UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

LUCAS TEIXEIRA

PLANEJAMENTO DE *DISASTER RECOVERY PLAN* COM *BACKUP* EM NUVEM, VISANDO APLICAÇÕES EM PEQUENAS OU MÉDIAS EMPRESAS

CRICIÚMA
2019

LUCAS TEIXEIRA

PLANEJAMENTO DE *DISASTER RECOVERY PLAN* COM *BACKUP* EM NUVEM, VISANDO APLICAÇÕES EM PEQUENAS OU MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. Me. Paulo João Martins

CRICIÚMA

2019

LUCAS TEIXEIRA

PLANEJAMENTO DE DISASTER RECOVERY PLAN COM BACKUP EM NUVEM, VISANDO APLICAÇÕES EM PEQUENAS OU MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Segurança da Informação.

Criciúma, 26 de junho de 2019.

BANCA EXAMINADORA

Prof. Paulo João Martins - Me – (Unesc) - Orientador

André Faria Ruaro - Me - (Prefeitura Municipal de Criciúma)

Prof. Sérgio Coral - Esp - (Unesc)

RESUMO

Uma empresa pode fazer uso de diversos sistemas de informação, quando utilizado, esses manipulam dados que possuem uma determinada importância para a corporação. A perda de dados muitas vezes pode acarretar em grandes impactos negativos para a empresa que os possui, podendo até mesmo serem irreversíveis. Para evitar problemas como este, ou ao menos reduzir seu impacto na empresa, é que o *Disaster Recovery Plan* (DRP) é criado, ele é um plano com um conjunto de ações a serem tomados pela equipe de TI, para manter seus dados arquivados em segurança e recuperá-los caso venha a ocorrer problemas que possam comprometer os seus sistemas ou informações. A utilização da nuvem como local de armazenamento dos *backups* da empresa é uma estratégia a ser levada em consideração, pois desse modo seguiria a orientação de manter os dados de *backup* armazenados em um local distante da base original, se precavendo de perder ambos em uma ocasião de desastre físico do ambiente. O objetivo deste trabalho é elaborar um DRP, utilizando a computação em nuvem como local de armazenamento dos *backups* de um ambiente empresarial simulado de pequeno ou médio porte. Com a implementação do cenário e elaboração do plano conforme os materiais obtidos no levantamento bibliográfico, foi possível testa-lo e realizar a verificação de como foi a aplicação do plano criado, e se o mesmo cumpriu com o seu objetivo.

Palavras-chave: *Disaster Recovery Plan*. Computação em nuvem. *Backup*.

ABSTRACT

A company can make use of several information systems, when used, these manipulate data that have a certain importance for the corporation. The loss of data can often lead to large negative impacts on the company that owns them, and may even be irreversible. To avoid problems like this, or at least reduce its impact on the company, is that the Disaster Recovery Plan (DRP) is created, it is a plan with a set of actions to be taken by IT staff, to keep your archived data safe and to recover it if you experience problems that could compromise your systems or information. Using the cloud as a storage location for company backups is a strategy to take into account, as this would follow the guideline of keeping backup data stored in a location far from the original base, being careful to lose both on an occasion physical disaster of the environment. The objective of this work is to elaborate a DRP, using cloud computing as the storage location for backups of a small or medium-sized simulated business environment. With the implementation of the scenario and preparation of the plan according to the materials obtained in the bibliographical survey, it was possible to test it and carry out the verification of how the plan was implemented, and whether it fulfilled its objective.

Keywords: Disaster Recovery Plan. Cloud computing. Backup.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BCM	*Business Continuity Management*
CD	*Compact Disc*
DRP	*Disaster Recovery Plan*
DVD	*Digital Versatile Disc*
ERP	*Enterprise Resource Planning*
HD	*Hard Drive*
IaaS	*Infrastructure as a Service*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
ISO	*International Organization for Standardization*
NIST	*National Institute of Standards and Technology*
PaaS	*Platform as a Service*
RPO	*Recovery Point Objectives*
RTO	*Recovery Time Objectives*
SaaS	*Software as a Service*
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

O mundo encontra-se cada vez mais na era da informação, esse cenário faz com que as empresas tenham que se adaptar para continuar competindo. Essa exigência por mudanças está tornando o ambiente corporativo mais dependente da infraestrutura tecnológica que gerencia seus dados (BAZZOTTI; GARCIA, 2006).

Algumas empresas possuem diversas aplicações que são essenciais para o gerenciamento e controle dentro da mesma. Existem variados tipos de sistemas que podem estar sendo utilizados dentro de um ambiente empresarial, mesmo em pequenas e médias empresas, e muitos destes, manipulam e gerenciam dados cruciais. Assim como citado por Aguiar Junior (2012) qualquer tipo de interrupção nos sistemas que gere perda de dados, poderá representar um grande impacto financeiro para uma empresa.

Na atual realidade, e a relevância que os dados de uma empresa possuem, é de extrema importância que haja a conscientização de dispor de backups seguros, e um plano para recupera-los após qualquer eventualidade. O Plano de Recuperação de Desastres, do inglês *Disaster Recovery Plan* (DRP), é um documento que deve abranger a descrição das ações indispensáveis para a recuperação dos serviços, principalmente os críticos, após um determinado evento inesperado, deve conter os passos para preparar o local de *backup*, as funções e responsabilidades do pessoal envolvido, além de definir o inventário de *hardware* e *software* para a execução do plano (ANDRADE et al.,2011).

Segundo Westcon (2017), pequenas e médias empresas geralmente não possuem equipe especializada para a elaboração de um DRP, constantemente recorrendo apenas ao *backup*. Contudo, dependendo da maneira e frequência que o *backup* é feito, a empresa corre o risco de perder volumes de dados, ou considerando-se que o mesmo seja armazenado localmente, e o desastre comprometa a estrutura física da empresa, como os causados por incêndios, a mesma poderá perder todo o seu volume de dados.

Visando cenários empresarias como o citado anteriormente por Westcon (2017), onde a empresa de pequeno ou médio porte, não possua uma equipe treinada para a elaboração de um DRP, e que mantenha a segurança da informação confiada a *backups* armazenados localmente. A empresa estaria à mercê de um possível prejuízo, caso aconteça algum desastre.

Considerando possíveis problemas como o mencionado acima, o presente estudo teve a finalidade de conhecer a importância de se ter um DRP para empresas. Identificar as principais relevâncias que devem ser consideradas no momento da composição de um plano de recuperação de desastres. Deste modo criando um ambiente a fim de simular um cenário computacional empresarial de pequeno porte. Então elaborando um DRP, de acordo com o estudo realizado e o cenário feito, efetuando seus *backups* em nuvem, e assim podendo testa-lo para validar se o mesmo cumpri o proposito para ao qual foi elaborado.

1.1 OBJETIVO GERAL

Elaborar um estudo sobre a construção e aplicação de um *Disaster Recovery Plan*, utilizando a computação em nuvem como local de armazenamento dos *backups* de empresas de pequeno ou médio porte.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) compreender o conceito de computação em nuvem e sua utilização;
b) descrever o conceito e métodos de *Disaster Recovery Plan*;
c) entender o funcionamento de *backups* em empresas;
d) relatar a importância dos dados gerenciais no âmbito de uma empresa;
e) contribuir com o resultado de uma análise de implantação de um *Disaster Recovery Plan* para *backups* em nuvem, em um cenário de uma empresa de pequeno ou médio porte.

1.3 JUSTIFICATIVA

As empresas estão dependendo cada vez mais de sistemas de informações para auxiliar na gerência dos negócios. Essas necessitam que seja garantida a disponibilidade desses sistemas para manter seu negócio funcionando, tornando assim indispensável obter um DRP (ANDRADE et al.,2011). Por inúmeros motivos, mas principalmente pela falta de estratégia nas empresas, muitas são

surpreendidas por um acontecimento que pode ocasionar muitas perdas para a mesma.

Segundo Ávila, Soldan e Petroli Neto (2017), o uso de *backup* em nuvem já proporcionaria a retenção dos dados quando algo ocorrer inesperadamente com o *hardware* ou *software*, como desastres físicos, incêndios, roubos, ou por alguma falha humana. Tudo que possa danificar, ou pôr em risco de perda os dados de uma empresa, pode ser minimizado fazendo o uso de um *cloud backup* que possibilite a recuperação desses dados.

Considerando a importância que os dados possuem dentro de uma empresa, percebe-se a necessidade de obter-se uma solução viável e funcional, que possibilite a empresa recuperar seus dados e sistemas essenciais seguramente, evitando ou reduzindo seu prejuízo com o ocorrido.

Por este motivo, procura-se por meio deste trabalho, elaborar um DRP conforme estudos levantados, para ser aplicado em um ambiente de testes com um cenário aproximado a um ambiente computacional de uma pequena ou média empresa. Buscando constatar a viabilidade do plano elaborado e assim podendo servir de auxílio para empresas de pequeno ou médio porte, que despertem interesse em adotar um DRP para proteção de seus dados.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é composto por oito capítulos, sendo que o primeiro aborda uma introdução sobre o tema da pesquisa, o objetivo geral, objetivos específicos, justificativa e a própria estrutura do trabalho, aqui relatada.

O capítulo 2 descreve o *Disaster Recovery Plan*, onde é apresentado sua definição, o objetivo de sua aplicação e a responsabilidade imposta a um plano como esse, como também a sua relação com o plano de continuidade de negócios. Neste capítulo também é relatado a importância que um DRP tem para uma empresa, e é descrito como proceder para elaborar um planejamento de DRP.

No capítulo 3 é apresentado a definição de *backup*, suas modalidades, é descrito também seus principais tipos, locais de armazenamento e relatado a importância que o *backup* tem dentro de uma empresa.

O capitulo 4 caracteriza a computação em nuvem, descrevendo seu conceito e as vantagens de seu uso. O capitulo também apresenta uma definição dos

três principais modelos de serviço em nuvem. Buscando assim expressar um melhor entendimento sobre a computação em nuvem.

Os trabalhos correlatos que também foram utilizados como base para a realização deste projeto, estão apresentados no capítulo 5.

O capítulo 6 é composto pela metodologia aplicada no trabalho, além do trabalho desenvolvido, com a implementação do cenário, elaboração do DRP e a fase de testes.

No capítulo 7 é apresentado os resultados e discussões sobre o trabalho desenvolvido.

O capítulo 8, por fim, apresenta a conclusão do trabalho, juntamente com a sugestão de trabalhos futuros.

2 *DISASTER RECOVERY PLAN*

O *Disaster Recovery Plan* (DRP), ou Plano de Recuperação de Desastres em português, é um plano que possui nele descritos as medidas a serem tomadas para que haja a retomada dos serviços essenciais de TI, relatando as etapas a serem seguidas para a recuperação e disponibilização dos sistemas danificados por um desastre (ANDRADE et al.,2011).

Segundo Pinta (2011, tradução nossa) o DRP especifica as ações que serão realizadas imediatamente após a constatação de um incidente para o qual o plano foi projetado. Por esse motivo Aguiar Junior (2012) afirma que antes que se resolva acionar o plano em uma emergência, deve-se ter devidamente esclarecido em quais momentos o mesmo deve ser ativado.

O DRP é limitado aos recursos de TI, pois seu principal objetivo é recuperar a infraestrutura ou os sistemas danificados pelo desastre, com o menor espaço de tempo e o mínimo de perca de informação possível (PRAZERES, 2012).

Conforme Alhazmi e Malaiya (2013, tradução nossa), um conceito relevante em um DRP é a separação geográfica entre o site principal e o de *backup*. Visto que em escala global uma fração significativa de desastres são causados geograficamente pela natureza.

O *Disaster Recovery Plan*, é uma parte do plano de continuidade de negócios, é o componente responsável para manter e recuperar as informações ou sistemas, caso ocorra algum problema. No entanto o plano de continuidade de negócios contém a metodologia para manter os processos empresariais em ordem. (LUDESCHER; CUGNASCA, 2007, tradução nossa). Para Prazeres (2012) o DRP está ligado à infraestrutura, servidores, manutenção de aplicações, recuperação de sistemas e as informações em si. Diferentemente do plano de continuidade de negócios que possui um âmbito mais abrangente, focando na empresa como um todo, descrevendo componentes de negócio da organização referida, e seus elementos críticos, como por exemplo departamentos e áreas de negócio.

No ano de 2012 a Organização Internacional para Padronização, do inglês *International Organization for Standardization* (ISO) concebeu a ISO 22301:2012, que é uma padronização sobre Gestão de Continuidade de Negócios, do inglês *Business Continuity Management* (BCM). Essa norma descreve os requisitos para configurar e

gerenciar um sistema de gestão de continuidade de negócios (ISO, 2012, tradução nossa).

Em 2008 o Comitê Técnico Conjunto da ISO e da Comissão Eletrotécnica Internacional, do inglês *International Electrotechnical Commission* (IEC), produziram a ISO/IEC 24762. Esse padrão tem o intuito de amparar a operação de um sistema de gerenciamento de segurança da informação (SGSI), entregando orientações sobre o fornecimento de serviços de recuperação de desastres de tecnologia da informação e comunicação (ISO, 2008, tradução nossa). Porém, essa ISO consta como retirada do padrão internacional, desde 2014.

De acordo com Fernandes (2014) o processo de continuidade de negócios precisa do processo de recuperação de desastres para que a empresa possua suas operações retomadas. O plano de recuperação de desastres possui um processo mais técnico, descrevendo procedimentos, equipamentos, localizações e recursos humanos envolvidos, enquanto o plano de continuidade de negócios possui um processo mais ligado a gestão, que se destina a manter ou recuperar os processos de negócios da empresa, bens, e gestão de recursos humanos, após uma eventualidade.

2.1 TECNOLOGIA DA INFORMAÇÃO EM EMPRESAS

A tecnologia da informação é a parte tecnológica de um sistema de informação, é todo *software* e *hardware* que uma organização precisa para alcançar seus objetivos organizacionais. Incluindo não somente computadores, *disk drivers* e assistentes digitais, como também *softwares*, tais como: sistemas operacionais, pacotes *Office* e diversos outros programas computacionais que venham a ser utilizados em uma empresa (LAUDON; LAUDON, 2011). Melo (2008) amplia a ideia, definindo a tecnologia da informação como um recurso estratégico das empresas para obter vantagem competitiva, fazendo uso de todas as formas de informações, compreendendo aspectos organizacionais, administrativos e humanos.

Conforme Melo (2008) a tecnologia da informação possui uma grande importância para o sucesso das empresas, pois, é por meio dela que as mesmas são capazes de aprimorar seus fluxos de informação, integrar seus negócios e melhorar seu desempenho, de forma a preservar sua sobrevivência em mercados cada vez mais competitivos.

As empresas em geral utilizam suas informações como base para tomada de decisão, tornando esses dados algo vital para o desenvolvimento da organização. A perca dessas informações pode fragilizar a reputação da empresa e afetar diretamente as vantagens competitivas da mesma (NEVES, 2009).

2.1.1 O uso de sistemas de informação

Um sistema de informação pode ser definido como um grupo de componentes relacionados que recebem, fazem o processamento, armazenamento e distribuição de informações com o intuito de apoiar a tomada de decisões, controle e a administração de uma empresa. O sistema pode conter informações sobre pessoas, itens e locais significativos para a empresa ou para o meio ao seu redor (LAUDON; LAUDON, 2011).

Ainda conforme Laudon e Laudon (2011) uma empresa típica contará com sistemas que auxiliem os processos das principais funções de negócio, tais como, sistemas de vendas, produção, financeiro e recursos humanos. Entretanto, o autor afirma que os sistemas que funcionavam de forma independente uns dos outros estão cada vez mais ficando ultrapassados, sendo substituídos por sistemas que possibilitem a integração das atividades de processos de negócio.

Os sistemas de informação possuem um papel estratégico no mundo empresarial, sendo muito difundidos em grandes empresas, no entanto, possuem também uma grande importância para empresas de menor porte (GASQUES et al., 2016).

2.1.2 Pequenas e médias empresas

As pequenas e médias empresas possuem grande importância socioeconômica no Brasil, no que se refere à distribuição de empregos e renda (LIMA, 2001). Conforme Rossi e Theisen (2017) os empregos disponibilizados por pequenas e médias empresas tem um grande impacto na economia, pois enquanto grandes empresas cortam vagas para enfrentar as crises no mercado, as de menor porte fornecem muitas oportunidades e se beneficiam de profissionais qualificados disponíveis no mercado. No entanto, os autores afirmam que essas empresas de menor porte, de modo geral, tendem a ser menos formais e menos estruturadas.

Liderando assim os pedidos de falência e recuperação judicial em 2016, seguidas pelas médias e grandes empresas.

Segundo o BNDES (2019), as empresas podem ser classificadas conforme a tabela 1.

Tabela 1 – Classificação de porte empresarial conforme receita bruta anual

Porte	Receita Mínima	Receita Máxima
Pequenas Empresas	>R$ 360.000,00	<=R$ 4.800.000,00
Médias Empresas	>R$ 4.800.000,00	<=R$ 300. 000.000,00
Grandes Empresas	> R$ 300.000.000,00	-

Fonte: Adaptado de BNDES (2019).

De acordo com o SEBRAE (2014), também pode-se utilizar o número de pessoas ocupadas pela empresa como critério de classificação do porte da mesma, levando em consideração a atividade econômica da empresa, serviços e comércio ou indústria (tabela 2).

Tabela 2 – Classificação de porte empresarial conforme número de pessoas ocupadas na empresa

Porte	Serviços e Comércio	Indústria
Pequenas Empresas	De 10 a 49 Pessoas	De 20 a 99 Pessoas
Médias Empresas	De 50 a 99 Pessoas	De 100 a 499 Pessoas
Grandes Empresas	Acima de 100 Pessoas	Acima de 500 Pessoas

Fonte: Adaptado de SEBRAE (2014).

2.1.3 Importância do *disaster recovery plan* para empresas

A maioria das empresas dependem de seu ambiente computacional para manter seus negócios funcionando. Por isso é importante garantir a recuperação de seu ambiente computacional mesmo que em menor escala, após a ocorrência de um desastre (LUDESCHER; CUGNASCA, 2007, tradução nossa).

Vários tipos de desastres podem ocorrer a qualquer momento, sejam eles causado por problemas com o equipamento, falhas humanas, ou até mesmo desastres naturais. Dentre esses desastres, pode-se citar: problemas com equipamento e defeitos com *hardware*, falhas no servidor ou sistema operacional. Quando se trata de falhas humanas, considera-se como possíveis causas a negligência, sabotagem, atentados ou roubo de dados. Os desastres naturais são

eventos provocados por exemplo através de desabamento, enchente, chuvas fortes, tempestades ou até mesmo incêndios (LOPES, 2017). Segundo Netto e Silveira (2007) as pequenas e médias empresas também são atingidas por problemas computacionais e correm riscos com suas informações concentradas em um único lugar, porém as mesmas dispõem de menores recursos para investir em segurança da informação.

Conforme Prazeres (2012) ter um DRP é essencial para qualquer empresa, visto que uma falha nos servidores, comunicação ou suporte da informação que gere a indisponibilidade de serviços e a perca de informações, pode resultar em altos custos, principalmente monetários. Contudo a prevenção é bastante negligenciada e deixada para segundo plano, seja por descuido, por se negar a investir em prevenção, ou crença que só acontece aos outros. Porém o prejuízo com a falta de um DRP, tende a ser maior do que o gasto com a prevenção.

De acordo com Landry e Koger (2006, tradução nossa) desastres acontecem o tempo todo, inclusive cenários pouco prováveis não estão descartáveis de ocorrer em algum momento. O furacão Katrina demonstrou a importância de possuir um DRP bem-sucedido. Neste evento não se esperava que demoraria semanas para que as pessoas evacuadas conseguissem retornar a área metropolitana de Nova Orleans, e também não era esperado que residências e empresas ficassem sob água salgada durante semanas. Os sites da cidade permaneceram *off-line* porque não tinham um plano de recuperação de desastres. As fitas *backup* que sobreviveram por estarem localizadas nos níveis acima da água dos prédios inundados, acabaram danificadas por permanecerem semanas em um ambiente completamente úmido.

As organizações precisam entender que a recuperação de desastres é uma preocupação de segurança. Desastres que afetam equipamentos ou dados devem ser levados a sério, pois sem esses recursos, as organizações muitas vezes não podem trabalhar. O DRP é algo importante para todos os tipos de organizações, incluído as de pequeno e médio porte (LANDRY; KOGER, 2006, tradução nossa).

Conforme Andrade et al. (2011) é impossível ter um sistema sem que haja nenhuma vulnerabilidade e riscos, e muitas dessas situações de vulnerabilidade não são facilmente previstas. Por motivos como os tipos de desastres citados, que a instituição tem que estar sempre alerta, e essencialmente ter um bom plano para

resolver da forma mais rápida possível essas perdas de dados, visando reduzir o impacto causado a mesma (LOPES, 2017).

2.2 PLANEJAMENTO DE DRP

Na hora de fazer o planejamento de um DRP deve-se descrever os passos para preparar o local de *backup*, as funções e responsabilidades do pessoal envolvido, os eventos que retratam um desastre, além de definir o inventário de *hardware* e *software* para a execução do plano (ANDRADE et al.,2011).

Segundo Ávila, Soldan e Petroli Neto (2017), os profissionais de TI podem ter diversos planos de recuperação de dados, que vão desde replicação das informações em diferentes dispositivos, até a elaboração de estratégias de DRP baseado no *backup* em nuvem. Como esse trabalho tem como alvo a elaboração de um DRP para um cenário similar ao de uma pequena ou média empresa fazendo uso da última estratégia mencionada pelos autores, no capítulo 3 será feito um esclarecimento sobre *backups*, visando um maior embasamento sobre o assunto e no capítulo 4 será descrito uma visão geral para melhor entendimento sobre a computação em nuvem.

Um ponto muito importante é que a recuperação de um desastre é feita em um momento de crise e no menor tempo possível. Por esse motivo o DRP deve ser elaborado descrevendo as ações de forma precisa e clara, com a finalidade de facilitar suas execuções por profissionais que farão a recuperação (LUDESCHER, 2011).

Deve ser mencionado, quem pode executar o DRP, quem participará, qual é o objetivo e qual é o estado alvo que se deseja alcançar após a implementação do plano (PINTA, 2011, tradução nossa).

Conforme Ludescher e Cugnasca (2007) fazer uma análise de riscos é importante na elaboração de um DRP, pois essa análise fornece diretrizes para a concepção do processo de planejamento. Este tipo de análise, deve ser feita após o levantamento dos fatores mais prováveis que podem levar a um desastre que afete a empresa, para que após essa análise consiga-se criar maneiras de minimizar a exposição da empresa a esses desastres.

O plano também deve levar em consideração os impactos que a paralisação possa causar, além de o tempo máximo para restauração das atividades da organização (PEREIRA JUNIOR, 2008). Fazendo uma Análise de Impacto, torna-

se possível separar os serviços críticos utilizados na empresa, dos menos importantes para recuperação. (PINTA, 2011, tradução nossa). O princípio básico de uma Análise de Impacto, é que cada sistema da organização está ligado com a operação de outro, porém alguns sistemas são mais cruciais do que outros. Portanto por meio da análise de impacto deve-se fazer a identificação dos sistemas cruciais da empresa, para saber o efeito que uma interrupção nesses sistemas terá na mesma (FERNANDES, 2014).

Segundo Pinta (2011, tradução nossa) após a análise de risco e análise de impacto, deve-se construir a estratégia de recuperação, que envolve a configuração de parâmetros RPO e RTO em relação aos impactos da análise. Indicadores como *Recovery Point Objectives* (RPO) e Recovery *Time Objectives* (RTO), são elementos que auxiliam a definir requisitos reais para manter em operação os sistemas e promover soluções que pré-defina as prioridades de recuperação das funções e componentes de TI. O RTO representa o tempo máximo aceitável, que o negócio poderá permanecer com o processo interrompido, enquanto o RPO, representa um período de perda máxima de dados tolerada (figura 1).

Figura 1 - RTO vs. RPO

Fonte: Adaptado de Tozzi (2018).

De acordo com Barnoschi (2008, tradução nossa) deve-se elaborar um RTO e um RPO para cada sistema que se deseja proteger. Além de identificar de acordo com o seu orçamento, quantos dados necessitam de *backup*. Quanto mais rápido a organização necessitar da recuperação, e com menor perda de dados, maior será o investimento com a mesma (FERNANDES, 2014). Portanto o RTO e RPO, ajudam a evitar medidas desnecessárias, tendo em vista que o custo da implementação de recuperação de um sistema ou elemento de TI, deve estar equilibrado com o custo de seu impacto no negócio (PINTA, 2011, tradução nossa).

Conforme descrito por Ludescher e Cugnasca (2007) a etapa de testes do DRP é considerada extremamente importante, já que é a única maneira de garantir que o plano elaborado esteja funcionando de acordo com o esperado. Consegue-se efetuar os testes por meio de simulação de um desastre em sistemas alternativos,

sem que haja a preocupação de afetar os sistemas em produção. Há também a possibilidade de simular um desastre no ambiente em produção, porém esse tipo de teste causaria uma parada completa nos sistemas que estejam em funcionamento na empresa.

Para Snedaker (2014, apud ROCHA et al., 2018) a fase de testes do DRP deve-se fundamentar na rotina da empresa em que o plano será aplicado, para que de acordo com o cenário da mesma elabore-se um desastre em um ambiente de testes. O plano para o eventual desastre deve ser seguido e analisado, para que haja a possibilidade de melhorias caso necessário.

Com o plano ativo e testado, a organização pode no decorrer do tempo sofrer alterações em seu ambiente computacional. Necessitando assim de modificação no DRP da empresa. Os tipos de revisões e seus intervalos são determinados conforme a criticidade e a quantidade de mudanças sofridas no ambiente computacional da empresa (LUDESCHER; CUGNASCA, 2007, tradução nossa).

