A SEGURANÇA DE UMA ESTRUTURA DE DISASTER RECOVERY PLAN EM CLOUD COMPUTING

THE SECURITY OF A DISASTER RECOVERY PLAN STRUCTURE IN CLOUD COMPUTING

ÁVILA, Cleiton S.[1] SOLDAN, Evandro L.[2] PETROLI NETO, Silvio[3]
[1]Universidade São Francisco; [2] Universidade São Francisco; [3] Universidade São Francisco
evandro_soldan@hotmail.com

RESUMO. O modelo de computação em nuvem tem sido observado como uma solução para as crescentes demandas dos usuários dos serviços de tecnologia da informação, acessíveis de diferentes lugares via *Internet* e de diferentes dispositivos, tais como computadores e dispositivos móveis. Com todos esses benefícios, muitas organizações têm optado pelo uso de serviços de computação em nuvem. No entanto, o modelo de computação em nuvem traz uma série de desafios de segurança consigo que devem ser analisados e endereçados tanto por usuários como por provedores de serviços. A falta de atenção e entendimento às questões de segurança pode trazer reflexos negativos para os indivíduos e para as empresas que fazem uso desses serviços. Com isso muitas empresas possuem em sua estrutura de organização Planos de Recuperação de Desastre (*DRP*), que é um documento com um conjunto de ações que a equipe de TI deve tomar caso passe por problemas físicos ou técnicos. O objetivo deste trabalho é analisar a segurança em uma estrutura de *DRP* em *Cloud*, analisando o tráfego de dados a partir de diversos formatos de arquivos. Com a análise dos dados, será possível realizar a verificação dos serviços de *DRP* quanto à questão de segurança das informações, e elencar se existem garantias de que os dados são salvos com a devida privacidade, verificando assim a eficiência desta tecnologia em nuvem.

Palavras-chave: *cloud computing*, *DRP*, segurança.

ABSTRACT. Cloud computing has been observed as a solution to the increasing demands of users of information technology services accessible from different places by the Internet and from different devices such as computers and mobile devices. With all these benefits, many organizations have opted for the use of cloud computing services. However, the cloud computing brings a number of security challenges that must be analyzed and addressed by both users and service providers. Lack of attention and understanding of security issues can have negative consequences for individuals and companies that use these services. With this, many companies have a Disaster Recovery Plans (DRP) on its structure plan, which is a document with a set of actions that the IT team must take if it goes through physical or technical problems. The objective of this research is to analyze the security in a structure of DRP in Cloud Computing, analyzing the traffic of data from many formats of files. By analyzing the data, it will be possible to perform the verification of DRP services on the issue of information security, and whether there are guarantees that the data is saved with due privacy, thus verifying the efficiency of this cloud technology.

Keywords: *cloud computing*, DRP, security.

INTRODUÇÃO

O modelo de computação em nuvem (*Cloud Computing*) tem sido observado como uma solução para as crescentes demandas dos usuários dos serviços de tecnologia da informação, acessíveis de diferentes lugares via *Internet* e de diferentes dispositivos, tais como computadores e dispositivos móveis. Com todos esses benefícios, muitas organizações têm optado pelo uso de serviços de computação em nuvem.

O armazenamento de dados é feito em serviços que poderão ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet - daí a alusão à nuvem. O uso desse modelo (ambiente) é mais viável do que o uso de unidades físicas.

A computação em nuvem segundo o NIST (*National Institute of Standards and Technology*) define como um modelo de acesso conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços), como mostra a Figura 1, que podem ser adquiridos e liberados com mínimo esforço gerencial ou interação com o provedor de serviços.

Taurion complementa, afirmando que a computação em nuvem surge da necessidade de construir complexas infraestruturas de TI, onde os usuários não precisam realizar instalação, configuração e atualização de *softwares*. Além de que, recursos de *hardware* e computação possuem tendências a ficarem ultrapassados rapidamente.

