IMPLANTAÇÃO DE PROCESSO PARA GARANTIR A RECUPERAÇÃO DOS PRINCIPAIS DADOS E SISTEMAS DE UMA PME BRASILEIRA APÓS UM DESASTRE, MINIMIZANDO *DOWNTIME* E PERDA DE DADOS.[1]

Maurício Bento Ghem

Resumo: Vivemos em um país onde a vasta maioria das pequenas e médias empresas estão conectadas à internet, e usam a tecnologia para agregar em seus negócios. Independente do tamanho da empresa, as informações digitais são ativos primordiais para seu funcionamento, mas que muitas vezes são ignorados. Este trabalho tem como objetivo aperfeiçoar um processo de backup e recuperação já existente para que seja possível garantir a recuperação dos principais dados de sistemas, minimizando a perda de tempos e a indisponibilidade. Baseando-se nas referências bibliográficas e em uma pesquisa empírica aplicada, foi possível estabelecer um novo processo de backup e recuperação compatível com baixo custo para PMEs, utilizando o modelo de recuperação *pilot light*, backup *image-based* em nuvem e recuperação completa de servidor.

Palavras-chave: Backup em Nuvem, Cópia de Segurança, Recuperação de Desastres.

1 INTRODUÇÃO

Hoje em dia, as pequenas e médias empresas (PMEs) do Brasil não usam mais apenas o papel para armazenar sua informação. Pela facilidade e para acompanhar o avanço tecnológico, as PMEs se informatizaram, isso quer dizer que também os seus dados passaram de analógico para digital.

Antigamente, para evitar o acesso não-autorizado aos dados sigilosos da empresa, era necessário bloquear o acesso à uma sala de arquivos, onde muitos documentos físicos lá se encontravam. Essa não é a realidade nos dias de hoje, onde mais de 76% das PMEs brasileiras estão conectadas à internet, segundo (IBGE, 2010). Deste modo, torna-se necessária uma proteção digital para os dados, ou *backup*.

Muitas das funções do setor de Tecnologia da Informação (TI) de uma empresa é minimizar os riscos, reduzir os custos e melhorar a performance dos serviços. Esse é o principal objetivo de qualquer estratégia de *backup* e proteção de dados a ser implementada (PRESTON, 2007).

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão da Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão da Segurança da Informação.

Segundo Preston (2007), não importa se você consegue fazer um *backup,* e sim se é possível restaurá-lo. Porém se a restauração não for feita em tempo hábil (ex.: não adianta levar dias para retomar a operação de uma clínica médica) que não se recupere os dados (ex.: recuperar o trabalho feito até minutos antes do momento de um desastre), de nada serve a estratégia de *backup e* proteção de dados.

Este trabalho teve como motivação implantar um processo que vai além da simples proteção de dados, para que seja possível garantir a recuperação de dados e sistemas a ser implantado em uma PME brasileira. O autor Faria (2014) descreve que "garantir" a recuperação de dados, significa atender à dois requisitos de uma empresa: atender ao tempo de recuperação – do inglês *Recovery Time Objective* (RTO) - e ao ponto de recuperação - *Recovery Point Object (RPO)*.

Não basta uma simples estratégia de proteção de dados para atender à estes requisitos, por isso este presente trabalho teve como objetivo construir e implantar um processo completo para proteger e garantir a recuperação dos dados de PMEs brasileiras. Mais especificamente, o objetivo deste trabalho foi implantar um processo para garantir a recuperação dos principais dados e sistemas de uma PME brasileira com o mínimo de *downtime* e nenhuma perda de dados.

Além disso, buscou-se: desenvolver um subprocesso para manter atualizado requisitos de RPO e RTO, lista dos dados e sistemas críticos, também importantes para a empresa; enumerar principais ameaças de perdas de dados atuais e verificar qual método de backup (*file-level* ou *image-based)* se adequa melhor aos requisitos de RPO e RTO em cada situação; construir subprocesso de testes para validar se o processo de recuperação de dados atende aos requisitos de RPO, RTO e de integridade de dados; identificar melhorias e seu impacto para reduzir o tempo de backup e recuperação sem comprometer a integridade de dados.