Aguiar Junior (2012) em seu trabalho sobre planejamento de recuperação de desastres, fez uma adaptação do método PDCA (*Plan*, *Check*, *Do and Act*) que é um ciclo que serve como um controle para a elaboração de um projeto, garantindo sua melhoria continua. Essa adaptação buscou trazer as métricas de trabalho para a realidade de um DRP, e o ciclo adaptado permite identificar as etapas de elaboração de um plano como esse, condizendo com as orientações já descritas nesse capitulo (figura 2)

Figura 2 – Ciclo de vida de um DRP

Fonte: Adaptado de Aguiar Junior (2012).

3 *BACKUP*

Backup é o termo utilizado para descrever a cópia de segurança de dados digitais, arquivadas em um outro dispositivo de armazenamento físico ou virtuais, diferente do dispositivo que possui os dados originais. Essa cópia de segurança representa a garantia de recuperação de dados, caso ocorra algum problema que provoque a perda das informações na base principal (FURLAN; ASSIS, 2015).

A cópia de segurança pode ser feita em um dispositivo de armazenamento ou em outra localidade, protegendo desta forma, os dados contra acidentes ocorridos na estrutura física. Um *backup* considerado eficaz, consiste em minimizar as perdas, proporcionando a possibilidade de restauração dos dados no menor tempo e com a menor perda possível (FARIA, 2010).

Conforme Moraes (2007) o *backup* é considerado um dos principais métodos de proteção de dados, porém para que o *backup* seja considerado seguro e recuperável, se faz necessário a elaboração de estratégias para o mesmo, de acordo com as particularidades de cada empresa.

Segundo Furlan e Assis (2015) os *backups* podem ser feitos em duas modalidades, *online* e *off-line*. O *online* é a modalidade em que todo o conteúdo que está sendo efetuado o *backup*, também está acessível ao usuário. Enquanto na modalidade *off-line*, todo o conteúdo que está sendo efetuado o *backup*, fica inacessível aos usuários durante o processo de cópia.

3.1 TIPOS DE *BACKUP*

Considerando as modalidades de *backup online* e *off-line*, pode-se efetuar *backups* do tipo total/completo, incremental ou diferencial (FURLAN; ASSIS, 2015).

Rodrigues (2017) define os três principais tipos de *backup* como:

a) ***backup* completo:** é uma cópia total das informações, independentemente de elas possuírem alteração ou não. O *backup* completo possui todas as informações, incluindo os dados anteriores e os novos. Sendo assim, um único *backup* completo conterá todas as informações necessárias para uma restauração. Este tipo de *backup* costuma demorar mais para a conclusão da cópia, além de necessitar de um maior espaço para armazenamento;

b) ***backup* diferencial:** a cópia dos dados é feita considerando o último *backup* completo. Efetuando a cópia dos dados criados ou alterados após o último *backup* completo feito. Caso seja necessário fazer uma restauração dos dados, é necessário possuir o último *backup* completo além do *backup* diferencial do dia que se deseja restaurar. O *backup* diferencial necessita de um menor espaço de armazenamento, se comparado com um *backup* completo, porém o volume de dados tende a crescer consideravelmente;

c) ***backup* incremental:** a cópia é feita somente das informações que foram criadas ou alteradas no dia. Caso seja necessário efetuar a restauração, é necessário ter o último *backup* completo, além dos *backups* incrementais de cada dia. Nesse tipo de *backup* as cópias tendem a ser mais rápidas e necessitar de um menor espaço de armazenamento.

3.2 MÍDIAS DE ARMAZENAMENTO DE DADOS

Antes de uma empresa iniciar com o uso de *backups*, é importante escolher o melhor tipo de dispositivo de armazenamento para as cópias de segurança. Além da escolha da mídia, após as cópias feitas é preciso mantê-la em locais seguros, com a menor probabilidade possível de riscos (TELES JÚNIOR, 2011).

Segundo Jesus (2011), existem diversas mídias de armazenamento à disposição no mercado. Essas constantemente passam por processos de melhorias na capacidade de armazenamento, velocidade de gravação e acesso à informação, devido ao desenvolvimento e inovação tecnológica.

Conforme Silva (2015), as mídias mais comuns para armazenamento de *backup* são: mídias ópticas*, hard drive*, *flash drivers, solid-state drive*, fitas magnéticas e *backup* em nuvem.

A seguir são descritos cada um desses locais de armazenamento mencionados:

a) **mídias ópticas:** possui o formato de disco e a informação é gravada com feixes de luz chamado raio laser, tendo como exemplos o CD, DVD, Blu-ray (PIEROBON; TEODORO, 2014). Essas mídias se destacam por sua capacidade de armazenamento em um espaço

físico pequeno. Possuía diversas utilidades, como base de dados, *backups* e distribuição de *software* comercial (JESUS, 2011).

b) ***hard drive*****:** segundo Zenatti (2014) é popularmente conhecido como HD e apontado como a principal forma de armazenamento em massa. É uma memória não volátil, ou seja, os dados não são perdidos quando o computador é desligado ou fica sem energia. A cabeça de leitura e gravação de um *hard drive* trabalha como um eletroímã bastante preciso, tornando-se capaz de gravar trilhas de dados medindo menos de um centésimo de milímetro de largura. Para Silva (2015) o *hard drive* é uma opção viável para ser utilizado como mídia de *backup* em instituições de pequeno porte. Devido ao fato que o mesmo possui espaço, velocidade e durabilidade adequada considerando o seu custo, que o autor considera atingível pela maioria das empresas desse porte.

c) ***flash drivers*****:** de acordo com Silva (2015) dispositivos *flash drivers* são popularmente conhecidos como *pen drive,* é um dispositivo de memória composto por memória *flash.* São dispositivos compactos, velozes e possuem uma considerável capacidade de armazenamento. O *pen drive* é considerado uma boa opção para *backups* pessoais, porém em ambientes corporativos não é aconselhável seu uso para esse fim. Para empresas sugere-se a utilização de uma mídia que suporte um maior volume de dados do que os encontrados em flash drivers e que seja mais resistente e confiável.

d) ***solid-state drive*****:** é também conhecido por SSD são discos que utilizam chips de memória flash para o armazenamento. A sua principal vantagem é proporcionar um tempo de acesso bem baixo, além de excelentes taxas de leitura e gravação (GOMES, 2012).

e) **fitas magnéticas:** são dispositivos em rolos, cartuchos ou cassetes, para armazenamento de dados, as fitas magnéticas estão entre os principais modos de armazenamento, sendo o mais antigo que ainda é utilizado para *backups*. Se comparada com outras mídias de armazenamento, a vantagem do uso de fitas é sua grande capacidade de armazenamento, o seu baixo custo por unidade armazenada e a confiabilidade do armazenamento devido a sua longa expectativa de

vida útil, contudo suas desvantagens consiste em um acesso sequencial e o alto custo dos dispositivos de leitura e gravação, além de sua fragilidade (SILVA, 2015).

f) ***backup* em nuvem:** conforme Silva (2015) consiste em enviar seus dados para um outro local através da Internet, muitas vezes esse local pode ser uma empresa terceirizada. Como desastres podem ocorrer em qualquer lugar, é essencial que as cópias de segurança sejam mantidas distante da estrutura de dados principal, para o caso de uma ocasional perda de acesso a esses dados, ainda se tenha uma cópia disponível em outra localidade. Empresas grandes tem dificuldades de utilizar esse meio de armazenamento, devido à sobrecarga do uso da rede, e ter um custo adicional contratando a empresa que disponibilizará o serviço. Porém existem empresas que disponibilizam esses serviços de forma gratuita e com um tamanho muitas vezes atrativo e suficiente para realizar os *backups* de pequenas empresas.

3.3 IMPORTÂNCIA PARA UMA EMPRESA

De acordo com Silva (2015) a gestão das informações tem ligação direta com o desenvolvimento de uma organização, além de ser vital para a continuidade da mesma.

Todos os dias são manipulados e gerados enormes volumes de informações que as empresas utilizam para executar suas atividades, sendo assim necessário ter muita cautela com essas informações geradas (RODRIGUES, 2017). Conforme Teles Júnior (2011) é grande o número de empresas que perdem anos de existência através da perda de dados importantes, sejam estes causadas por problemas lógicos, humanos ou físicos.

Em caso de perda de dados em uma empresa, os efeitos causados são diversos desde retrabalho de funcionários e gestores, caso exista a possibilidade de repor as informações perdidas, até mesmo a paralisação das atividades primordiais que pode vir a acarretar em um comprometimento negativo moral e financeiro da empresa, podendo encaminhá-la à falência (FURLAN; ASSIS, 2015).

Segundo Rodrigues (2017) a necessidade de fazer cópias de segurança, se dá devido à importância que as informações têm para as empresas, e o impacto

que a perda das mesmas pode ocasionar no negócio, podendo muitas vezes ter um impacto irreversível que possa levar a inviabilização da continuidade da empresa. Contudo, realizar *backups* é algo fundamental para qualquer instituição que preze o valor de suas informações.

4 COMPUTAÇÃO EM NUVEM

Computação em nuvem é um paradigma computacional, que possui como seu objetivo principal o acesso facilitado a recursos computacionais de alto desempenho e escalabilidade por meio da Internet. Tornando assim desnecessário o investimento em equipamentos físicos de alto padrão (SILVA, 2013).

O termo computação em nuvem, surgiu como uma metáfora para a Internet. Esse nome veio decorrente ao seu uso comum em diagramas de rede na forma de nuvem. O conceito é datado de 1961, ano que o professor John McCarthy sugeriu que a tecnologia de compartilhamento de recursos poderia levar a um futuro, em que poder de computação e aplicativos específicos, são vendidos por um modelo de negócio utilitário. Essa ideia desapareceu quando se constatou que as tecnologias da época não eram capazes de sustentar um modelo computacional tão futurista. Entretanto, desde a virada do milênio o termo computação em nuvem foi revitalizado, e começou a surgir nos círculos da tecnologia (RITTINGHOUSE; RANSOME, 2009, tradução nossa).

De acordo com Taurion (2009), a Computação em Nuvem pode ser descrita como um ambiente computacional baseado em uma ampla rede de servidores, sejam estes físicos ou virtuais. Para simples definição, pode-se dizer que é um conjunto de recursos como capacidade de armazenamento, conectividade, processamento, plataformas, aplicações e serviços disponíveis na Internet. Isto é, a Computação em Nuvem é uma evolução do conceito de virtualização.

4.1 POR QUE USAR COMPUTAÇÃO EM NUVEM

Segundo Botacim et al*.* (2016), é fundamental que as pessoas acompanhem a evolução causada por vários avanços tecnológicos presente em nosso meio. Com essa evolução os usuários estão cada vez utilizando mais a computação em nuvem, pelo fato de a mesma oferecer mobilidade, portabilidade e facilidade.

Para usuários que desejam utilizar seus serviços em nuvem, é necessário apenas que em sua máquina possua um sistema operacional instalado, navegador e acesso à Internet. O usuário terá a sua disposição os recursos de *hardware* disponíveis na nuvem, sem que haja necessidade de a máquina local possuir todo o

poder de processamento para executar a tarefa desejada. Em caso de necessidade por mais poder de processamento, novos recursos de *hardware* podem ser adicionados para contribuir com os já existentes (SOUSA; MOREIRA; MACHADO, 2009).

A computação em nuvem possui a promessa de economia de custos combinados com maior agilidade de TI. Sendo assim considera-se a adoção da nuvem em governo e industrias em resposta a restrição econômica difícil (NIST, 2010, tradução nossa).

De acordo com Sobragi (2012), os fatores que levam a adotar a computação em nuvem são: acesso pela rede, segurança, escalabilidade, confiabilidade, interoperabilidade, privacidade, economia e sustentabilidade (figura 3).

Figura 3 – Fatores de Adoção da computação em Nuvem

Fonte: Sobragi (2012).

A seguir são descritos cada um desses fatores:

a) **acesso pela rede:** os recursos estão disponíveis para acesso pela rede, por meio de mecanismos que promovem o uso por plataformas heterogêneas, como celulares e notebook (ZISSIS; LEKKAS, 2010, tradução nossa);
b) **confiabilidade:** acontece por meio do uso de vários sites redundantes, tornando a computação em nuvem adequada para continuidade de

negócios e recuperação de desastres (ZISSIS; LEKKAS, 2010, tradução nossa);

c) **economia:** conforme exemplificado por Sultan (2010, tradução nossa), em tecnologia da informação existem altos custos com consumo de eletricidade, necessários para executar *hardware*, PCs, resfriamento, e unidades de *backup*. Custos estes que a adoção da computação em nuvem ajudará a reduzir;
d) **escalabilidade:** a arquitetura em nuvem pode ter seus recursos ajustada horizontal ou verticalmente, de acordo com a demanda necessária (ZISSIS; LEKKAS, 2010, tradução nossa);
e) **interoperabilidade:** permitirá que a nuvem evolua para um mundo de plataformas transparentes em que as aplicações não são restritas a nuvens corporativas e fornecedores de serviços em nuvem (DIKAIAK OS et al., 2009, tradução nossa). Segundo Shilawat (2018, tradução nossa), o Instituto de Engenheiros Elétricos e Eletrônicos (IEEE) e o Instituto Nacional de Padrões e Tecnologia (NIST) estão trabalhando em padrões de interoperabilidade em nuvem. O empenho está em criar tecnologias nativas da nuvem, independentes de fornecedor. Para NIST (2013, tradução nossa) a interoperabilidade da nuvem permite a troca e o uso contínuo de dados e serviços entre várias ofertas de infraestrutura de nuvem e a utilização dos dados e serviços, para permitir que eles operem juntos de forma eficiente;
f) **privacidade:** segundo Rittinghouse e Ransome (2009, tradução nossa), a questão de privacidade na nuvem, varia significativamente de acordo com os termos de serviço e política de privacidade estabelecida pelo provedor da nuvem;
g) **segurança:** implementações em nuvem contêm tecnologias de segurança avançadas, devido principalmente à centralização dos dados e arquitetura universal (ZISSIS; LEKKAS, 2010, tradução nossa). Para NIST (2013, tradução nossa) a adoção da computação em nuvem envolve riscos de segurança específicos associados ao tipo de nuvem adotada e ao modo de implantação. Porém muitas dessas ameaças podem ser tratadas através de processos tradicionais de segurança e

mecanismos como políticas de segurança, criptografia, gerenciamento de identidade e análise de vulnerabilidade;

h) **sustentabilidade:** ocorre por meio da utilização aprimorada de seus recursos, sistemas mais eficientes e neutralização dos níveis de emissão de carbono (ZISSIS; LEKKAS, 2010, tradução nossa).

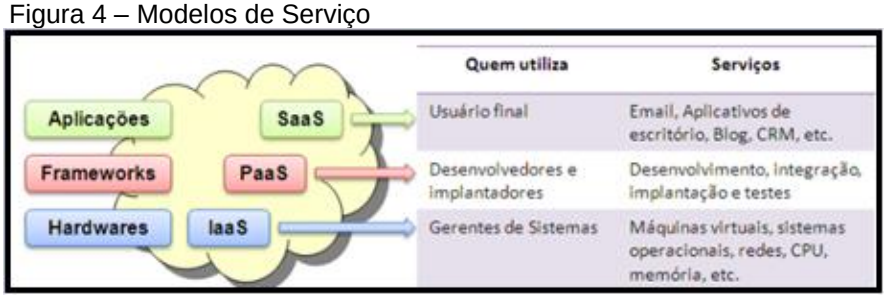
4.2 MODELOS DE SERVIÇO

Um provedor de computação em nuvem dispõe de um modelo de gerência centralizado, que consiste em uma empresa ser proprietária de toda a infraestrutura, eliminando assim a divergência entre variadas políticas de segurança da informação (ALLES, 2018).

De acordo com Mell e Grance (2011, tradução nossa), a computação em nuvem é um modelo para permitir acesso de rede sob demanda a um conjunto compartilhado de recursos de computação configuráveis, que pode ser liberado de forma rápida e com esforço mínimo de interação ou gerenciamento com o provedor de serviços.

Conforme Alles (2018), a utilização de uma infraestrutura sob demanda, faz com que o recurso computacional em questão não seja mais visto como um produto, e sim como um serviço. O uso dessa abordagem, possibilita um modelo de pagamento onde o contratante é cobrado somente pelos recursos utilizados. Desse modelo de negócio que surgiu os conceitos típicos de Infraestrutura como um serviço do inglês *Infrastructure as a Service* (IaaS), Plataforma como um serviço do inglês *Platform as a Service* (PaaS) e Software como um serviço do inglês *Software as a Service* (SaaS) (figura 4).

Figura 4 – Modelos de Serviço



Fonte: Borges (2013).

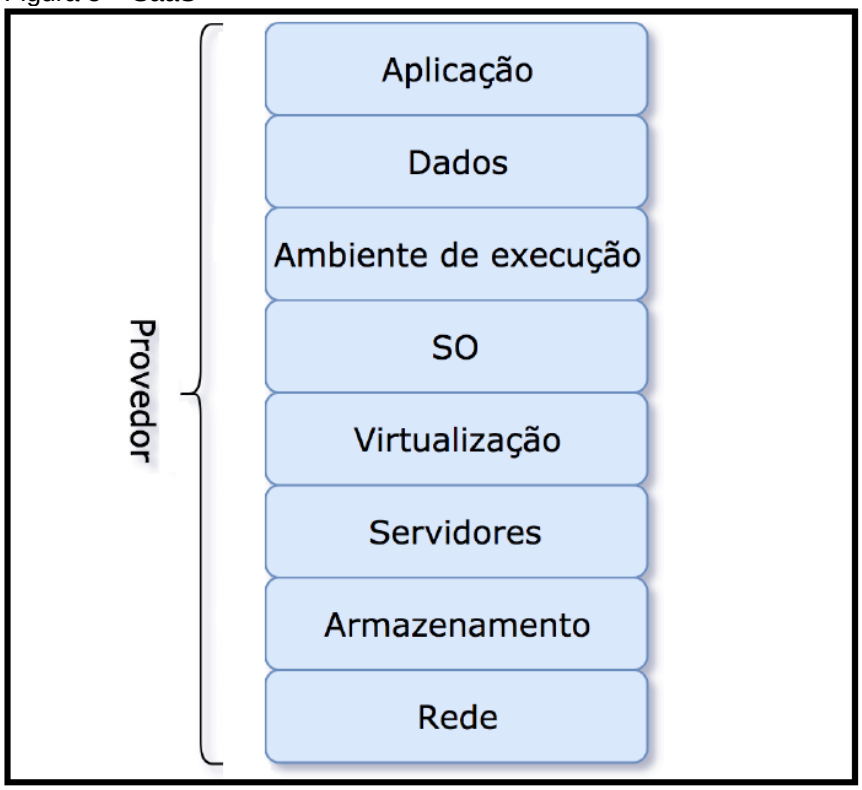
4.2.1 Software como um serviço

O objetivo do modelo SaaS, é proporcionar a substituição de algumas aplicações que rodam nos computadores, para o uso na nuvem. Assim o usuário paga pelo que é usado do SaaS, ao invés de comprar o software por um preço relativamente alto (RODRIGUES, 2014).

O software como um serviço é um conceito atrativo para profissionais de TI que constantemente precisam enfrentar atualizações, correções e gerenciar licenças de software. Representa a camada mais externa da computação em nuvem, ela é composta por aplicativos que são executados diretamente na nuvem. Os softwares disponíveis por esse modelo são acessados por meio de uma interface web, que permite o acesso por diversos dispositivos do usuário e de qualquer lugar com acesso à Internet (BORGES, 2013).

Segundo Alles (2018), nesse modelo o provedor é responsável por todos os aspectos, desde a infraestrutura até a manutenção do software (figura 5). Os exemplos mais comuns de SaaS são ferramentas de e-mail como Gmail e Outlook, ou de armazenamento em nuvem como o Google Drive e OneDrive.

Figura 5 – SaaS



Fonte: Adaptado de Bernheim (2017)

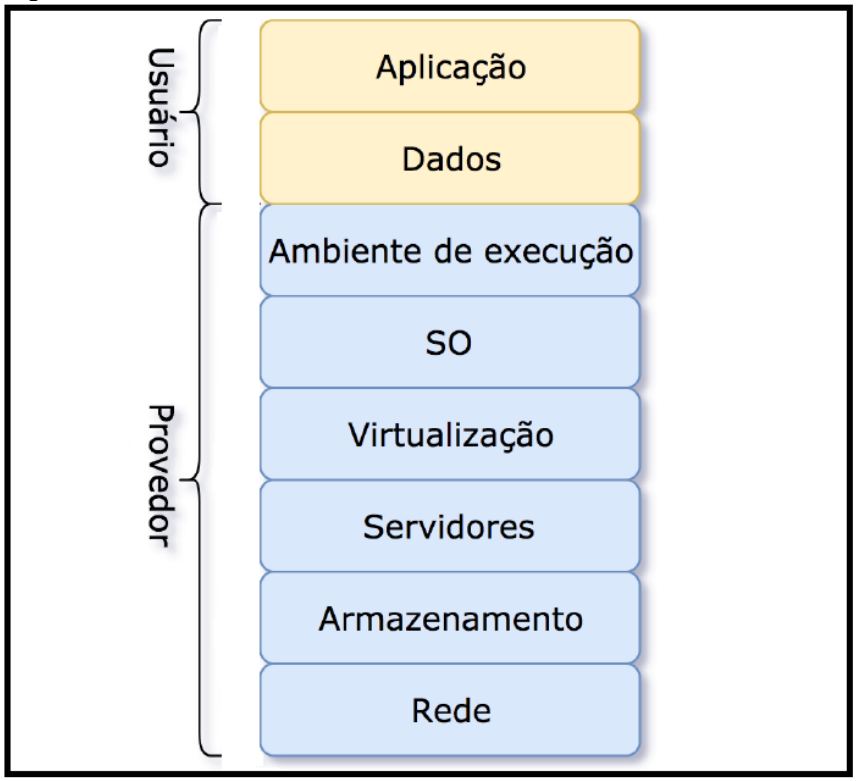
4.2.2 Plataforma como um serviço

O modelo PaaS, consiste em uma plataforma voltada para desenvolvedores. Esse modelo adota o uso de inteligência artificial para aumentar ou reduzir a capacidade do *hardware*, não proporcionando a manipulação direta do mesmo. Sendo assim, a nuvem que é encarregada de efetuar o balanceamento de carga do software (GARBELINI; LIMA, 2013).

A plataforma como um serviço corresponde a camada intermediária da computação em nuvem, sendo formada por *hardware* virtual disponibilizado como serviço. Uma PaaS disponibiliza ambientes de desenvolvimento e facilita a implantação de *softwares*, sem os custos e complicações relacionadas a compra e gerenciamento de *hardware* e *software* (BORGES, 2013).

De acordo com Alles (2018), no modelo PaaS o provedor fornece a infraestrutura de *hardware* em uma plataforma que já vem com o sistema operacional e ambientes de desenvolvimento e execução, abstraindo os detalhes de baixo nível (figura 6). Exemplos de PaaS são ferramentas de gerência de banco de dados e serviços de versionamento de código.

Figura 6 – PaaS



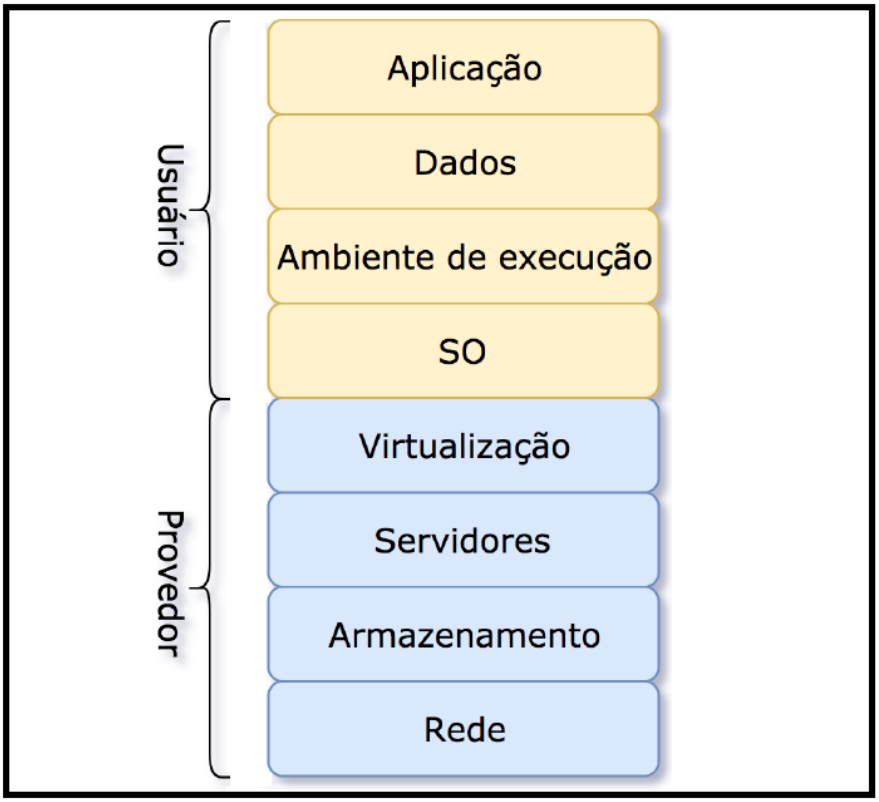
Fonte: Adaptado de Bernheim (2017).

4.2.3 Infraestrutura como um serviço

A IaaS, constitui em disponibilizar ao consumidor a capacidade de processamento, armazenamento, redes e outros recursos computacionais. O usuário não controla e nem gerencia a infraestrutura subjacente, mas tem todo o controle sobre o armazenamento sistemas operacionais e aplicativos (MELL; GRANCE, 2011, tradução nossa).

