PROPOSTA DE PLANO DE CONTINUIDADE DE NEGÓCIO EM TI PARA UM HOSPITAL NORTE CATARINENSE

SILVA, Eduardo Prestes[1]
MISAGHI, Dr. Mehran[2]

RESUMO

Os Sistemas de informação tem assumido cada vez mais um papel estratégico nas organizações, ao mesmo ponto que as tornam cada vez mais dependentes da sua efetividade para assegurar a continuidade dos seus processos de trabalho. A Segurança da informação, por sua vez, busca garantir a continuidade e minimizar os impactos nos negócios. Esse trabalho tem como objetivo elaborar uma proposta de Plano de Continuidade de Negócios (PCN), voltado para a área de Tecnologia de Informação (TI) em um ambiente Hospitalar, baseado em normas e boas práticas no ambiente de TI, identificando os processos organizacionais mais críticos para com isso elaborar estratégias que assegurem a continuidade das operações de trabalho mesmo em eventos de disrupção.

Palavras-chave: Plano de Continuidade de Negócios; Incidente; Sistemas de informação; Tecnologia; Segurança da informação.

1 INTRODUÇÃO

No mundo dos negócios, os dados e a informação são considerados a moeda de ouro da vez. A Tecnologia da Informação (TI), torna-se cada vez mais imprescindível e estratégica para as organizações. No universo hospitalar a realidade não é diferente, ao passo que cada vez mais são implementados sistemas para agilizar e suportar seus processos, aumentando cada vez mais sua dependência da TI.

Dentro desse contexto, a Segurança da Informação (SI) é um ponto crucial para as organizações. Vivemos a mercê de condições adversas as quais podemos ser submetidos a qualquer momento, como tempestades, incêndios, crises e

[1] Eduardo Prestes Graduando do Curso de Sistemas de Informação do Centro Universitário UNISOCIESC, eduardoprestes29@gmail.com;
[2] Professor orientador: Dr. Mehran Misaghi, Centro Universitário UNISOCIESC, mehran.misaghi@unisociesc.com.br;

imprevistos que fogem ao nosso controle, sem deixar de mencionar as ações humanas de terrorismo cibernético com o objetivo de invadir e sequestrar dados para fins ilícitos.

Quando um incidente causa perdas e prejuízos significativos, a organização pode se sentir amedrontada, principalmente se houver interrupção nos negócios e na TI, onde o perfil de infraestrutura corporativa sustenta áreas de negócios. As perdas também podem motivar e convencer quando há avaliação e previsão (MARINHO, 2018). Nesse cenário, onde o ambiente hospitalar é ainda mais crítico e a TI é essencial para o bom funcionamento dos fluxos de processo dentro do Hospital, será que estamos preparados para agir frente a essas situações atípicas?

No funcionamento das organizações, os Sistemas de informação são elementos essenciais para a continuidade e sucesso de seus objetivos, e observa-se que cada vez mais esses sistemas assumem um papel estratégico e de relevância, vitais para elas, devido a fidelidade das informações em relação aos dados, visando verificar se os resultados obtidos estão corretos ou não (GIL; ARIMA, 2018).

O mercado da saúde também segue a crescente informatização dos serviços médico-hospitalares, demonstrando enorme avanço e tem contribuído para uma maior eficiência e qualidade. A boa estruturação da informática também promove o desenvolvimento empresarial destas organizações (LONDOÑO; LAVERDE; LONDOÑO, 2016).

Diante desse cenário, onde os processos de trabalho são cada vez mais dependentes dos SI, alguns questionamentos se fazem pertinentes: Como preparar as empresas para garantir a continuidade de seu negócio em uma 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?

Para isso o objetivo principal deste trabalho, é a elaboração de uma proposta de Plano de Continuidade de Negócios para os serviços mais críticos de TI dentro do ambiente hospitalar, a fim de mitigar os impactos de uma possível interrupção dos serviços, e também desenvolver um plano para restabelecê-los no tempo mais breve possível.

Este trabalho consiste em um roteiro de atividades a serem seguidas e um conjunto de artefatos. As atividades envolvem o mapeamento de riscos nos processos de negócio, a definição das ações para tratamento desses riscos, os planos de resposta a incidentes e planos de recuperação de desastres e o processo de execução e monitoramento das ocorrências e também um estudo de caso dentro da unidade hospitalar. Os artefatos gerados serão documentos do processo, incluindo o plano concreto de continuidade de negócios.

2 REFERENCIAL TEÓRICO

De acordo com o IT Governance (2019), a continuidade de negócio é a disciplina focada principalmente em manter a capacidade de uma organização em funcionar durante um evento disruptivo, proporcionando a continuidade das suas funções mais críticas, mesmo que de forma reduzida.

O surgimento de pandemias, por exemplo, tem sido um desafio para muitas pessoas e organizações, afetando suas rotinas e impactando nas atividades econômicas com perdas significativas. De acordo com Manoel (2019), pandemias já eram tidas como ameaças em potencial para a Continuidade dos Negócios, a crise do Ebola na África Ocidental e o surto do *zika* vírus já demonstravam o potencial desse tipo de ameaça.

Ter um Plano de Continuidade de Negócios (PCN), pode ser eficaz tanto para o tratamento de incidentes repentinos - como uma pandemia, quanto para incidentes graduais. Ao focar no impacto da interrupção e não na causa, a Continuidade de Negócios pode identificar os processos críticos para a organização, reconhecendo como agir para proteger seus principais ativos de informação, a sua cadeia de suprimentos, as partes interessadas e sua imagem (MANOEL, 2019).

O PCN é um processo que contempla um conjunto de normas e ações a serem executadas pelas organizações, a fim de garantir que não exista uma interrupção das atividades do negócio. Desta forma, a gestão deve informar o desastre no momento do ocorrido, ou antes (risco conhecido). Se não, o sucesso da continuidade do negócio estará em risco (BURTLES; FRY, 2016).

Um bom Plano de Continuidade é vivo e adaptável. Isto quer dizer que pode ser desenvolvido tanto na fase inicial de uma empresa, como em qualquer outro estágio de seu desenvolvimento (DORNELAS, 2016).

