Disponibilizar novo servidor virtual e restaurar backup ou transportar a base ele.	Parada do banco de dados Progress; Corrompimento da base de dados do EMS	12	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Banco
Retornar banco de dados ao ambiente de produção	Retornar o banco para ambiente de produção recuperado ou otimizar o ambiente de contingência criado para assumir a produção.	Parada do banco de dados Progress	48	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Coordenador de TI	Diretor Financeiro	Consultor Progress; Consultor Banco
Restaurar Active Directory em novo servidor	Restuarar Backup do AD em servidor virtual disponibilizado. (ou restaurar a partir do backup da VM do AD)	Falha no Active Directory	12	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Citrix
Ativar direct Attach entre Storage e Servidores	Configurar Storage e servidores de Virtualização e Banco para conectarem diretamente no Storage, sem necessidade de Switch.	Falha no Switch SAN	8	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux

Reinstalar switch SAN em produção	Instalar novo (ou reparado) Switch SAN no Data Center e reconfigurá-lo para conectar Storage e Servidores	Falha no Switch SAN	144	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux
Subir VMs Críticas em único host	Manter somente as VMs críticas em no Host operante enquanto o segundo não é reparado.	Falha parcial em servidor de virtualização	2	Faturamento e Expedição	Manual	Contingência	Coordenador de TI	Analista de Suporte	Coordenador de TI	Consultor Linux
Reconfigurar Host com problemas em produção	Reconfiguar o Host de Virtualização que apresentou problemas em produção e iniciar as demais VMs no ambiente.	Falha parcial em servidor de virtualização	48	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Linux
Utilizar telefonia móvel como contingência	Utilizar telefone Celular para efetuar ligações enquanto a Central não está disponível	Falha na Central Telefônica	1	Faturamento e Expedição	Manual	Contingência	Coordenador de Expedição	Analista de Suporte	Coordenador de Expedição	
Reparar a Central telefônica	Acionar o terceiro para corrigir problemas com a central.	Falha na Central Telefônica	48	Faturamento e Expedição	Manual	Retorno em produção	Coordenador de TI	Analista de Suporte	Coordenador de Expedição	Consultor Telefonia; Gerente Telefonia
Acionar suporte para manutenção do Exchange	Acionar terceiro para corrigir problemas no Exchange. Emails podem ser enviados e somente serão liberados após normalização do serviço.	Falha no servidor de E-mail	8	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Consultor Microsoft
Restaurar servidor Exchange a partir de backup	Restaurar o servidor Exchange a partir do backup diário em novo ambiente.	Base do Exchange corrompida	72	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Consultor Microsoft; Consultor Linux
Verificar e corrigir problemas de funcionamento do coletor	Verificação de problemas como conexão a rede, funcionamento do Laser e configurações gerais do coletor.	Falha no coletor de dados	1	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	
Acionar suporte local dos coletores	Encaminhar coletor para conserto no Terceiro localizado em Caxias do Sul	Falha no coletor de dados	72	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Suporte Coletores SA; Consultor Coletor
Enviar coletor à assistência Motorola	Enviar coletor de dados para a Motorola em caso de danos físicos mais graves	Falha no coletor de dados	720	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Coordenador de TI	Coordenador de TI	Suporte Coletores SA
Reiniciar e reconfigurar rede Wireless	Reiniciar e reconfigurar a rede Wireless	Desconfiguração da rede Wireless	4	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Coordenador de TI	Consultor Coletor; Suporte Coletores SA
Acionar suporte para manutenção das antenas	Acionar o suporte da Coletores SA para corrigir o problema com a Antena.	Falha nas antenas WiFi	8	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Analista de Suporte	Gerente de Logística	Suporte Coletores SA; Consultor Coletor
Adquirir e trocar Antena com problema	Adquirir nova antena para substituir uma com defeito irreparável.	Falha nas antenas WiFi	72	Faturamento e Expedição	Manual	Recuperação	Coordenador de TI	Gerente de Logística	Gerente de Logística	Consultor Coletor; Suporte Coletores SA

Item 9.1. ATIVAÇÃO DA RECUPERAÇÃO DE DESASTRES											
Plano de Recuperação de Desastres	**Definição do desastre**	**Plano de Continuidade**	**Local definido para a continuidade de negócios**	**Responsável pela ativação**	**Responsável pelas ações**	**Responsável pelas tomadas de decisão**	**Responsável Financeiro**	**Responsável pelas aquisições**	**Quem deve ser informado?**	**Plano aprovado por**	**SLA**
Recuperação emergencial	Interrupção total do Data Center da empresa, tendo seu Hardware danificado e necessária a substituição por equipamentos novos mas com recursos mínimos a fim de recuperar o ambiente parcialmente, garantindo a operação de negócio.	Faturamento e Expedição	Sala da Expedição	Coordenador de TI	Coordenador de TI	Diretor Financeiro	Diretor Financeiro	Gerente de Logística	Diretor Financeiro	Diretor Financeiro	80