A Infraestrutura como um serviço equivale a camada mais inferior da computação em nuvem, sendo responsável por fornecer a infraestrutura necessária para as demais camadas (PEDROSA; NOGUEIRA, 2011). Conforme Alles (2018), nesse modelo o provedor oferece todos recursos físicos de rede, armazenamento e processamento (servidores), e o contratante tem controle sobre sistema operacional, dados armazenados, ambiente de execução e aplicações (figura 7). Como exemplos de IaaS temos a *Elastic Compute Cloud* da Amazon e a Compute Engine da Google, que possibilita a cobrança por tempo de uso das maquinas virtuais contratadas.

Figura 7 – IaaS



Fonte: Adaptado de Bernheim (2017).

5 TRABALHOS CORRELATOS

No decorrer dos levantamentos bibliográficos foi realizado pesquisas no âmbito nacional e internacional de trabalhos que tratam de temas semelhantes aos abordados no presente projeto. Dos referenciais obtidos, buscou-se identificar os trabalhos que tinham maior relação com o proposto e que serviriam de maior base para elaboração do trabalho, para que fossem mencionados como trabalhos correlatos.

5.1 A SEGURANÇA DE UMA ESTRUTURA DE *DISASTER RECOVERY PLA*N EM *CLOUD COMPUTING*

A segurança de uma estrutura de *disaster recovery pla*n em *cloud computing*, trabalho realizado por Ávila, Soldan e Petroli Neto, na Universidade São Francisco, localizada em Bragança Paulista no ano de 2017, onde os autores elaboraram um *Disaster Recovery Plan* em nuvem, e realizaram uma avaliação de segurança. No trabalho, os autores criaram um ambiente de TI virtualizado para simular uma empresa. Foi utilizado em uma máquina virtual, um sistema de controle de tickets que havia sido desenvolvido para a disciplina de desenvolvimento de *software*. Regras de *backup* foram criadas, armazenando esses dados em duas nuvens, Microsoft *OneDrive* e Google *Drive*. Após a definição do DRP, foi realizado o teste e análise da segurança com o uso do *software Wireshark*, visando ter uma análise do fluxo de rede e seus protocolos, entre os dados enviados e recebidos das duas nuvens.

Como resultado, foi observado que tanto o *software* do *OneDrive*, quanto o do Google *Drive*, utilizam o protocolo TCP para transferência de pacotes e TLSV 1.2 para criptografia desses pacotes. Uma das dificuldades enfrentadas com este modelo foi a velocidade da Internet, que interferiu no tempo de realização *backups* e restaurações, visto que foi utilizado um pacote de dados com baixa taxa de transferência.

Com base nos resultados obtidos concluiu-se que a segurança está diretamente relacionada com o sistema de armazenamento em nuvem utilizado. Além de que com os testes realizados, foi possível garantir que as plataformas do Google *Drive* e Microsoft *OneDrive* são seguras, devido ambas fazerem uso de um padrão de

criptografia através dos protocolos TCP e TLS, responsáveis pela transmissão e segurança do trafego do pacote de dados. Podendo então afirmar que uma estrutura de *Disaster Recovery Plan* em *Cloud Computing* os dados são criptografados sem interferências garantindo a segurança para empresas que fazem uso desse modelo.

5.2 PLANO DE RECUPERAÇÃO DE DESASTRES: UMA PESQUISA-AÇÃO EM EMPRESA DO SETOR ENERGÉTICO

Plano de recuperação de desastres: uma pesquisa-ação em empresa do setor energético, trabalho realizado por Aguiar Junior na Universidade Estadual Paulista, localizada em Guaratinguetá no ano de 2012, onde o autor teve como objetivo criar um plano que estruture de maneira sistêmica ações para executar de modo que a empresa possa retomar o processamento normal de suas aplicações críticas dentro de um tempo aceitável.

Para isso foi escolhido uma corporação, que é um dos maiores grupos empresariais brasileiros, formado por 4 empresas, identificadas como Empresa A, Empresa B, Empresa C e Empresa D.

Na elaboração do plano foi utilizado um método chamado *Plan, Check, Do and Act* (PDCA), que propõe além de auxiliar como controle para a elaboração, também garante a sua melhoria continua. Desse modo cada ciclo que se reinicia, corrige as falhas encontradas. Foi feita uma adaptação do método trazendo as métricas de trabalho para a realidade de um plano de recuperação de desastres. Foi também alterado os passos do modelo, ficando como primeira etapa a análise de riscos, segunda etapa analise de impacto nos negócios, terceira etapa selecionar estratégia, quarta etapa o desenvolvimento e execução do plano, e como quinta etapa os testes e manutenção do plano. Dessa forma a manutenção do plano reinicia o ciclo de forma que o plano esteja sempre atualizado.

Como resultado após os testes, o autor relatou um resultado satisfatório, tendo 85% de sucesso nos testes feitos, e objetivando-se uma melhoria continua, foram estudadas soluções para melhorar a taxa de sucesso do próximo teste.

5.3 PLANEAMENTO DE ESTRATÉGIAS DE SALVAGUARDA E REPOSIÇÃO DE DADOS/INFORMAÇÃO BASEADO EM ALGORITMO DE OPTIMIZAÇÃO DE REQUISITOS MULTIDIMENSIONAIS

Planeamento de Estratégias de Salvaguarda e Reposição de Dados/Informação baseado em Algoritmo de Optimização de requisitos Multidimensionais, trabalho realizado por Fernandes na Universidade Católica Portuguesa, localizada em Lisboa, Portugal no ano de 2014, onde o autor propôs criar um *Framework* que proporcionasse uma eficiência significativa nos esforços de salvaguarda e restauração de dados.

Para a concepção desse Framework o autor estudou sobre continuidade de negocio e recuperação de desastres, além da importância que os sistemas de informações possuem dentro das organizações. Para isso foi realizado uma análise de mercado que tornou possível constatar que pequenas e médias empresas não consideram que a prevenção de desastres é uma prioridade, por mais que essas empresas estejam sujeitas aos mesmos fenômenos e evidentemente aos mesmos efeitos, porém com capacidades financeiras reduzidas.

Com a conclusão da análise de mercado, verificou-se que no cenário do estudo, caso venha a ocorrer um desastre, algumas organizações serão forçadas a encerrar a sua atividade. Sendo que um simples planejamento bem estruturado já permitiria a proteção da mesma e de seus clientes.

Para obter os resultados, o autor criou um simulador, e de acordo com as entradas fornecidas, era esperada a produção de um ficheiro que indicasse o plano de execução mais eficaz para o exemplo criado.

Com os resultados produzidos pelos algoritmos, o autor concluiu que encontrar a melhor solução para problemas complexos em situações reais, requer funções de avaliação extremamente pesadas, que podem vir a necessitar de horas para serem processadas e por vezes nem conseguem ser reproduzidas. Como conclusão geral foi possível demonstrar a necessidade de a solução estar dotada de recursos humanos especializados apenas no início, para que seja recolhida as informações da forma mais precisa possível. Contudo, comprovou-se que a qualidade de um bom plano depende da qualidade das informações recolhidas e produzidas para o cenário.

5.4 RECUPERAÇÃO DE DESASTRE PARA A BIBLIOTECA DO CENTRO DA CIÊNCIA DA SAÚDE NA UENP - METODOLOGIA E ESTUDO DE CASO

Recuperação de desastre para a biblioteca do centro da ciência da saúde na UENP – metodologia e estudo de caso, trabalho realizado por Lopes na Fatec, localizada em Ourinhos no ano de 2017, onde o autor propôs um modelo e metodologia para a elaboração de um plano de recuperação de desastres, para a biblioteca do Centro da Ciência da Saúde (CCS) pertencente à Universidade Estadual do Norte do Paraná (UENP). No qual a instituição utiliza um sistema para gestão de pequenos, médios e grandes acervos de livro e não possui nenhum plano para a recuperação de desastres.

A metodologia aplicada na realização do trabalho, foi formada com base no referencial teórico obtidos pelo autor. Para analisar os níveis de risco foi criado uma metodologia de análise dividida em 3 camadas, a análise da camada de aplicação que incluía navegadores e plugins de acesso ao sistema, a análise de rede que continha o fluxo de dados, e análise física que continha os equipamentos e inventários.

O autor criou uma tabela de inventário que contém os equipamentos utilizados na biblioteca, analisou o fluxo de dados da aplicação utilizada na biblioteca, e realizou um levantamento da estrutura de rede utilizada na biblioteca e na sala do Núcleo de Tecnologia da Informação (NTI).

Foi concluído que a instituição necessitava de um segundo link de rede para não ficar à mercê do único que a instituição tem. Também foi identificado que para amenizar os problemas com falta de energia, foi proposto o uso de nobreaks, para estarem ligados aos computadores e equipamentos nos setores da biblioteca e na sala do NTI como por exemplo o servidor. Com os possíveis defeitos identificados nas máquinas da biblioteca, o autor propôs manter um computador pré-instalado e configurado com o sistema, para uma imediata troca em caso de defeito, eliminando assim o tempo de indisponibilidade que se tem até que uma nova máquina seja instalada e configurada adequadamente.

6 METODOLOGIA

Para a elaboração deste projeto, foi realizado um levantamento bibliográfico acerca dos conceitos necessários para a resolução desta pesquisa, tais como: *Backups*, Computação em Nuvem e *Disaster Recovery Plan,* sua importância no âmbito da tecnologia da informação empresarial, além de como realizar esse planejamento. Durante a fase de levantamento bibliográfico, optou-se por livros, artigos científicos, e a outros trabalhos desenvolvidos sendo de graduação, pós-graduação, dissertações de mestrado ou teses de doutorado. Dando preferência a documentos mais atuais.

Na etapa do desenvolvimento foi necessário projetar e criar uma máquina virtual de forma a representar um ambiente próximo a um cenário empresarial de pequeno porte, para que assim fosse realizados os experimentos necessários. Criado o cenário então foi elaborado um *Disaster Recovery Plan* para esse ambiente, visando manter suas informações o mais seguras possível. No final do desenvolvimento, tem-se a fase de testes, onde o objetivo foi verificar se o DRP cumpre com seus objetivos propostos.

6.1 PROJETO E IMPLEMENTAÇÃO DO CENÁRIO

Nesta fase, foi criado um cenário para simular um ambiente de TI empresarial de pequeno porte. O cenário possuiu um link ADSL de 15 Mbps de download e 1,5 Mbps de upload. Para criar o cenário, foi utilizado um *notebook* e um *desktop* com as configurações abaixo.

Notebook:

a) **modelo *notebook*:** Samsung *Odyssey* NP800G5M;
b) **processador:** Intel *Core* i5-7300HQ 2.5 GHz;
c) **memória:** 8 GB;
d) **HD:** SSD 240GB Sandisk *Plus*;
e) **sistema operacional:** *Windows* 10 Pro – 64 bits.

Desktop:

a) **processador:** Intel *Core* i5-7400 3.00 GHz;
b) **memória:** 8 GB;
c) **HD:** SSD 240GB WD *Green*;

d) **sistema operacional:** *Windows* 10 Pro – 64 bits.

No cenário para aplicação do DRP, foi definido o *notebook* como máquina principal, e o *desktop* como estoque de contingência[1] do mesmo. Desse modo foi instalado no *notebook* uma máquina virtual fazendo uso do *software VirtualBox*, que é uma solução profissional da *Oracle*. A escolha desse *software* de virtualização, se deu ao fato de o mesmo ser gratuito, ter a possibilidade de ser executado em *hosts Windows*, Linux, Macintosh e Solaris e suportar um grande número de sistemas operacionais para serem instalados em suas máquinas virtuais.

A máquina virtual criada como servidor para os testes possui a seguinte configuração:

a) **processador:** 4 CPU (Intel *Core* i5-7300HQ 2.5 GHz);

b) **memória:** 4 GB;

c) **HD:** 50 GB (alocados dinamicamente);

d) **sistema operacional:** *Windows* 10 Pro – 64 bits.

Nesse servidor *Windows* foi instalado o software Xampp, que é uma ferramenta gratuita, e está possui um pacote que inclui banco de dados MySQL e Apache com suporte à linguagem PHP, para utilização dos sistemas *web* desse cenário empresarial.

Para simular a utilização de sistemas empresariais, foi utilizado dois *softwares* para auxiliar os processos das principais funções de negócio, ambos gratuitos. O primeiro é o Akaunting[2], que é um software contábil, que possui recursos como: painel com informações de fluxo de caixa, cadastro e controle de itens e estoque, faturas de contas a receber e a pagar, gestão de clientes e fornecedor, além de relatórios financeiros. O segundo é o *osTicket*[3], que é um sistema de suporte ao cliente, onde os mesmos abrem seus *tickets*/chamados, para terem o devido suporte dos atendentes da empresa.

Após a instalação do *software* Akaunting, o mesmo foi configurado com seu padrão de moeda (Real), categorias de produtos, despesas e rendas, além de ser realizado os devidos cadastros de produtos, clientes e fornecedores. Os produtos

---

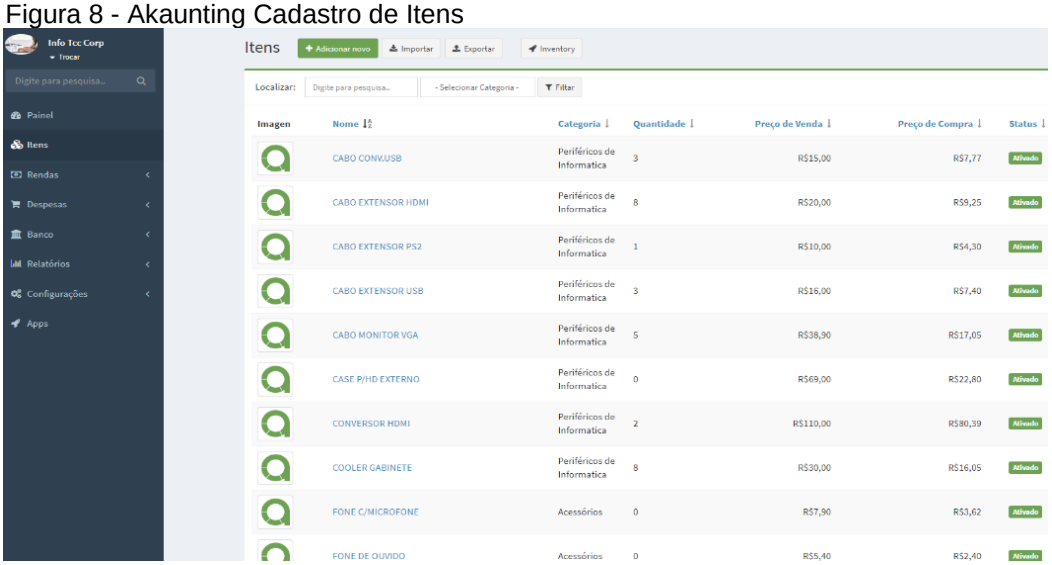
[1] Estoque de contingência é o estoque mantido para cobrir potenciais situações de falhas na empresa (TSESTOQUE, 2019).

[2] Akaunting. Disponível em: <https://akaunting.com/>. Acesso em: 13 maio 2019.

[3] OsTicket. Disponível em: <https://osticket.com/>. Acesso em: 13 maio 2019.

inseridos foram obtidos de uma base real empresarial, com informações de preço de venda, preço de custo, descrição e quantidade (figura 8). Foram realizados centenas de cadastros de clientes, além de cadastrar fornecedores para cada tipo de categoria dos produtos. Os cadastros de clientes e fornecedores foram realizados com dados fictícios.

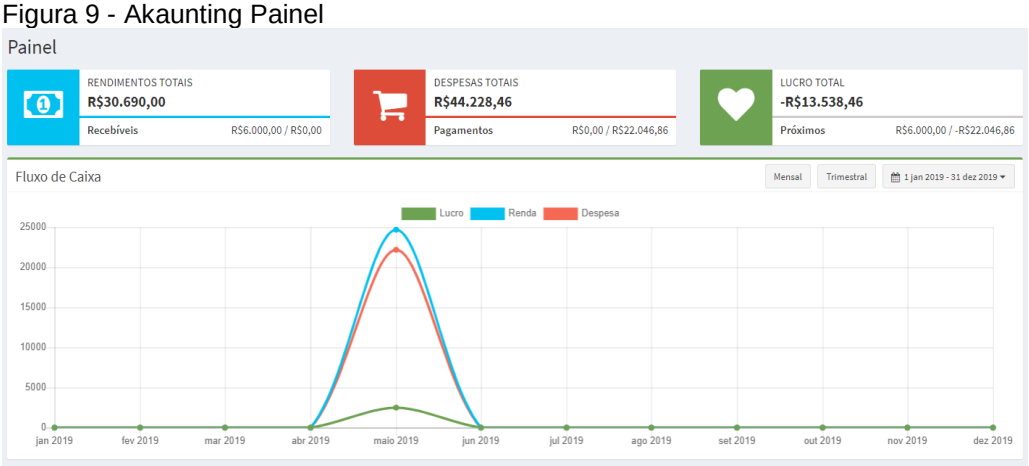
Figura 8 - Akaunting Cadastro de Itens



Fonte: Do autor.

Para gerar um maior volume de dados, foi efetuado diversos cadastros de compras de produtos, para assim gerar títulos a pagar, além de diversos registros de venda de produtos, para gerar títulos a receber. Dentre esses títulos, alguns tiveram seu pagamento ou recebimento confirmados, e outros permaneceram pendentes, para que fosse possível obter uma visualização geral no painel financeiro da aplicação (figura 9).

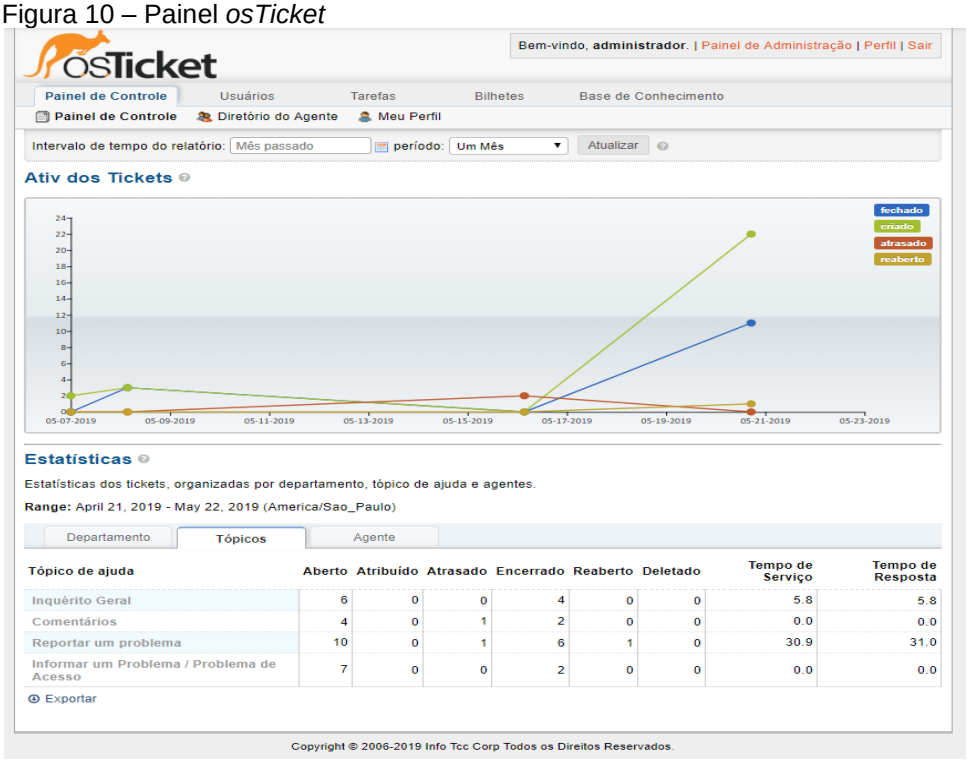
Figura 9 - Akaunting Painel



Fonte: Do autor.

Após o termino dos ajustes do Akaunting, iniciou-se a instalação e configuração do *software osTicket*. Foram realizadas todas as configurações necessárias para que o *software* de suporte ao cliente estivesse funcional, tais como: aplicação de pacote de linguagem, cadastros de atendentes, equipes e departamento. Para gerar mais dados, foram abertos diversos tickets de solicitação de serviço por meio da *web*, utilizando o *notebook* e o *desktop*. Todos esses tickets possuem interações de um ou mais atendentes, dentre esses, alguns foram marcados como resolvido e assim encerrados, e outros foram mantidos em atendimento (figura 10).

Figura 10 – Painel *osTicket*



Fonte: Do autor.

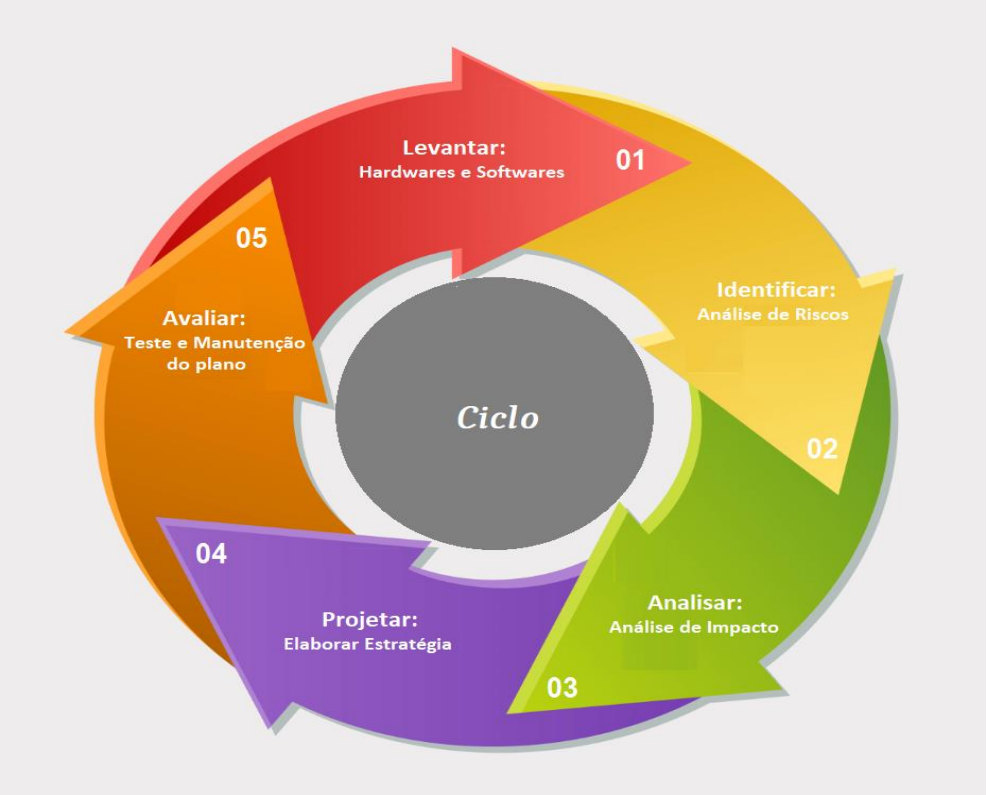
Como esse trabalho propõe utilizar a nuvem como local de *backup*, foi utilizado duas contas gratuitas, uma da empresa Google e outra da Microsoft para esse fim. Para fazer uso dessas contas, utilizou-se dois *softwares* de sincronização, um já disponível no *Windows* o *OneDrive*, e o Google *Drive*, que foi necessário fazer o *download* da versão de sincronização para *desktop*. Foi utilizado duas nuvens para o armazenamento dos *backups* buscando se precaver de uma eventual indisponibilidade de uma das plataformas no momento que for necessário a recuperação dos dados. A escolha dessas duas plataformas, se deu pelo fato de ambas terem a possibilidade de criar contas com um determinado espaço de

armazenamento gratuito e suficiente para dar suporte ao projeto desenvolvido. Além de que Ávila, Soldan e Petroli Neto (2017), afirmam com base em testes realizados, que ambas plataformas são seguras.

6.2 ELABORAÇÃO DO DRP

A elaboração do DRP, foi baseado em um compilado do referencial teórico obtidos sobre o assunto, dentre eles, os trabalhos correlatos, para conseguir compreender quais informações são importantes para se ter em um plano como esse, e como deve ser seu ciclo. As orientações para essa elaboração estão citadas no item 2.2, planejamento de DRP. Inclusive, o ciclo criado para esse DRP, foi baseado no ciclo adaptado por Aguiar Junior (2012), que foi criado com base no método PDCA de melhoria continua do processo. O ciclo criado para o plano foi dividido em cinco etapas (figura 11).

Figura 11 – Ciclo para elaboração e constante melhoria do DRP



Fonte: Do autor.

Como relatado por Andrade et al. (2011) o inventário de *hardware* e *software* são necessários para a execução de um DRP. Portanto, a primeira etapa conteve o levantamento dos *hardwares* e *softwares* utilizados no ambiente

computacional criado. A tabela 3, contém o inventário para o projeto, e este deve estar sempre atualizado e a disposição do responsável pela aquisição de equipamentos da empresa, e esse responsável deve manter-se sempre atualizado sobre quais fornecedores possuem esses equipamentos para reposição rápida.

Tabela 3 – Inventário de *hardware* e *software*

Hardwares Produção	*Hardwares* Contingência	*Softwares*
Notebook Samsung *Odyssey*	Computador *Desktop* Completo	*Windows*
Roteador Tp-*link Archer* C25	Roteador Tp-*link* wr 741nd	*VirtualBox*
	Memória para *notebook* 8 GB	XAMP
	SSD 240GB	Akaunting
		osTicket
		Google *Drive*
		OneDrive

Fonte: Do autor.