A Continuidade de Negócios pode ser percebida no dia-dia, desde a infância, como o ato de levar uma caixa cheia de brinquedos para brincar, no caso de ocorrer a quebra de algum brinquedo e precise ser substituído, até mesmo em situações mais complexas, como o soar de um alarme de incêndio em um edifício, onde ter tido um treinamento de evacuação anteriormente pode fazer toda a diferença para salvar sua vida (MANOEL, 2019).

Na Figura 1 são apresentadas as principais motivações para se realizar um Sistema de Gestão de Continuidade de Negócio em uma organização, apresenta-se os argumentos em ordem de criticidade.

Figura 1: Motivações do SGCN

Fonte: Sérgio da Silva Manoel (2019)

São várias as motivações para se implantar um PCN, entre elas, a preservação da vida das pessoas. *Compliance*[3] com leis e regulamentações também se destacam, como por exemplo a adaptação das organizações às leis da Lei Geral de Proteção de Dados (LGPD) no Brasil.

Outra motivação é a geração de um diferencial competitivo, já que uma empresa com consciência resiliente tende a enfrentar com mais facilidade situações adversas. E também é claro, a garantia da manutenção da disponibilidade dos negócios da organização (MANOEL, 2019).

2.1 DEFINIÇÃO DO ESCOPO DE TRABALHO

Conforme Oliveira (2020), no escopo devem-se conter os sistemas utilizados, serviços, funcionários, equipamentos e tudo o que for considerado crítico para o funcionamento do negócio. Desta forma, a proposta deste trabalho é focar na Tecnologia da Informação, visando implementar e aprender com o SGCN.

Ao passo em que os resultados da implementação em TI forem apresentados aos demais setores da organização, já com certo grau de experiência e maturidade, vislumbra-se a sensibilização dos demais setores para a importância do projeto, com foco em ampliar o escopo do SGCN para abranger outros processos críticos do negócio.

2.2 ANÁLISE DE IMPACTO NO NEGÓCIO

A Análise de Impacto de Negócio (BIA), em tradução livre, é um dos principais documentos gerados pelo Sistema de Gestão de Continuidade de Negócios (SGCN). Com base nesse documento criado por intermédio de entrevistas, serão elaboradas as ações a serem tomadas para mitigação dos possíveis riscos e também os planos a serem executados caso algum processo crítico seja afetado.

O resultado do relatório gerado pela BIA serve como base para a construção de um PCN, pois representa uma análise completa dos eventos dos quais a

[3] Conjunto de ações cujas consequências se refletem em estar incorporado ao cotidiano de um negócio ou relação da empresa com todos, materializando conceitos de fraude, corrupção, conflitos de interesses, etc. (MARINHO, 2018).

organização deve estar preparada para se recuperar. Nesse resultado são relacionados eventos que podem atrasar ou até mesmo encerrar as atividades da organização (SÊMOLA, 2014).

Como a BIA é gerada com base em entrevistas realizadas por meio de questionários, Manoel (2019) recorda sobre a importância de saber quais perguntas devem ser feitas aos entrevistados e também reitera sobre a importância de se levar em consideração os mais variados cenários durante essa fase.

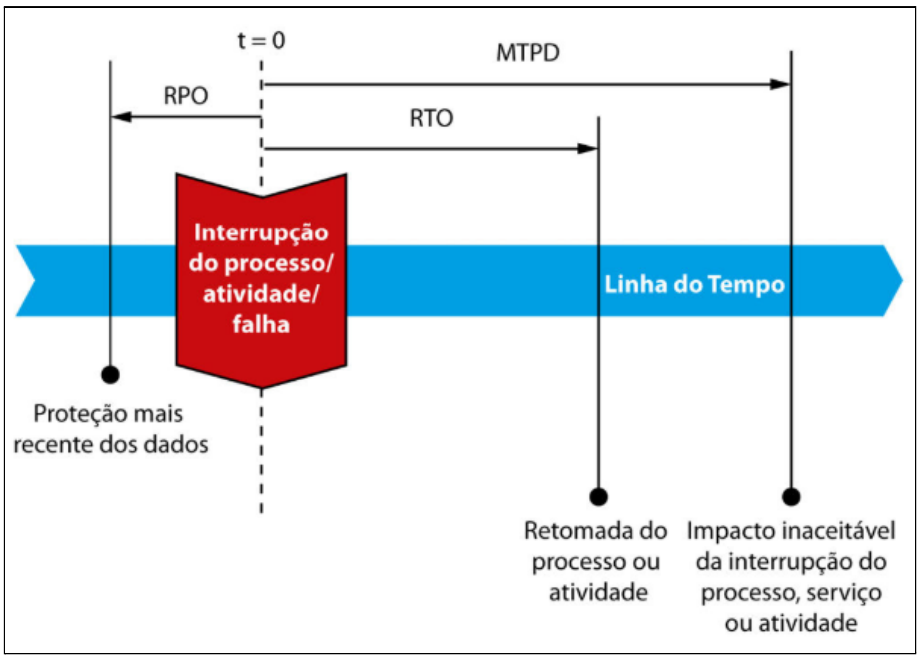
De acordo com Oliveira (2020), o objetivo do BIA é identificar os processos do negócio, as atividades e recursos fundamentais para o seu bom funcionamento, realizando uma análise de impactos relacionada a esses processos, sejam eles impactos operacionais, financeiros ou de imagem.

Alevate (2014), destaca sobre a importância da criação de uma análise de impactos que envolva uma relação financeira com o negócio, ou seja, que apresente resultados numéricos sobre possíveis perdas referentes a paradas nos processos críticos, já que esse com esse tipo de visualização torna-se mais fácil justificar todo o processo de SGCN.

Conforme Manoel (2019) o sucesso de todo o SGCN depende de uma boa análise de impactos de negócio, do inglês *Business Impact Analisys* (BIA), já que todas as tomadas de decisão serão feitas com base nesse documento que define a prioridade na recuperação dos processos visando a proteção do quê é tido como mais importante para a organização.

O tempo é um fator fundamental quando se está em uma situação de contingência. A Figura 2 ilustra um esquema onde são apresentadas algumas métricas de tempo relacionadas no processo SGCN.