Item 9.2.1. ATIVOS DE TI PARA A RECUPERAÇÃO DE DESASTRES								
Plano de recuperação de desastres	**Ativo para recuperação**	**Tipo de ativo**	**Quantidade**	**Descrição detalhada**	**Possui redundância?**	**Custo aproximado**	**Prioridade**	**Responsável**
Recuperação emergencial	Rack de servidores	Meio físico e infraestrutura	1	Rack de 42U com 2 unidades de distribuição de energia estabilizada. Marca independe.	NÃO	R$ 5.000,00	Baixa	Coordenador de TI
Recuperação emergencial	Switch Camada 2	Interface de comunicação	1	Switch Core de Rede Camada 3	NÃO	R$ 5.000,00	Alta	Coordenador de TI
Recuperação emergencial	Servidor para virtualização de serviços críticos do negócio	Equipamento de processamento de dados	1	Servidor para hospedagem dos demais servidores Virtuais. Sistema operacional Xen Server (Free Edition) , 2 Processadores Xeon Quad Core, 48 Gb de Memória, 6 portas de Rede (4 On Board, 2 Off Board), 8 discos de 600 Gb SAS 15k HotPlug.	NÃO	R$ 25.000,00	Alta	Coordenador de TI
Recuperação emergencial	Sala para servidores	Edificações	1	Sala para instalação dos Servidores	NÃO		Média	
Recuperação emergencial	Link de internet 10Mbps	Interface de comunicação	1	Link de comunicação com a Internet , Largura de banda 10Mbps dedicado	NÃO		Alta	
Recuperação emergencial	Microsoft Active Directory - Servidor Virtual ADVIRTUAL05	Equipamento de processamento de dados	1	Servidor Virtual com Microsoft Windows Server 2008 R2 A empresa conta com Backup do AD e da VM completa em si, apenas necessitando a atualização da VM com o Bkp diário do AD.	SIM		Alta	
Recuperação emergencial	Microsoft File Server - Servidor Virtual SERVER18	Mídia de dados	1	Servidor Virtual Microsoft Windows Server 2008 R2 A empresa possui backup dos diretórios e arquivos. É necessário apenas reinstalar um servidor e configurar o compartilhamento.	SIM		Média	
Recuperação emergencial	ERP14 - Servidor virtual de aplicações ERP	Equipamento de processamento de dados	1	Servidor Virtual Microsoft Windows Server 2008 Existe backup diário dos Programas e o backup da VM completa. É possível restaurar o Backup da VM e então atualizar com o bkp diário dos programas.	SIM		Alta	
Recuperação emergencial	SQL Server 2012 - Servidor Virtual SQLDB2012	Equipamento de processamento de dados	1	Servidor Virtual Microsoft Windows Server 2008 R2 com Microsoft SQL Server 2012 instalado. Existe Backup desta VM bem como Bkp diário dos bancos de Dados. Deve-se restaurar a VM e então atualizá-la com os dados.	SIM		Alta	

Recuperação emergencial	Totvs TSS NFe - Servidor Virtual NFETSS	Equipamento de processamento de dados	1	Servidor Virtual Microsoft Windows Server 2008 Existe Backup desta VM e backup Diário dos dados em Fita. Deve-se restaurar a VM e então restaurar o Backup diário dos dados.	SIM		Alta	
Recuperação emergencial	Totvs TSS NFe - Sistema de emissão de Nota Fiscal Eletrônica	Aplicações de negócio padronizadas	1	Sistema de Emissão de Nota Fiscal Eletrônica Totvs TSS 2.22 É realizado backup diário dos dados e do banco de Dados (SQL Server). Deve-se restaurar na VM NFETSS	SIM		Alta	
Recuperação emergencial	Microsoft EOpen	Mídia de dados	1	Website Microsoft com informações de Licneças e Mídias de instalação dos produtos Microsoft.	SIM		Média	
Recuperação emergencial	Servidor Linux CentOS para Banco de Dados Progress	Equipamento de processamento de dados	1	Servidor (físico ou Virtual) Linux CentOS 5.5 com PRogress Open Edge 10.2a instalado. Servidor não possui backup (somente do banco) e deverá ser reinstalado.	NÃO		Alta	
Recuperação emergencial	Unidade de Fita Dell LTO-4	Outros tipos de mídia	1	Unidade de Fita LTO-4 com conexão e cabo SAS para instalação em Servidor Físico. Necessária para restaurar os Backups.	NÃO	R$ 6.000,00	Alta	Coordenador de TI
Recuperação emergencial	HP Data Protector	Software de serviço, manutenção ou administração	1	Software de Backup HP Data Protector Necessário para restauração dos Backups. Instalar com Licença aberta e depois aplicá-la a partir do Backup dos arquivos de licença.	SIM		Alta	
Recuperação emergencial	Servidor para restauração dos Backups	Equipamento de processamento de dados	1	Servidor Físico Windows Server 2008 R2 para instalação do Data Protector e restauração dos Backups 1 Processador Xeon, 4Gb Memória RAM, 2 Discos 500Gb Sata, 2 Placas de Rede 1Gbps	NÃO	R$ 4.000,00	Alta	Coordenador de TI
Recuperação emergencial	Licence Server Datasul	Aplicações de negócio específicas	1	License Server Datasul Pode ser instalado no servidor usado para Restauração dos Backups. (Baixar mídia do Portal Totvs http://suporte.suporteerp.com.br)	SIM		Média	
Recuperação emergencial	Hardlock de Licenças Datasul	Mídia de dados	1	Hardlock Totvs para uso do Servidor de Licenças Datasul. Deve ser solicitado na Totvs por outra unidade através do Gerente de Contas Totvs.	NÃO		Média	