Para atingir estes objetivos, inicialmente, pensava-se em utilizar apenas a pesquisa empírica aplicada. Porém, além da pesquisa foi utilizado um processo existente de backup e recuperação como *baseline*, já seguido na empresa do autor. Este processo já existente foi aprimorado na presente pesquisa. A metodologia utilizada foi dividida em 4 macro etapas.

Na primeira etapa, foi efetuada uma coleta de dados através de pesquisa digital com clientes atuais e pequenas e médias empresas brasileiras com objetivo de construir conhecimento da atual situação e de suas expectativas com relação ao processo de recuperação dos principais dados e sistemas. Em outras palavras, foi elaborada uma pesquisa empírica para coletar dados de PMEs quanto a seu conhecimento, segurança e capacidade de recuperação de dados.

Na segunda etapa, foi analisado e computado estas informações para verificar qual é o ponto mais carente de trabalho a ser feito para ter um ganho real na expectativa do pequeno empresário.

A terceira etapa foi de construção de documentos que foram incluídos no processo de backup e recuperação *baseline,* já com a motivação de evoluí-lo dentro do objetivo do trabalho. Esta documentação serviu para evitar a perda de dados no backup por atualização de sistema e possível mudança de pastas.

Na quarta etapa, foi aplicado este novo processo em laboratório, para verificar se o novo processo poderia atender as requisitos de RPO e RTO definidos.

Na próxima seção, será apresentada a fundamentação teórica que possibilitou construir o presente trabalho. Cada um dos conceitos é explicado de acordo com o objetivo do trabalho.

Em seguida, é detalhado cada um dos itens descritos da metodologia, para então realizar as conclusões do trabalho descrevendo a melhoria do processo que foi além da simples proteção de dados, mas que fosse possível garantir a recuperação de dados e sistemas, para ser implantado em uma PME brasileira.

2 A TEORIA SOBRE BACKUP

Neste tópico serão abordados os conceitos teóricos que subsidiam o tema desse estudo. Inicialmente o conceito de *backup* dentro do universo da TI e o porque é importante realiza-lo. Em seguida, serão abordadas as métricas importantes em serem observadas tanto neste processo quanto no de recuperação, então será apresentado os tipos de backup e os destinos para o backup ser salvo. Por fim, o foco da fundamentação teórica passa a ser no processo de recuperação após um desastre. Portanto serão apresentados os diversos modelos de recuperação de desastres existentes, bem como seus prós e contras, e por fim desta seção, será apresentado o conceito de plano de recuperação de desastres e os itens essenciais que devem estar presentes, para que seja de total valia para uma PME.

Desastres são inevitáveis e em sua maior parte imprevisíveis, e variam em tipo e magnitude. A melhor estratégia é ter algum tipo de plano de recuperação de desastres em vigor, para retornar ao normal após a desastre aconteceu. Para uma empresa, um desastre significa interrupção abrupta de todo ou parte de operações comerciais, que podem resultar diretamente em perda de receita. Para minimizar as perdas por desastres, é muito importante ter um bom

plano de recuperação de desastre, um *disaster recovery* (DR) para cada subsistema de negócios e operação dentro de uma empresa (CISCO SYSTEMS INC, 2008).

A Cisco Systems Inc (2008) ainda destaca o ciclo de uma recuperação de desastres, que é: (a) operação normal; (b) desastre acontece; (c) operações afetadas; (d) DR recuperou as operações; (e) desastre resolvido; (f) processo de reconstituição; e volta a operação normal. É de suma importância compreender este processo, pois serão utilizadas métricas para medir especialmente os tempos de (b) até (d). Também, o autor destaca a importância que o plano DR deve sempre estar atualizado, incluindo novas tecnologias, e sugere que este documento deve ser auditado a cada trimestre.