Figura 2: Linha de tempo SGCN



Fonte: Manoel(2019)

Para melhor entendimento do esquema da Figura 2, as métricas de tempo são explicadas nos itens a, b e c:

a) RPO - Ponto Objetivado de Recuperação: *Recovery point* ou *last backup*, quanto a empresa pode perder de dados e informações: um minuto, uma hora. Ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada.

B) MTPD - Período Máximo de Interrupção Tolerável: Trata-se do período máximo executado em estado de contingência. Tempo necessário para os impactos adversos se tornarem inaceitáveis, que podem surgir como resultado de não executar um processo ou fornecer um produto/serviço ou realizar uma atividade.

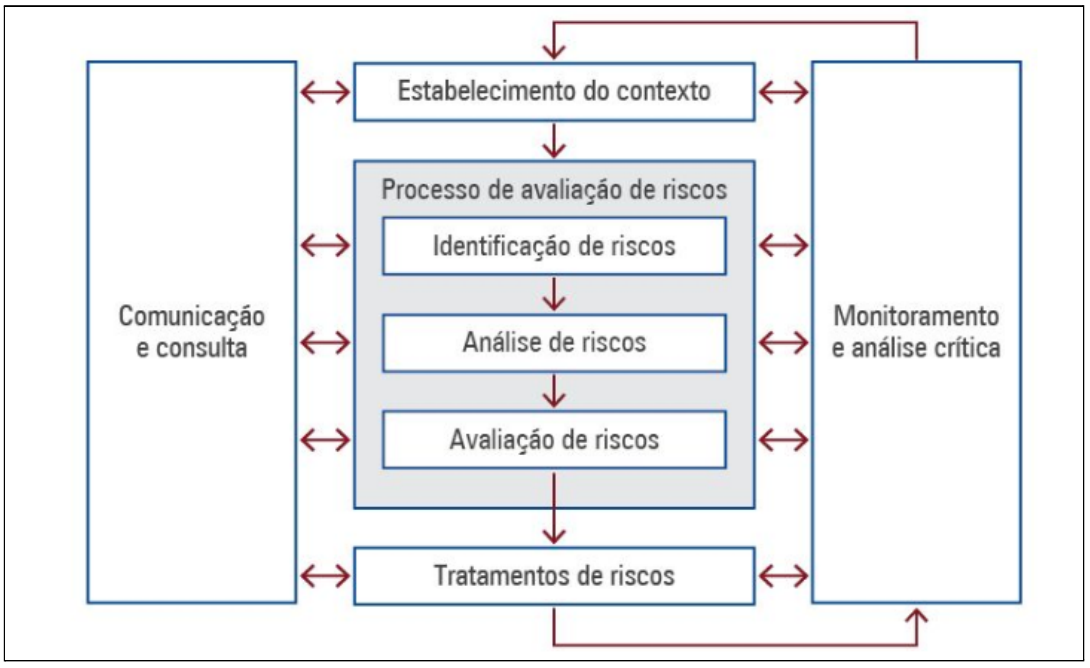
c) RTO - Objetivo do Tempo de Recuperação: *Recovery time*, limite de tempo para se ativar o PCN. O RTO é um indicador que expressa o valor de tempo máximo aceitável em que um sistema ou uma informação pode ficar indisponível após uma falha.

2.3 AVALIAÇÃO DE RISCOS

Com o relatório do BIA em mãos, já conhecendo todos os processos do negócio e o nível de criticidade dos mesmos para a organização, parte-se para a etapa de definição dos processos mais críticos a serem trabalhados.

Segundo a norma ISO 27005 (ISO/IEC 27005:2011), o processo de gestão de riscos é dividido em seis partes: definição do contexto, análise e avaliação dos riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco e o monitoramento e análise crítica de riscos. Na Figura 3, é representado esse esquema adaptado da norma ISO/IEC 27005:2011.

Figura 3: Processo de gestão de riscos



Fonte: Oliveira (2020)

.

2.3.1 Comunicação e consulta

A comunicação é um elemento fundamental em todos os momentos da gestão de risco, assim como a consulta a todas as partes pertinentes envolvidas.

2.3.2 Estabelecimento do contexto

Para Oliveira (2020), na etapa de definição do contexto, alguns fatores como cultura, política, financeiro, entre outros, são de vital importância e devem ser levados em conta para que tudo saia conforme o planejado e os objetivos sejam alcançados com sucesso.

2.3.3 Processo de avaliação dos riscos

Deve-se levar em consideração, a contratação de um profissional, para auxiliar na tarefa de identificação dos riscos (OLIVEIRA, 2020).

Na estimativa de riscos, deve-se determinar a atribuição de valor ao impacto que um risco pode ter, levando em consideração o tamanho, a complexidade e o volume de operações (ASSI, 2021).

2.3.4 Tratamento de riscos

Contempla todas as estratégias, técnicas e métodos aplicados no tratamento dos riscos, além de contribuir no apoio à tomada de decisão (OLIVEIRA, 2020).

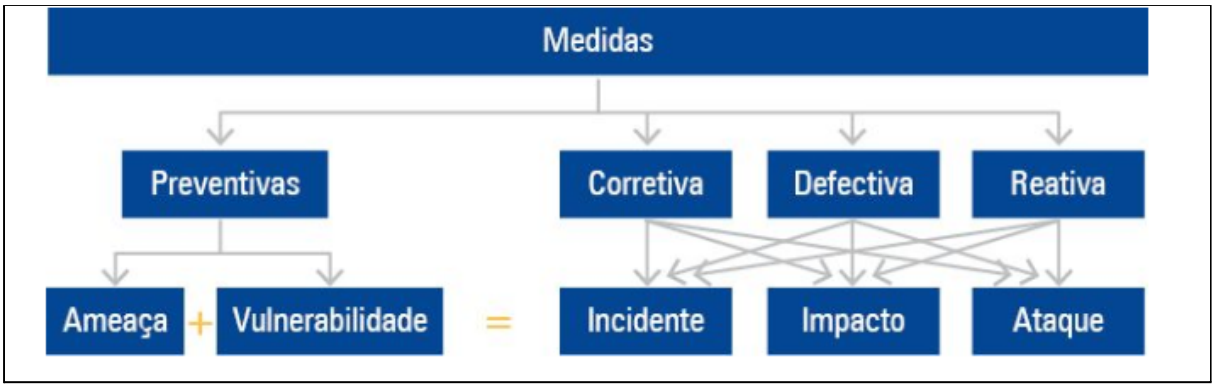
2.3.5 Monitoramento e análise crítica dos riscos

Devem ser realizadas periodicamente, para checar e reavaliar os riscos (OLIVEIRA, 2020).