Recuperação emergencial	Chave de emergência Datasul	Informação	1	Chave de Emergência para uso no Sistema Datasul. Deve ser solicitada no Portal Totvs (http://suporte.suporteerp.com.br) e aplicada para uso do sistema na ausência do License Server.	NÃO		Alta
Recuperação emergencial	Banco de Dados Progress - Datasul EMS	Aplicações de negócio padronizadas	1	Bancos de Dados do Sistema ERP Datasul. É realizado backup diário do banco em fita. Deve ser restaurado após a instalação de novo servidor pra Banco de Dados Progress.	SIM		Alta
Recuperação emergencial	Microcomputador de Faturamento	Equipamento fixo	1	Micro computador com Windows 7 para faturamento. Core i3, 4Gb Memória, HD 250Gb com Microsoft Office Standard 2010 e Client do Progress (ERP Datasul)	NÃO	R$ 3.000,00	Média
Recuperação emergencial	Switch Camada 2 para rede Expedição	Interface de comunicação	1	Switch para distribuição de rede na Expedição. 16 Portas, Layer 1 ou superior.	NÃO	R$ 800,00	Média
Recuperação emergencial	Impressora Laser Samsung Scx5835	Equipamento fixo	1	Impressora Laser para impressãod e Notas Fiscais. Solicitar impressora nova com a Suporte Print	SIM		Média
Recuperação emergencial	Energia necessária para ligar os equipamentos	Meio físico e infraestrutura	1	Fornecimento de Energia para Servidores e Microcomputadores. A Manutenção deve entregar energia (estabilizada ou não) para funcionamento do Hardware.	NÃO		Alta
Recuperação emergencial	Sistema Datasul EMS	Aplicações de negócio padronizadas	1	Sistema ERP Datasul EMS2.06 funcional com faturamento disponibilizado.	SIM		Alta
Recuperação emergencial	Processo de faturamento não-automatizado	Processos e atividades de negócio	1	Processo de faturamento sem a necessidade de utilização dos coletores de Dados e o sistema WMS. Utilizado somente em situação de desastre e emergência.	NÃO		Alta

Item 9.2.2. ATIVOS DE TI PARA A RECUPERAÇÃO DE DESASTRES							
Plano de recuperação	**Profissional necessário**	**Descrição detalhada**	**Qtd.**	**Presente?**	**Natureza**	**Criticidade**	**Responsável**
Recuperação emergencial	Expedidor	Expedidor para efetuar as tarefas de Separação.	4	SIM	Interno	Alta	Coordenador de Expedição
Recuperação emergencial	Coordenador de Equipe	Profissional para coordenar os separadores e faturistas no processo	1	SIM	Interno	Média	Gerente de Logística
Recuperação emergencial	Faturista	PRofissional para executar as tarefas de faturamento no sistema	1	SIM	Interno	Alta	Coordenador de Expedição
Recuperação emergencial	TI	PRofissional capacitdado em Tecnologia da Informação para realizar as operações de restauração da InfraEstrutura	1	SIM	Interno	Alta	Coordenador de TI
Recuperação emergencial	Especialista em Infraestrutura e Storage	Profissional com alto nível de conhecimento em ambiente de Infraestrutura (Storage, Servers e SAN). Responsável por reestabelecer o funcionamento da estrutura de TI. A SuporteTI possui equipe especializada para atender esta demanda.	1	NÃO	Externo	Alta	Coordenador de TI
Recuperação emergencial	Especialista em Tecnologia Datasul	Profissional da TOTVS especializado em Banco de Dados Progress e Datasul, contratado para restaurar o ambiente do ERP Datasul.	1	NÃO	Externo	Alta	Coordenador de TI
Recuperação emergencial	Eletricista de Manutenção	Profissional capacitado para administrar e operar uma central elétrica e fornecer energia elétrica para um setor de trabaho.	2	SIM	Interno	Alta	Coordenador de Manutenção

Item 9.2.3. SERVIÇOS DE TERCEIROS PARA A RECUPERAÇÃO DE DESASTRES							
Plano de recuperação	**Serviço**	**Descrição detalhada**	**Custo aproximado**	**Necessidade de acionamento**	**Contato**	**Empresa**	**Responsável interno**
Recuperação emergencial	Restauração da infraestrutura de TI	Profissional com alto nível de conhecimento em ambiente de Infraestrutura (Storage, Servers e SAN). Responsável por reestabelecer o funcionamento da estrutura de TI. A SuporteTI possui equipe especializada para atender esta demanda.		Alta	Consultor Storage; Consultor Linux	SuporteTI; SuporteTI	Coordenador de TI
Recuperação emergencial	Restauração do ambiente Datasul	Profissional especialista em Ambiente Progress e Datasul para reinstalar os bancos de Dados e colocar o Sistema operante no ar.		Alta	Consultor Progress; Consultor Banco	SuporteERP SA; SuporteERP SA	Coordenador de TI
Recuperação emergencial	Restauração do fornecimento de Energia	Empresa fornecedora de Energia à Infraestrutura da empresa.		Alta	Eletricista Eletro; Eletricista EnergiaSA	Eletro Instalações Elétricas Ltda; Energia SA	Coordenador de Manutenção
Recuperação emergencial	Restauração dos serviços Microsoft	PRofissional capacitado para restaurar e reconfigurar os serviços de TI Microsoft como Active Directory e SQL Server		Alta	Consultor Microsoft; Consultor Storage	SuporteTI; SuporteTI	Coordenador de TI