Numa pequena ou média empresa, o recurso financeiro não é abundante e por isso, geralmente ela não se preocupa em antecipar o desastre de sua TI, e sim apenas em fazê-la funcionar. Neste contexto que entra um processo muito importante para o DR que é o ato de fazer *backup.*

Backup dentro do contexto de TI é o simples ato de copiar um dado de um lugar para o outro, geralmente em outro formato (PRESTON, 2007). Conforme a TI evoluiu, e houve um aumento crescente da informatização e o acesso à internet por parte das empresas (IBGE, 2010), aumentou a opção de soluções comerciais de backup, o que tornou a possibilidade de criar um plano de recuperação de desastres mais robusto.

Ainda segundo Preston (2007), um bom backup e um sistema de recuperação é essencial para empresas de qualquer tamanho. Infelizmente, seu departamento de Tecnologia da Informação (TI) geralmente não recebe a verba necessária. Na essência, backup segundo Priberam (2018), é a cópia que se destina a guardar dados armazenados no caso de uma eventual perda de informação, traduzido literalmente como: cópia de segurança. Os principais dados e informações de sistemas operacionais da empresa precisam ser incluídas no backup, para evitar o pior caso: a empresa ir a falência por perder dados de clientes, pedidos, histórico de pagamento e tudo que for importante.

Muitos são os problemas existentes no processo de backup e recuperação, porém dois problemas que motivam a realização deste trabalho, são (PRESTON, 2007):

1. Teste dos Backups: ele fala das inúmeras histórias que conheceu de administradores de TI experientes que deixaram apenas para testar que era possível recuperar os dados, no momento crítico – quando de fato houve uma falha imensa no departamento de TI e foi necessário recuperá-los. Ele comenta que não foram todos os casos que foi possível recuperar todos os dados sem

perdas e isso impactou financeiramente nas organizações, no pior dos casos fechando empresas.

2. Tempo de Recuperação: não adianta ter cópias dos arquivos se levam dias ou até semanas para recuperar os dados. Por isso, é muito importante se ter métricas e controle do RTO e do RPO.

Existem duas métricas importantíssimas no processo de DR, onde está incluído o *backup* de dados que se referem ao tempo de recuperação – do inglês *Recovery Time Objective* (RTO) - e ao ponto de recuperação - *Recovery Point Object (RPO)*.

Preston, 2007 vai mais a fundo e fala que o RTO é a medida do quão rápido se quer recuperar o sistema e que é uma medida que varia de zero segundos até muitos dias ou até semanas. Cada pedaço da informação faz parte de uma função no negócio, portanto a grande questão é: quanto tempo a empresa pode viver sem esta informação? Qual o impacto financeiro ficar sem esta informação? Portanto, o período entre a ocorrência do desastre e o tempo em que a aplicação, servidor ou atividades do negócio estão de volta no ar e rodando, na sua ordem devida, isso é definido como o objetivo de tempo de recuperação, ou do inglês *recovery time objective* (RTO) (YARRAPOTHU, 2015).

Além disso, Preston, 2007, também aborda o RPO e resume em quantos dados pode se dar o luxo a perder. Por exemplo, se ao perder os últimos 3 dias de trabalho, tem-se tem um RPO = 3 dias. Agora, numa pequena ou média empresa onde se tem pedidos de clientes todos os dias, provavelmente é necessário decidir que não pode perder nenhum deles, neste caso tem-se um RPO = 0 para esta aplicação. Logo, quando ocorre um desastre, o tempo que antecede a ocorrência do desastre no qual dados são perdidos, e essa perda é permitida, esse limite é definido como objetivo de ponto de recuperação, do inglês *recovery point objective* (RPO) (YARRAPOTHU, 2015).