Posteriormente, foi documentado de forma geral os principais eventos que retratariam um desastre. Assim criando quatro tabelas que cobrem a segunda etapa do plano, identificação e análise de risco, contendo a descrição do desastre, responsabilidades dos envolvidos e o objetivo alvo que é o restabelecimento das atividades.

A tabela 4 cobre desastres ocasionados a partir de uma atualização de *software*, sejam eles os sistemas utilizados pela empresa, ou o sistema operacional do servidor.

Tabela 4 – Desastres por atualizações de *software*

Ativação do DRP	Cenário
Definição de Desastre	Atualizações malsucedidas dos sistemas
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Não
Quem deve ser informado	Responsável por setores que fazem uso do sistema afetado
Prazo Estimado para Reestabelecimento das atividades	3 horas

Fonte: Do autor.

A tabela 5, busca cobrir desastres ocasionados por falhas humanas ou não, que resulte a perda de dados, sejam essas falhas por negligência, sabotagem ou algum problema que possa ter afetado o banco de dados mesmo sem a colaboração direta de uma pessoa.

Tabela 5 – Desastres que ocasionem perdas de dados

Ativação do DRP	Cenário
Definição de Desastre	Falhas com ou sem interação humana, que ocasione perda ou modificação de dados
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Não
Quem deve ser informado	Responsável por setores que fazem uso dos dados afetados.
Prazo Estimado para Reestabelecimento das atividades	30 minutos

Fonte: Do autor.

A tabela 6, cobre desastres ocasionados por falhas humanas ou não, mas que diferentemente da tabela anterior, essa é para desastres que ocasione defeitos ligados ao *hardware*.

Tabela 6 – Desastres que ocasionem defeito com *hardware*

Ativação do DRP	Cenário
Definição de Desastre	Falhas com ou sem interação humana, que ocasione defeito ligado ao *hardware*
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Sim
Responsável pelas Aquisições	Responsável pelo comercial (ou outra pessoa que possua essa função e contato com fornecedores)
Quem deve ser informado	Responsável por setores que fazem uso dos sistemas, caso acarrete em uma paralisação dos mesmos
Prazo Estimado para Reestabelecimento das atividades	4 horas

Fonte: Do autor.

A tabela 7, busca cobrir desastres ocasionados por forças tanto naturais quanto criminais, e que comprometa a infraestrutura computacional.

Tabela 7 – Desastres que comprometam a infraestrutura computacional

Ativação do DRP	Cenário
Definição de Desastre	Desastres naturais ou criminosos que comprometam a infraestrutura computacional
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Sim
Responsável pelas Aquisições	Responsável pelo comercial (ou outra pessoa que possua essa função e contato com fornecedores)
Quem deve ser informado	Responsável por setores que fazem uso do sistema ou dos dados afetados, além da diretoria da empresa
Prazo Estimado para Reestabelecimento das atividades	8 horas

Fonte: Do autor.

Como citado por Fernandes (2014), deve-se fazer uma análise de impacto para conseguir identificar os sistemas mais cruciais e os menos cruciais. A análise de impacto desse trabalho que cobriria a terceira etapa do plano, baseou-se em uma empresa real, que o autor do mesmo está empregado, neste contexto descrita como empresa A, para não expor a mesma neste cenário. Esta empresa faz uso de diversos tipos de sistemas, dentre eles um *software* de Planejamento de Recursos Empresariais, do inglês *Enterprise Resource Planning* (ERP) e um *software* de solicitação de chamados, que contém funções semelhantes ao Akaunting e ao *osTicket* instalados no servidor do cenário criado. Analisando o impacto que esses dois *softwares* em específicos têm dentro da empresa A, foi notório que os dados do ERP são considerados mais importantes, e em caso de perda de dados, existe um grande impacto negativo para a organização. Por esse motivo seus dados são tratados com mais cuidado, visto que os *backups* do ERP são feitos mais de 2 vezes por dia, enquanto o *software* de solicitação de chamados possui o *backup* de seus

dados feito apenas 1 vez por dia. Diante disso o trabalho irá seguir essa hierarquia de criticidade.

Tendo definido a criticidade de um sistema sobre o outro, foi criado os parâmetros RTO e RPO para cada sistema. Assim foi definido que o *software* Akaunting terá um RTO de 8 horas e um RPO de 6 horas, ou seja, o tempo máximo de inatividade tolerado é de 8 horas e a quantidade de dados tolerada para ser perdida no caso de um desastre, são 6 horas. Já o *osTicket* foi definido com um RTO de 14 horas e um RPO de 12 horas, sendo assim é tolerado a inatividade do mesmo por 14 horas e uma quantidade de dados a serem perdidas de até 12 horas de informações antecedentes ao desastre (tabela 8).

Tabela 8 – RTO e RPO definido

	RTO	*RPO*
Akaunting	8 horas	6 horas
osTicket	14 horas	12 horas

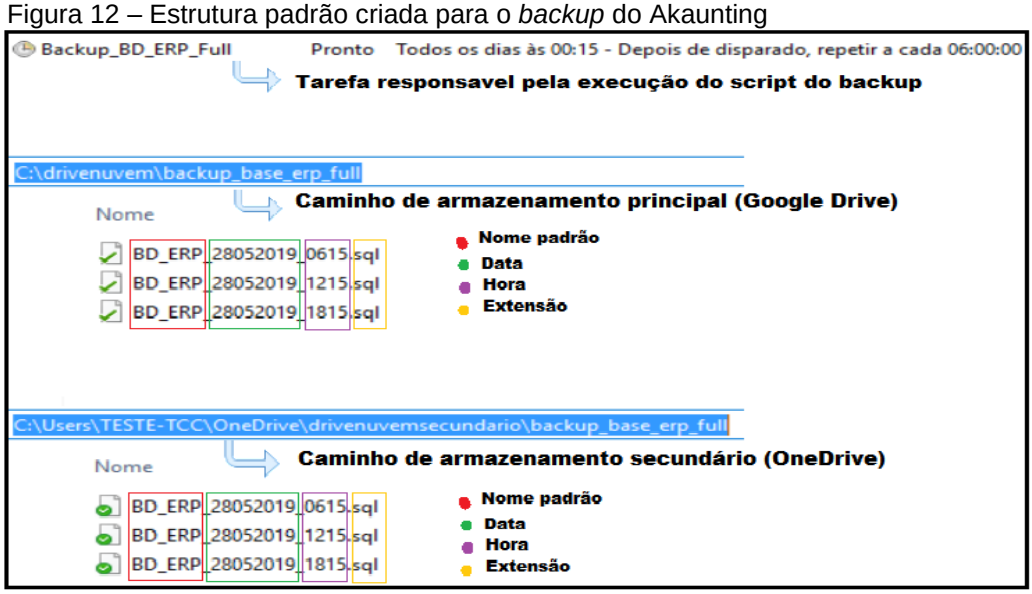
Fonte: Do autor.

Posteriormente foi criado as estratégias que buscam cobrir a quarta etapa do plano, elaborando as regras para os *backups* e restauração do ambiente. O *backup* da máquina virtual completa será realizado manualmente uma vez por semana, toda sexta-feira depois do fechamento da empresa. Exclusivamente esse *backup*, será armazenado na máquina que hospeda a máquina virtual, além de arquivar uma cópia da mesma na máquina de contingência. Como o *backup* da máquina virtual será realizado uma vez por semana, se faz necessário obter outras estratégias para manter a salvo os dados nesses intervalos. Para isso, foram elaborados alguns *scripts* com o intuito de realizar os *backups* de forma automática, para que não haja necessidade de executar todos os *backups* manualmente no horário correto, e assim não correr o risco de algum desses ser esquecido ou ser feito em outro horário por algum motivo.

O *backup* do banco de dados do Akaunting será realizado de forma *full* quatro vezes ao dia, em uma delas, no horário considerado de almoço que é 12:15 horas, outro no horário após o fechamento da mesma, que seria 18:15 horas, e duas vezes durante a noite/madrugada, para evitar de perder algum dado que por ventura venha a ser alterado ou adicionado por algum funcionário que excedeu seu horário de trabalho, esses *backups* serão realizados as 00:15 e as 6:15 horas. Desse modo, foi

criado uma tarefa no agendador do *Windows*, que executará o *script* responsável por esse *backup* a cada 6 horas, salvando-o na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário (figura 12). Antes de definir a escolha de qual local de armazenamento seria considerado o principal e qual seria o secundário, foram realizados diversos testes, colocando arquivos de diversos tamanhos e acompanhando a sincronização das duas nuvens simultaneamente, e foi observado que ambas faziam o *upload* do arquivo com tempos realmente muito próximos. Portanto a escolha do Google *Drive* como armazenamento principal, foi opção pessoal do acadêmico, por sua maior familiarização com a plataforma e pôr a mesma oferecer 15 GB de armazenamento gratuito, contra 5 GB disponibilizado pelo *OneDrive*.

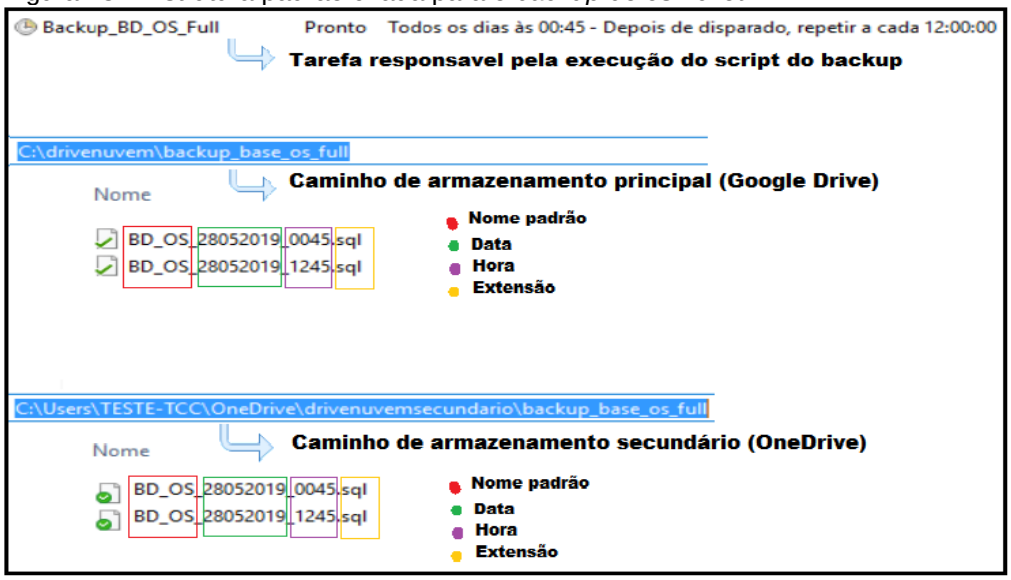
Figura 12 – Estrutura padrão criada para o *backup* do Akaunting



Fonte: Do autor.

O *backup* do banco de dados do *osTicket* será realizado de forma *full* duas vezes ao dia, o primeiro, meia hora após iniciar o *backup* do Akauting que é realizado no horário do almoço, que nesse caso coloca esse *backup* do *osTicket* para as 12:45 horas. O segundo *backup* será realizado 12 horas depois do primeiro, e após a empresa ter encerrado o expediente, assim fixando o horário para as 00:45 horas. Desse modo, foi criado uma tarefa no agendador do *Windows*, para executar o *script* a cada 12 horas, salvando o *backup* na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário (figura 13).

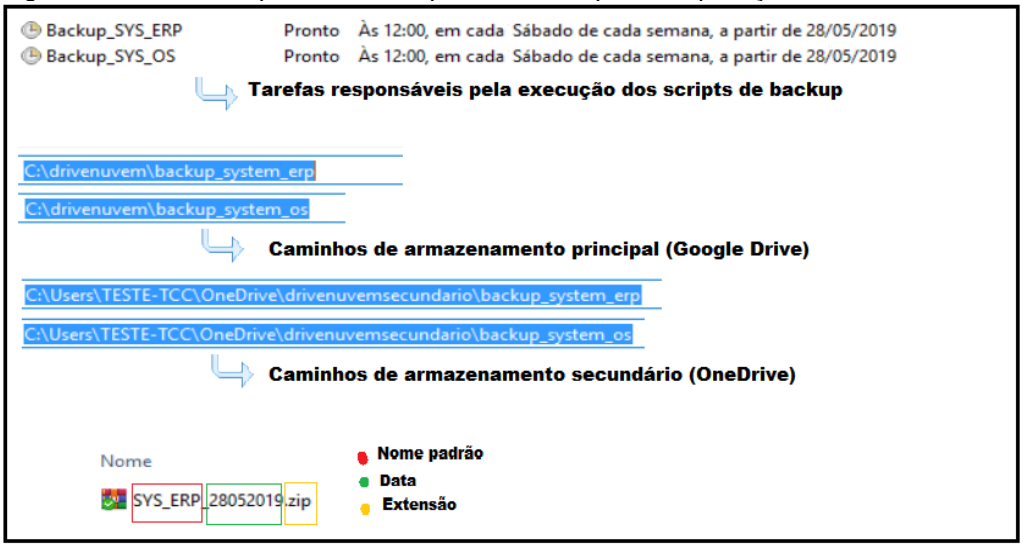
Figura 13 – Estrutura padrão criada para o *backup* do *osTicket*



Fonte: Do autor.

A estratégia mencionada acima, busca alcançar uma garantia de obtenção do RPO estipulado para cada sistema. Porém visando garantir o também cumprimento do RTO dos sistemas, foi elaborado *scripts* que façam a sua devida compactação no formato ZIP e os *backups* de forma automática das duas aplicações da empresa, para que se tenha pré-preparada uma recuperação que estabeleça o sistema com o máximo possível de atualizações que haviam sido aplicadas nos mesmos. Esses *backups* serão realizados semanalmente, as 12:00 horas de sábado, salvando-os na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário (figura 14).

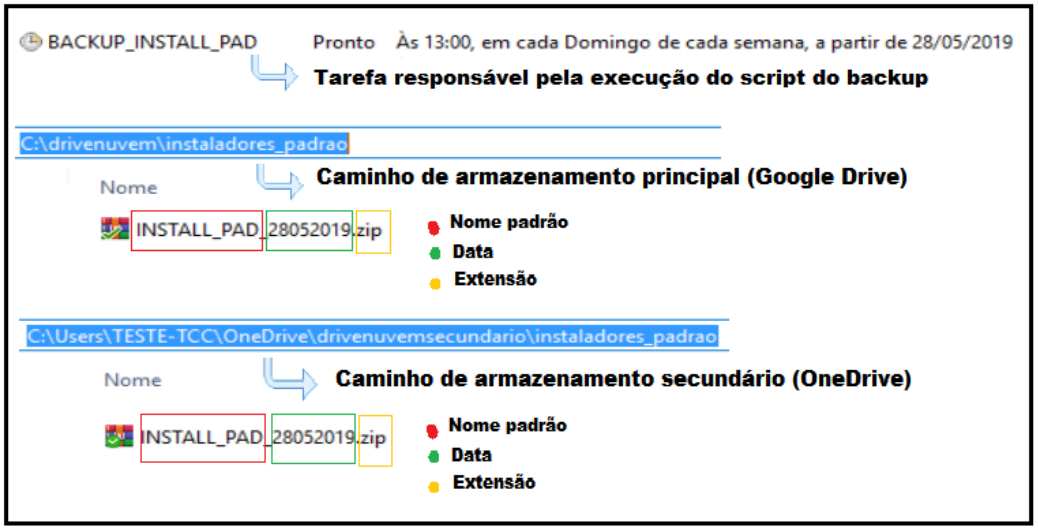
Figura 14 – Estrutura padrão criada para os *backups* das aplicações



Fonte: Do autor.

Tendo em vista uma possível instalação de algum novo programa necessário para a usabilidade dos sistemas da empresa, foi criado uma pasta com o seguinte nome: *instaladores_padrao*. Nessa pasta deve-se colocar todos os instaladores dos programas que forem necessários para o bom funcionamento do servidor e dos sistemas. Para efetuar o *backup* da mesma foi criado um *script* que faça a compactação no formato ZIP e efetue o *backup* dos mesmos. Esse *backup* será realizado semanalmente, as 13:00 horas de domingo, salvando-os na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário (figura 15).

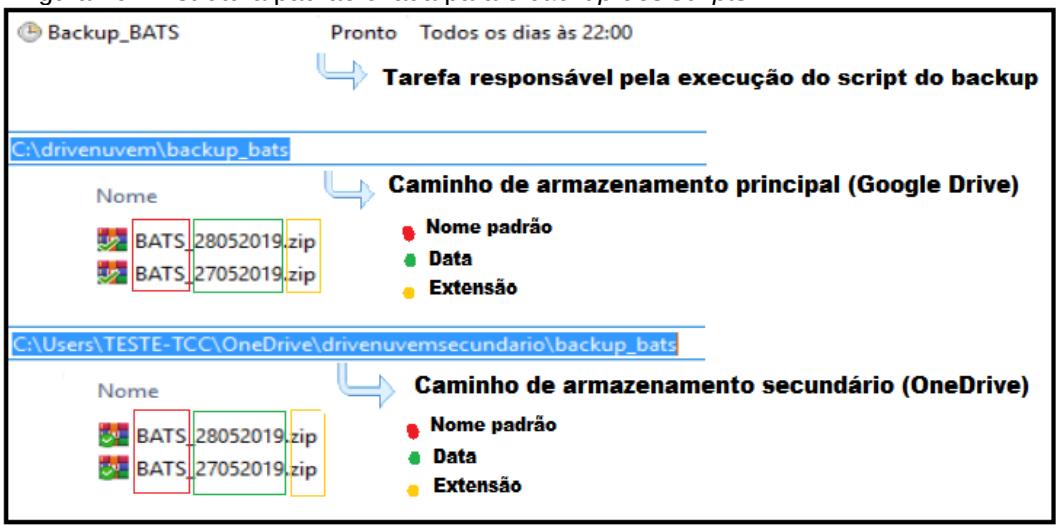
Figura 15 – Estrutura padrão criada para os *backups* dos programas padrão



Fonte: Do autor.

Os *backups* são realizados por *scripts* com o formato *bat*, e esses podem sofrer alterações caso algum caminho ou nome de arquivo mude, ou até mesmo novos sejam criados. Para garantir que nenhum desses arquivos responsáveis pelos *backups* automáticos sejam perdidos, foi criado uma tarefa no agendador do *Windows*, e esta executará um *script,* a fim de realizar a compactação e *backup* de todos os arquivos de scripts da pasta onde os mesmos encontram-se. Essa tarefa será executada diariamente as 22:00 horas, e seguirá o mesmo padrão de todas as outras, armazenando o *backup* no Google *Drive* como local principal e no *OneDrive* como local secundário (figura 16).

Figura 16 – Estrutura padrão criada para o *backup* dos *scripts*



Fonte: Do autor.

Por fim foi elaborado um *script* que exclua de ambos locais de armazenamento, os arquivos que possuam as extensões ZIP e SQL e estejam a mais de 15 dias nas pastas de sincronização. Esse *script* foi colocado para ser executado pelo agendador de tarefas do *Windows* a cada 15 dias, as 04:00 horas. O intuito do mesmo, é auxiliar para que não haja mais dados ocupando espaço na nuvem, do que o necessário.

Como nesse cenário os *backups* de sistemas, programas e dados são realizados em nuvem, e possuem seu caminho definido com sua devida estrutura de pastas conforme mostrado nas figuras anteriores. É necessário que ao criar um novo servidor desde a instalação do sistema operacional, deve-se sempre respeitar a estrutura e nome da máquina e das pastas, para que não se tenha problemas na realização dos *backups* automáticos.

Para a recuperação do ambiente, deve ser analisado qual desastre que afetou o mesmo. Cada categoria de desastre possui um responsável técnico, responsável de aquisição de bens, pessoas que deveram ser informadas, prazo para reestabelecimento das atividades e um impacto diferente no ambiente, portanto irá ser recuperado de maneira especifica.

Desastres conforme a tabela 4 que são causados por atualização de software, a recuperação é feita através do *download* e restauração do último *backup* feito na nuvem do sistema afetado, ou no caso de o problema estiver no sistema operacional, resolve-se importando o último *backup* da máquina virtual ou até mesmo

fazendo a formatação da máquina em questão, e reinstalando os *softwares* por meio dos seus devidos *backups*.

Em desastres conforme a tabela 5, que se refere a desastres que ocasionem perda de dados, a recuperação é feita através do *download* e restauração do último *backup* feito desses dados, e a importação do arquivo no devido banco de dados afetado.

Para desastres de acordo com a tabela 6 que se refere a desastres que ocasionem defeito com *hardware*, a empresa nesse cenário deve possuir *hardwares* de contingência para que nesses casos que haja a necessidade de substituição do *hardware*, o mesmo seja trocado, e a partir desse ponto verificar se algum *software* também foi afetado, para que seja feito o *download* do devido *backup* para recuperação. Em desastres assim, haverá a necessidade de aquisição de um novo *hardware* do mesmo modelo do substituído ou superior para suprir o estoque de contingência, por esse motivo o inventário de *hardware* e *software* deve ser atualizado.

Em desastres como o da tabela 7 que são desastres que comprometam a infraestrutura computacional, dependendo da gravidade, a recuperação tende a ser mais demorada caso afete muitos *hardwares* do ambiente. Nesses casos os *hardwares* devem ser substituídos por aqueles que estão no estoque de contingência e deve-se recuperar sistemas e dados com o *backup* mais atualizado disponível na nuvem para *download*. É necessário que o responsável técnico solicite ao responsável pelas compras de TI, uma nova aquisição para repor o estoque dos itens afetados, já que nesse momento a empresa estaria funcionando com os *hardwares* de contingência. Caso os equipamentos de contingência também venham a ser afetados pela severidade do desastre, o responsável técnico deve repassar ao responsável por aquisição de equipamentos, uma lista com todos os *hardwares* que estão sem reposição, para que seja adquirido os mesmos com o devido fornecedor no menor tempo possível. E assim que a nova máquina estiver pronta, deve-se instalar a nova máquina virtual com o mesmo nome e configuração da anterior, e baixar os últimos *backups* dos sistemas e bases, para que a empresa restabeleça suas atividades. Dando sempre prioridade para ao sistema com menor RTO definido.

Depois de desenvolvido o DRP, inicia-se a fase de testes, constituindo a quinta etapa do plano, que busca verificar se o plano está de acordo com a sua proposta, trazendo a devida segurança na recuperação do ambiente criado. Durante a fase de testes, podem haver sugestões de manutenção do plano, dependendo dos

resultados obtidos nessa etapa. Essas manutenções buscam manter o plano sempre atualizado e funcional.

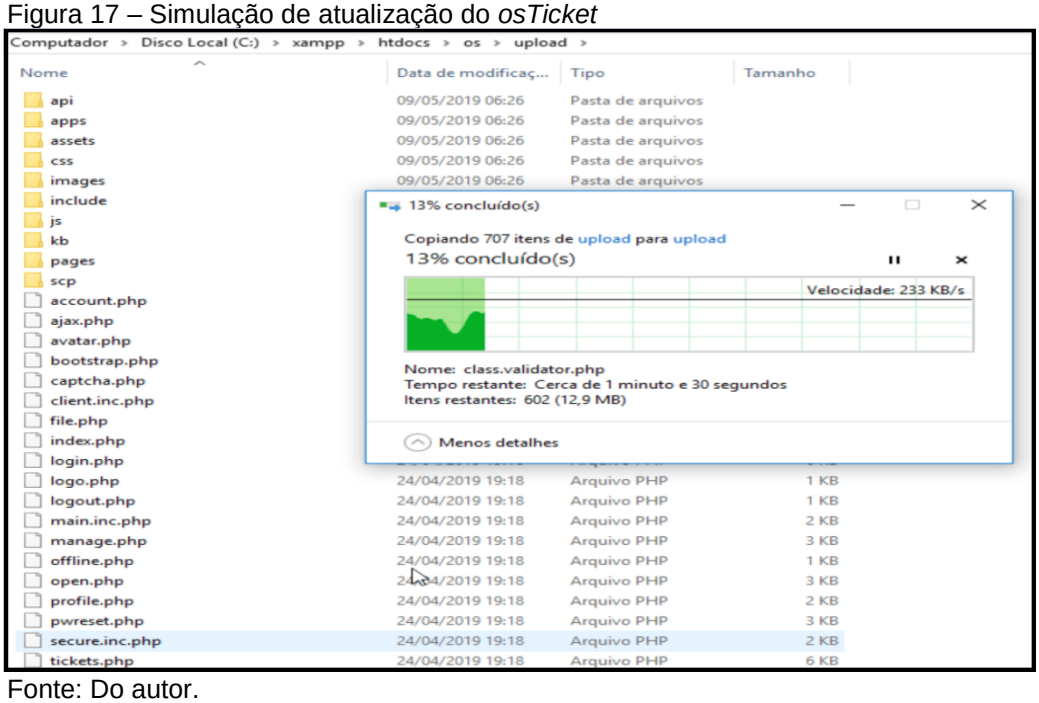
6.3 TESTES

Para a realização dos testes, foi utilizado o procedimento passo a passo, simulando a ocorrência de um evento para cada uma das quatro tabelas de desastres criadas no DRP, e uma simulando a perca total de ambos os hardwares, tanto de produção quanto o de contingência. Esses testes tem o intuito de verificar se o DRP elaborado está de fato trazendo a segurança desejada para os dados do ambiente criado.

6.3.1 Teste 1

O primeiro teste foi simulando uma atualização de *software* malsucedida no sistema de suporte ao cliente, que no cenário criado está instalado com sua versão 1.12. Para tentar causar o problema foi feito *download* do *osTicket*, porém de uma versão mais antiga, nesse caso a 1.10.1, e foi substituído a pasta ‘upload’ da versão instalada pela pasta de mesmo nome da antiga versão, pasta essa que possui arquivos de configuração (figura 17).