Item 10.1. AÇÕES DO PLANO DE RECUPERAÇÃO DE DESASTRES												
Plano de recuperação	Ação	Descrição da ação	Nº Ação	Tipo de ação	SLA	Responsável	Dependente de ação	Ativos para recuperação habilitados	Quem deve ser comunicado na ocorrência?	Quem deve ser comunicado após realização?	Quem pode ser acionado?	OLA
Recuperação emergencial	Estabelecer e organizar local para instalação dos equipamentos de TI	Definir com a equipe de Gestão qual será o local para reestruturar a TI da empresa. O local deve ser pensado para tornar mais rápida a recuperação.	10	Reinstalação	1	Diretor Financeiro			Diretor Financeiro	Coordenador de TI		
Recuperação emergencial	Fornecer energia para o local de recuperação	Equipe de manutenção deve fornecer energia para o local onde será reestabelecida a infraestrutura de TI para a recuperação de desastre.	20	Reinstalação	8	Coordenador de Manutenção	Estabelecer e organizar local para instalação dos equipamentos de TI	Energia necessária para ligar os equipamentos	Coordenador de Manutenção	Coordenador de TI	Eletricista EnergiaSA; Eletricista Eletro	
Recuperação emergencial	Aquisição de Servidor para Restauração dos Backups	Entrar em contato com Fornecedor PArceiro e adquirir uma máquina para restauração dos arquivos. A máquina pode ser "locada" ao invés de comprada visto que servirá para restaurar os backups apenas.	30	Reinstalação	2	Coordenador de TI			Diretor Financeiro	Coordenador de TI	Vendedor SuporteTI; Consultor Storage; Diretor SuporteTI	
Recuperação emergencial	Solicitar novo Hardlock à TOTVS	Solicitar através do suporte Totvs (4003 0015) um novo Hardlock para instalação do license server Totvs.	35	Reinstalação	1	Coordenador de TI			Coordenador de TI	Coordenador de TI	TOTVS Suporte	
Recuperação emergencial	Adquirir novos servidores para hospedar os servidores virtuais restaurados	Adquirir novos servidores para a recuperação de desastre. Estes servidores podem ser "Locados" no primeiro momento para adiantar o processo de recuperação de desastres.	40	Reinstalação	4	Coordenador de TI			Diretor Financeiro	Coordenador de TI	Diretor SuporteTI; Consultor Storage; Vendedor SuporteTI	
Recuperação emergencial	Adquirir Switch para gerenciamento e distribuição das redes	ADquriir Switch para gerenciar a rede. Poder ser "locado" com fornecedores.	45	Reinstalação	1	Coordenador de TI			Diretor Financeiro	Coordenador de TI	Vendedor SuporteTI; Diretor SuporteTI	
Recuperação emergencial	Estabelecer conexão com Internet	Acionar a Telecom SA para instalar linha de conexão a Internet emergencial para retomar as atividades	50	Reinstalação	48	Coordenador de TI	Estabelecer e organizar local para instalação dos equipamentos de TI	Link de internet 10Mbps	Coordenador de TI	Coordenador de TI	Suporte Telecom SA; Gerente Telecom SA;	
Recuperação emergencial	Adqurir computador para uso no faturamento	Adqurir computador com fornecedores parceiros. O micro pode ser "Locado" para emergência.	55	Reinstalação	1	Coordenador de TI			Coordenador de TI	Diretor Financeiro	Vendedor SuporteTI; PC Suporte Ltda	
Recuperação emergencial	Adquirir unidade de fita LTO-4	Adquirir (ou Locar) unidade de Fita LTO-4 para realizar a restauração dos Backups em fita	60	Reinstalação	8	Coordenador de TI			Diretor Financeiro;#5	Coordenador de TI	Vendedor SuporteTI; Consultor Storage; Diretor SuporteTI	
Recuperação emergencial	Instalar e configurar servidor para recuperação	Instalar o Microsft Windows Server 2008 R2 , configurar o servidor com acesso a Internet e instalar o HP Data Protector	70	Reinstalação	8	Coordenador de TI	Aquisição de Servidor para Restauração dos Backups; Estabelecer e organizar local para instalação dos equipamentos de TI	Servidor para restauração dos Backups	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux; Consultor Citrix	
Recuperação emergencial	Instalar e configurar a unidade de Fita no servidor de backup	Realizar instalação da unidade de Fita no servidor de backup. Esta atividade pode ser feita pelos técnicos da SuporteTI, previsto em contrato.	80	Reinstalação	4	Coordenador de TI	Instalar e configurar servidor para recuperação; Adquirir unidade de fita LTO-4	Unidade de Fita Dell LTO-4	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux	
Recuperação emergencial	Instalar e configurar servidor Host de Virtualização	Instalação do Servidor para hospedar as VMs . Instalar sistema operacional Xen Server (SuporteTI possui a mídia, ou baixar do site da Citrix) e configurar uma Pool única.	90	Reinstalação	3	Coordenador de TI	Adquirir novos servidores para hospedar os servidores virtuais restaurados	Servidor para virtualização de serviços críticos do negócio	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux; Consultor Citrix	