Outras quatro métricas também importantes são:

- Idade do Backup: medida em dias, horas ou versões. A idade do backup também pode ser referenciada como política de retenção, e se refere ao período de tempo que a cópia do backup vai ser preservada (YARRAPOTHU, 2015).
- Tempo para fazer o backup: tempo levado para o backup ser executado e armazenado com sucesso.
- Tempo para recuperar o backup: tempo que leva para recuperar todos perdidos dados no servidor. Este tempo depende de variáveis como: velocidade da rede,

tamanho dos dados, tamanho da rede, necessidade de aquisição de novos equipamentos (WIBOONRATR, 2009).

- TCO: *Total Cost of Ownership* (TCO) é a estimativa financeira do plano de backup e de recuperação de desastre em uma empresa. Essa métrica inclui ambas despesas financeiras e operacionais para funcionar. As despesas financeiras referem-se aos custos em implantar uma rotina de backup e recuperação de desastres e a despesa operacional se refere ao custo em manter os equipamentos e serviços.

Para atender estas métricas, existem diversos tipos de backup, porém os mais aceitos e destacados, são o *file-based e device-based (*CHERVENAK ET AL, 2010).

O *file-based* entende apenas estrutura de pastas e arquivos. A grande diferença entre estes dois formatos de backup se dão porque os arquivos dentro do sistema operacional consistem de um agrupamento lógico de blocos. Estes blocos possuem um tamanho fixo que varia conforme sistemas operacionais, e cada um destes blocos lógicos representam um bloco físico no disco. Em outras palavras, um arquivo grande não necessariamente tem armazenado seus blocos físicos continuamente, pode estar um bloco no início do disco e outro no final. Para um volume grande de arquivos ou de dados, isso pode impactar na performance.

Em contraste, *(*CHERVENAK ET AL, 2010) o *device-based*, ou também referido como *image-based backup,* que ignora a estrutura de arquivos quando copia blocos de disco para a mídia de destino do backup. Isso aumenta a performance, porque o processo de cópia demanda menos operações de consulta à disco, e o faz de continuamente, bloco após bloco. Em contrapartida, dependendo de como a ferramenta de backup salva estas informações, para se recuperar apenas 1 arquivo, pode ser um processo lento. Esta abordagem é muito útil para recuperar um sistema inteiro, especialmente quando fazendo um backup local para ser recuperado num provedor de nuvem, como a Amazon Web Services.

Todo tipo de backup seja ele *file-based* ou *image-based*, precisa ser armazenado num destino de backup. Nesse contexto, o armazenamento de dados evoluiu bastante nos últimos anos. O que antes era feito com a Fita DAT, equipamento quase ultrapassado, agora começa a ser substituído pela nuvem. No entanto, existem destinos de backup que se tornam muito atrativos, como o HD externo pelo seu custo/GB. Porém sua economia, pode gerar uma perda de dados se for derrubado de uma mesa, ou estiver conectado no momento que pegar um vírus ou sofrer um sequestro de dados com *ransomware*.

Existem diversos destinos de backup aceitos na atualidade, porém como foi feito uma pesquisa empírica, o resultado revelou que apenas dois destinos eram amplamente utilizados. Por isso, esta seção foi limitado apenas a dois destinos, descritos a seguir.

O HD Externo ou pen drive é um destino bastante utilizado por pequenas e médias empresas por conta do custo baixo recorrente após a aquisição dos dispositivos. Associado a um software que faça a cópia, é possível ter automação no backup. Uma grande ameaça deste destino de backup é que existe a possibilidade de perda de dados, por conta de vírus, sequestro de dados, furto do HD ou mesmo queda no chão. Seu ponto positivo é que realizando backup em HD externo e seu backup estiver intacto, você consegue ter uma recuperação bastante rápida, pois estará com os dados dentro da empresa. Após testar 85,467 HDs (BACKBLAZE, 2007), concluiu-se que os HD que mais eram propensos a falhar eram os de 1TB 1,5TB e 3TB. Nota que estes HDs são os mais utilizados por conta do seu preço, o que torna comum seu uso.