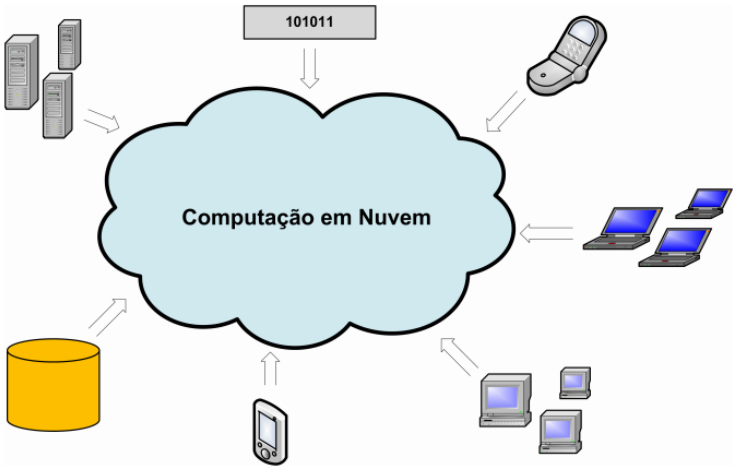

Figura 1 - Visão geral de uma nuvem computacional <fonte: https://www.researchgate.net/profile/Javam_Machado/publication/237644729_Computacao_em_Nuvem_Conceitos_Tecnologias_Aplicacoes_e_Desafios/links/56044f4308aea25fce3121f3.pdf>

Na literatura em nuvem o modelo encontrado com maior frequência é composto por três camadas, sendo que ele define um padrão arquitetural para soluções em computação em nuvem, assim como mostra a Figura 2.

Nesse projeto, o modelo que se encontra em evidência é a camada *Software como Serviço (SaaS).* Ela corresponde a camada mais externa do modelo conceitual, sendo composta por aplicativos que são executados no ambiente da nuvem.

Os sistemas de *software* devem estar disponíveis na *internet* através de uma interface com um navegador *web*, com isso podem ser acessados de qualquer lugar a partir dos variados tipos de dispositivos. Exemplos de *SaaS* são o *Google Drive*® e *Microsoft OneDrive*®. (SOUZA, 2009).

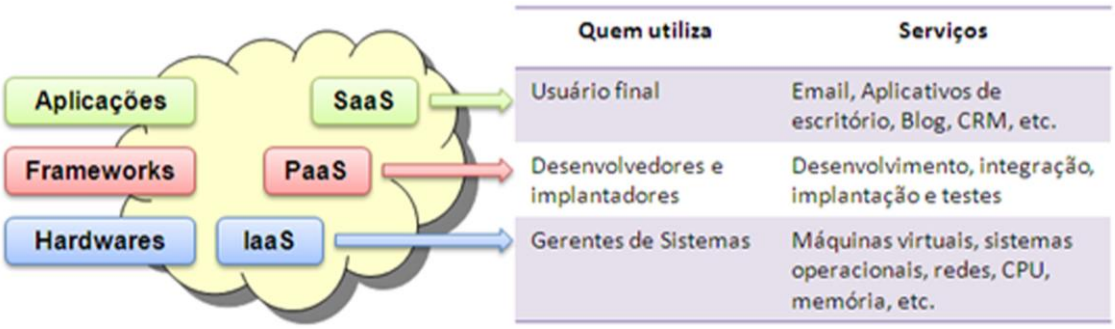

Figura 2 – Modelo de Serviço <fonte: http://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%C3%87%C3%83O%20EM%20NUVEM.pdf>

Quando se trata da disponibilidade e acesso a ambientes de computação em nuvem, existem diferentes tipos de modelos de implantação. Certas empresas desejam que nem todos os seus usuários possam ter acesso e utilizar alguns recursos no ambiente de computação em nuvem. Neste ponto, a necessidade de ambientes mais restritos, torna-se fundamental. Para isso os modelos de implantação podem ser divididos em pública, privada, comunidade e híbrida (MELL e GRANCE, 2009 *apud* SOUSA; MOREIRA; MACHADO, 2010). No modelo de nuvem privada mostrado na Figura 3, a nuvem é exclusiva de uma organização, sendo ela local ou remota e a própria empresa ou terceiros a administram. Neste modelo são empregados políticas de acesso aos serviços [SOUSA; MOREIRA; MACHADO, 2010].