Recuperação emergencial	Restaurar Backup da imagem do Servidor do AD	Restaurar o Backup de Disco da VM completa no ambiente de Virtualização.	100	Reinstalação	1	Coordenador de TI	Instalar e configurar servidor Host de Virtualização; Instalar e configurar servidor para recuperação		Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux
Recuperação emergencial	Atualizar AD pelo Backup diário de Fita LTO e configurar em novo ambiente	Atualizar a base do AD com o último backup diário realizado (Fita) e configurá-lo na nova estrutura do domínio.	110	Recuperação	4	Coordenador de TI	Restaurar Backup da imagem do Servidor do AD	Microsoft Active Directory - Servidor Virtual ADVIRTUAL05	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux; Consultor Microsoft
Recuperação emergencial	Configurar Switch para distribuir a rede para a expedição	Configurar Switch para distribuir a Rede gerenciada pelo AD	120	Reinstalação	1	Coordenador de TI	Restaurar Backup da imagem do Servidor do AD		Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux
Recuperação emergencial	Instalar e configurar Switch para gerenciamento e distribuição da rede	Instalar o Switch na rede e configurar o Acesso à Internet diretamente por ele, sendo o AD como distribuidor DNS e DHCP.	130	Reinstalação	2	Coordenador de TI	Adquirir Switch para gerenciamento e distribuição das redes	Switch Camada 2 para rede Expedição	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux
Recuperação emergencial	Instalar servidor virtual Linux CentOS para Progress	Instalar Criar VM com Sistema Operacional CentOS no servidor de virtualização. A SuporteTI fornece suporte à este processo enquantoa Totvs pode fornecer serviço de otimização.	140	Reinstalação	4	Coordenador de TI	Instalar e configurar servidor Host de Virtualização	Servidor Linux CentOS para Banco de Dados Progress	Coordenador de TI	Coordenador de TI	Consultor Linux; Consultor Storage; Consultor Progress
Recuperação emergencial	Instalar banco de dados Progress	Serviço de reinstalação do Progress e configuração do SGBD no servidor Linux. Serviço prestado pela equipe de Tecnologia da Totvs.	150	Reinstalação	4	Coordenador de TI	Instalar servidor virtual Linux CentOS para Progress		Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Banco
Recuperação emergencial	Restaurar bancos Datasul a partir de backup diário	Restaurar Backups a partir do bkp diário em fita. Reconfigurar banco e colocá-lo em produção. Serviço realizado pela equipe de tecnologia da Totvs.	160	Recuperação	8	Coordenador de TI	Instalar banco de dados Progress; Instalar e configurar a unidade de Fita no servidor de backup	Banco de Dados Progress - Datasul EMS	Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Linux; Consultor Banco
Recuperação emergencial	Restaurar backup da VM do sistema Datasul	Restaurar backup completo da VM ERP14 no novo ambiente de virtualização.	170	Recuperação	4	Coordenador de TI	Instalar e configurar servidor Host de Virtualização		Coordenador de TI	Coordenador de TI	Consultor Linux; Consultor Storage; Consultor Citrix
Recuperação emergencial	Restaurar Backup diário dos programas Datasul no ERP14	Recuperar os programas atualizados da fita de bkp e restaurá-los no servidor virtual ERP14. Realizar os ajustes para operar o Sistema Datasul. Serviço realizado pela equipe de Tecnologia da Totvs.	180	Recuperação	4	Coordenador de TI	Restaurar backup da VM do sistema Datasul	ERP14 - Servidor virtual de aplicações ERP	Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Linux; Consultor Banco
Recuperação emergencial	Instalar computador para Faturamento	Instalar e configurar o microcomputador de faturamento no domínio restaurado da empresa. Instalar o pacote Office, antivirus genérico e cliente do Progress.	190	Reinstalação	4	Coordenador de TI	Configurar Switch para distribuir a rede para a expedição; Restaurar Backup da imagem do Servidor do AD	Microcomputador de Faturamento	Analista de Suporte;#2	Coordenador de TI	
Recuperação emergencial	Restaurar backup da NFETSS	Restaurar backup completo da VM NFETSS para rodar o sistema de Emissão de Nota Fiscal Eletrônica. Serviço pode ser realizado pela consultoria da SuporteTI.	200	Recuperação	4	Coordenador de TI	Instalar e configurar servidor Host de Virtualização; Instalar e configurar servidor para recuperação	Totvs TSS NFe - Servidor Virtual NFETSS	Coordenador de TI	Coordenador de TI	Consultor Linux; Consultor Storage
Recuperação emergencial	Restaurar backup diário do Servidor de NFe	Restaurar backup diário do TSS armazenado em fita e reconfigurar o ambiente de produção para a emissão de Nota Eletrônica. É necessário o suporte da equipe de NFe da Totvs.	210	Recuperação	8	Coordenador de TI	Restaurar backup da NFETSS;#22	Totvs TSS NFe - Sistema de emissão de Nota Fiscal Eletrônica	Coordenador de TI	Coordenador de TI	Consultor Linux; Consultor NFe
Recuperação emergencial	Aplicar chave de emergência no sistema EMS	Solicitar chave de emergência no Portal Totvs para liberar acesso ao sistema Datasul	215	Reinstalação	1	Coordenador de TI	Restaurar Backup diário dos programas Datasul no ERP14	Chave de emergência Datasul	Coordenador de TI	Coordenador de TI	