Nesse contexto, algumas medidas de proteção podem ser tomadas para mitigação dos riscos. Levando sempre em consideração que a prevenção é o melhor remédio, já que depois que o incidente ocorre certamente o custo para correção ou amenização do impacto certamente será maior (OLIVEIRA, 2020).

A Figura 4 ilustra um esquema envolvendo as medidas a serem tomadas nas respectivas ocasiões.

Figura 4: Medidas de proteção



Fonte: Oliveira (2020)

Para Oliveira (2020), existem algumas categorias de riscos já mapeadas as quais o ambiente de TI está exposto inevitavelmente: riscos de segurança, riscos de disponibilidade, riscos de performance, riscos de conformidade, riscos de confidencialidade e riscos de integridade.

O apetite ao risco se refere ao quanto de risco uma organização está disposta a sofrer, mantendo os objetivos planejados no seu SGCN. Utilizando parâmetros financeiros torna-se mais fácil o compreendimento desse fator, por exemplo, qual o valor aceitável de perdas e quais níveis devem ser obrigatoriamente observados na fase de tratamento de riscos (MANOEL, 2019).

Implementar a gestão de riscos dentro de uma empresa, é uma forma de regulamentar, criar uma cultura organizacional e disseminar o conhecimento além de tornar a organização resiliente perante as mais diversas situações.

2.4 A GESTÃO DO CONHECIMENTO E A CONTINUIDADE DO NEGÓCIO

A Gestão do Conhecimento (GC) existe nas organizações com o objetivo de preservar o conhecimento, garantindo a continuidade dos processos organizacionais, entre outros fatores, como por exemplo, a promoção da vantagem competitiva (BUOGO et al., 2016).

Um exemplo a ser apontado é a Pandemia do Coronavírus (2019). De acordo com Irkey e Tüfekci (2021), a troca de conhecimento entre os países desempenhou um papel importante durante todas as fases, desde o surgimento do COVID-19 até os governos tomarem medidas para combater a pandemia, embasadas em informações obtidas pelos primeiros países afetados.

Uma organização tem como principais fatores geração, aquisição, compartilhamento e exploração de conhecimento; essenciais para o seu sucesso. Deste modo, um dos desafios de sua gestão é reconhecer e trocar conhecimentos entre diferentes grupos e organizações (BESSANT; TIDD, 2019).

Quando o conhecimento é gerenciado de forma adequada, coopera para o gerenciamento de uma crise como uma pandemia; em uma escala menor, pode garantir que uma empresa afetada permaneça no mercado, dando a continuidade aos negócios (IRKEY; TÜFEKCI, 2021).

3 METODOLOGIA

Neste capítulo serão apresentados os procedimentos metodológicos necessários para a elaboração de um PCN dentro do ambiente hospitalar. Com o intuito de alcançar os objetivos propostos no início deste trabalho, esta pesquisa seguiu algumas etapas, sendo elas a pesquisa bibliográfica que se baseou na literatura encontrada disponível sobre o tema e também alguns estudos de caso já realizados até o presente momento.

3.1 CARACTERIZAÇÃO DA PESQUISA

Uma pesquisa baseia-se em investigação, indagação e busca, e o tipo de pesquisa aplicado neste trabalho é o descritivo. A pesquisa descritiva retrata o que é existente, estuda novos significados, determina a frequência de certas ocorrências, inclui a descrição de conceitos e também, desenvolvimento de hipóteses que providenciam base para a pesquisa quantitativa.

Uma pesquisa bibliográfica, por sua vez, corresponde à etapa inicial de todo o trabalho acadêmico ou científico, tendo por objetivo reunir informações e dados que serão utilizados como base para construir a investigação proposta, a partir de determinado tema.

Dentre os diversos tipos de pesquisa, ainda há a pesquisa de campo, onde é realizada a observação do cenário, fazendo coleta de dados, analisando e interpretando os resultados estudados, diretamente do ambiente natural ou da referida realidade onde ocorre.

3.2 AMBIENTE DA PESQUISA

O estudo presente neste trabalho foi realizado em um hospital público de grande porte, situado no município de Joinville, Estado de Santa Catarina, que teve sua inauguração em 1906.

A estrutura física do hospital conta com mais de 200 leitos e 70 leitos de Unidade de Terapia Intensiva (UTI).

Como parte da infraestrutura, se destacam a recepção, que conta com 4 recepcionistas, onde cada uma utiliza um computador e os médicos que utilizam seus computadores individuais, para atualização do estado do paciente e geração de receitas e atestados.

A infraestrutura ainda conta com 480 computadores *desktop*, 105 impressoras multifuncionais, 15 impressoras de etiqueta/pulseira, 5 *notebooks*, 8 servidores físicos e 18 máquinas virtuais[4].

Referente ao setor da TI, o hospital possui atualmente um coordenador e três analistas auxiliares. Os serviços de suporte aos sistemas e às impressoras são realizados por uma empresa terceirizada.

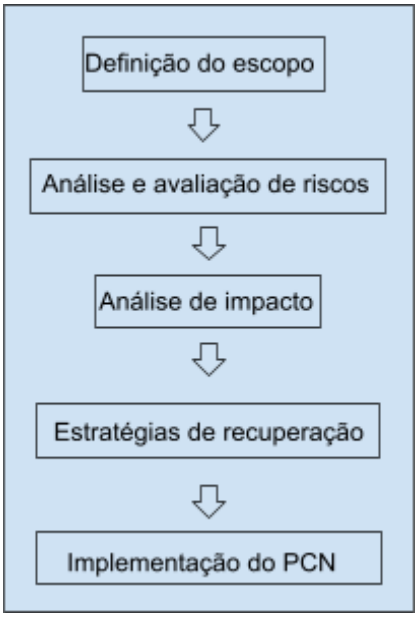
3.3 ETAPAS DA PESQUISA

A primeira etapa realizada, foi a pesquisa bibliográfica, conforme apresentado no tópico 3.2. Após esta etapa, foi realizada a pesquisa de campo, que se deu por meio de uma entrevista, em forma de questionário, o qual continha 10 questões objetivas, respondidas pelo coordenador responsável pela equipe de TI do hospital.