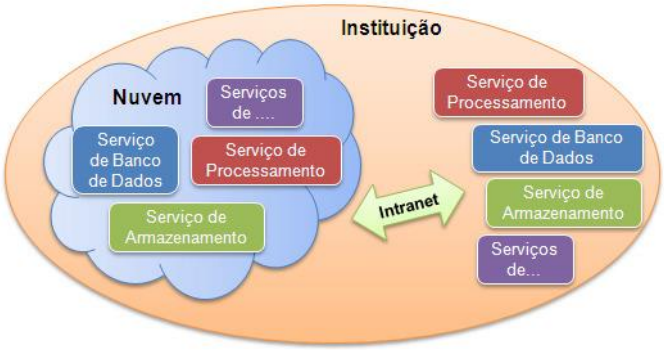

Figura 3 – Nuvem Privada <fonte: http://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%C3%87%C3%83O%20EM%20NUVEM.pdf>

No modelo de nuvem pública mostrado na Figura 4, a infraestrutura é disponibilizada para todo o público, sendo que qualquer usuário que conheça a localização do serviço pode acessá-la. Neste modelo não se aplica restrições de acesso quanto ao gerenciamento de redes (SOUSA; MOREIRA; MACHADO, 2010).

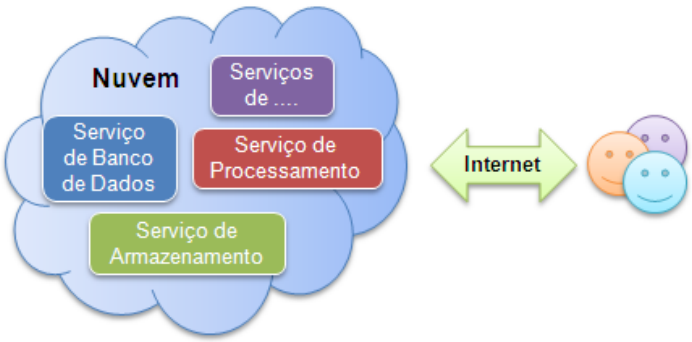

Figura 4 – Nuvem Pública <fonte: http://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%C3%87%C3%83O%20EM%20NUVEM.pdf>

No modelo de nuvem comunidade como mostra a Figura 5, ocorre o compartilhamento por diversas empresas que partilham seus interesses, como a missão, política, requisitos de segurança, e considerações sobre flexibilidade (SOUSA; MOREIRA; MACHADO, 2010).

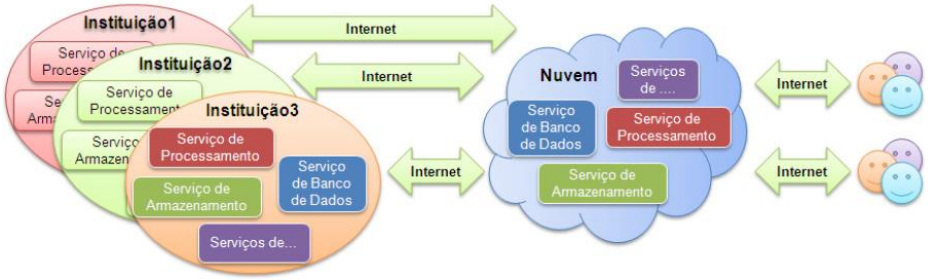

Figura 5 – Nuvem Comunitária <fonte: http://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%C3%87%C3%83O%20EM%20NUVEM.pdf>

No modelo de nuvem híbrida representado na Figura 6, dois ou mais métodos se unem, mantendo como entidades únicas e que permite a portabilidade de dados e aplicações (SOUSA; MOREIRA; MACHADO, 2010).

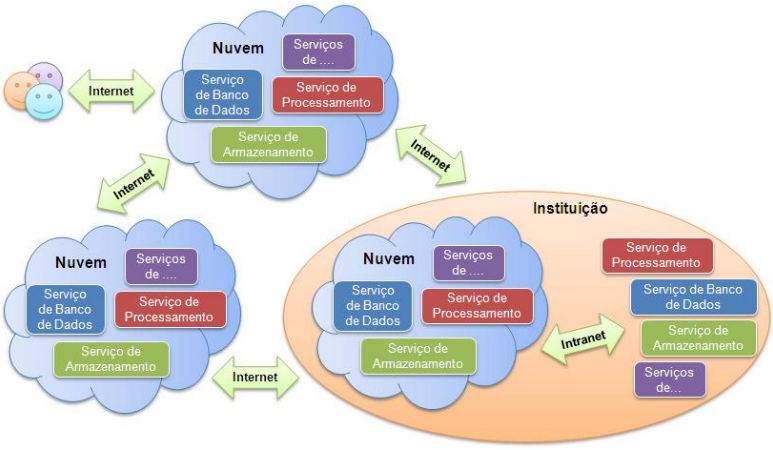

Figura 6 – Nuvem Híbrida <fonte: http://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%C3%87%C3%83O%20EM%20NUVEM.pdf>

No entanto, o modelo de computação em nuvem traz uma série de desafios de segurança consigo que devem ser analisados e endereçados tanto por usuários como por provedores de serviços. A falta de atenção e entendimento às questões de segurança pode trazer reflexos negativos para os indivíduos e para as empresas que fazem uso desses serviços.