Recuperação emergencial	Operacionalizar o sistema EMS	Realizar testes de acesso ao sistema ERP e validar sua funcionalidade.	220	Reinstalação	2	Coordenador de TI	Restaurar bancos Datasul a partir de backup diário; Restaurar backup diário do Servidor de NFe; Restaurar Backup diário dos programas Datasul no ERP14; Instalar computador para Faturamento; Estabelecer conexão com Internet	Sistema Datasul EMS	Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Linux; Consultor Banco
Recuperação emergencial	Desabilitar processo de WMS no ERP	Desabilitar a função WMS e configurando armazem para faturamento não automatizado. É necessário a suporte da consultoria de Negócios em WMS da Totvs para executar a tarefa.	230	Reinstalação	8	Coordenador de TI	Operacionalizar o sistema EMS		Coordenador de Expedição	Gerente de Logística	Consultor WMS
Recuperação emergencial	Criar novo servidor de Arquivos de Rede	Criar novo servidor de Arquivos para armazenamento dos documentos de apoio ao processo e de registros. Criar VM conforme Ativo de reucperação - Servidor de Arquivos	240	Recuperação	6	Coordenador de TI	Instalar e configurar servidor Host de Virtualização; Atualizar AD pelo Backup diário de Fita LTO e configurar em novo ambiente		Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux
Recuperação emergencial	Restaurar backup diário dos arquivos de rede	Restaurar os arquivos de rede através da fita de bkp diário. Reconfigurar servidor conforme mapeamentos de rede e permissões necessária para operar o negócio.	250	Recuperação	8	Coordenador de TI	Criar novo servidor de Arquivos de Rede	Microsoft File Server - Servidor Virtual SERVER18	Coordenador de TI	Coordenador de TI	Consultor Storage; Consultor Linux; Consultor Microsoft
Recuperação emergencial	Instalar Hardlock Totvs no servidor de recuperação	Conectar e instalar o Hardlock de licenças no servidor utilizado para Restauração	255	Reinstalação	1	Coordenador de TI	Solicitar novo Hardlock à TOTVS; Instalar e configurar servidor para recuperação	Hardlock de Licenças Datasul	Coordenador de TI	Coordenador de TI	
Recuperação emergencial	Instalar Licence Server Datasul	Instalar e configurar o Servidor de Licenças Datasul no servidor usado para Recuperação dos backups. Serviço pode ser realizado pela consultoria em tecnologia da Totvs.	260	Reinstalação	4	Coordenador de TI	Aplicar chave de emergência no sistema EMS	Licence Server Datasul	Coordenador de TI	Coordenador de TI	Consultor Progress; Consultor Banco

Item 11.1. ACORDOS DE NÍVEL OPERACIONAL - OLA				
Ação	**Tipo de OLA**	**Instruções operacionais**	**Responsável**	**Quem pode ser acionado?**
Derrubar usuários do EMS	Plano de resposta a incidentes	Acessar através de um client TTY, via SSH, o servidor de banco de dados Datasul 192.200.0.3 Utilizar o usuário e senha do operador Progress para acessar o menu de opções. no menu, acessar a opção 21 (Derruba Usuários) Selecionar o sistema que deseja derrubar o usuário Digitar o usuário que deseja ser derrubado e pressionar enter. Avançar todas as tela e confirmar a desconexão do usuário.Guia para Derrubar os usuários no EMS206 e EMS506.docx	Coordenador de TI	Consultor Progress

Item 12.1. APROVAÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRES						
Plano de continuidade	**Aprovador**	**Parecer**	**Etapa**	**Avaliação**	**Observações**	**Papel**
Faturamento e Expedição	Coordenador de TI	Aprovado	Definição do escopo; Análise de riscos; Plano de continuidade de negócios	Aprovado	Plano de continuidade foi elaborado de maneira a tornar viável uma recuperação de desastres e ter respostas definidas para os riscos possíveis de acontecer com os ativos de TI no processo de faturamento.	Gestor da Continuidade
Faturamento e Expedição	Coordenador de Expedição	Aprovado com ressalvas	Definição do escopo; Análise de riscos; Plano de continuidade de negócios	Aprovado	O plano ainda não trata todos os problemas possíveis, mas trata os que possuem maior impacto no processo. Ainda temos problemas com assuntos fora do escopo como a devlução e cancelamento de NF.	Gestor do Processo
Faturamento e Expedição	Gerente de Logística	Aprovado	Definição do escopo; Análise de riscos; Plano de continuidade de negócios	Aprovado	Com o plano de continuidade temos condições de imaginar um tempo mínimo para a recuperação do processo em caso de desastre. O objetivo é formalizar as ações a serem realizadas para que o faturamento não seja interrompido.	Patrocinador
Faturamento e Expedição	Diretor Financeiro	Aprovado	Definição do escopo; Análise de riscos; Plano de continuidade de negócios	Aprovado	O plano de continuidade, principalmente quando avaliamos os riscos, nos permite enxergar o prejuízo que a empresa pode ter caso não possua controles eficientes. PAra os próximos semetres será ampliado o orçamento para investimento em ações de tratamento, tratando os riscos de forma proativa.	Patrocinador

Item 14.1. INDICADORES DA CONTINUIDADE DE NEGÓCIOS			
Plano de Continuidade de Negócios	**Indicador de performance**	**Meta**	**Realizado**
Faturamento e Expedição	Quantidade de horas perdidas por usuários devido à inoperância não planejada dos sistemas		10
Faturamento e Expedição	Porcentagem de incidentes atendidos e solucionados pelos planos de resposta a incidentes		95%
Faturamento e Expedição	Porcentagem de incidentes atendidos e solucionados dentro do prazo do SLA		95%
Faturamento e Expedição	Porcentagem de ativos cobertos pelo plano de continuidade de negócios		100%
Faturamento e Expedição	Frequencia de interrupção de serviços nos sistemas críticos	Nunca	
Faturamento e Expedição	Sucesso na recuperação de desastres através do plano	Sim	
Faturamento e Expedição	Desastres ocorridos		0