A nuvem é um destino de backup que começou a se falar quando surgiu a AWS (Amazon Web Services) e em 2009, foram disponibilizados serviços no Brasil. Por armazenar os dados em blocos, permite evitar que de forma fácil *ransomwares* ou vírus possam manipular os arquivos. Assim, a possibilidade de se perder dados após se ter um processo de backup neste tipo de nuvem é praticamente zero. O ponto negativo é que depende do link de internet para fazer os backups e para recuperar os dados. Hoje, são 2,7 milhões de empresas que tem acesso à internet e precisam trocar informações (IBGE, 2012). Esta informação cresce ano após ano, e isso esta direcionando provedores de internet a aumentarem suas capacidades, para fornecer maiores links de acesso à rede. O backup na nuvem vem ajudando empresas a evitar perder dados, por mau uso de HDs externos, por isso este modelo será utilizado no presente trabalho.

3 A RECUPERAÇÃO DE DESASTRES

Para se atingir o objetivo de recuperar os dados e os sistemas após um desastre, é necessário ter todo o processo documentado, testado e validado. Mesmo que sejam feitas rotinas de backup para copiar os arquivos, esta já é uma forma eficaz de proteger os dados das empresas.

A seguir são apresentados os formatos de recuperação de desastres possíveis.

Segundo Dolgner (2017), para evoluir em seu plano de recuperação de desastres é necessário ter um ponto de partida e escalar este plano para cima. Por exemplo, é possível uma

empresa ter apenas o modelo de Apenas Backup e Recuperação, e evoluir para um *Pilot Ligh*t por necessidades do negócio.

Existem 4 modelos de recuperação de desastres em termos de complexidade e tempo: backup e recuperação, *pilot light*, *warm standby* e multi-site.

O modelos de recuperação de Backup e Recuperação (sem resiliência) é garantido apenas que caso queime um equipamento, pelo menos os dados do sistema estão protegidos, para voltar a funcionar. Talvez, não saibam nem a especificação ou fornecedores para compra do servidor, por isso constar essas informações no plano de recuperação de desastres é essencial. Para recuperar após um desastre no formato sem resiliência, em caso de uma pane é necessário formatar a máquina ou comprar uma máquina nova. Por isso, é deve-se tomar nota dos seguintes itens primordiais (CISCO SYSTEMS INC, 2008): contato de fornecedores, de técnicos e Suporte; especificação de hardware e software; e procedimento a seguir de compra, instalação e reativação.

No modelo *Pilot Light*, tem-se um servidor simplicado em espera permite ter um tempo de recuperação muito mais rápido que o de Backup e Recuperação porque as partes fundamentais necessárias para recuperar seu sistema já estão rodando, e estão sendo atualizadas periodicamente (DOLGNER, 2017). Ele ainda não é tão eficaz quanto o *warm standby*, porém já acelera a recuperação para a casa de dezenas de minutos. Este modelo possui a tendência de ser mais caro que o formato anterior, por conta de ter alguns recursos já provisionados todo tempo até acontecer um desastre. Porém, alia muito bem custo com tempo baixo de recuperação. Mesmo já provisionado, estes recursos podem estar com uma capacidade bastante reduzida, podendo na hora do desastre, ser ajustado o tamanho do recurso. Este formato utilizada a configuração de *failover* ativo/passivo.

O próximo modelo é o *Warm Standby,* onde tem-se um servidor completo em espera, e este modelo de recuperação de desastres é ainda mais rápido que o *Pilot Light*, porém perde apenas para o Multi-site em termos de velocidade de recuperação. Sua diferença entre o *Pilot Light* é que ao invés de ter apenas os itens essenciais do servidor disponível, possui uma versão completa do ambiente rodando, só que com uma capacidade reduzida. Como não possui apenas os elementos básicos, o custo para implantar este modelo de recuperação tende a ser mais alto. Da mesma forma que o cenário anterior, para este funcionar este cenário precisar ter uma replicação constante de dados, tanto da camada de banco de dados quanto de dados transientes. Este modelo utiliza o modelo ativo/passivo de configuração *failover*.