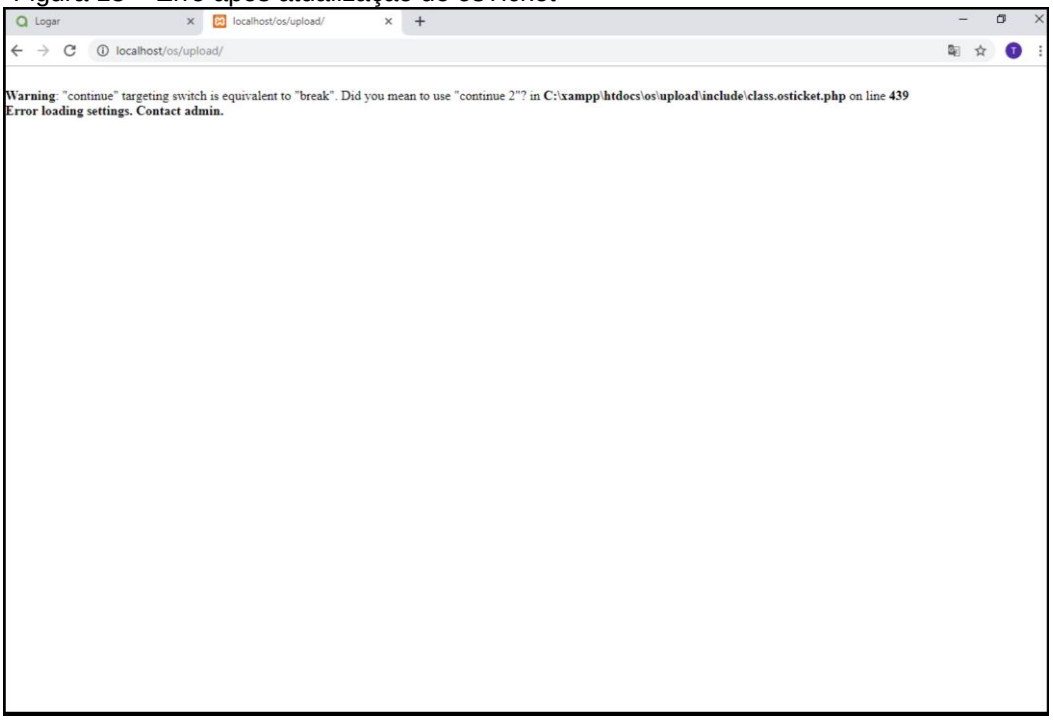
Figura 17 – Simulação de atualização do *osTicket*



Fonte: Do autor.

Com isso não foi mais possível acessar o sistema (figura 18).

Figura 18 – Erro após atualização do *osTicket*



Fonte: Do autor.

Para a correção do problema, foi restaurado o último *backup* realizado do sistema *osTicket* que estava armazenado em nuvem. Portanto o arquivo compactado foi extraído e substituído pela pasta da aplicação inteira que estava com problema. Feito isso a aplicação voltou a funcionar normalmente (figura 19).

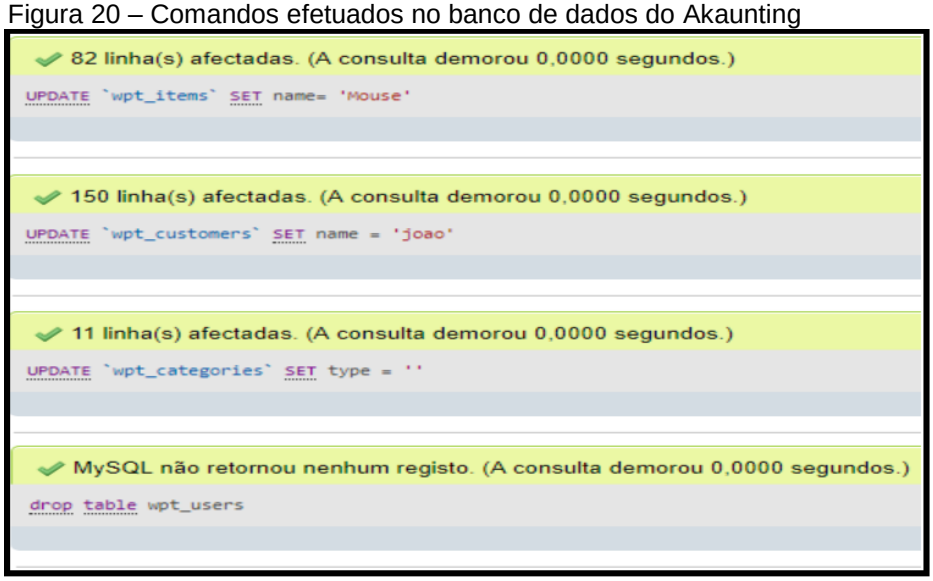
Figura 19 – *osTicket* após recuperação de desastre por atualização de *software*

Fonte: Do autor.

6.3.2 Teste 2

O segundo teste foi simulando uma falha que ocasionasse perda de dados, que nesse teste foi ocasionado por uma falha humana. Para realização desse teste, foi efetuado diversos comandos no banco de dados do programa Akaunting, '*updates*' sem nenhuma cláusula do tipo '*where*', inclusive na tabela de itens do mesmo. Além disso foi efetuado o comando do tipo '*drop table*' na tabela de usuários (figura 20).

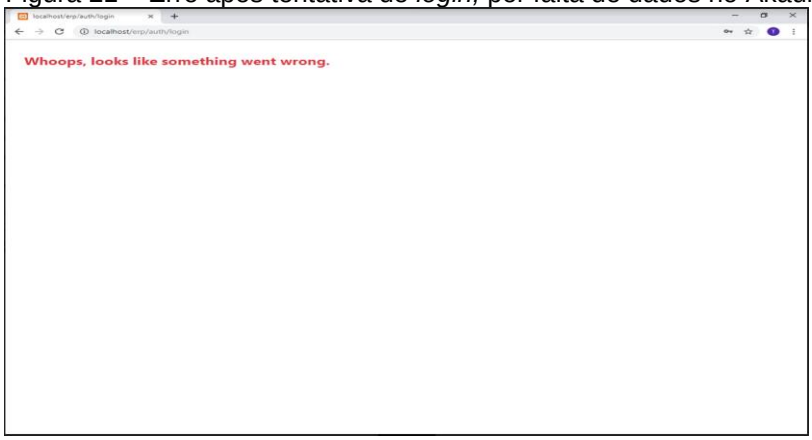
Figura 20 – Comandos efetuados no banco de dados do Akaunting



Fonte: Do autor.

Com todas essas alterações por erro humano, além de diversos dados terem perdido sua autenticidade, não foi mais possível acessar o sistema, devido a não existir mais a tabela de usuários (figura 21).

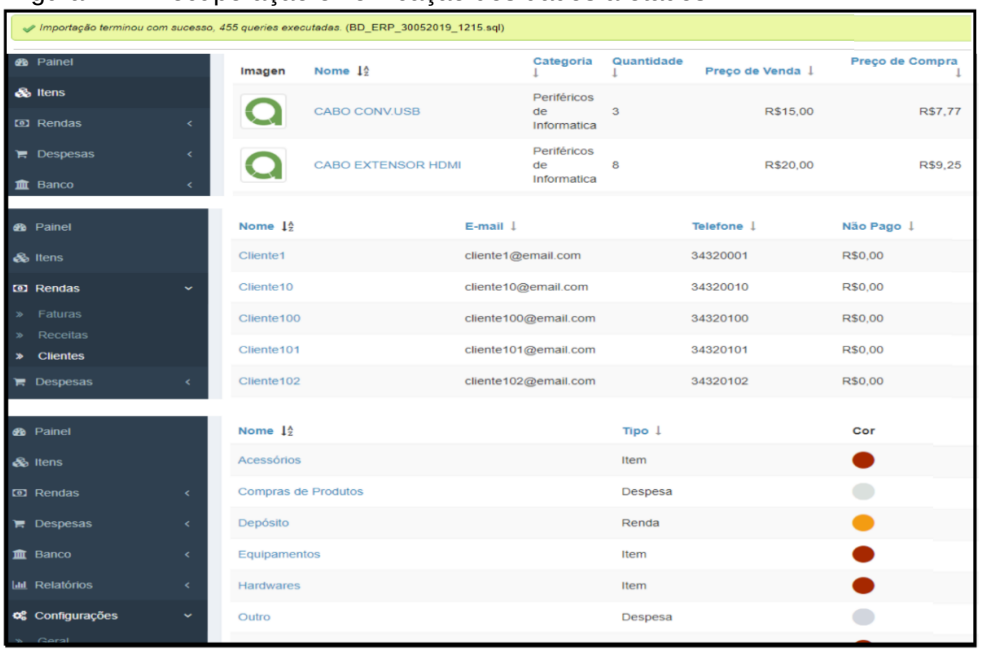
Figura 21 – Erro após tentativa de *login,* por falta de dados no Akaunting



Fonte: Do autor.

Com o intuito de recuperar os dados do sistema, foi restaurado o último *backup* do banco de dados do Akaunting que estava armazenado em nuvem. Importando assim o arquivo no phpMyAdmin para a base de dados do sistema. Após a importação com sucesso dos dados, foi possível acessar o *software* e verificar se os dados afetados estavam recuperados conforme anteriormente ao desastre (figura 22).

Figura 22 – Recuperação e verificação dos dados afetados

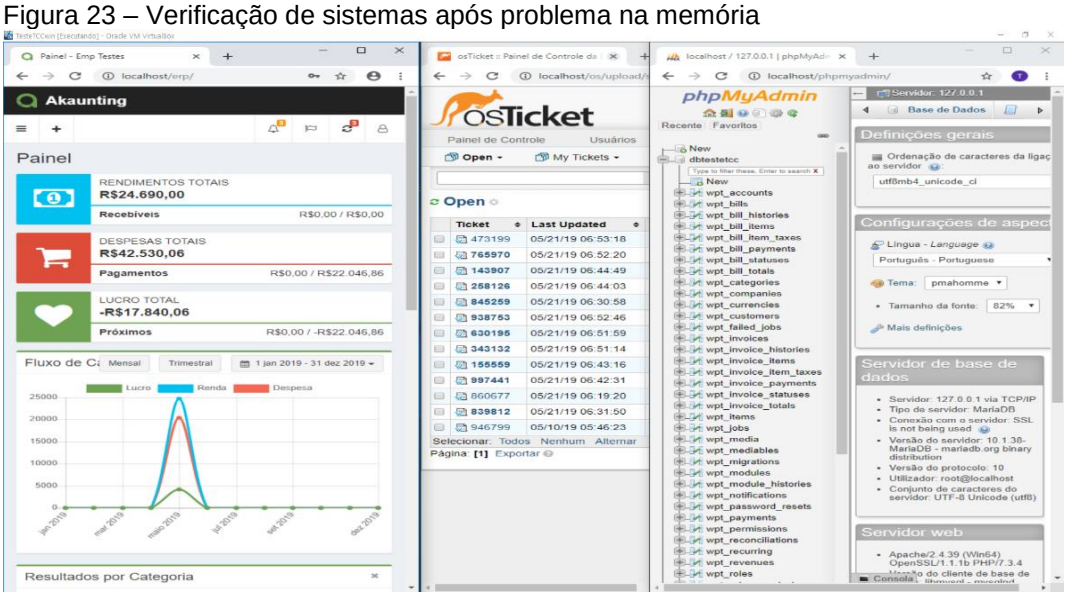


Fonte: Do autor.

6.3.3 Teste 3

O terceiro teste foi simulando uma falha devido a problemas no *hardware*, dessa vez uma falha que não foi causada por interação humana. Nesse caso foi simulado que o problema ocorreu com a memória da máquina *host*, que nesse cenário seria o *notebook*. O mesmo foi desligado completamente de forma repentina e efetuado a troca da memória que estaria afetada. Após a troca, foram ligados o *notebook* e a máquina virtual, e foi verificado se algum sistema ou banco foi afetado com essa queda repentina (figura 23).

Figura 23 – Verificação de sistemas após problema na memória



Fonte: Do autor.

Caso algum sistema ou dado tivesse sido afetado, seria necessário fazer a recuperação do mesmo. Porém nos 3 testes feitos simulando esse mesmo desastre, nenhum *software* ou dado foi afetado.

Depois de constatado que ambos estavam funcionando corretamente, o inventario é atualizado, para que o responsável pela aquisição de equipamentos possa repor o *hardware* utilizado (tabela 9).

Tabela 9 – Inventário de *hardware* e *software* após problema com um *hardware*

Hardwares Produção	*Hardwares* Contingência	*Softwares*
Notebook Samsung *Odyssey*	Computador *Desktop* Completo	*Windows*
Roteador Tp-*link Archer* C25	Roteador Tp-*link* wr 741nd	*VirtualBox*
	SSD 240GB	XAMP
		Akaunting
		osTicket
		Google *Drive*
		OneDrive

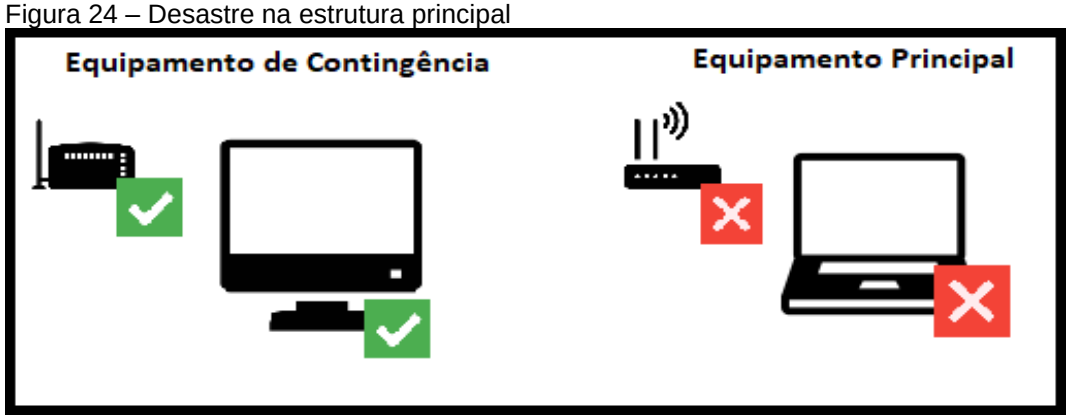
Fonte: Do autor.

6.3.4 Teste 4

O quarto teste foi simulando um desastre que comprometesse a infraestrutura do cenário criado. Nessa ocasião foi simulado uma queda devida a algum problema elétrico que acarretasse a queima dos equipamentos em produção,

roteador e a máquina *host*, que seria o *notebook*. Para isso o notebook e o roteador foram desligados repentinamente. Sem os equipamentos de produção funcionando, foi substituído o roteador danificado pelo reserva, e ativado a máquina de contingência (figura 24).

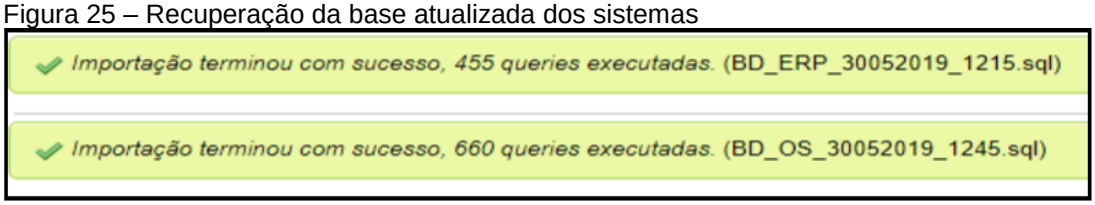
Figura 24 – Desastre na estrutura principal



Fonte: Do autor.

Com a máquina reserva ligada, foi importado no VirtualBox da mesma o último *backup* realizado da máquina virtual. A partir dessa recuperação, foi feito *download* do último *backup* do banco de dados do *osTicket* e Akaunting, levando em consideração que após o último *backup* da máquina virtual, alguns dados da base desses sistemas poderiam ter sofrido alguma alteração, assim fazendo-se necessário a recuperação dos *backups* desses dados (figura 25).

Figura 25 – Recuperação da base atualizada dos sistemas



Fonte: Do autor.

Após a recuperação dos sistemas e constatação que ambos estavam funcionando em produção no *host* de contingência, iniciou-se o que seria o levantamento dos *hardwares* afetados. Esse levantamento possui o intuito de atualizar a tabela de inventario de *hardware* e *software*, para que fosse encaminhado ao responsável pelas compras de equipamentos, e o mesmo possa realizar as devidas aquisições (tabela 10).

Tabela 10 – Inventário de *hardware* e *software* após queima dos equipamentos principais.

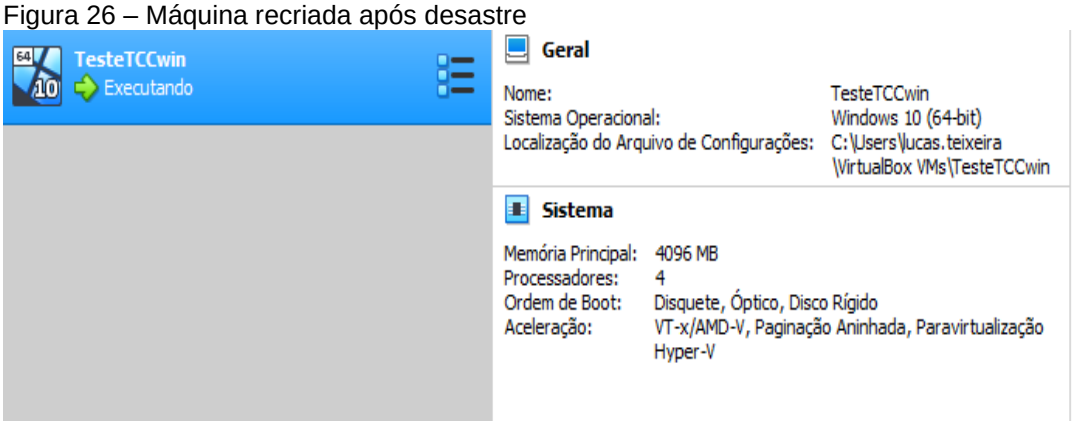
Hardwares Produção	*Hardwares* Contingência	*Softwares*
	Computador *Desktop* Completo	*Windows*
	Roteador Tp-*link* wr 741nd	*VirtualBox*
	Memória para *notebook* 8 GB	XAMP
	SSD 240GB	Akaunting
		osTicket
		Google *Drive*
		OneDrive

Fonte: Do autor.

6.3.5 Teste 5

Por fim foi simulado um desastre que comprometesse não somente os equipamentos em produção, mas também o de contingência. Após a reposição dos equipamentos afetados, tanto os principais quanto os de contingência já adquiridos pelo responsável das compras. A máquina *host* principal foi devidamente instalada, e se fez necessário instalar o servidor virtual desde o início, já que o *backup* da máquina virtual completa era armazenado nas máquinas físicas atingidas pelo desastre. A nova máquina virtual criada, seguiu as mesmas configurações relatadas nesse trabalho anteriormente, além de ser criada com o mesmo nome padrão da anterior (figura 26).

Figura 26 – Máquina recriada após desastre

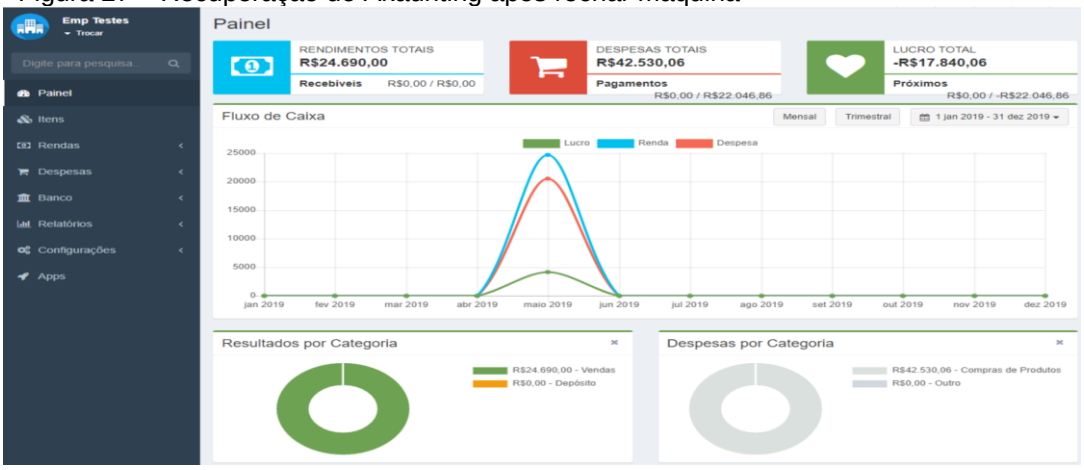


Fonte: Do autor.

Com a máquina virtual devidamente instalada, foi feito *download* do último *backup* realizado dos programas padrões, e assim instalado cada um desses, além de já entrar nas contas do Google *Drive* e *OneDrive* nos seus respectivos sincronizadores. Depois foi feito *download* do último *backup* realizado do *software*

Akaunting e sua base de dados, já que esse *software* possui um menor RTO, portanto sua prioridade é maior. A pasta do *software* Akaunting baixada foi colocada na devida pasta do Xampp, e no phpMyAdmin foi criado uma nova base de dados com o mesmo nome utilizado na máquina anterior, e o arquivo da base do Akaunting baixado foi importado para essa base de dados. Após isso foi verificado que o Akaunting voltou a funcionar normalmente (figura 27).

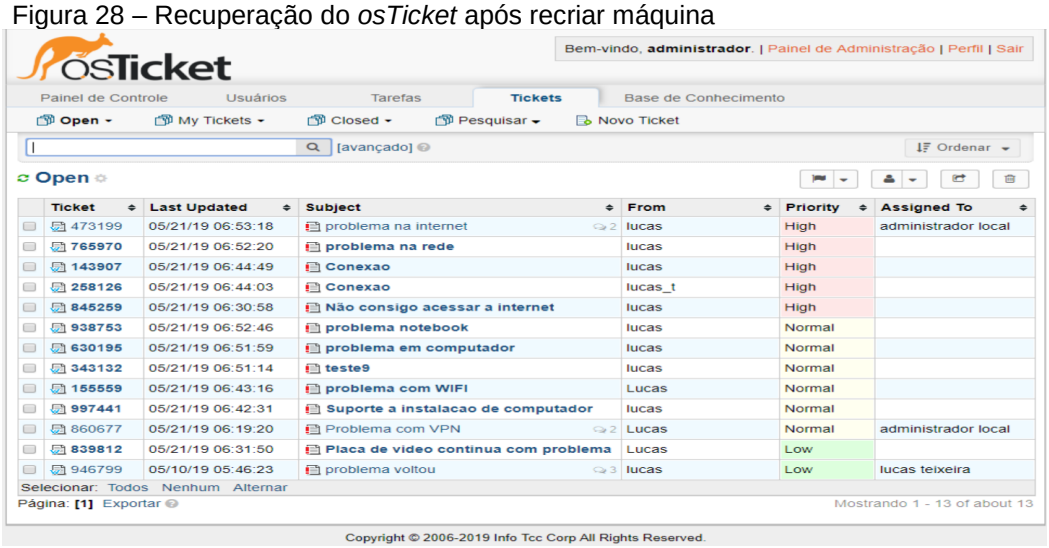
Figura 27 – Recuperação do Akaunting após recriar máquina



Fonte: Do autor.

O próximo passo foi fazer *download* do último *backup* realizado do *software osTicket* e sua base de dados. A pasta do *software osTicket* baixada foi colocada na devida pasta do Xampp, e no phpMyAdmin foi criado uma nova base de dados com o mesmo nome da que era utilizada na máquina anterior para esse *software*, e o arquivo da base do osTicket baixado foi importado para essa base de dados. Feito isso foi constatado que o *osTicket* voltou a funcionar normalmente, e com sua base de dados devidamente restaurada (figura 28).

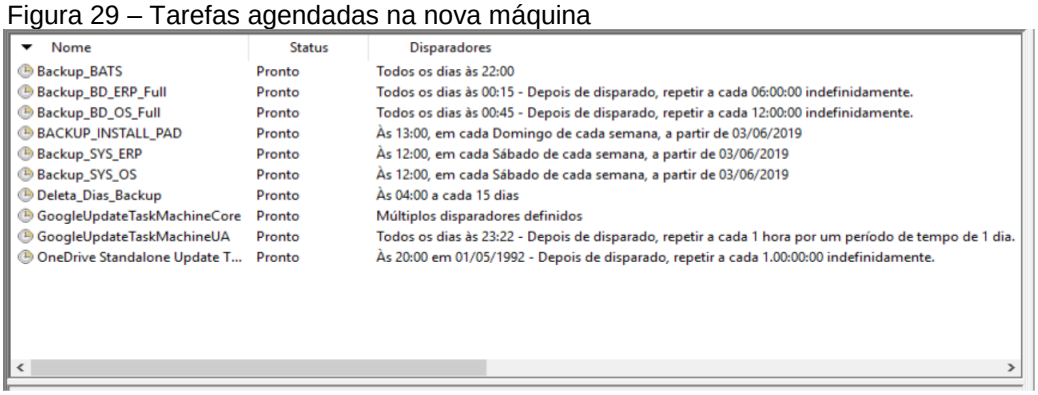
Figura 28 – Recuperação do *osTicket* após recriar máquina



Fonte: Do autor.

Com os dois sistemas da empresa funcionando devidamente em produção, restou apenas realizar as configurações para que os *backups* automáticos voltassem a funcionar nessa nova máquina. Para isso foi feito *download* do último *backup* realizado dos *scripts*, e a partir daí os mesmos foram colocados na pasta padrão desses *scripts* e novas tarefas para a execução dos mesmos foram criadas no agendador do *Windows*, seguindo as instruções e horários estabelecidos no DRP (figura 29).