Item 15.1. INDICADORES DA CONTINUIDADE DE NEGÓCIOS							
Plano de testes	**Ação de teste**	**Ações a serem testadas**	**Objetivo**	**Complexidade**	**Periodicidade de realização**	**Responsável**	**OLA**
Teste de VMotion	Interromper um Host de virtualização, forçando a migração das VMs para o outro	Subir VMs Críticas em único host	Validar o SLA de parada para executar o Vmotion e analisar o desempenho dos servidores	Baixa	Trimestral	Coordenador de TI	
Avaliar Data Center sem Ar Condicionado	Desativar o Ar Condicionado do Data Center	Abrir as janelas do Data Center	Acompanhar o funcionamento do Data Center sem Ar Condicionado	Baixa	Anual	Coordenador de TI	
Troca de servidor de acesso ao TS	Realizar o acesso remoto dos coletores WMS em servidor secundário	Ativar emissão de NF em contingência	Verificar o funcionamento da ação de resposta	Baixa	Semestral	Coordenador de TI	
Emissão de Nfe em Contingência	Ativar a emissão de Nota Fiscal em contingência no ERP	Direcionar TS para outro servidor temporário	Acompanhar a emissão de nota fiscal em formulário de contingência, sem o servidor de Nfe	Média	Anual	Coordenador de TI	

Item 16.1. REVISÃO E MANUTENÇÃO DO PLANO DE CONTINUIDADE						
Plano de continuidade	**Etapa**	**Revisão realizada**	**Objetivos**	**Frequência de revisão**	**Responsável pela revisão**	**Responsável pela aprovação**
Faturamento e Expedição	Definição dos papéis e responsabilidades	Revisar e atualizar equipe	Manter um cadastro real dos colaboradores que pertencem a equipe.	Mensal	Coordenador de TI	Gerente de Logística
Faturamento e Expedição	Mapeamento do Processo	Revisar mapeamento do processo	Identificar alterações no processo de negócio	Semestral	Coordenador de TI	Gerente de Logística
Faturamento e Expedição	Identificação dos ativos	Reidentificação dos ativos	Identificar alterações nos ativos mapeados e atualizar o Plano de Continuidade	Bimestral	Coordenador de TI	Coordenador de Expedição
Faturamento e Expedição	Análise de riscos	Revisão dos riscos dos ativos do processo	Revisar possíveis riscos envolvendo ativos existentes e novos identificados	Bimestral	Coordenador de TI	Gerente de Logística
Faturamento e Expedição	Elaboração das ações de tratamento do risco	Atualizar ações de tratamento do risco	Identificar e gerar novs ações de tratamento para riscos emergentes ou levantados nas demais revisões.	Trimestral	Coordenador de TI	Gerente de Logística
Faturamento e Expedição	Implementação da documentação e controles (OLAs)	Implementação e Atualização dos OLAs	Atualizar existente e implementar novos OLAs para atender todas as ações do Plano.	Conforme demais alterações	Coordenador de TI	Coordenador de TI
Faturamento e Expedição	Elaboração do plano de resposta a incidentes	Revisão da documentação do plano de resposta a incidentes	Verificar a abrangência do plano de resposta a incidentes com os riscos emergentes ou identificados nas revisões.	Trimestral	Coordenador de TI	Coordenador de TI
Faturamento e Expedição	Elaboração do plano de recuperação de desastres	Revisão do plano de recuperação de desastres	Verificar se as condições, ativos e ações do plano de recuperação continuam condizentes com a situação do processo e da empresa.	Anual	Coordenador de TI	Coordenador de TI

Item 17.1. CONTATOS								
Contato	**Empresa**	**Responsável**	**Ações envolvidas**	**Endereço**	**Telefone**	**Celular**	**E-mail**	**Outras formas de contato**
Consultor NFe	SuporteERP SA	Diretor SuporteERP	Consultor responsável pelo suporte ao sistema Totvs NFe			54 9999 9999	consultor.nfe@suporteerp.com.br	Skype: sonsultornfe
Consultor Linux	SuporteTI	Diretor SuporteTI	Suporte a Linux e ambiente de Virtualização		51 3222 2221	51 9999 9999	consultor.linux@suporteti.com.br	
Consultor Storage	SuporteTI	Diretor SuporteTI	Suporte a infra estrutura e Citrix		51 3222 2221	51 9999 9999	consultor.storage@suporteti.com.br	
Consultor SQL	SuporteTI	Diretor SuporteTI	Suporte a banco de dados SQL Server e Microsoft Sharepoint		51 3222 2221	51 9999 9999	consultor.sql@suporteti.com.br	
Consultor Citrix	SuporteTI	Diretor SuporteTI	Suporte a infra Estrutura e Citrix		51 3222 2221	51 9999 9999	consultor.citrix@suporteti.com.br	
Consultor Progress	SuporteERP SA	Diretor SuporteERP	Suporte a banco de dados Progress e Tecnologia Datasul		54 3222 2222	51 9999 9999	consultor.progress@suporteerp.com.br	
Consultor Banco	SuporteERP SA	Diretor SuporteERP	Suporte a banco de dados Progress e Tecnologia Datasul		54 3222 2222	54 9999 9999	consultor.banco@suporteerp.com.br	
Consultor WMS	SuporteERP SA	Diretor SuporteERP	Suporte ao sistema WMS e Faturamento		54 3222 2222	54 9999 9999	consultor.wms@suporteerp.com.br	
Programador WMS	SuporteERP SA	Programador ERP	Desenvolvedora de programas para o WMS		54 3222 2222	54 9999 9999	programador.wms@suporteerp.com.br	
Programador ERP	SuporteERP SA	Diretor SuporteERP	Gerente de desenvolvimento da Totvs		54 3222 2222	54 9999 9999	programador.erp@suporteerp.com.br	
Suporte Nobreak	EletroRede Ltda	Diretor Eletrorede	Manutenção Elétrica e No-Breaks		54 3222 2222		suporte@eletrorede.com.br	
Manutentor de Rede	InfraRede Ltda	Manutentor de Rede	Serviço de cabeamento de rede		54 3222 2222	54 9999 9999	infrarede.solucoes@gmail.com	
Barras	Barras Automação Ltda	Gerente Técnico Barras	Manutenção nas impressoras de Etiquetas		54 3222 2222	54 9999 9999	edson@barras.com.br	
Dell Suporte	Dell Computadores		Suporte em garantia aos equipamentos de informática		0800 111 2222			www.dell.com.br / support.dell.com
PC Suporte Ltda	PC Suporte Ltda	Diretor Pc Suporte	Suporte a microinformatica		54 3222 2222		suporte@pcsuporte.com.br	
Suporte Print	Suporte Print Informática Ltda	Gerente Comercial Print	Manutenção de impressoras Laser		54 3222 2222		suporte@suporteprint.com.br	