Por fim, o modelo Multi-site, tem-se uma cópia inteira do ambiente ao vivo. Este plano de recuperação de desastres é o mais caro, porém é o que proporciona maior velocidade de recuperação após um desastre. O Multi-site é uma cópia 1-pra-1 de toda infraestrutura localizada em um ambiente fora da empresa (na nuvem) e que está em execução a todo momento. O modelo de Multi-site utiliza a configuração de *failover* ativo/ativo, e por conta disso se torna o mais caro. Este modelo entrega o melhor RPO e RTO isso porque nenhum *downtime* é esperado e praticamente nenhuma perda de dados é experienciada (DOLGNER, 2017).

4 RESULTADOS DA PESQUISA

Na introdução, foi mencionado o processo de backup e recuperação *baseline*, que consiste em 4 passos: (a) descobrimento de dados essenciais a fazer backup; (b) instalação de agente para backup e recuperação; (c) monitoramento de cada backup; (d) construção de plano de recuperação de desastres. Este processo se mostra eficiente para novas ativações, porém possui algumas lacunas se ocorrem mudanças na infraestrutura ou nos sistemas.

A pesquisa foi feita através de um questionário, onde buscou-se a resposta de 100 pessoas de PME, nos cargos de sócio/dono, diretores e gestores nos estados da região sul e sudeste do Brasil. Esta pesquisa foi veiculada através de redes sociais através de um link, e ficou aberta para respostas do dia 16 a 20 de agosto de 2019. O objetivo da pesquisa era descobrir como o backup, sistemas e a perda de dados está presente nas organizações no ponto de vista dos usuários.

Ao analisar a pesquisa, a resposta das seguintes perguntas foram vitais para as melhorias descobertas para o processo *baseline*:

- O Sistema utilizado na empresa, recebe atualizações da empresa que o criou?

- Quando foi a última vez que foi instalado um sistema?

- Você usa quantos sistemas na empresa?

Percebeu-se na maioria das respostas da pesquisa que os sistemas recebem atualizações, que novos sistemas são instalados de em 1 a 3 meses e que a maioria das pessoas usa mais do que 2 sistemas. A conclusão após analisar estas respostas é que o processo *baseline* de backup e recuperação, na fase de descobrimento de dados essenciais para se fazer o backup, não pode ser feita apenas uma vez, e sim deve ser um processo contínuo de descobrimento constante. Além

disso, ao analisar a resposta da pergunta: “Você tem um departamento de informática dentro da empresa, ou é um terceiro que cuida”, foi percebido que 70% tem suporte de TI. Ou seja, possui um técnico, empresa externa ou funcionário do departamento de TI que presta suporte.

Portanto, a maneira encontrada para evoluir o processo *baseline* foi de elaborar um formulário de cadastro que vai ser disponibilizado na primeira etapa do processo, e que periodicamente (entre 3 a 6 meses) vai ser enviado novamente para buscar atualizações das informações técnicas, tais como:

- Nome do Sistema e versão:

- Banco de dados e versão:

- Pasta de arquivos do sistema:

- Pastas do banco de dados do sistema:

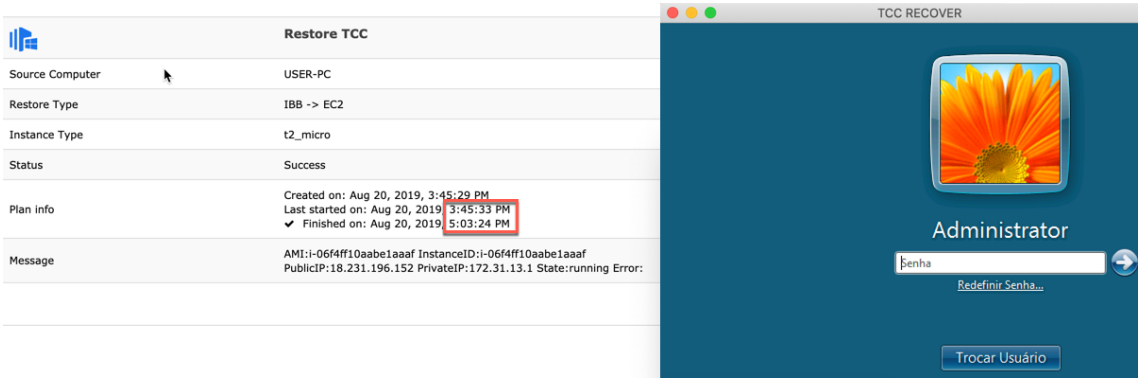
Este formulário e esta mudança proposta no processo pode parecer simples, mas parece ser uma solução definitiva para evitar perder dados ao longo do tempo, por causa de mudanças não reportadas. Portanto, após esta nova descoberta a sugestão para mudança do processo *baseline,* passa a ser: (a) descobrimento de dados essenciais a fazer backup/alinhamento para novos sistemas; (b) instalação de agente para backup e recuperação; (c) monitoramento de cada backup; (d) construção de plano de recuperação de desastres; e (e) alinhamento para novos sistemas;

Para validar esta adaptação no processo, foi feito a implementação em um cliente atual para verificar a etapa de alinhamento de novos sistemas, e verificar a aceitação e como vai funcionar a inclusão de um novo sistema, por parte do cliente.

Outra mudança feita no processo, foi que ao invés apenas de fazer o backup *file-based*, agora além deste está sendo feito o backup *image-based*, desta forma é possível prevenir a perda de dados, pois todo o servidor é salvo na nuvem, e não apenas algumas pastas. Esta mudança possibilita evitar perder dados antes não salvos, e também agora possibilita a recuperação em até 1 hora do servidor em nuvem, trabalho futuro a ser verificado numa próxima etapa. Assim, também é possível reduzir ainda mais o RTO, permitindo recuperar o servidor direto na nuvem com um custo baixo, utilizando a metodologia de recuperação *Pilot Light*.

Por fim, foi realizado um experimento de recuperação utilizando *software* WSpeed Backup com modelo *Pilot light*, simulando uma parada total do servidor do pseudo-cliente, e um servidor cuja imagem possuía 38,6GB de dados. O tempo total até recuperação em nuvem,

estar apto para funcionar e realizar o acesso remoto foi de apenas 78 minutos. Tendo em vista que 67% dos entrevistados falou que aceitaria esperar no mínimo 1 hora, este tempo está completamente dentro do esperado. Abaixo, é apresentada uma imagem da execução do plano de recuperação e tela de acesso do terminal:



5 CONCLUSÕES

O principal objetivo deste estudo foi implantar um processo que vai além da simples proteção de dados, mas que fosse possível garantir a recuperação de dados e sistemas a ser implantado em uma PME brasileira. Este processo precisava minimizar a perda de dados e reduzir ao máximo o tempo de parada de sistemas, fatos que se mostraram positivos após a conclusão da pesquisa.

O estudo apontou que o processo *baseline* de backup e recuperação era falho e iria causar perda de dados, após cruzar com as expectativas da amostragem de pesquisa. Seria necessário realizar ajustes, para que fosse possível reduzir o tempo de recuperação de sistemas. Também, a pesquisa apontou que a vasta maioria dos entrevistados usa 2 ou mais sistemas que recebem atualizações constantes, e que já foi perdido dados por conta de mudança de pastas de sistemas que não foi incluído no backup. E por isso, o ajuste no processo de backup de começar a adotar o *image-based* backup em conjunto com de uma evolução na comunicação, resolve esta possibilidade de perder dados.