Figura 29 – Tarefas agendadas na nova máquina



Fonte: Do autor.

7 RESULTADOS E DISCUSSÕES

A partir do levantamento bibliográfico, foi possível ter um entendimento geral do conceito, importância e de como elaborar um *Disaster Recovery Plan*. E esse conhecimento adquirido foi essencial para o desenvolvimento de todo o trabalho, desde a criação do ambiente computacional até a fase de testes.

Ao iniciar a projeção e criação do cenário, foi-se deparado com o primeiro desafio, pois foi necessário adquirir mais conhecimento sobre máquinas virtuais. Para isso, fez-se a primeira máquina virtual somente para compreender o funcionamento do *software* de virtualização, para que depois fosse criado a máquina virtual que seria a mesma utilizada no ambiente simulado.

Com a máquina virtual criada, foi iniciado a tentativa de instalação dos dois *softwares* escolhidos para fazerem parte do ambiente computacional. Para a instalação do Akaunting não foram encontradas grandes complicações, porém para a instalação do *osTicket* foi aplicado muito tempo de pesquisa, pois a primeira versão que foi baixada não se conseguiu fazer funcionar. Buscando entender como funcionava a instalação e configuração, para ser capaz de fazer o mesmo funcionar corretamente, foi feito diversas pesquisas na internet.

Quando os *softwares* foram enfim instalados corretamente, foi necessário abastecer os sistemas com dados. Para que os dados fossem inseridos de maneira funcional, foi aplicado conhecimentos que foram adquiridos ao longo da vida profissional do acadêmico. Buscou-se inserir as informações de maneira que se aproximasse de informações reais empresariais.

Com o ambiente devidamente pronto, foi criado um DRP que buscasse corresponder à altura do mesmo. O plano abrangeu as especificações encontradas nos materiais utilizados no levantamento bibliográfico. Contendo regras para os *backups* de cada sistema e dados do ambiente, tempo previsto de recuperação e ações a serem tomadas pelos envolvidos após a ocorrência de cada tipo de desastre especificado.

A fase de testes, envolveu simulações de desastres no ambiente com a pretensão de serem o mais próximas possíveis de um cenário real. Foram feitos cinco testes com desastres de diferentes tipos. Em todos os desastres simulados, a recuperação dos sistemas e dados foram feitas com êxito, com um tempo abaixo do

que era previsto para restabelecimento das atividades do determinado desastre, e cumprindo com sucesso o RTO e RPO estipulados para cada sistema da empresa.

Buscando esses resultados positivos, e obter um aperfeiçoamento do modelo de *backup* do DRP utilizado no trabalho correlato de Ávila, Soldan e Petroli Neto (2017), que era feito manualmente, foi elaborado para que nesse cenário criado os *backups* fossem realizados de forma automatizada. Para conseguir fazer isso, foi necessário estudar maneiras de gerá-los automaticamente. A forma escolhida foi através de scripts do tipo *bat*, que foram criados para serem adicionados como tarefas no agendador do *Windows*, e assim fazendo o que foram programados para realizar, de maneira automática. O resultado de automatização foi bastante satisfatório, pois cumpriu com o desejado, que era realizar os *backups* de todos os sistemas e dados, além de a própria limpeza dos dados antigos na nuvem, sem haver a necessidade de interação direta humana.

No momento de elaborar uma forma satisfatória de realizar os *backups* em nuvem, foi analisado o tempo que demoraria para fazer *upload* dos mesmos, com o pacote de dados disponível para o ambiente. Cada *backup* de sistema e dados, possuiu um tempo de sincronização considerado aceitável, tempo esse sempre menor que 15 minutos nos testes realizados. No entanto, na tentativa de armazenar o *backup* da máquina virtual inteira em nuvem, a previsão de sincronização apresentadas por ambas as nuvens, foi de quase 40 horas. Por esse motivo optou-se por armazenar os *backups* da máquina virtual somente na máquina *host* e com uma cópia na do estoque de contingência. Porém, em um desastre que afetasse ambos os ambientes, o *backup* armazenado nas mesmas poderia ser perdido. Por esse motivo foi revisto as regas do *backup* criado, para que fosse possível elaborar de uma maneira que tudo o que fosse necessário para a recuperação do ambiente estivesse salvo em nuvem.

Com todos os *softwares* e dados necessários para recriar a máquina salvos em nuvem, foi possível fazer a restauração geral da máquina virtual e deixar o ambiente totalmente recuperado, sem ter o *backup* completo da mesma. Fazendo somente uma nova instalação de uma máquina virtual *Windows*, seguindo as mesmas especificações e nomes da anterior, e com a mesma criada, fazer a recuperação dos programas e dados já devidamente armazenados em nuvem. Sendo assim, todo esse processo, mesmo sem o *backup* da máquina virtual completa, foi realizado dentro do prazo previsto e ainda cumprindo com uma certa folga o RTO e RPO estabelecidos.

8 CONCLUSÃO

O presente trabalho se constituiu na elaboração e testes de um *Disaster Recovery Plan* para um ambiente empresarial criado, efetuando seu *backup* em nuvem. Durante a criação do cenário e elaboração do plano, se encontrou algumas dificuldades conforme relatado no capitulo de resultados e discussões, mas todas essas foram resolvidas à medida que os conhecimentos foram aprofundados.

O estudo atingiu seus objetivos através dos materiais obtidos no levantamento bibliográfico, e colocando em pratica no ambiente criado o conhecimento adquirido com os mesmos.

A aplicação do *Disaster Recovery Plan* no ambiente simulado, se mostrou bastante eficiente e cumpriu com as expectativas depositadas no mesmo. Visto que em todos os testes efetuados foi possível realizar as recuperações em um tempo menor que o previsto no plano.

Com base nos resultados expressados neste trabalho, que teve como objetivo geral elaborar um estudo sobre a construção e aplicação de um *Disaster Recovery Plan*, utilizando a computação em nuvem como local de armazenamento dos *backups* de empresas de pequeno ou médio porte. Pode-se concluir que para obter sucesso na aplicação de um DRP, a elaboração do mesmo deve ser trabalhada em conjunto com o cenário da empresa em que o mesmo será aplicado. Visto que cada empresa tem suas particularidades, orçamento, horários e equipamentos, portanto o DRP deve ser adequado para atender as expectativas e necessidades da mesma.

No entanto é importante ressaltar que a partir dos testes, ficou claro que a qualidade do pacote de dados da empresa é essencial para se conseguir obter uma boa eficiência ao se aplicar um *Disaster Recovery Plan* em nuvem. Visto que a qualidade desse pacote de dados possui influência no tempo de *backup* e restauração dos dados empresariais.

Como sugestão para trabalhos futuros seguindo essa mesma base, sugere-se a aplicação de um DRP utilizando alguma infraestrutura em nuvem como estoque de contingência, e analisar as dificuldades e soluções de aplicar essa pratica. Como também elaborar um DRP com estratégias de *backup* utilizando algum *software* de *backup* gratuito que possua maiores funcionalidades, e possibilidade de fazê-los de

forma incremental e diferencial, para que se possa verificar as vantagens e desvantagens de utilizar um *software* de *backup* pronto.

REFERÊNCIAS

AGUIAR JUNIOR, Ubirajara Ferreira de. **PLANO DE RECUPERAÇÃO DE DESASTRES: UMA PESQUISA-AÇÃO EM EMPRESA DO SETOR ENERGÉTICO.** 2012. 42 f. TCC (Graduação) - Curso de Engenharia Mecânica, Universidade Estadual Paulista, Guaratinguetá, 2012. Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/117957/aguiarjunior_uf_tcc_guara.pdf?sequence=1&isAllowed=y. Acesso em: 25 set. 2018.

ALHAZMI, Omar H.; MALAIYA, Yashwant K.. Evaluating disaster recovery plans using the cloud. **2013 Proceedings Annual Reliability And Maintainability Symposium (rams)**, Orlando, p.1-6, jan. 2013. Disponível em: https://ieeexplore.ieee.org/document/6517700. Acesso em: 28 set. 2018.

ALLES, Guilherme Rezende. **Análise da utilização de tecnologias de contêineres para aplicações de alto desempenho.** 2018. 59 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/175014/001065151.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2019.

ANDRADE, Daniel*. et al*. **PLANO DE CONTINGÊNCIA DE TI: PREPARANDO SUA EMPRESA PARA REAGIR A DESASTRES E MANTER A CONTINUIDADE DO NEGÓCIO.** 2011. 14 f. Monografia (Especialização) - Curso de Segurança da Informação, Senac, Brasília, 2011.

ÁVILA, Cleiton Silva de; SOLDAN, Evandro Luis; PETROLI NETO, Silvio. A SEGURANÇA DE UMA ESTRUTURA DE DISASTER RECOVERY PLAN EM CLOUD COMPUTING. **Ensaios Usf**, Bragança Paulista, v. 1, n. 1, p.103-116, 2017. Disponível em: http://ensaios.usf.edu.br/ensaios/article/view/61. Acesso em: 09 ago. 2018.

BARNOSCHI, Adriana. BACKUP AND DISASTER RECOVERY FOR MODERN ENTERPRISE. **5th International Scientific Conference Business And Management.** Vilnius, p. 630-635. mai 2008. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.4838&rep=rep1&type=pdf. Acesso em: 27 set. 2018.

BAZZOTTI, Cristiane; GARCIA, Elias. **A importância do sistema de informação gerencial para tomada de decisões.** Disponível em: http://www.waltenomartins.com.br/sig_texto02.pdf. Acesso em: 12 de Ago. 2018.

BERNHEIM, Laura. **IaaS vs. PaaS vs. SaaS Cloud Models (Differences & Examples).** 2017. Disponível em: https://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/. Acesso em: 20 mar. 2019.

BNDES. **Porte de empresa.** Disponível em: https://www.bndes.gov.br/wps/portal/site/home/financiamento/guia/porte-de-empresa. Acesso em: 01 jul. 2019.

BORGES, Hélder Pereira. **GERNU: UMA ABORDAGEM PARA GERÊNCIAMENTO DE NUVENS BASEADA NOS REQUISITOS DO USUÁRIO, CRIAÇÃO DINÂMICA DOS SERVIÇOS E DEFINIÇÃO DE ATRIBUTOS DE QUALIDADE.** 2013. 197 f. Tese (Doutorado) - Curso de Doutorado em Ciência da Computação, Universidade Federal do Ceará, Fortaleza, 2013. Disponível em: http://www.repositorio.ufc.br/bitstream/riufc/18679/1/2013_tese_hpborges.pdf. Acesso em: 12 set. 2018.

BOTACIM, Renato Sousa *et al.* COMPUTAÇÃO NAS NUVENS: EVOLUÇÃO E PECULIARIDADE DOS SERVIÇOS E DA SEGURANÇA DA INFORMAÇÃO. **Reinpec**, Itaperuna, v. 2, n. 1, p.259-270, jan./jun. 2016. Disponível em: http://reinpec.srvroot.com:8686/reinpec/index.php/reinpec/article/view/168. Acesso em: 11 set. 2018.

DIKAIAKOS, Marios D*. et al*. Cloud Computing: Distributed Internet Computing for IT and Scientific Research. **IEEE Internet Computing**, p.10-13, set. 2009. Disponível em: https://ieeexplore.ieee.org/document/5233607. Acesso em: 12 set. 2018.

FARIA, Heitor Medrado de. **Bacula: Ferramenta Livre de Backup.** Brasport, 2010.

FERNANDES, Luis Miguel Ferreira. **Planeamento de Estratégias de Salvaguarda e Reposição de Dados/Informação baseado em Algoritmo de Optimização de requisitos Multidimensionais.** 2014. 105 f. Dissertação (Mestrado) - Curso de Segurança de Sistemas de Informação, Universidade Católica Portuguesa, 2014. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/14681/1/Final_v504_184308008.pdf.Acesso em: 27 set. 2018.

FURLAN, Marcos da Silva; ASSIS, Naziro Hamed de. **Backup: Proteção e segurança de dados e informações em ambientes corporativos.** 2015. 54 f. Monografia (Especialização) - Curso de Pós-graduação em Infraestrutura de Redes de Computadores, Fundação de Assistência e Educação - Faesa, Vitória, 2015. Disponível em: https://docplayer.com.br/20019367-Backup-protecao-e-seguranca-de-dados-e-informacoes-em-ambientes-corporativos.html.Acesso em: 09 ago. 2018.

GARBELINI, Jader Maikol Caldonazzo; LIMA, Moisés Fernando. VIRTUALIZAÇÃO DE SERVIDORES EM AMBIENTES DE COMPUTAÇÃO EM NUVEM. **Revista Eletrônica de Computação**, Londrina, v. 1, n. 1, p.41-53, jan./jun. 2013. Disponível em: http://www.unifil.br/portal/images/pdf/documentos/revistas/revista-eletronica/computacao/computacao-2013.pdf.Acesso em: 10 set. 2018.

GASQUES, Ana Carla Fernandes *et al*. Sistemas de Informação em Pequenas Empresas: Uma Análise Teórica. In: ENCONTRO DE ENGENHARIA DE PRODUÇÃO AGROINDUSTRIAL, 10., 2016, Campo Mourão. **Anais... .** Campo Mourão, 2016.

GOMES, Jeremias Moreira. A forense computacional e os discos de estado sólido. In: ICOFCS, 2012, Brasília. **Proceeding.** Brasília: Abeat, 2012. p. 7 - 11. Disponível em: http://icofcs.org/2012/ICoFCS2012_Full.pdf#page=9. Acesso em: 29 mar. 2019.

ISO. **ISO / IEC 24762: 2008:** Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services. 2008. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:24762:ed-1:v1:en. Acesso em: 22 out. 2018.

ISO. **ISO 22301:2012:** Societal security — Business continuity management systems --- Requirements. 2012. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en:e. Acesso em: 22 out. 2018.

JESUS, Joana D'arc Pereira de. **Preservação da informação digital: estudo de caso na Biblioteca Digital de Monografias da Universidade de Brasília.** 2011. 69 f. TCC (Graduação) - Curso de Biblioteconomia, Universidade de Brasília, Brasília, 2011. Disponível em: http://bdm.unb.br/bitstream/10483/2466/1/2011_JoanaDarcPereiradeJesus.pdf. Acesso em: 26 mar. 2019.

LANDRY, Brett J. L.; KOGER, M. Scott. Dispelling 10 Common Disaster Recovery Myths: Lessons Learned from Hurricane Katrina and Other Disasters. **Acm Journal on Educational Resources in Computing.** p. 1-14. dez. 2006. Disponível em: https://dl.acm.org/citation.cfm?doid=1248453.1248459. Acesso em: 29 out. 2018.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação gerenciais.** 9. ed. São Paulo: Pearson, 2011. 448 p.

LIMA, Edmilson de Oliveira. AS DEFINIÇÕES DE MICRO, PEQUENA E MÉDIA EMPRESAS BRASILEIRAS COMO BASE PARA A FORMULAÇÃO DE POLÍTICAS PÚBLICAS. In: EGEPE, 2., 2001, Londrina. **Anais... .** Londrina, 2001. p. 421 - 436. Disponível em: http://www.anegepe.org.br/edicoesanteriores/londrina/GPE2001-03.pdf. Acesso em: 16 abr. 2019.

LOPES, Maico Cristiano Fonlor. **RECUPERAÇÃO DE DESASTRE PARA A BIBLIOTECA DO CENTRO DA CIÊNCIA DA SAÚDE NA UENP METODOLOGIA E ESTUDO DE CASO.** 2017. 35 f. TCC (Graduação) - Curso de Segurança da Informação, Fatec Ourinhos, Ourinhos, 2017.

LUDESCHER, W.; CUGNASCA, P.S. A model for evaluating the reliability of computational systems disaster recovery plans. **Risk, Reliability And Societal Safety.** London, p. 2371-2376. 2007. Disponível em: https://docplayer.net/8982352-A-model-for-evaluating-the-reliability-of-computational-systems-disaster-recovery-plans.html. Acesso em: 09 out. 2018.

LUDESCHER, Wagner. **MODELO PARA AVALIAÇÃO DA QUALIDADE DE PROJETOS DE PLANOS DE CONTINUIDADE DE NEGÓCIOS APLICADOS A SISTEMAS COMPUTACIONAIS.** 2011. 275 f. Tese (Doutorado) - Curso de Doutorado em Engenharia, Universidade de São Paulo, São Paulo, 2011. Disponível em: http://www.teses.usp.br/teses/disponiveis/3/3141/tde-10082011-142221/pt-br.php. Acesso em: 10 out. 2018.

MELL, Peter M.; GRANCE, Timothy. **The NIST Definition of Cloud Computing.** 2011. Disponível em:

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Acesso em: 12 set. 2018.

MELO, Daniel Reis Armond de. A importância da tecnologia da informação nas estratégias das organizações contemporâneas: breve revisão de literatura. In: V CONVIBRA – CONGRESSO VIRTUAL BRASILEIRO DE ADMINISTRAÇÃO, 5., 2008, Manaus. **Anais...** , 2008. Disponível em: http://www.convibra.com.br/2008/artigos/412_0.pdf. Acesso em: 08 abr. 2019.

MORAES, Eliana Márcia. **PLANEJAMENTO DE BACKUP DE DADOS.** 2007. 125 f. Dissertação (Mestrado) - Curso de Mestrado em Gestão e Desenvolvimento Regional, Universidade de Taubaté, Taubaté, 2007. Disponível em: http://www.ppga.com.br/mestrado/2007/moraes-eliana_marcia.pdf. Acesso em: 09 ago. 2018.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. GESTÃO DA SEGURANÇA DA INFORMAÇÃO: FATORES QUE INFLUENCIAM SUA ADOÇÃO EM PEQUENAS E MÉDIAS EMPRESAS. **Revista de Gestão da Tecnologia e Sistemas de Informação**, São Caetano do Sul, v. 4, n. 3, p.375-397, 2007. Disponível em: http://www.scielo.br/pdf/jistm/v4n3/07.pdf. Acesso em: 02 abr. 2019.

NEVES, Jorge Manuel Mack. **Tomada de Decisão sobre Estratégias de Recuperação de Desastre em Tecnologia e Sistemas de Informação.** 2009. 310 f. Tese (Mestrado) - Curso de Sistemas de Informação, Universidade do Minho, Braga, 2009. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/26314/1/2009_MSc_JorgeNeves.pdf. Acesso em: 24 set. 2018.

NIST. **NIST Cloud Computing Program - NCCP.** 2010. Disponível em: https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp. Acesso em: 01 jul. 2019.

NIST. **NIST Cloud Computing Standards Roadmap.** 2013. Disponível em: https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf. Acesso em: 01 jul. 2019.

PEDROSA, Paulo H. C; NOGUEIRA, Tiago. **Computação em Nuvem.** 2011. Disponível em: http://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf. Acesso em: 14 set. 2018.

PEREIRA JUNIOR, Jorge Hosni Pereira de. **Plano de continuidade de negócios aplicado à segurança da informação.** 2008. 60 f. Monografia (Especialização) - Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/15974/000695265.pdf. Acesso em: 04 out. 2018.

PIEROBON, Sandro Jose; TEODORO, Edivaldo. RECUPERAÇÃO DE DADOS EM UNIDADES DE ARMAZENAMENTO, AMBIENTE WINDOWS. **Technologies**, Nova Odessa, v. 8, n. 1, p.53-66, 2014. Disponível em: http://www.nwk.edu.br/intro/wp-

content/uploads/2014/05/Technologies-2014-.pdf#page=53. Acesso em: 26 mar. 2019.

PINTA, Jan. Disaster Recovery Planning as part of Business Continuity Management. **Agris on-line Papers in Economics and Informatics.** Prague, p. 55-61. 2011. Disponível em: http://ageconsearch.umn.edu/record/120243/files/agris_on-line_2011_4_pinta.pdf. Acesso em: 27 set. 2018.

PRAZERES, Antero José Maia. **Continuidade de Negócio, Disaster Recovery e estratégias de implementação na Santa Casa da Misericórdia de Lisboa.** 2012. 99 f. Dissertação (Mestrado) - Curso de Desenvolvimento de Software e Sistemas Interactivos, Instituto Politécnico de Castelo Branco, Castelo Branco, 2012. Disponível em: https://repositorio.ipcb.pt/bitstream/10400.11/1472/1/disserta%C3%A7%C3%A3o.pdf. Acesso em: 15 mai. 2017.

RITTINGHOUSE, John W; RANSOME, F. James. **Cloud Computing: Implementation, Management and Security.** CRC PRESS, 2009.

ROCHA, Clécio Teixeira *et al.* **Plano de Recuperação de Desastres utilizando ferramenta Veeam Backup & Replication em falha do Active Directory.** Disponível em: http://www.unibratec.edu.br/tecnologus/wp-content/uploads/2015/12/tecnologus_edicao_09_artigo_02.pdf. Acesso em: 08 nov. 2018.

RODRIGUES, Ricardo Batista. **RECCLOUD: UM MODELO DE RECOMENDAÇÃO DE ARQUIVOS PARA SISTEMAS DE ARMAZENAMENTO EM NUVEM.** 2014. 75 f. Dissertação (Mestrado) - Curso de Ciência da Computação., Universidade Federal de Pernambuco, Recife, 2014. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/11974/1/DISSERTA%C3%87%C3%83O%20Ricardo%20Batista%20Rodrigues.pdf. Acesso em: 11 set. 2018.

RODRIGUES, Wilson Flávio. **ANÁLISE DOS PROCEDIMENTOS DE BACKUP DOS INSTITUTOS FEDERAIS.** 2017. 140 f. Dissertação (Mestrado) - Curso de Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2017. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/25612/1/DISSERTA%C3%87%C3%83O%20Wilson%20Fl%C3%A1vio%20Rodrigues.pdf. Acesso em: 13 nov. 2018.

ROSSI, Vagner Costa; THEISEN, Cleonir Paulo. MICRO, PEQUENAS E MÉDIAS EMPRESAS: O DESAFIO DAS MPMEs DE SOBREVIVEREM DIANTE DA INSTABILIDADE ECONÔMICA. **Revista Tecnológica / Issn 2358-9221**, [s.i], v. 6, n. 1, p.212-232, set. 2017. Disponível em: https://uceff.edu.br/revista/index.php/revista/article/view/226. Acesso em: 16 abr. 2019.

SEBRAE. **Participação das Micro e Pequenas Empresas na Economia Brasileira.** Brasília, 2014. Disponível em: http://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Estudos%20e%20Pesquisas/Participacao%20das%20micro%20e%20pequenas%20empresas.pdf. Acesso em: 18 abr. 2019.

SHILAWAT, Sandeep. **Cloud Interoperability and Portability.** 2018. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2018/06/22/cloud-interoperability-and-portability/#4e64954d4577. Acesso em: 12 set. 2018.

SILVA, Edenilson Tondo da. **SOFTWARE LIVRE NO MONITORAMENTO DE SERVIÇOS E BACKUP DE DADOS POR MEIO DE REDES DE COMPUTADORES.** 2015. 73 f. Monografia (Especialização) - Curso de Especialização em Redes de Computadores, Universidade Tecnológica Federal do Paraná, Pato Branco, 2015. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/5903/1/PB_ESPRC_II_2015_04.pdf. Acesso em: 13 nov. 2018.

SILVA, Rhenann Granado Cottar Marçal. CLOUD COMPUTING E GRID COMPUTING: UM ESTUDO DE CASO. **Revista Eletrônica de Computação**, Londrina, v. 1, n. 1, p.2-12, jan./jun. 2013. Disponível em: http://www.unifil.br/portal/images/pdf/documentos/revistas/revista-eletronica/computacao/computacao-2013.pdf. Acesso em: 10 set. 2018.

SOBRAGI, Cyro Gudolle. **ADOÇÃO DE COMPUTAÇÃO EM NUVEM: ESTUDO DE CASOS MÚLTIPLOS.** 2012. 155 f. Monografia (Especialização) - Curso de Pós-graduação em Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2012. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/49406/000837499.pdf?sequence=1&isAllowed=y. Acesso em: 11 set. 2018.

SOUSA, Flávio R. C.; MOREIRA, Leonardo O.; MACHADO, Javam C.. **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios.** Ercemapi. Teresina, 2009. Disponível em: https://www.researchgate.net/profile/Javam_Machado/publication/237644729_Computacao_em_Nuvem_Conceitos_Tecnologias_Aplicacoes_e_Desafios/links/56044f4308aea25fce3121f3/Computacao-em-Nuvem-Conceitos-Tecnologias-Aplicacoes-e-Desafios.pdf. Acesso em: 11 set. 2018.

SULTAN, Nabil. Cloud computing for education: A new dawn? **Elsevier: International Journal of Information Management.** Liverpool, p. 109-116. 2010. Disponível em: https://www.sciencedirect.com/science/article/pii/S0268401209001170. Acesso em: 12 set. 2018.

TAURION, Cezar. **Cloud computing: computação em nuvem: transformando o mundo da tecnologia da informação.** Rio de Janeiro: Brasport, 2009.

TELES JÚNIOR, Namedin Pereira. **Backup Markup Language (BKPML): Uma Proposta para Interoperabilidade e Padronização de Backup de Dados.** 2011. 122 f. Dissertação (Mestrado) - Curso de Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/2328/1/arquivo2997_1.pdf. Acesso em: 13 nov. 2018.

TOZZI, Chirstopher. **RTO vs. RPO: Two Means toward the Same End.** Disponível em: https://www.cloudberrylab.com/blog/rto-vs-rpo-difference/. Acesso em: 05 nov. 2018.

TSESTOQUE. Tipos de estoques: você sabe quais são os principais? Disponível em: http://universidadeestoque.com.br/blog/index.php/tipos-de-estoque-voce-sabe-quais-sao-os-principais/. Acesso em: 03 jun. 2019.