As etapas da pesquisa podem ser representadas de acordo com a Figura 5, que apresenta a sequência operacional que este trabalho seguiu para alcançar seus objetivos, iniciando pela definição do escopo e encerrando com a implementação do PCN.

[4] Simula um ambiente real (físico), que proporciona a utilização de diversos recursos e sistemas, sem a necessidade de acesso físico à máquina que os hospeda (VELLOSO, 2017).

Figura 5 - Etapas Operacionais



Fonte: O Autor (2021)

3.3.1 Definição do escopo

O escopo foi definido e elaborado de acordo com as áreas a serem estudadas e observadas dentro do ambiente hospitalar, ou seja, os setores de farmácia e recepção.

3.3.2 Análise e avaliação de riscos

Após escolha do hospital a ser aplicado o projeto, e aceitação do estudo de caso, foi encaminhado um questionário com algumas perguntas para conhecimento do nível de maturidade do mesmo em relação ao tema apresentado e também obter algum direcionamento para o rumo da pesquisa. Essas perguntas estão disponíveis no apêndice A, e foram formuladas com base na literatura consultada na etapa de pesquisa.

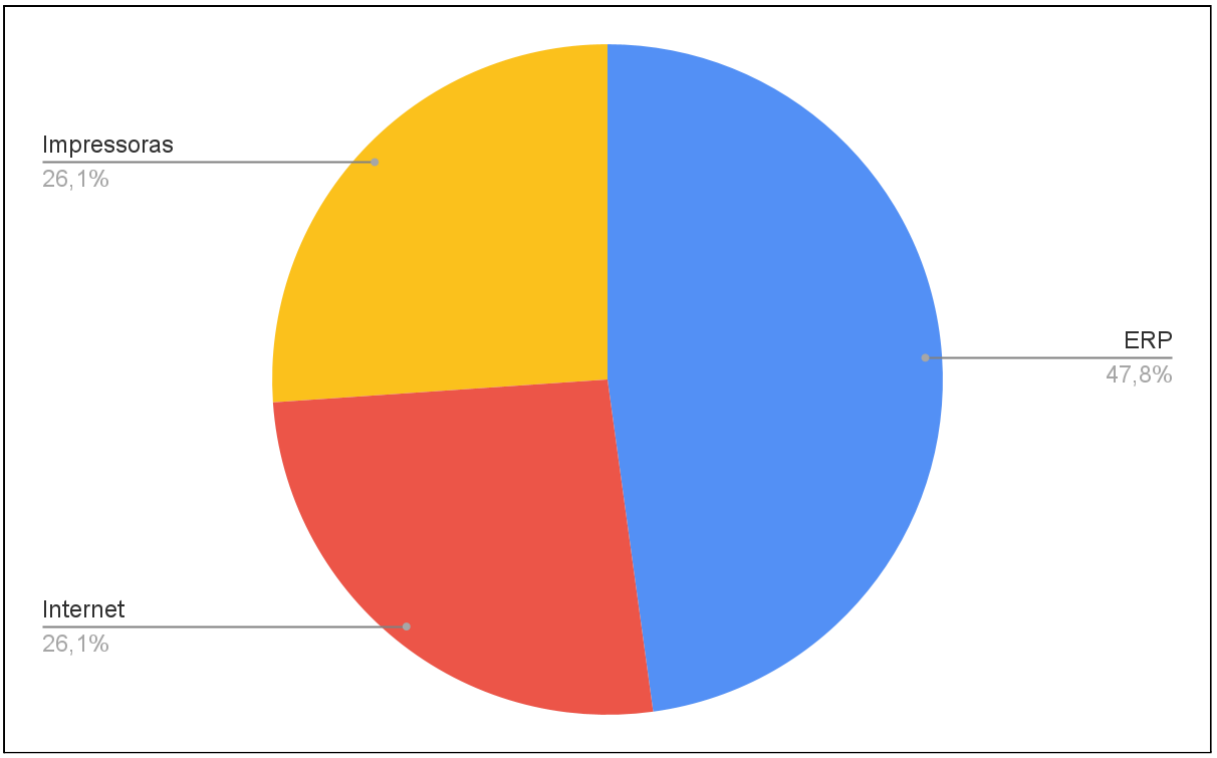
Posteriormente em reunião com o time de TI para formalização da proposta, foi debatido um pouco mais sobre o tema, inclusive sobre algumas respostas do questionário enviado previamente, para entender como funciona e como está estruturada a configuração atual de TI dentro do hospital. Nessa mesma ocasião também foi apresentado o ambiente de infraestrutura.

Já definido o escopo de trabalho, foi dado início ao acompanhamento das rotinas de trabalho dos setores de recepção e de farmácia. Este trabalho foi realizado entre junho de 2020 até junho de 2021.

Em conversa com os responsáveis pelo setor de TI, para conhecer como o sistema efetivamente está estruturado e também sondar estratégias para mitigar os impactos causados pela parada do serviço de impressão nos determinados setores, foram coletadas algumas informações referentes a eventos de falha nos sistemas de impressoras, Enterprise Resource Planning (ERP) e internet.

A figura 6 indica os eventos de falha de maior impacto registrados no período de monitoramento, os quais tiveram maior índice de recorrência em relação ao sistema ERP, com 11 ocorrências. As ocorrências de falha em impressoras e Intranet foram apontadas 6 vezes, cada uma. Foram desprezados eventos relacionados à lentidão no sistema.