Afinal, nenhuma área da tecnologia da informação está 100% a salvo de sofrer uma baixa a qualquer momento. É claro que bons profissionais de TI vão sempre ter planos B, C e Z de recuperação de dados frente a desastres, que podem ir desde a replicação das informações em diferentes dispositivos até a formulação de estratégias de *Disaster Recovery Plan* (*DRP*) no *backup* em nuvem.

O próprio *backup* já assegura a retenção de vários dados quando algo ocorre da maneira errada, como falhas de *hardware* e *software*, incidentes físicos ao *data center* da empresa, como roubos e incêndios, ou quando alguém comete uma falha humana que comprometa os sistemas de informação.

Em teoria, tudo o que possa danificar os dados da empresa, ou colocá-los em risco de perda permanente, consegue ser minimizado através de um *cloud backup* que permita a restauração dos dados.

E com isso, muitas empresas possuem em sua estrutura de organização Planos de Recuperação de Desastre (*DRP*), um documento com um conjunto de ações que a equipe de TI deve tomar caso passe por problemas físicos ou técnicos.

O *Disaster Recovery Plan* (*DRP*), em português Plano de Recuperação de Desastres (PRD) deve conter as ações necessárias para a retomada de todos os serviços, ou apenas os serviços críticos, possibilitando a retomada das operações. O documento deve oferecer uma sequência de eventos necessária para preparar o local de *backup* e as funções e responsabilidades de todo o pessoal envolvido. (ANDRADE, 2011)

As organizações estão sujeitas aos mais diversos tipos de ataques e ameaças à segurança da informação que cada dia se tornam mais ambiciosos e sofisticados. A função do *DRP* na segurança da informação é permitir que uma organização sobreviva a um desastre e que possa restabelecer as operações dos negócios (FAGUNDES, 2011; ABNT NBR ISO/IEC 17799:2005)

Para definir um *DRP* adequado para o negócio é necessário identificar os sistemas, processos e funções críticas, identificar também quais eventos representam possíveis desastres. Essa análise deve avaliar qual o impacto ao negócio causa a restrição de acesso a esses sistemas e serviços, apresentando assim o tempo necessário para a recuperação parcial e total do ambiente de tecnologia da informação. (ANDRADE, 2011; FAGUNDES, 2011)

O *DRP* é parte essencial do Plano de continuidade de negócios que visa garantir a continuidade de processos e informações vitais à sobrevivência da empresa, com finalidade de dar continuidade às suas operações num nível predefinido como aceitável. (Silva, 2011)

Desse modo, toda vez que a empresa passar por uma situação crítica, os danos causados pela falta de sistemas ou por eventuais perdas de dados serão reduzidos ao máximo.

A segurança e a privacidade da informação de uma organização, ou mesmo pessoais, é uma preocupação corrente em todas as esferas de negócio. Segundo França e Teruel, a segurança na computação em nuvem traz vários desafios a gestores de TI e a diversas áreas, contudo, muitos desses obstáculos podem ser identificados traçando um bom planejamento de migração de dados.

A CSA (*Cloud Security Alliance*) complementa dizendo que é preciso ter ciência sobre quais serviços pode se tirar proveito e quais implicações e regulamentações podem ocorrer na migração de serviços.

Quando se fala de segurança na rede, nunca se deve esquecer dos protocolos de comunicação, que segundo Kurose e Ross, protocolos definem formatos, ordens de mensagens enviadas e recebidas entre entidades de rede, e ações tomadas.