Consultor Firewall	Suporte Firewall Informática	Consultor Firewall	Suporte ao Firewall Sonic Wall	54 3222 2222	51 9999 9999	consultor@suportefirewall.com.br	
Suporte Firewall	Suporte Firewall Informática	Consultor Firewall	Suporte ao firewall Sonicwall	54 3222 2222		suporte@suportefirewall.com.br	http://support.suportefirewall.com.br/
TOTVS Suporte	TOTVS SA		Suporte ao sistema Datasul EMS	4000 0000			http://suporte.suporteerp.com.br
Consultor Microsoft	SuporteTI	Diretor SuporteTI	Suporte ao ambiente Microsoft	51 3222 2221	51 9999 9999	consultor.microsoft@suporteti.com.br	
Consultor Telefonia	Suporte Telefonia Ltda	Gerente Telefonia	Suporte a telefonia e Central Telefônica	54 3222 2222		consultor@suptelefonia.com.br	
Gerente Telefonia	Suporte Telefonia Ltda	Gerente Telefonia	Suporte a telefonia e Central telefônica	54 3222 2222	54 9999 9999	gerente@suptelefonia.com.br	
Consultor Coletor	Coletores SA	Gerente Coletor	Suporte aos coletores de dados Motorola	54 3222 2222	54 9999 9999	consultor@coletoressa.com.br	
Suporte Coletores SA	Coletores SA	Gerente Coletor	Suporte aos coletores de dados Motorola	54 3222 2222		suporte@coletoressa.com.br	
Eletricista Eletro	Eletro Instalações Elétricas Ltda	Eletricista Eletro	Manutenção e apoio no Fornecimento de Energia Elétrica externa.		54 9999 9999		
Eletricista EnergiaSA	Energia SA	Eletricista EnergiaSA	Manutenção e apoio no Fornecimento de Energia elétrica externa	54 3222 2222	54 9999 9999	carlos@energiasa.com.br	
Vendedor SuporteTI	SuporteTI	Diretor SuporteTI	Consultor de vendas da DELL. Necessário para novas aquisições.	51 3222 2221	54 9999 9999	vendedor@suporteti.com.br	
Diretor SuporteTI	SuporteTI	Diretor SuporteTI	Diretor responsável pela SuporteTI SA. Fornece suporte em definições comerciais e de serviços. Deve ser acionado na recuperação de desastres.	51 3222 2221	51 9999 9999	diretor@suporteti.com.br	
Suporte Telecom SA	Telecom SA	Gerente Telecom SA	Suporte ao fornecimento de Link de Internet	0800 000 1111			
Gerente Telecom SA	Telecom SA	Gerente Telecom SA	Pós Vendas Telecom SA, suporte ao fornecimento de Link de Internet	51 3222 2221	51 9999 9999	gerente@telecomsa.com.br	

ANEXO E – Questionário para avaliação do plano de continuidade

Anexo E. Questionário para avaliação da Continuidade de Negócios na empresa		
Questão	**Parecer do gestor**	**Pontuação**
O escopo da continuidade de negócios foi determinado?	Sim	2
O Plano de Continuidade atende todo o processo definido no escopo?	Sim	2
Há responsáveis por ações do Plano não relacionadas na equipe definida?	Sim	2
Existe comprometimento da alta gestão na implantação da continuidade de negócios?	Parcialmente	1
A continuidade de negócios faz parte da estratégia da empresa?	Não	0
Os objetivos e benefícios da continuidade de negócios estão sendo disseminados na organização?	Não	0
Foi realizada uma análise de riscos e impacto ?	Sim	2
A TI da empresa é responsável pelo plano de continuidade?	Sim	2
Foram disponibilizados recursos financeiros para realizar as ações de tratamento e elaboração do plano de continuidade de negócios?	Parcialmente	1
As definições de processos que a empresa toma estão alinhadas com o processo de continuidade?	Parcialmente	1
A continuidade de negócio está envolvida em algum padrão (ISO) ou outros critérios de qualidade de alguma forma?	Sim	2
A empresa está utilizando uma ferramenta para gerenciar a continuidade de negócios?	Sim	2
O plano de recuperação de desastres garante segurança na retomada do negócio em caso de ocorrência de desastres?	Sim	2
Você se sente seguro com o plano de continuidade?	Sim	2
Resultado da avaliação	81%	21
Respondido por:	Diretor Financeiro	