Figura 6: Eventos de falha

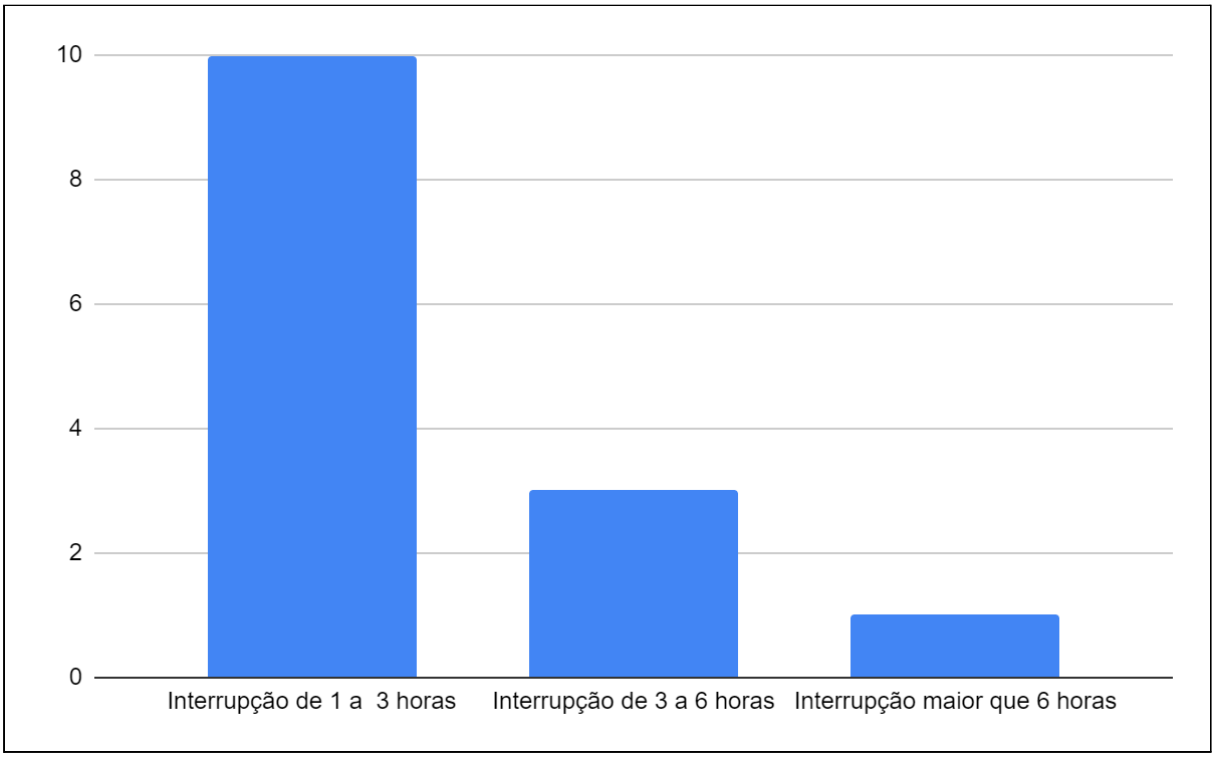


Fonte: O autor (2021)

Os eventos de falha mencionados na Figura 6, acarretam em erros ou até mesmo geram interrupções nos processos de trabalho. Essas interrupções normalmente são resolvidas em períodos de até 3 horas, salvo algumas exceções

que ocasionalmente dependem de serviços terceirizados. Os dados relativos aos períodos de interrupção estão representados na Figura 7.

Figura 7: Período de interrupção dos processos de trabalho



Fonte: O autor (2021)

Em paralelo ao trabalho de coleta dos dados e observação em campo, foram realizadas entrevistas com os operadores do sistema e atendentes, com o objetivo de ouvir as demandas, entender a rotina de trabalho e descobrir os pontos críticos do negócio, identificando os riscos aos quais as operações estão expostas e sua respectiva magnitude.

Juntando os relatórios de paradas dos sistemas, questionários e entrevistas foi possível apontar os possíveis eventos e as funções que deverão ser priorizadas durante uma contingência.

Com base na pesquisa de campo, foram identificados alguns possíveis riscos, os quais foram apontados com recorrência nos chamados internos da equipe de TI.

Os riscos referente à infraestrutura apontaram maior incidência de erros em impressoras. Referente aos sistemas, foi identificado maior incidência em falhas que

param o processo, acarretando em demora na conclusão de tarefas e por vezes, o cancelamento do processo digital, passando a ser manual.

3.3.3 Análise de impacto

Identificados os possíveis riscos, foi necessário analisar o impacto que estes podem causar na organização, caso se tornem muito recorrentes ou se atrelem a outros riscos similares. O Quadro 2 demonstra os possíveis impactos atrelados à parada dos principais processos críticos de trabalho identificados na organização.

Quadro 1 - Análise de impacto no negócio

Ocorrência	**Tipos de impactos: O - Operacional I - Imagem P - Pessoas**	**Tempo para impacto severo nesta metodologia será o RTO - Tempo Objetivado de recuperação 0 = duas semanas ou mais 1 = 1 semana 5 = menor que 3 dias 10 = 1 dia 20 = 4 horas 40 = imediato**	**Impacto operacional: 0 = nenhum 1 = baixo 3 = médio 5 = alto 7 = extremo**	**Impacto de imagem: 0 = nenhum 1 = baixo 3 = médio 5 = alto 7 = extremo**	**Impacto em pessoas: 0 = nenhum 1 = baixo 3 = médio 5 = alto 7 = extremo**	**Soma total:**
Queda do sistema de ERP	O, I, P	20	5	3	3	31
Queda do sistema de Internet	O, I, P	20	3	1	1	25
Queda do sistema de Impressão	O, I, P	20	5	3	1	29
Queda do sistema de Banco de dados	O, I, P	40	7	3	3	53

Fonte: O autor (2021)

Um dos pontos de impacto identificados foi referente ao Servidor de Banco de Dados, pois havendo falha no *Host* do Banco de Dados, o sistema irá parar até que o reparo seja executado. Caso a falha seja relacionada a algum outro sistema que está em *Cloud*[5], os que permanecem ativos trabalham em redundância.

3.3.4 Estratégias de recuperação

Sabendo dos impactos que os riscos podem causar na organização, sejam eles: operacionais, financeiros ou de imagem, foram elaboradas estratégias de longo prazo, as quais serão aplicadas de forma preventiva em novo projeto, que será apresentado pela equipe de TI à direção do hospital.