O modelo ISO/OSI (*International Organization for Standardization / Open Systems Interconnection*) permite o intercâmbio de informações entre computadores de fabricantes distintos, dividindo suas funcionalidades e capacidades em sete camadas (Física, Enlace, Rede, Transporte, Sessão, Apresentação e Aplicação). Para que as camadas se comuniquem devem especificar o mesmo protocolo. Em nosso projeto os protocolos analisados foram o *TCP* e *TLS*

De acordo com Forouzan o *TCP* (*Trabsmission Control Protocol*) fornece serviços de camada de transporte completos para os aplicativos. O *TCP* é um protocolo de transporte de fluxo confiável. Neste contexto, o termo fluxo significa orientado a conexões.

Para que exista a transmissão de dados antes deve existir uma conexão entre as extremidades, os dados são segmentados e mantem uma sequência numérica para a posterior reorganização.

Segundo Forouzan o *TLS* (*Transport Layer Security*) foi projetado para fornecer segurança à camada de transporte. O *TLS* foi derivado de um protocolo de segurança chamado SSl (*Secure Socktes Layer*).

Uma vantagem do *TLS* é que é independente do protocolo de aplicação. Protocolos de nível superior podem ficar em cima do protocolo *TLS* de forma transparente.

Desse modo esse trabalho tem como objetivo analisar a segurança em uma estrutura de *Disaster Recovery Plan* em *Cloud Computing*, analisando o tráfego de dados a partir de diversos formatos de arquivos e sistemas, simulando assim um ambiente de TI de uma empresa.

Com a análise dos dados, será possível realizar a verificação da segurança das informações presente na estrutura de *Cloud Computing*, e elencar se existem garantias de que os dados são salvos com a devida privacidade, verificando assim a eficiência desta tecnologia em nuvem.

METODOLOGIA

Na realização do projeto dividimos ele em 4 partes, que são: Virtualização, *Cloud Computing*, *Disaster Recovery Plan* (*DRP*) e Análise de Segurança.

Virtualização

Para a realização da análise das estruturas de tecnologia da informação, simulamos um pequeno ambiente de TI empresarial, fazendo com que fique mais próximo possível de um ambiente real.

Inicialmente para a realização dos testes disponibilizamos um computador com as seguintes configurações:

- Computador: *All in One Itautec*® *- InfoWay* AT0100
- Processador: AMD *Athlon* II X2 260u 1,80 GHz
- Memória: 4 GB
- HD: 500 GB
- Sistema Operacional: *Windows* 10 Pro® - 64 bits

O sistema operacional foi instalado do zero, permitindo assim que o mínimo de *softwares* estivesse rodando na máquina, assim tornando possível a obtenção de dados mais limpos nos testes de monitoramento de rede e protocolos de transferência.

Para o ambiente simulado usamos dois servidores virtuais e para a instalação destes servidores foi utilizado o software *Oracle VM VirtualBox*® com distribuição gratuita. O software gerenciador das máquinas virtuais foi escolhido devido alguns pontos interessantes de destacar:

- *Software* gratuito e desenvolvido por uma das maiores empresas de TI do Mundo.
- Compatibilidade com formatos de disco que permitem migrar as máquinas virtuais, opção essencial para a criação de um bom *DRP*.
- Facilidade no uso do *software* e documentação de ajuda eficiente.

Para a criação das máquinas virtuais foi utilizada a opção VMDK (*Virtual Machine Disk*), formato usado pela *VMware*, que nos garante a compatibilidade e a versatilidade para a criação do *DRP*.

As máquinas virtuais criadas como servidores para os testes foram:

Ubuntu Server® 14.04.5 - 32 bits

- Memória: 1 GB
- HD: 10GB (alocados dinamicamente)
- Processador: 1 CPU (AMD *Athlon* II X2 260u 1,80 GHz)

Windows Server 2003® - 32 bits

- Memória: 512 MB
- HD: 20GB (alocados dinamicamente)

- Processador: 1 CPU (AMD *Athlon* II X2 260u 1,80 GHz)

No Servidor *Ubuntu*® foi configurado a função de compartilhamento de arquivos através do aplicativo Samba, assim permitindo o compartilhamento dos arquivos de rede entre os servidores e o computador cliente. Objetivando uma configuração que estivesse o mais próximo ao ambiente de uma empresa.

Foi configurado no *Windows Server*® um servidor Apache e banco de dados *MySql*® para utilização do sistema *web* da empresa. Para exemplificarmos a utilização de um sistema empresarial utilizamos um sistema de controle de tickets LCEG, um projeto desenvolvido para a disciplina de desenvolvimento de *software* pelos autores deste artigo no passado.