WESTCON, Equipe. **O que é um plano de recuperação de desastres**. Disponível em: http://microsoft.westcon.com/?/post/141/o-que-e-um-plano-de-recuperacao-de-desastres/. Acesso em: 15 Ago. 2018.

ZENATTI, Pedro Diego. **RECUPERAÇÃO DE DADOS: ESTUDO DE VIABILIDADEDE IMPLANTAÇÃO DE CLÍNICA DE RECUPERAÇÃO DE DADOS.** 2014. 52 f. TCC (Graduação) - Curso de Sistemas de Informação, Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Ijuí, 2014. Disponível em: http://bibliodigital.unijui.edu.br:8080/xmlui/bitstream/handle/123456789/2380/pedro%20zenatti%20tcc.pdf?sequence=1. Acesso em: 27 mar. 2019.

ZISSIS, Dimitrios; LEKKAS, Dimitrios. Addressing cloud computing security issues. **Elsevier: Future Generation Computer Systems.** Syros, p. 583-592. 2010. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X10002554. Acesso em: 12 set. 2018.

APÊNDICE

APÊNDICE A – Artigo

Planejamento de disaster recovery plan com backup em nuvem, visando aplicações em pequenas ou médias empresas

Lucas Teixeira[1], Paulo João Martins[2]

[1]Acadêmico do Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma/SC

[2]Professor do Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma/SC

lucasteixeira.tr@hotmail.com, pjm@unesc.net

Abstract. *A company can make use of several information systems, when used, these manipulate data that have a certain importance for the corporation. The loss of data can often lead to large negative impacts on the company that owns them, and may even be irreversible. To avoid problems like this, or at least reduce its impact on the company, is that the Disaster Recovery Plan (DRP) is created, it is a plan with a set of actions to be taken by IT staff, to keep your archived data safe and to recover it if you experience problems that could compromise your systems or information. The objective of this work is to elaborate a DRP, using cloud computing as the storage location for backups of a small or medium-sized simulated business environment. With the implementation of the scenario and preparation of the plan according to the materials obtained in the bibliographical survey, it was possible to test it and carry out the verification of how the plan was implemented, and whether it fulfilled its objective.*

Resumo. *Uma empresa pode fazer uso de diversos sistemas de informação, quando utilizado, esses manipulam dados que possuem uma determinada importância para a corporação. A perda de dados muitas vezes pode acarretar em grandes impactos negativos para a empresa que os possui, podendo até mesmo serem irreversíveis. Para evitar problemas como este, ou ao menos reduzir seu impacto na empresa, é que o Disaster Recovery Plan (DRP) é criado, ele é um plano com um conjunto de ações a serem tomados pela equipe de TI, para manter seus dados arquivados em segurança e recuperá-los caso venha a ocorrer problemas que possam comprometer os seus sistemas ou informações. O objetivo deste trabalho é elaborar um DRP, utilizando a computação em nuvem como local de armazenamento dos backups de um ambiente empresarial simulado de pequeno ou médio porte. Com a implementação do cenário e elaboração do plano conforme os materiais obtidos no levantamento bibliográfico, foi possível testa-lo e realizar a verificação de como foi a aplicação do plano criado, e se o mesmo cumpriu com o seu objetivo.*

1. Introdução

O mundo encontra-se cada vez mais na era da informação, esse cenário faz com que as empresas tenham que se adaptar para continuar competindo. Essa exigência por mudanças está tornando o ambiente corporativo mais dependente da infraestrutura tecnológica que gerencia seus dados (BAZZOTTI; GARCIA, 2006).

Algumas empresas possuem diversas aplicações que são essenciais para o gerenciamento e controle dentro da mesma. Existem variados tipos de sistemas que podem estar sendo utilizados dentro de um ambiente empresarial, mesmo em pequenas e médias empresas, e muitos destes, manipulam e gerenciam dados cruciais. Assim como citado por Aguiar Junior (2012) qualquer tipo de interrupção nos sistemas que gere perda de dados, poderá representar um grande impacto financeiro para uma empresa.

Na atual realidade, e a relevância que os dados de uma empresa possuem, é de extrema importância que haja a conscientização de dispor de backups seguros, e um plano para recupera-los após qualquer eventualidade. O Plano de Recuperação de Desastres, do inglês Disaster Recovery Plan (DRP), é um documento que deve abranger a descrição das ações indispensáveis para a recuperação dos serviços, principalmente os críticos, após um determinado evento inesperado, deve conter os passos para preparar o local de backup, as funções e responsabilidades do pessoal envolvido, além de definir o inventário de hardware e software para a execução do plano (ANDRADE et al.,2011).

Segundo Westcon (2017), pequenas e médias empresas geralmente não possuem equipe especializada para a elaboração de um DRP, constantemente recorrendo apenas ao backup. Contudo, dependendo da maneira e frequência que o backup é feito, a empresa corre o risco de perder volumes de dados, ou considerando-se que o mesmo seja armazenado localmente, e o desastre comprometa a estrutura física da empresa, como os causados por incêndios, a mesma poderá perder todo o seu volume de dados.

Visando cenários empresarias como o citado anteriormente por Westcon (2017), onde a empresa de pequeno ou médio porte, não possua uma equipe treinada para a elaboração de um DRP, e que mantenha a segurança da informação confiada a backups armazenados localmente. A empresa estaria à mercê de um possível prejuízo, caso aconteça algum desastre.

Considerando possíveis problemas como o mencionado acima, o presente estudo teve a finalidade de conhecer a importância de se ter um DRP para empresas. Identificar as principais relevâncias que devem ser consideradas no momento da composição de um plano de recuperação de desastres. Deste modo criando um ambiente a fim de simular um cenário computacional empresarial de pequeno porte. Então elaborando um DRP, de acordo com o estudo realizado e o cenário feito, efetuando seus backups em nuvem, e assim podendo testa-lo para validar se o mesmo cumpri o proposito para ao qual foi elaborado.

2. Disaster recovery plan

O Disaster Recovery Plan (DRP), ou Plano de Recuperação de Desastres em português, é um plano que possui nele descritos as medidas a serem tomadas para que haja a retomada dos serviços essenciais de TI, relatando as etapas a serem seguidas para a recuperação e disponibilização dos sistemas danificados por um desastre (ANDRADE et al.,2011).

O DRP é limitado aos recursos de TI, pois seu principal objetivo é recuperar a infraestrutura ou os sistemas danificados pelo desastre, com o menor espaço de tempo e o mínimo de perca de informação possível (PRAZERES, 2012).

Conforme Alhazmi e Malaiya (2013, tradução nossa), um conceito relevante em um DRP é a separação geográfica entre o site principal e o de backup. Visto que em escala global uma fração significativa de desastres são causados geograficamente pela natureza.

2.1. Planejamento de DRP

Na hora de fazer o planejamento de um DRP deve-se descrever os passos para preparar o local de backup, as funções e responsabilidades do pessoal envolvido, os eventos que retratam um

desastre, além de definir o inventário de hardware e software para a execução do plano (ANDRADE et al.,2011).

Segundo Ávila, Soldan e Petroli Neto (2017), os profissionais de TI podem ter diversos planos de recuperação de dados, que vão desde replicação das informações em diferentes dispositivos, até a elaboração de estratégias de DRP baseado no backup em nuvem.

Deve ser mencionado, quem pode executar o DRP, quem participará, qual é o objetivo e qual é o estado alvo que se deseja alcançar após a implementação do plano (PINTA, 2011, tradução nossa).

Conforme Ludescher e Cugnasca (2007) fazer uma análise de riscos é importante na elaboração de um DRP, pois essa análise fornece diretrizes para a concepção do processo de planejamento. Este tipo de análise, deve ser feita após o levantamento dos fatores mais prováveis que podem levar a um desastre que afete a empresa, para que após essa análise consiga-se criar maneiras de minimizar a exposição da empresa a esses desastres.

O plano também deve levar em consideração os impactos que a paralisação possa causar, além de o tempo máximo para restauração das atividades da organização (PEREIRA JUNIOR, 2008). Fazendo uma Análise de Impacto, torna-se possível separar os serviços críticos utilizados na empresa, dos menos importantes para recuperação. (PINTA, 2011, tradução nossa).

Ainda segundo Pinta (2011, tradução nossa) após a análise de risco e análise de impacto, deve-se construir a estratégia de recuperação, que envolve a configuração de parâmetros RPO e RTO em relação aos impactos da análise. Indicadores como Recovery Point Objectives (RPO) e Recovery Time Objectives (RTO), são elementos que auxiliam a definir requisitos reais para manter em operação os sistemas e promover soluções que pré-defina as prioridades de recuperação das funções e componentes de TI. O RTO representa o tempo máximo aceitável, que o negócio poderá permanecer com o processo interrompido, enquanto o RPO, representa um período de perda máxima de dados tolerada.

Conforme descrito por Ludescher e Cugnasca (2007) a etapa de testes do DRP é considerada extremamente importante, já que é a única maneira de garantir que o plano elaborado esteja funcionando de acordo com o esperado. Consegue-se efetuar os testes por meio de simulação de um desastre em sistemas alternativos, sem que haja a preocupação de afetar os sistemas em produção. Há também a possibilidade de simular um desastre no ambiente em produção, porém esse tipo de teste poderia causar uma parada completa nos sistemas que estejam em funcionamento na empresa.

3. Backup

Backup é o termo utilizado para descrever a cópia de segurança de dados digitais, arquivadas em um outro dispositivo de armazenamento físico ou virtuais, diferente do dispositivo que possui os dados originais. Essa cópia de segurança representa a garantia de recuperação de dados, caso ocorra algum problema que provoque a perda das informações na base principal (FURLAN; ASSIS, 2015).

A cópia de segurança pode ser feita em um dispositivo de armazenamento ou em outra localidade, protegendo desta forma, os dados contra acidentes ocorridos na estrutura física. Um backup considerado eficaz, consiste em minimizar as perdas, proporcionando a possibilidade de restauração dos dados no menor tempo e com a menor perda possível (FARIA, 2010).

Segundo Rodrigues (2017) a necessidade de fazer cópias de segurança, se dá devido à importância que as informações têm para as empresas, e o impacto que a perda das mesmas pode ocasionar no negócio, podendo muitas vezes ter um impacto irreversível que possa levar

a inviabilização da continuidade da empresa. Contudo, realizar backups é algo fundamental para qualquer instituição que preze o valor de suas informações.

4. Computação em nuvem

Computação em nuvem é um paradigma computacional, que possui como seu objetivo principal o acesso facilitado a recursos computacionais de alto desempenho e escalabilidade por meio da Internet. Tornando assim desnecessário o investimento em equipamentos físicos de alto padrão (SILVA, 2013).

De acordo com Taurion (2009), a Computação em Nuvem pode ser descrita como um ambiente computacional baseado em uma ampla rede de servidores, sejam estes físicos ou virtuais. Para simples definição, pode-se dizer que é um conjunto de recursos como capacidade de armazenamento, conectividade, processamento, plataformas, aplicações e serviços disponíveis na Internet. Isto é, a computação em nuvem é uma evolução do conceito de virtualização.

A computação em nuvem possui a promessa de economia de custos combinados com maior agilidade de TI. Sendo assim considera-se a adoção da nuvem em governo e industrias em resposta a restrição econômica difícil (NIST, 2010, tradução nossa).

De acordo com Mell e Grance (2011, tradução nossa), a computação em nuvem é um modelo para permitir acesso de rede sob demanda a um conjunto compartilhado de recursos de computação configuráveis, que pode ser liberado de forma rápida e com esforço mínimo de interação ou gerenciamento com o provedor de serviços.

Conforme Alles (2018), a utilização de uma infraestrutura sob demanda, faz com que o recurso computacional em questão não seja mais visto como um produto, e sim como um serviço. O uso dessa abordagem, possibilita um modelo de pagamento onde o contratante é cobrado somente pelos recursos utilizados. Desse modelo de negócio que surgiu os conceitos típicos de Infraestrutura como um serviço do inglês Infrastructure as a Service (IaaS), Plataforma como um serviço do inglês Platform as a Service (PaaS) e Software como um serviço do inglês Software as a Service (SaaS).

5. Metodologia

Para a elaboração deste trabalho, foi realizado um levantamento bibliográfico acerca dos conceitos necessários para a resolução desta pesquisa, tais como: Backups, Computação em Nuvem e Disaster Recovery Plan, sua importância no âmbito da tecnologia da informação empresarial, além de como realizar esse planejamento.

Na etapa do desenvolvimento foi necessário projetar e criar uma máquina virtual de forma a representar um ambiente próximo a um cenário empresarial de pequeno porte, para que assim fosse realizados os experimentos necessários. Criado o cenário então foi elaborado um Disaster Recovery Plan para esse ambiente, visando manter suas informações o mais seguras possível. No final do desenvolvimento, tem-se a fase de testes, onde o objetivo foi verificar se o DRP cumpre com seus objetivos propostos.

5.1. Projeto e implementação do cenário

Nesta fase, foi criado um cenário para simular um ambiente de TI empresarial de pequeno porte. O cenário possuiu um link ADSL de 15 Mbps de *download* e 1,5 Mbps de *upload*. Para criar o cenário, foi utilizado um notebook e um *desktop* com as configurações abaixo.

Notebook:

a) **modelo *notebook*:** Samsung *Odyssey* NP800G5M;

b) **processador:** Intel *Core* i5-7300HQ 2.5 GHz;

c) **memória:** 8 GB;

d) **HD:** SSD 240GB Sandisk *Plus*;

e) **sistema operacional:** *Windows* 10 Pro – 64 bits.

Desktop:

a) **processador:** Intel *Core* i5-7400 3.00 GHz;

b) **memória:** 8 GB;

c) **HD:** SSD 240GB WD *Green*;

d) **sistema operacional:** *Windows* 10 Pro – 64 bits.

No cenário para aplicação do DRP, foi definido o notebook como máquina principal, e o *desktop* como estoque de contingência do mesmo. Desse modo foi instalado no notebook uma máquina virtual fazendo uso do *software* VirtualBox, que é uma solução profissional da Oracle. A escolha desse software de virtualização, se deu ao fato de o mesmo ser gratuito, ter a possibilidade de ser executado em *hosts Windows*, Linux, Macintosh e Solaris e suportar um grande número de sistemas operacionais para serem instalados em suas máquinas virtuais.

A máquina virtual criada como servidor para os testes possui a seguinte configuração:

a) **processador:** 4 CPU (Intel *Core* i5-7300HQ 2.5 GHz);

b) **memória:** 4 GB;

c) **HD:** 50 GB (alocados dinamicamente);

d) **sistema operacional:** *Windows* 10 Pro – 64 bits.

Nesse servidor *Windows* foi instalado o software Xampp, que é uma ferramenta gratuita, e está possui um pacote que inclui banco de dados MySQL e Apache com suporte à linguagem PHP, para utilização dos sistemas web desse cenário empresarial. Para simular a utilização de sistemas empresariais, foi utilizado dois softwares para auxiliar os processos das principais funções de negócio, ambos gratuitos. O primeiro é o Akaunting que é um *software* contábil, que possui recursos como: painel com informações de fluxo de caixa, cadastro e controle de itens e estoque, faturas de contas a receber e a pagar, gestão de clientes e fornecedor, além de relatórios financeiros. O segundo é o *osTicket*, que é um sistema de suporte ao cliente, onde os mesmos abrem seus tickets/chamados, para terem o devido suporte dos atendentes da empresa.

Após a instalação do *software* Akaunting, o mesmo foi configurado com seu padrão de moeda (Real), categorias de produtos, despesas e rendas, além de ser realizado os devidos cadastros de produtos, clientes e fornecedores. Os produtos inseridos foram obtidos de uma base real empresarial, com informações de preço de venda, preço de custo, descrição e quantidade. Foram realizados centenas de cadastros de clientes, além de cadastrar fornecedores para cada tipo de categoria dos produtos. Os cadastros de clientes e fornecedores foram realizados com dados fictícios.

Após o termino dos ajustes do Akaunting, iniciou-se a instalação e configuração do software *osTicket*. Foram realizadas todas as configurações necessárias para que o *software* de suporte ao cliente estivesse funcional, tais como: aplicação de pacote de linguagem, cadastros de atendentes, equipes e departamento. Para gerar mais dados, foram abertos diversos tickets de solicitação de serviço por meio da web, utilizando o notebook e o *desktop*. Todos esses tickets possuem interações de um ou mais atendentes, dentre esses, alguns foram marcados como resolvido e assim encerrados, e outros foram mantidos em atendimento.

Como esse trabalho propõe utilizar a nuvem como local de *backup*, foi utilizado duas contas gratuitas, uma da empresa Google e outra da Microsoft para esse fim. Para fazer uso dessas contas, utilizou-se dois *softwares* de sincronização, um já disponível no Windows o OneDrive, e o Google Drive, que foi necessário fazer o download da versão de sincronização para desktop. Foi utilizado duas nuvens para o armazenamento dos *backups* buscando se precaver de uma eventual indisponibilidade de uma das plataformas no momento que for necessário a recuperação dos dados. A escolha dessas duas plataformas, se deu pelo fato de ambas terem a possibilidade de criar contas com um determinado espaço de armazenamento gratuito e suficiente para dar suporte ao projeto desenvolvido. Além de que Ávila, Soldan e Petroli Neto (2017), afirmam com base em testes realizados, que ambas plataformas são seguras.

5.2. Elaboração do DRP

A elaboração do DRP, foi baseado em um compilado do referencial teórico obtidos sobre o assunto, para conseguir compreender quais informações são importantes para se ter em um plano como esse, e como deve ser seu ciclo. Inclusive, o ciclo criado para esse DRP, foi baseado no ciclo adaptado por Aguiar Junior (2012), que foi criado com base no método PDCA de melhoria continua do processo. O ciclo criado para o plano foi dividido em cinco etapas (figura 1).

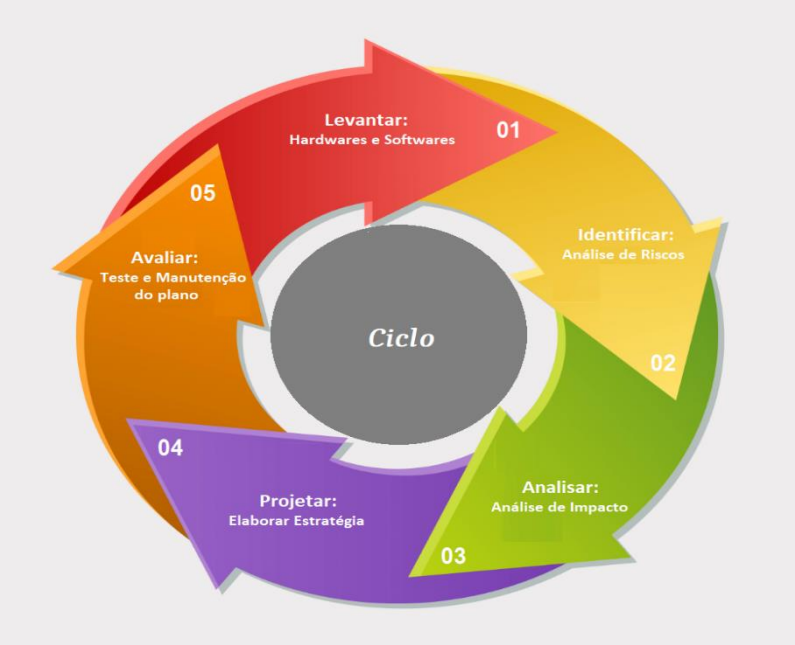


Figure 1. Ciclo para elaboração e constante melhoria do DRP

Como relatado por Andrade et al. (2011) o inventário de hardware e software são necessários para a execução de um DRP. Portanto, a primeira etapa conteve o levantamento dos *hardwares* e *softwares* utilizados no ambiente computacional criado. A tabela 1, contém o inventário para o projeto, e este deve estar sempre atualizado e a disposição do responsável pela aquisição de equipamentos da empresa, e esse responsável deve manter-se sempre atualizado sobre quais fornecedores possuem esses equipamentos para reposição rápida.

Table 1. Inventário de hardware e software

Hardwares Produção	*Hardwares* Contingência	*Softwares*

Notebook Samsung *Odyssey*	Computador *Desktop* Completo	*Windows*
Roteador Tp-*link Archer* C25	Roteador Tp-*link* wr 741nd	*VirtualBox*
	Memória para *notebook* 8 GB	XAMP
	SSD 240GB	Akaunting
		osTicket
		Google *Drive*
		OneDrive

Posteriormente, foi documentado de forma geral os principais eventos que retratariam um desastre. Assim criando quatro tabelas que cobrem a segunda etapa do plano, identificação e análise de risco, contendo a descrição do desastre, responsabilidades dos envolvidos e o objetivo alvo que é o restabelecimento das atividades.

A tabela 2 cobre desastres ocasionados a partir de uma atualização de *software*, sejam eles os sistemas utilizados pela empresa, ou o sistema operacional do servidor.

Table 2. Desastres por atualizações de software

Ativação do DRP	Cenário
Definição de Desastre	Atualizações malsucedidas dos sistemas
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Não
Quem deve ser informado	Responsável por setores que fazem uso do sistema afetado
Prazo Estimado para Reestabelecimento das atividades	3 horas

A tabela 3, busca cobrir desastres ocasionados por falhas humanas ou não, que resulte a perda de dados, sejam essas falhas por negligência, sabotagem ou algum problema que possa ter afetado o banco de dados mesmo sem a colaboração direta de uma pessoa.

Table 3. Desastres que ocasionem perdas de dados

Ativação do DRP	Cenário
Definição de Desastre	Falhas com ou sem interação humana, que ocasione perda ou modificação de dados
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Não
Quem deve ser informado	Responsável por setores que fazem uso dos dados afetados.
Prazo Estimado para Reestabelecimento das atividades	30 minutos

A tabela 4, cobre desastres ocasionados por falhas humanas ou não, mas que diferentemente da tabela anterior, essa é para desastres que ocasione defeitos ligados ao *hardware*.

Table 4. Desastres que ocasionem defeito com *hardware*

Ativação do DRP	Cenário
Definição de Desastre	Falhas com ou sem interação humana, que ocasione defeito ligado ao *hardware*
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Sim
Responsável pelas Aquisições	Responsável pelo comercial (ou outra pessoa que possua essa função e contato com fornecedores)
Quem deve ser informado	Responsável por setores que fazem uso dos sistemas, caso acarrete em uma paralisação dos mesmos
Prazo Estimado para Reestabelecimento das atividades	4 horas

A tabela 5, busca cobrir desastres ocasionados por forças tanto naturais quanto criminais, e que comprometa a infraestrutura computacional.

Table 5. Desastres que comprometam a infraestrutura computacional

Ativação do DRP	Cenário
Definição de Desastre	Desastres naturais ou criminosos que comprometam a infraestrutura computacional
Responsável Técnico	Responsável pelo TI da empresa
Requer Aquisição de Equipamento	Sim
Responsável pelas Aquisições	Responsável pelo comercial (ou outra pessoa que possua essa função e contato com fornecedores)
Quem deve ser informado	Responsável por setores que fazem uso do sistema ou dos dados afetados, além da diretoria da empresa
Prazo Estimado para Reestabelecimento das atividades	8 horas

Como citado por Fernandes (2014), deve-se fazer uma análise de impacto para conseguir identificar os sistemas mais cruciais e os menos cruciais. A análise de impacto desse trabalho que cobriria a terceira etapa do plano, baseou-se em uma empresa real, que o autor do mesmo está empregado, neste contexto descrita como empresa A, para não expor a mesma neste cenário. Esta empresa faz uso de diversos tipos de sistemas, dentre eles um *software* de Planejamento de Recursos Empresariais, do inglês *Enterprise Resource Planning* (ERP) e um *software* de solicitação de chamados, que contém funções semelhantes ao Akaunting e ao *osTicket* instalados no servidor do cenário criado. Analisando o impacto que esses dois *softwares* em específicos têm dentro da empresa A, foi notório que os dados do ERP são considerados mais importantes, e em caso de perda de dados, existe um grande impacto

negativo para a organização. Por esse motivo seus dados são tratados com mais cuidado, visto que os *backups* do ERP são feitos mais de 2 vezes por dia, enquanto o *software* de solicitação de chamados possui o *backup* de seus dados feito apenas 1 vez por dia. Diante disso o trabalho irá seguir essa hierarquia de criticidade.

Tendo definido a criticidade de um sistema sobre o outro, foi criado os parâmetros RTO e RPO para cada sistema. Assim foi definido que o *software* Akaunting terá um RTO de 8 horas e um RPO de 6 horas, ou seja, o tempo máximo de inatividade tolerado é de 8 horas e a quantidade de dados tolerada para ser perdida no caso de um desastre, são 6 horas. Já o *osTicket* foi definido com um RTO de 14 horas e um RPO de 12 horas, sendo assim é tolerado a inatividade do mesmo por 14 horas e uma quantidade de dados a serem perdidas de até 12 horas de informações antecedentes ao desastre (tabela 6).

Table 6. RTO e RPO definido

	RTO	*RPO*
Akaunting	8 horas	6 horas
osTicket	14 horas	12 horas

Posteriormente foi criado as estratégias que buscam cobrir a quarta etapa do plano, elaborando as regras para os *backups* e restauração do ambiente. O *backup* da máquina virtual completa será realizado manualmente uma vez por semana, toda sexta-feira depois do fechamento da empresa. Exclusivamente esse *backup*, será armazenado na máquina que hospeda a máquina virtual, além de arquivar uma cópia da mesma na máquina de contingência. Como o *backup* da máquina virtual será realizado uma vez por semana, se faz necessário obter outras estratégias para manter a salvo os dados nesses intervalos. Para isso, foram elaborados alguns *scripts* com o intuito de realizar os *backups* de forma automática, para que não haja necessidade de executar todos os *backups* manualmente no horário correto, e assim não correr o risco de algum desses ser esquecido ou ser feito em outro horário por algum motivo.