Uma das estratégias do hospital é manter *backups,* que são geridos pela Prefeitura Municipal de Joinville (PMJ), e são realizados três vezes ao dia, utilizando um sistema *Shadow*[6] e uma vez ao dia os *backups* incrementais. Os arquivos que são mantidos nas máquinas locais não entram na rotina de *backup*.

4 RESULTADOS E DISCUSSÕES

Conforme realizadas as etapas da pesquisa e a análise final, foi possível identificar que atualmente no hospital os problemas são resolvidos conforme vão surgindo, embora os setores já possuam estratégias para contornar as constantes paradas no sistema, conforme observado *in-loco*.

Na recepção, por exemplo, onde é feita a triagem dos pacientes, caso ocorra uma parada no sistema e eventualmente chegue algum paciente grave, ou a parada no sistema não tenha previsão de retorno breve, são utilizadas fichas manuscritas para abertura dos atendimentos dos pacientes, que posteriormente são lançadas no sistema. Alguns pontos de alerta referente a essa solução: quando essas fichas forem efetivamente lançadas no sistema, não será a hora exata em que o paciente deu entrada. A comunicação com prescrição de medicamentos e exames também se torna algo muito mais complexo, já que foge da rotina e controles habituais estabelecidos para um ambiente ideal com o funcionamento pleno dos sistemas.

---

[5] Computação em nuvem, que permite substituir os recursos de armazenamentos físicos por armazenamento (principalmente de servidor) e processamento compartilhado (CARVALHO; LORENA, 2017).

[6] Um arquivo shadow pode ser lido apenas por usuários com privilégios administrativos (como encarregados e gestores) (BASTA; BASTA; BROWN, 2015).

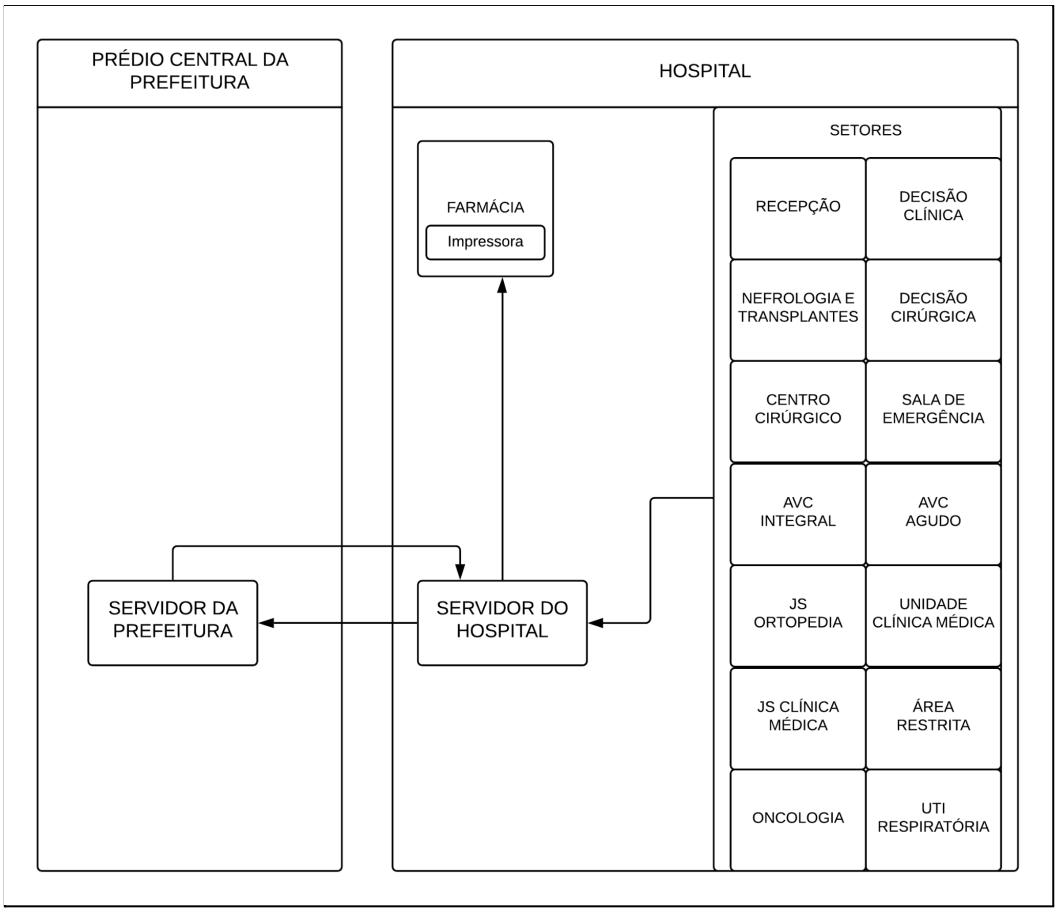
Outro ambiente observado foi a área de farmácia, pois conforme já mencionado, as prescrições de medicamentos ficam comprometidas com a instabilidade/queda dos sistemas, já que o controle e dispensação dos medicamentos são efetuados todos com o auxílio deles. Ainda em entrevista com os servidores do ambiente de farmácia, foi possível detectar unanimidade com relação a indisponibilidade dos serviços por conta da impressora que realiza a impressão das prescrições.

Tanto no setor de recepção quanto no setor de farmácia foi observado que a indisponibilidade das impressoras é uma falha recorrente, que ocorre com determinada frequência e afeta os trabalhos de forma significativa.

Como proposta de PCN para o problema citado, após análise de caso e possibilidades de resolução, chegou-se a algumas alternativas:

1. Uma impressora redundante em cada setor devidamente configurada, ligada diretamente via USB aos computadores. Essa opção é uma solução relativamente simples, que resolveria o problema para o não funcionamento das impressoras quando esse se tratar de indisponibilidade da rede. No entanto, foi questionada pelos administradores de TI, já que prejudicaria o controle do quantitativo de impressões que é realizado mensalmente, visto que o serviço de impressão é realizado por uma empresa terceirizada no município.
2. Criar um servidor de impressão exclusivamente para o hospital: visto que atualmente o servidor de impressão fica localizado no prédio central da prefeitura do município localizado a vários quilômetros, ou seja a cada nova impressão, é realizada uma requisição ao servidor da prefeitura que registra e libera a solicitação novamente para o hospital, conforme esquema representado na Figura 6. Ou seja, além dos problemas com a rede interna do hospital, atualmente podem ocorrer eventuais rompimentos da rede, ou até mesmo problemas no servidor da PMJ, que são fatores do ambiente externo que acabam afetando serviços críticos do hospital, com a aplicação dessa solução seriam eliminados os fatores externos ao hospital.