O ambiente criado conta com três dispositivos que se comunicam através de uma rede virtual criada de maneira *default* pelo *VirtualBox*®. Assim simulamos um ambiente de uma empresa com dois servidores e que realizará seus *backups* em nuvem, necessitando validar a segurança de ter seu *DRP* em nuvem.

Para que as máquinas virtuais se comunicassem foi criada uma interface de rede *host-only* no seu *VirtualBox*®, nesta rede a placa fica para uso exclusivo do hospedeiro, ou seja, a interface servirá apenas para comunicação entre Máquina Virtual (que é o hóspede) e a Máquina Física (que é o hospedeiro), assim as máquinas podem ser configuradas com um IP Fixo permitindo a comunicação entre elas.

Cloud Computing

Em nosso projeto, o *backup* que utilizamos em nuvem conta com dois sistemas, das maiores empresas de tecnologia presentes no mercado: *Google*® e *Microsoft*®, onde utilizamos contas gratuitas e configuradas da seguinte forma:

Microsoft OneDrive®

- Tipo da Conta: Gratuita
- Total de Armazenamento: 5GB
- *Software*: Instalada versão de sincronização *desktop*.

Google Drive®

- Tipo da Conta: Gratuita
- Total de Armazenamento: 15GB
- *Software*: Instalada versão de sincronização *desktop*.

Disaster Recovery Plan

Para a construção do nosso *DRP*, foi criado um plano de recuperação que consiste de algumas regras de *backup*, sendo que há dois tipos de *backup* de dados, *backup on-line* e *backup off-line*, ambos podem ser também dos tipos: completo ou incremental.

O *backup off-line* é feito quando o sistema não está em operação. Os usuários não podem conectar a uma aplicação ou à base de dados e nesse período não haverá nenhuma atividade no sistema, exceto o processo de *backup*.

O *backup on-line* permite a execução do *backup*, mesmo com o sistema em operação. Neste período os usuários podem utilizar a aplicação e/ou a base de dados e executar ações normais, tais como a atualização e a recuperação dos dados com o sistema funcionando normalmente.

O *backup* completo é o *backup* de todas as bases de dados e também de todos os arquivos envolvidos na aplicação.

O *backup* incremental é o *backup* dos dados que foram modificados. Esse *backup* somente conterá os dados modificados desde o último *backup* completo ou desde o último *backup* incremental.

O *backup* também pode ser local ou remoto. O *backup* local é feito no mesmo lugar em que se encontram os dados originais, e o *backup* remoto é a cópia segura dos dados em local distante dos dados principais.

Em nosso projeto para que pudéssemos configurar o *backup* de todo o ambiente, primeiramente foi necessário separar por áreas, assim criamos níveis de situações de desastres, permitindo que a recuperação ocorra com mais eficiência e eficácia, pois o tempo de restauração é menor e proporcional ao nível de desastre enfrentado.

O backup do banco de dados será realizado uma vez por dia de forma completa e será salvo remotamente no *Google Drive*® como armazenamento principal e no *Microsoft OneDrive*® como armazenamento secundário. Será realizado manualmente no final do expediente de trabalho seguindo os passos abaixo:

- Acessar o servidor *Windows Server* 2003® através do sistema *VirtualBox*® no computador hospedeiro
- No servidor acessar o navegador *web* e a página de administração do *phpMyAdmin*®.
- Selecionar o banco de dados do sistema
- Exportar o banco em formato SQL
- Salvar o arquivo na pasta compartilhada na rede local, respeitando a estrutura de datas e áreas do *backup*, o local é estruturado da seguinte maneira:

\\"IP_do_Servidor_Linux"\tcc_shared\Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo

- Utilizando o computador hospedeiro.
- Salvar o arquivo no armazenamento do *Google Drive*® seguindo a estrutura.

Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo

- Salvar o arquivo no armazenamento do *Microsoft OneDrive*® seguindo a estrutura.

Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo

Para os arquivos, o *backup* será realizado de forma completa semanalmente no final do expediente de trabalho do dia em questão e será salvo remotamente no *Google Drive*® como armazenamento principal e no *Microsoft OneDrive*® como armazenamento secundário. O *backup* deverá ser realizado da seguinte forma:

- Utilizando o computador hospedeiro.
- Acessar o local de rede dos arquivos:

\\"IP_do_Servidor_Linux"\tcc_shared\Arquivos

- Criar um arquivo compactado da pasta toda.
- Salvar o arquivo na pasta compartilhada na rede local, respeitando a estrutura de datas e áreas do *backup*, o local é estruturado da seguinte maneira:

\\"IP_do_Servidor_Linux"\tcc_shared\Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo

- Salvar o arquivo no armazenamento do *Google Drive*® seguindo a estrutura.

Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo

- Salvar o arquivo no armazenamento do *Microsoft OneDrive*® seguindo a estrutura.

Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo

O *backup* do Sistema deverá ser realizado mensalmente também no final do expediente de trabalho do dia em questão e será salvo remotamente no *Google Drive*® como armazenamento principal e no *Microsoft OneDrive*® como armazenamento secundário. O *backup* deverá ser realizado da seguinte forma:

- Utilizando o computador hospedeiro.
- Acessar o local de rede dos arquivos:

\\"IP_do_Servidor_Windows"\LCEG

- Criar um arquivo compactado da pasta toda.
- Salvar o arquivo na pasta compartilhada na rede local, respeitando a estrutura de datas e áreas do *backup*, o local é estruturado da seguinte maneira:

\\"IP_do_Servidor_Linux"\tcc_shared\Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo

- Salvar o arquivo no armazenamento do *Google Drive*® seguindo a estrutura. *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Salvar o arquivo no armazenamento do *Microsoft OneDrive*® seguindo a estrutura. *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*

Os servidores virtuais que são gerenciados pelo *VirtualBox*® devem ter seus *backups* realizados trimestralmente, iniciando no final do expediente de trabalho do dia em questão e será salvo remotamente no *Google Drive*® como armazenamento principal e no *Microsoft OneDrive*® como armazenamento secundário. O *backup* deverá ser realizado da seguinte forma:

- Os servidores deverão ser desligados.
- Através do sistema *VirtualBox*® no computador hospedeiro.
- Utilizar a opção exportar *appliance* e selecionar as máquinas virtuais.
- Salvar o arquivo no armazenamento do *Google Drive*® seguindo a estrutura. *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Salvar o arquivo no armazenamento do *Microsoft OneDrive*® seguindo a estrutura. *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*

Esta é a parte mais importante e crítica do *DRP*, pois é necessário garantir que estes arquivos de *backup* irão funcionar adequadamente e não estejam corrompidos. Como o intuito principal deste artigo é validar a segurança deste *DRP* que utiliza armazenamento em nuvem para salvar estes arquivos, os passos de restauração utilizam etapas de acordo com os níveis de desastres.

Primeiramente, em um nível mais baixo de desastre, temos problemas isolados nos sistemas, como por exemplo banco de dados corrompidos, sistema de *tickets* com problemas ou atualização má sucedida e arquivos perdidos.

Quando o desastre ocorrer isoladamente no banco de dados é necessário seguir os passos para restauração. Acessando o armazenamento do *Google Drive*® como armazenamento principal e do *Microsoft OneDrive*® como armazenamento secundário, em caso de problemas com o arquivo armazenado na nuvem.

- Utilizando o computador hospedeiro, acessar o local de armazenamento em nuvem.
- Baixar o arquivo de *backup* mais recente, seguindo a estrutura de armazenamento: *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Utilizando a pasta de compartilhamento de rede local salvar o arquivo baixado: *\\"IP_do_Servidor_Linux"\tcc_shared\Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Acessar o servidor *Windows Server* 2003® através do sistema *VirtualBox*® no computador hospedeiro
- No servidor acessar o navegador *web* e a página de administração do *PHPMyAdmin*®.
- Importar o banco e validar a restauração.

Neste caso, quando necessário restaurar arquivos, deve-se seguir os passos para restauração. Também acessando o armazenamento do *Google Drive*® como armazenamento principal e do *Microsoft OneDrive*® como armazenamento secundário.

- Utilizando o computador hospedeiro acessar o local de armazenamento em nuvem.
- Baixar o arquivo de *backup* mais recente, seguindo a estrutura de armazenamento: *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Descompactar o arquivo na pasta compartilhada na rede local, respeitando a estrutura de datas e áreas do *backup*, o local é estruturado da seguinte maneira: *\\"IP_do_Servidor_Linux"\tcc_shared\Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Após descompactar é necessário validar se a restauração é necessária para um ou todos os arquivos e realizar a substituição.