O *backup* do banco de dados do Akaunting será realizado de forma *full* quatro vezes ao dia, em uma delas, no horário considerado de almoço que é 12:15 horas, outro no horário após o fechamento da mesma, que seria 18:15 horas, e duas vezes durante a noite/madrugada, para evitar de perder algum dado que por ventura venha a ser alterado ou adicionado por algum funcionário que excedeu seu horário de trabalho, esses *backups* serão realizados as 00:15 e as 6:15 horas. Desse modo, foi criado uma tarefa no agendador do *Windows*, que executará o *script* responsável por esse *backup* a cada 6 horas, salvando-o na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário. Antes de definir a escolha de qual local de armazenamento seria considerado o principal e qual seria o secundário, foram realizados diversos testes, colocando arquivos de diversos tamanhos e acompanhando a sincronização das duas nuvens simultaneamente, e foi observado que ambas faziam o *upload* do arquivo com tempos realmente muito próximos. Portanto a escolha do Google *Drive* como armazenamento principal, foi opção pessoal do acadêmico, por sua maior familiarização com a plataforma e pôr a mesma oferecer 15 GB de armazenamento gratuito, contra 5 GB disponibilizado pelo *OneDrive*.

O *backup* do banco de dados do *osTicket* será realizado de forma *full* duas vezes ao dia, o primeiro, meia hora após iniciar o *backup* do Akauting que é realizado no horário do almoço, que nesse caso coloca esse *backup* do *osTicket* para as 12:45 horas. O segundo *backup* será realizado 12 horas depois do primeiro, e após a empresa ter encerrado o expediente, assim fixando o horário para as 00:45 horas. Desse modo, foi criado uma tarefa no agendador do *Windows*, para executar o *script* a cada 12 horas, salvando o *backup* na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário.

A estratégia mencionada acima, busca alcançar uma garantia de obtenção do RPO estipulado para cada sistema. Porém visando garantir o também cumprimento do RTO dos sistemas, foi elaborado *scripts* que façam a sua devida compactação no formato ZIP e os *backups* de forma automática das duas aplicações da empresa, para que se tenha pré-preparada uma recuperação que estabeleça o sistema com o máximo possível de atualizações que haviam sido aplicadas nos mesmos. Esses *backups* serão realizados semanalmente, as 12:00 horas de sábado, salvando-os na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário.

Tendo em vista uma possível instalação de algum novo programa necessário para a usabilidade dos sistemas da empresa, foi criado uma pasta com o seguinte nome: *instaladores_padrao*. Nessa pasta deve-se colocar todos os instaladores dos programas que forem necessários para o bom funcionamento do servidor e dos sistemas. Para efetuar o *backup* da mesma foi criado um *script* que faça a compactação no formato ZIP e efetue o *backup* dos mesmos. Esse *backup* será realizado semanalmente, as 13:00 horas de domingo, salvando-os na pasta do Google *Drive* como armazenamento principal e na pasta do *OneDrive* como armazenamento secundário.

Os *backups* são realizados por *scripts* com o formato *bat*, e esses podem sofrer alterações caso algum caminho ou nome de arquivo mude, ou até mesmo novos sejam criados. Para garantir que nenhum desses arquivos responsáveis pelos *backups* automáticos sejam perdidos, foi criado uma tarefa no agendador do *Windows*, e esta executará um *script,* a fim de realizar a compactação e *backup* de todos os arquivos de scripts da pasta onde os mesmos encontram-se. Essa tarefa será executada diariamente as 22:00 horas, e seguirá o mesmo padrão de todas as outras, armazenando o *backup* no Google *Drive* como local principal e no *OneDrive* como local secundário.

Por fim foi elaborado um *script* que exclua de ambos locais de armazenamento, os arquivos que possuam as extensões ZIP e SQL e estejam a mais de 15 dias nas pastas de sincronização. Esse *script* foi colocado para ser executado pelo agendador de tarefas do *Windows* a cada 15 dias, as 04:00 horas. O intuito do mesmo, é auxiliar para que não haja mais dados ocupando espaço na nuvem, do que o necessário.

Como nesse cenário os *backups* de sistemas, programas e dados são realizados em nuvem, e possuem seu caminho definido com sua devida estrutura de pastas, É necessário que ao criar um novo servidor desde a instalação do sistema operacional, deve-se sempre respeitar a estrutura e nome da máquina e das pastas, para que não se tenha problemas na realização dos *backups* automáticos.

Para a recuperação do ambiente, deve ser analisado qual desastre que afetou o mesmo. Cada categoria de desastre possui um responsável técnico, responsável de aquisição de bens, pessoas que deveram ser informadas, prazo para reestabelecimento das atividades e um impacto diferente no ambiente, portanto irá ser recuperado de maneira especifica.

Desastres conforme a tabela 2 que são causados por atualização de software, a recuperação é feita através do *download* e restauração do último *backup* feito na nuvem do sistema afetado, ou no caso de o problema estiver no sistema operacional, resolve-se importando o último *backup* da máquina virtual ou até mesmo fazendo a formatação da máquina em questão, e reinstalando os *softwares* por meio dos seus devidos *backups*.

Em desastres conforme a tabela 3, que se refere a desastres que ocasionem perda de dados, a recuperação é feita através do *download* e restauração do último *backup* feito desses dados, e a importação do arquivo no devido banco de dados afetado.

Para desastres de acordo com a tabela 4 que se refere a desastres que ocasionem defeito com *hardware*, a empresa nesse cenário deve possuir *hardwares* de contingência para que nesses casos que haja a necessidade de substituição do *hardware*, o mesmo seja trocado, e a partir desse ponto verificar se algum *software* também foi afetado, para que seja feito o *download* do devido *backup* para recuperação. Em desastres assim, haverá a necessidade de aquisição de um novo *hardware* do mesmo modelo do substituído ou superior para suprir o estoque de contingência, por esse motivo o inventário de *hardware* e *software* deve ser atualizado.

Em desastres como o da tabela 5 que são desastres que comprometam a infraestrutura computacional, dependendo da gravidade, a recuperação tende a ser mais demorada caso afete muitos *hardwares* do ambiente. Nesses casos os *hardwares* devem ser substituídos por aqueles que estão no estoque de contingência e deve-se recuperar sistemas e dados com o *backup* mais atualizado disponível na nuvem para *download*. É necessário que o responsável técnico solicite ao responsável pelas compras de TI, uma nova aquisição para repor o estoque dos itens afetados, já que nesse momento a empresa estaria funcionando com os *hardwares* de contingência. Caso os equipamentos de contingência também venham a ser afetados pela severidade do desastre, o responsável técnico deve repassar ao responsável por aquisição de equipamentos, uma lista com todos os *hardwares* que estão sem reposição, para que seja adquirido os mesmos com o devido fornecedor no menor tempo possível. E assim que a nova máquina estiver pronta, deve-se instalar a nova máquina virtual com o mesmo nome e configuração da anterior, e baixar os últimos *backups* dos sistemas e bases, para que a empresa restabeleça suas atividades. Dando sempre prioridade para ao sistema com menor RTO definido.

Depois de desenvolvido o DRP, inicia-se a fase de testes, constituindo a quinta etapa do plano, que busca verificar se o plano está de acordo com a sua proposta, trazendo a devida segurança na recuperação do ambiente criado. Durante a fase de testes, podem haver sugestões de manutenção do plano, dependendo dos resultados obtidos nessa etapa. Essas manutenções buscam manter o plano sempre atualizado e funcional.

5.3. Testes

Para a realização dos testes, foi utilizado o procedimento passo a passo, simulando a ocorrência de um evento para cada uma das quatro tabelas de desastres criadas no DRP, e uma simulando a perca total de ambos os hardwares, tanto de produção quanto o de contingência. Esses testes tem o intuito de verificar se o DRP elaborado está de fato trazendo a segurança desejada para os dados do ambiente criado.

O primeiro teste foi simulando uma atualização de *software* malsucedida no sistema de suporte ao cliente, que no cenário criado está instalado com sua versão 1.12. Para tentar causar o problema foi feito *download* do *osTicket*, porém de uma versão mais antiga, nesse caso a 1.10.1, e foi substituído a pasta ‘upload’ da versão instalada pela pasta de mesmo nome da antiga versão, pasta essa que possui arquivos de configuração. Após isso não foi mais possível acessar o sistema.

Para a correção do problema, foi restaurado o último *backup* realizado do sistema *osTicket* que estava armazenado em nuvem. Portanto o arquivo compactado foi extraído e substituído pela pasta da aplicação inteira que estava com problema. Feito isso a aplicação voltou a funcionar normalmente.

O segundo teste foi simulando uma falha que ocasionasse perda de dados, que nesse teste foi ocasionado por uma falha humana. Para realização desse teste, foi efetuado diversos comandos no banco de dados do programa Akaunting, ‘*updates*’ sem nenhuma cláusula do tipo

‘*where*’, inclusive na tabela de itens do mesmo. Além disso foi efetuado o comando do tipo ‘*drop table*’ na tabela de usuários. Com todas essas alterações por erro humano, além de diversos dados terem perdido sua autenticidade, não foi mais possível acessar o sistema, devido a não existir mais a tabela de usuários.

Com o intuito de recuperar os dados do sistema, foi restaurado o último *backup* do banco de dados do Akaunting que estava armazenado em nuvem. Importando assim o arquivo no phpMyAdmin para a base de dados do sistema. Após a importação com sucesso dos dados, foi possível acessar o *software* e verificar se os dados afetados estavam recuperados conforme anteriormente ao desastre.

O terceiro teste foi simulando uma falha devido a problemas no *hardware*, dessa vez uma falha que não foi causada por interação humana. Nesse caso foi simulado que o problema ocorreu com a memória da máquina *host*, que nesse cenário seria o *notebook*. O mesmo foi desligado completamente de forma repentina e efetuado a troca da memória que estaria afetada. Após a troca, foram ligados o *notebook* e a máquina virtual, e foi verificado se algum sistema ou banco foi afetado com essa queda repentina. Caso algum sistema ou dado tivesse sido afetado, seria necessário fazer a recuperação do mesmo. Porém nos 3 testes feitos simulando esse mesmo desastre, nenhum *software* ou dado foi afetado. Depois de constatado que ambos estavam funcionando corretamente, o inventario é atualizado, para que o responsável pela aquisição de equipamentos possa repor o *hardware* utilizado.

O quarto teste foi simulando um desastre que comprometesse a infraestrutura do cenário criado. Nessa ocasião foi simulado uma queda devida a algum problema elétrico que acarretasse a queima dos equipamentos em produção, roteador e a máquina *host*, que seria o *notebook*. Para isso o notebook e o roteador foram desligados repentinamente.

Sem os equipamentos de produção funcionando, foi substituído o roteador danificado pelo reserva, e ativado a máquina de contingência. Com a máquina reserva ligada, foi importado no VirtualBox da mesma o último *backup* realizado da máquina virtual. A partir dessa recuperação, foi feito *download* do último *backup* do banco de dados do *osTicket* e Akaunting, levando em consideração que após o último *backup* da máquina virtual, alguns dados da base desses sistemas poderiam ter sofrido alguma alteração, assim fazendo-se necessário a recuperação dos *backups* desses dados. Após a recuperação dos sistemas e constatação que ambos estavam funcionando em produção no *host* de contingência, iniciou-se o que seria o levantamento dos *hardwares* afetados. Esse levantamento possui o intuito de atualizar a tabela de inventario de *hardware* e *software*, para que fosse encaminhado ao responsável pelas compras de equipamentos, e o mesmo possa realizar as devidas aquisições.

Por fim foi simulado um desastre que comprometesse não somente os equipamentos em produção, mas também o de contingência. Após a reposição dos equipamentos afetados, tanto os principais quanto os de contingência já adquiridos pelo responsável das compras. A máquina *host* principal foi devidamente instalada, e se fez necessário instalar o servidor virtual desde o início, já que o *backup* da máquina virtual completa era armazenado nas máquinas físicas atingidas pelo desastre. A nova máquina virtual criada, seguiu as mesmas configurações relatadas nesse trabalho anteriormente, além de ser criada com o mesmo nome padrão da anterior.

Com a máquina virtual devidamente instalada, foi feito *download* do último *backup* realizado dos programas padrões, e assim instalado cada um desses, além de já entrar nas contas do Google *Drive* e *OneDrive* nos seus respectivos sincronizadores. Depois foi feito *download* do último *backup* realizado do *software* Akaunting e sua base de dados, já que esse *software* possui um menor RTO, portanto sua prioridade é maior. A pasta do *software* Akaunting baixada foi colocada na devida pasta do Xampp, e no phpMyAdmin foi criado uma nova base de dados

com o mesmo nome utilizado na máquina anterior, e o arquivo da base do Akaunting baixado foi importado para essa base de dados. Após isso foi verificado que o Akaunting voltou a funcionar normalmente. O próximo passo foi fazer *download* do último *backup* realizado do *software osTicket* e sua base de dados. A pasta do *software osTicket* baixada foi colocada na devida pasta do Xampp, e no phpMyAdmin foi criado uma nova base de dados com o mesmo nome da que era utilizada na máquina anterior para esse *software*, e o arquivo da base do osTicket baixado foi importado para essa base de dados. Feito isso foi constatado que o *osTicket* voltou a funcionar normalmente, e com sua base de dados devidamente restaurada.

Com os dois sistemas da empresa funcionando devidamente em produção, restou apenas realizar as configurações para que os *backups* automáticos voltassem a funcionar nessa nova máquina. Para isso foi feito *download* do último *backup* realizado dos *scripts*, e a partir daí os mesmos foram colocados na pasta padrão desses *scripts* e novas tarefas para a execução dos mesmos foram criadas no agendador do *Windows*, seguindo as instruções e horários estabelecidos no DRP.

6. Resultados e Discussões

A partir do levantamento bibliográfico, foi possível ter um entendimento geral do conceito, importância e de como elaborar um *Disaster Recovery Plan*. E esse conhecimento adquirido foi essencial para o desenvolvimento de todo o trabalho, desde a criação do ambiente computacional até a fase de testes.

Ao iniciar a projeção e criação do cenário, encontrou-se desafios, pois foi necessário adquirir mais conhecimento sobre máquinas virtuais para conseguir criar o servidor virtual. Outro desafio foi a instalação e configuração do *osTicket*, foi aplicado muito tempo de pesquisa, pois as primeiras versões que foi tentado instalar, são se teve sucesso em fazê-lo funcionar.

Quando os *softwares* foram enfim instalados corretamente, foi necessário abastecer os sistemas com dados. Para que os dados fossem inseridos de maneira funcional, foi aplicado conhecimentos que foram adquiridos ao longo da vida profissional do acadêmico. Buscou-se inserir as informações de maneira que se aproximasse de informações reais empresariais.

Com o ambiente devidamente pronto, foi criado um DRP que buscasse corresponder à altura do mesmo. O plano abrangeu as especificações encontradas nos materiais utilizados no levantamento bibliográfico. Contendo regras para os *backups* de cada sistema e dados do ambiente, tempo previsto de recuperação e ações a serem tomadas pelos envolvidos após a ocorrência de cada tipo de desastre especificado.

A fase de testes, envolveu simulações de desastres no ambiente com a pretensão de serem o mais próximas possíveis de um cenário real. Foram feitos cinco testes com desastres de diferentes tipos. Em todos os desastres simulados, a recuperação dos sistemas e dados foram feitas com êxito, com um tempo abaixo do que era previsto para restabelecimento das atividades do determinado desastre, e cumprindo com sucesso o RTO e RPO estipulados para cada sistema da empresa.

Buscando esses resultados positivos, e obter um aperfeiçoamento do modelo de *backup* do DRP utilizado no trabalho de Ávila, Soldan e Petroli Neto (2017), que era feito manualmente, foi elaborado para que nesse cenário criado os *backups* fossem realizados de forma automatizada. Para conseguir fazer isso, foi necessário estudar maneiras de gerá-los automaticamente. A forma escolhida foi através de scripts do tipo *bat*, que foram criados para serem adicionados como tarefas no agendador do *Windows*, e assim fazendo o que foram programados para realizar, de maneira automática. O resultado de automatização foi bastante satisfatório, pois cumpriu com o desejado, que era realizar os *backups* de todos os sistemas e

dados, além de a própria limpeza dos dados antigos na nuvem, sem haver a necessidade de interação direta humana.

No momento de elaborar uma forma satisfatória de realizar os *backups* em nuvem, foi analisado o tempo que demoraria para fazer *upload* dos mesmos, com o pacote de dados disponível para o ambiente. Cada *backup* de sistema e dados, possuiu um tempo de sincronização considerado aceitável, tempo esse sempre menor que 15 minutos nos testes realizados. No entanto, na tentativa de armazenar o *backup* da máquina virtual inteira em nuvem, a previsão de sincronização apresentadas por ambas as nuvens, foi de quase 40 horas. Por esse motivo optou-se por armazenar os *backups* da máquina virtual somente na máquina *host* e com uma cópia na do estoque de contingência. Porém, em um desastre que afetasse ambos os ambientes, o *backup* armazenado nas mesmas poderia ser perdido. Por esse motivo foi revisto as regas do *backup* criado, para que fosse possível elaborar de uma maneira que tudo o que fosse necessário para a recuperação do ambiente estivesse salvo em nuvem.

Com todos os *softwares* e dados necessários para recriar a máquina salvos em nuvem, foi possível fazer a restauração geral da máquina virtual e deixar o ambiente totalmente recuperado, sem ter o *backup* completo da mesma. Fazendo somente uma nova instalação de uma máquina virtual *Windows*, seguindo as mesmas especificações e nomes da anterior, e com a mesma criada, fazer a recuperação dos programas e dados já devidamente armazenados em nuvem. Sendo assim, todo esse processo, mesmo sem o *backup* da máquina virtual completa, foi realizado dentro do prazo previsto e ainda cumprindo com uma certa folga o RTO e RPO estabelecidos.

7. Conclusão

O presente trabalho se constituiu na elaboração e testes de um *Disaster Recovery Plan* para um ambiente empresarial criado, efetuando seu *backup* em nuvem. Durante a criação do cenário e elaboração do plano, se encontrou algumas dificuldades conforme relatado no capitulo de resultados e discussões, mas todas essas foram resolvidas à medida que os conhecimentos foram aprofundados.

O estudo atingiu seus objetivos através dos materiais obtidos no levantamento bibliográfico, e colocando em pratica no ambiente criado o conhecimento adquirido com os mesmos.

A aplicação do *Disaster Recovery Plan* no ambiente simulado, se mostrou bastante eficiente e cumpriu com as expectativas depositadas no mesmo. Visto que em todos os testes efetuados foi possível realizar as recuperações em um tempo menor que o previsto no plano.

Com base nos resultados expressados neste trabalho, que teve como objetivo geral elaborar um estudo sobre a construção e aplicação de um *Disaster Recovery Plan*, utilizando a computação em nuvem como local de armazenamento dos *backups* de empresas de pequeno ou médio porte. Pode-se concluir que para obter sucesso na aplicação de um DRP, a elaboração do mesmo deve ser trabalhada em conjunto com o cenário da empresa em que o mesmo será aplicado. Visto que cada empresa tem suas particularidades, orçamento, horários e equipamentos, portanto o DRP deve ser adequado para atender as expectativas e necessidades da mesma.

No entanto é importante ressaltar que a partir dos testes, ficou claro que a qualidade do pacote de dados da empresa é essencial para se conseguir obter uma boa eficiência ao se aplicar um *Disaster Recovery Plan* em nuvem. Visto que a qualidade desse pacote de dados possui influência no tempo de *backup* e restauração dos dados empresariais.

Como sugestão para trabalhos futuros seguindo essa mesma base, sugere-se a aplicação de um DRP utilizando alguma infraestrutura em nuvem como estoque de contingência, e analisar as dificuldades e soluções de aplicar essa pratica. Como também elaborar um DRP com estratégias de *backup* utilizando algum *software* de *backup* gratuito que possua maiores funcionalidades, e possibilidade de fazê-los de forma incremental e diferencial, para que se possa verificar as vantagens e desvantagens de utilizar um *software* de *backup* pronto.

Referências

AGUIAR JUNIOR, Ubirajara Ferreira de. **PLANO DE RECUPERAÇÃO DE DESASTRES: UMA PESQUISA-AÇÃO EM EMPRESA DO SETOR ENERGÉTICO.** 2012. 42 f. TCC (Graduação) - Curso de Engenharia Mecânica, Universidade Estadual Paulista, Guaratinguetá, 2012. Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/117957/aguiarjunior_uf_tcc_guara.pdf?sequence=1&isAllowed=y. Acesso em: 25 set. 2018.

ALHAZMI, Omar H.; MALAIYA, Yashwant K.. Evaluating disaster recovery plans using the cloud. **2013 Proceedings Annual Reliability And Maintainability Symposium (rams)**, Orlando, p.1-6, jan. 2013. Disponível em: https://ieeexplore.ieee.org/document/6517700. Acesso em: 28 set. 2018.

ALLES, Guilherme Rezende. **Análise da utilização de tecnologias de contêineres para aplicações de alto desempenho.** 2018. 59 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/175014/001065151.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2019.

ANDRADE, Daniel*. et al*. **PLANO DE CONTINGÊNCIA DE TI: PREPARANDO SUA EMPRESA PARA REAGIR A DESASTRES E MANTER A CONTINUIDADE DO**

NEGÓCIO. 2011. 14 f. Monografia (Especialização) - Curso de Segurança da

Informação, Senac, Brasília, 2011.

ÁVILA, Cleiton Silva de; SOLDAN, Evandro Luis; PETROLI NETO, Silvio. A SEGURANÇA DE UMA ESTRUTURA DE DISASTER RECOVERY PLAN EM CLOUD COMPUTING. **Ensaios Usf**, Bragança Paulista, v. 1, n. 1, p.103-116, 2017. Disponível em: http://ensaios.usf.edu.br/ensaios/article/view/61. Acesso em: 09 ago. 2018.

BAZZOTTI, Cristiane; GARCIA, Elias. **A importância do sistema de informação gerencial para tomada de decisões.** Disponível em: http://www.waltenomartins.com.br/sig_texto02.pdf. Acesso em: 12 de Ago. 2018.

FARIA, Heitor Medrado de. **Bacula: Ferramenta Livre de Backup.** Brasport, 2010.

FURLAN, Marcos da Silva; ASSIS, Naziro Hamed de. **Backup: Proteção e segurança de dados e informações em ambientes corporativos.** 2015. 54 f. Monografia (Especialização) - Curso de Pós-graduação em Infraestrutura de Redes de Computadores, Fundação de Assistência e Educação - Faesa, Vitória, 2015. Disponível em: https://docplayer.com.br/20019367-Backup-protecao-e-seguranca-de-dados-e-informacoes-em-ambientes-corporativos.html.Acesso em: 09 ago. 2018.

LUDESCHER, W.; CUGNASCA, P.S. A model for evaluating the reliability of computational systems disaster recovery plans. **Risk, Reliability And Societal Safety.** London, p. 2371-2376. 2007. Disponível em: https://docplayer.net/8982352-A-model-for-evaluating-the-reliability-of-computational-systems-disaster-recovery-plans.html. Acesso em: 09 out. 2018.

MELL, Peter M.; GRANCE, Timothy. **The NIST Definition of Cloud Computing.** 2011. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Acesso em: 12 set. 2018.

NIST. **NIST Cloud Computing Program - NCCP.** 2010. Disponível em: https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp. Acesso em: 01 jul. 2019.

PEREIRA JUNIOR, Jorge Hosni Pereira de. **Plano de continuidade de negócios aplicado à segurança da informação.** 2008. 60 f. Monografia (Especialização) - Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/15974/000695265.pdf. Acesso em: 04 out. 2018.

PINTA, Jan. Disaster Recovery Planning as part of Business Continuity Management. **Agris on-line Papers in Economics and Informatics.** Prague, p. 55-61. 2011. Disponível em: http://ageconsearch.umn.edu/record/120243/files/agris_on-line_2011_4_pinta.pdf. Acesso em: 27 set. 2018.

PRAZERES, Antero José Maia. **Continuidade de Negócio, Disaster Recovery e estratégias de implementação na Santa Casa da Misericórdia de Lisboa.** 2012. 99 f. Dissertação (Mestrado) - Curso de Desenvolvimento de Software e Sistemas Interactivos, Instituto Politécnico de Castelo Branco, Castelo Branco, 2012. Disponível em: https://repositorio.ipcb.pt/bitstream/10400.11/1472/1/disserta%C3%A7%C3%A3o.pdf. Acesso em: 15 mai. 2017.

RODRIGUES, Wilson Flávio. **ANÁLISE DOS PROCEDIMENTOS DE BACKUP DOS INSTITUTOS FEDERAIS.** 2017. 140 f. Dissertação (Mestrado) - Curso de Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2017. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/25612/1/DISSERTA%C3%87%C3%83O%20Wilson%20Fl%C3%A1vio%20Rodrigues.pdf. Acesso em: 13 nov. 2018.

SILVA, Rhenann Granado Cottar Marçal. CLOUD COMPUTING E GRID COMPUTING: UM ESTUDO DE CASO. **Revista Eletrônica de Computação**, Londrina, v. 1, n. 1, p.2-12, jan./jun. 2013. Disponível em: http://www.unifil.br/portal/images/pdf/documentos/revistas/revista-eletronica/computacao/computacao-2013.pdf. Acesso em: 10 set. 2018.

TAURION, Cezar. **Cloud computing: computação em nuvem: transformando o mundo da tecnologia da informação.** Rio de Janeiro: Brasport, 2009.

WESTCON, Equipe. **O que é um plano de recuperação de desastres**. Disponível em: http://microsoft.westcon.com/?/post/141/o-que-e-um-plano-de-recuperacao-de-desastres/. Acesso em: 15 Ago. 2018.