Figura 8 - Fluxo do servidor de impressão



Fonte: O autor (2021)

Conforme pode-se observar na Figura 6, o fluxo do servidor de impressão é complexo e demorado, o que ocasiona alguns contratempos críticos, gerando chamados para a TI constantemente.

CONSIDERAÇÕES FINAIS

O estudo apresentado validou a possibilidade do desenvolvimento de uma proposta de Plano de Continuidade de Negócios para o hospital público do presente estudo de caso, onde com base na bibliografia disponível na fase de pesquisa, foram seguidas as etapas de implementação do PCN, possibilitando a identificação dos riscos envolvidos nos processos de trabalho relativos a área de TI e dessa forma, auxiliando na prevenção de erros conhecidos e desconhecidos, utilizando

meios de continuar os atendimentos e agendamentos, mesmo em momentos de queda dos sistemas e impressoras. Os resultados da pesquisa aplicada comprovaram o ganho de tempo entre a identificação do problema e sua resolução.

REFERÊNCIAS

ASSI, Marcos. **Controles Internos E Cultura Organizacional**: Como Consolidar A Confiança Na Gestão Dos Negócios. São Paulo: Saint Paul, 2020. 174 p.

ASSI, Marcos. **Gestão de riscos com controles internos**. 2. ed. São Paulo: Saint Paul, 2021. 218 p.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. São Paulo: Cengage Learning Edições Ltda, 2015. 376 p.

BESSANT, John; TIDD, Joe. **Inovação e empreendedorismo**. 3. ed. Porto Alegre: Bookman, 2019. 528 p.

BRASIL. ABNT. . **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. 2011. Disponível em: https://intranet.cade.gov.br/folder/files/arquivo/2018/07/36d5971bffbd671093ce8accf56a2895_43f5489ccd57165e9d2ce51b64c1aaea.pdf. Acesso em: 17 nov. 2011.

BUOGO, M., et al. (2016). **Metodologias de gestão do conhecimento considerando melhores práticas para segurança da informação**. In: 16º Conferência da Associação Portuguesa de Sistemas de Informação, 22 a 24 de setembro, Porto, Portugal.

BURTLES, Jim; FRY, Kristen Noakes. Principles and Practice of Business Continuity. Brookfield: Rothstein, 2016. 464 p.

CARVALHO, André C. P. L. F. de; LORENA, Ana Carolina. **Introdução à computação**: hardware, software e dados. Rio de Janeiro: Abdr, 2017. 200 p.

GIL, Antonio de Loureiro; ARIMA, Carlos Hideo. **Auditoria do Negócio com TI**: gestão e operação. São Paulo: Saraiva Educação S.A, 2018. 208 p.

IRKEY, Tuana; TüFEKCI, Aslıhan. **The Importance of Business Continuity and Knowledge Management during the Pandemic Period**. In: INTERNATIONAL MANAGEMENT INFORMATION SYSTEMS CONFERENCE. 7., 2020, Online. 2021.

IT Governance (Fev. 2019), **Business Continuity and ISO 22301.** disponível em https://www.itgovernance.co.uk/resources/green-papers/business-continuity-management-the-nine-step-appro. SL, 2019.

LONDOÑO, Gustavo Malagón; LAVERDE, Gabriel Pontón; LONDOÑO, Jairo Reynales. **Gestão hospitalar para uma administração eficaz**. 4. ed. Rio de Janeiro: Guanabara Koogan Ltda, 2016. 588 p.

MANOEL, Sergio Silva da. **Sistema de Gestão de Continuidade de Negócios**: esteja preparado para salvar a sua vida e os negócios em caso de um incidente ou desastre. 1. ed. Rio de Janeiro: Brasport, 2019. 354 p.

MARINHO, Fernando. **Plano de continuidade de negócios (PCN)**. Rio de Janeiro: Elsevier, 2018. 127 p.

MARTINS, Renato Cesar da Silva. **GESTÃO DA CONTINUIDADE DE NEGÓCIOS**: análise de impacto de negócio para entidades fechadas de previdência complementar (efpc). 2014. 88 f. Tese (Doutorado) - Curso de Redes de Computadores Com Ênfase em Segurança, Instituto Ceub de Pesquisa e Desenvolvimento - Icpd, Brasília, 2016.

OLIVEIRA, Roberto C. Q.. **Gestão de riscos e continuidade nos negócios**. São Paulo: Senac, 2020. 123 p.

SÊMOLA, Marcos. **Segurança da Informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014. 171 p.

VELLOSO, Fernando. **Informática**: conceitos básicos. Rio de Janeiro: Elsevier, 2017. 448 p.

Apêndice

Apêndice A: Roteiro utilizado na entrevista

No presente Apêndice é apresentado o roteiro utilizado na entrevista aplicada ao gestor da área de TI.

a) Como funcionaria a área de negócios se desktops, laptops, servidores, e-mail e acesso a internet não estiverem disponíveis?

b) Existe algum ponto de falha, ou seja, um único ativo que se falhar interrompe todo o fluxo de informação do processo?

c) Quais são os controles de Segurança da Informação implementados ou de gerenciamento de riscos que estão atualmente implantados?

d) Quais são as relações e dependências críticas dos prestadores de serviços?

e) Durante uma interrupção, quais soluções existem para os principais processos de negócios?

f) Qual é o número mínimo de funcionários necessários e quais as funções que eles precisam para realizar as suas responsabilidades em um ambiente de contingência?

g) Com que frequência são feitos backups?

h) Há Gestão do Conhecimento?

i) Há um responsável pela Gestão da Segurança da Informação ou uma empresa terceirizada?

j) Qual a estrutura de infra implantada atualmente (computadores e servidores), e quantas pessoas fazem parte do time de TI?