Foi possível validar este novo processo em laboratório, e este novo processo se mostrou bastante eficaz, pois é possível ter um tempo fixo de RTO, o tempo de recuperação, quando se recuperando em nuvem. Desta forma, é possível prever as expectativas do negócio e ao passo que a equipe de TI interno do cliente comece os trabalhos para recuperação interno, é possível em pararelo ativar a recuperação em nuvem e continuar os trabalhos.

O benefício trazido pelos resultados obtidos com este trabalho são ipara organizações de pequeno e médio porte, afinal eles possuem pouca verba para investir com TI, e ao utilizar o

backup e recuperação do servidor em nuvem, é possível minimizar o tempo de parada da empresa e ainda assim prever o tempo que leva para retornar as operações. Assim, é possível preparar as equipes internas, e alinhar com terceiros e clientes de que mesmo numa parada é possível retornar os trabalhos em menos de 2 horas.

Vale ressaltar que para trabalhos futuros pode ser simulado testes de penetração, simulando ataques hackers, ou mesmo vírus para aí colocar à prova o plano de recuperação de desastres utilizando a recuperação em nuvem.

REFERÊNCIAS

PRESTON, Curtis W. **Backup & Recovery**. Estados Unidos: O'Reilly Media, 729 p. 2007**.**

FARIA, Heitor Medrado de. **Bacula: Ferramenta livre de backup** – 2.ed. - Rio de Janeiro: Brasport, 224 p. 2014.

KASPERSKY LAB. **KSN Report: Ransomware and malicious cryptominers 2016-2018**. Disponível em < https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf>. 2018. Acesso em Março/2019.

IBGE – Instituto Brasileiro de Geografia de Estatística. **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nas Empresas**. Disponível em < https://ww2.ibge.gov.br/home/estatistica/economia/tic_empresas/2010/default_xls_dados.shtm >. 2010. Acesso em Abril/2019.

CISCO SYSTEMS INC. **Disaster Recovery: Best Practices.** Disponível em < https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-453495.pdf>. 2008. Acesso em Abril/2019.

CHILDS, Donna R.; DIETRICH, Stefan. **Contingency Planning and Disaster Recovery: A Small Business Guide** – 2.ed. – Estados Unidos: John Wiley & Sons Inc, 239p. 2002.

CHERVENAK, Ann L.; VELLANKI, Vivekanand; KURMAS, Zachary. **Protecting File Systems: A Survey of Backup Techniques**. Estados Unidos: Georgia Tech University. 2010.

YARRAPOTHU, Sindhura. **Effectiveness of Backup and Disaster Recovery in Cloud: A Comparative study on Disk and Cloud based Backup and Disaster Recovery**. Suécia: Faculty of Computing. 2015.

WIBOONRATR, Montril; KOSAVISUTTE, Kitti. **Optimal strategic decision for disaster recovery**. Inglaterra: International Journal of Management Science and Engineering Management. Disponível em <https://pdfs.semanticscholar.org/47de/7a51dbe6a2f91898e9a8b02ddf5ffab1bac2.pdf>. 2009. Acesso em Agosto/2019.

DOLGNER, Everett; **Disaster Recovery Options with AWS**. United States. Media Amazon Web Services. Disponível em <https://pt.slideshare.net/AmazonWebServices/disaster-recovery-options-with-aws>. 2017. Acesso em Agosto/2019.

PRIBERAM. **Backup em Dicionário da Língua Portuguesa –** 2008-2013. Brasil. Disponível em: <https://dicionario.priberam.org/backup>. 2019. Acesso em Agosto/2019.

RODRIGUES, Wilson F.; **Análise dos Procedimentos de Backup dos Institutos Federais**. Recife: Universidade Federal de Pernambuco. 2017.