A restauração é necessária quando houver problemas com o sistema de controle, como atualizações malsucedidas e/ou arquivos corrompidos deve-se seguir os passos para restauração.

- Utilizando o computador hospedeiro acessar o local de armazenamento em nuvem.
- Baixar o arquivo de *backup* mais recente, seguindo a estrutura de armazenamento: *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Descompactar o arquivo na pasta compartilhada na rede local, respeitando a estrutura de datas e áreas do backup, o local é estruturado da seguinte maneira: *\\"IP_do_Servidor_Linux"\tcc_shared\Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Acessar o local de rede dos arquivos e substituir toda a pasta. *\\"IP_do_Servidor_Windows"\LCEG*

Quando houver algum erro com o servidor e não for passível de recuperação é necessário recuperar todo o servidor ou todos os servidores, para isso deve-se seguir os passos para restauração.

- Utilizando o computador hospedeiro acessar o local de armazenamento em nuvem.
- Baixar o arquivo de *backup* mais recente, seguindo a estrutura de armazenamento: *Backups\"ano"\"mes"\"area"\"nome_AAAA-MM-DD".tipo*
- Através do sistema *VirtualBox*®.
- Utilizar a opção importar *appliance* e selecionar as máquinas virtuais para a restauração.

Pode ser necessário realizar os procedimentos de recuperação do banco de dados, sistema e arquivos. Isso está relacionado diretamente com a data do *backup*.

Para o nível de maior desastre temos a perda total do computador hospedeiro, neste caso em uma nova máquina de mesma capacidade ou superior deve-se instalar o sistema *VirtualBox*® e sistemas de armazenamento em nuvem do *Google Drive*® e *Microsoft OneDrive*®, então seguir os procedimentos de restauração dos servidores.

Análise de Segurança

Após a definição do *DRP* e a criação das máquinas virtuais, começamos a executar os testes em cada sistema. Para fazer tal análise, foi instalado o *software Wireshark*® com o intuito de análise do fluxo de rede e seus protocolos, dados enviados e recebidos através dos *softwares Microsoft OneDrive*® e *Google Drive*®. Assim será possível verificar a segurança disponível em cada padrão de protocolo utilizado, utilizando bases de conhecimentos especialistas em segurança da informação.

RESULTADOS E DISCUSSÃO

Ao realizarmos os procedimentos para a criação do ambiente simulado nos deparamos com situações que nos levaram a aplicar conhecimentos que adquirimos ao longo do curso, e principalmente ao longo da vida profissional. Como a intenção era a simulação de um ambiente profissional, a criação das máquinas virtuais foram indispensáveis e apresentaram desempenho que superaram as expectativas.

Com as máquinas virtuais preparadas para o ambiente simulado, foi criado um *DRP* à altura do mesmo. Este plano de recuperação de desastre definiu como deveriam ser realizados os *backups* rotineiros e também como proceder em casos de necessidade de recuperação, definindo por níveis de restauração.

O nível mais baixo de restauração é quando existe um problema apenas em um dos ambientes, por exemplo a recuperação de um arquivo ou exclusivamente do banco de dados. Já um nível mais alto de desastre afetaria todo o ambiente sendo necessária a recuperação de todos os servidores e arquivos.

Então, foram iniciados os testes das ferramentas de armazenamento em nuvem *Google Drive*® e *Microsoft OneDrive*®, realizando o *backup* e a restauração de acordo com as rotinas definida no *DRP*, como mostrado nas Figuras 7 e 8.

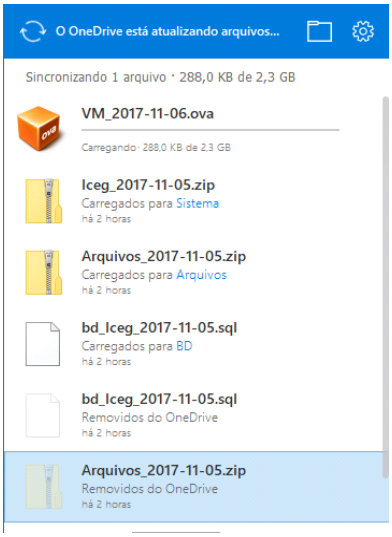

Figura 7 - Painel de status de atualização de arquivos do *Microsoft OneDrive*® (Fonte: Próprio autor).

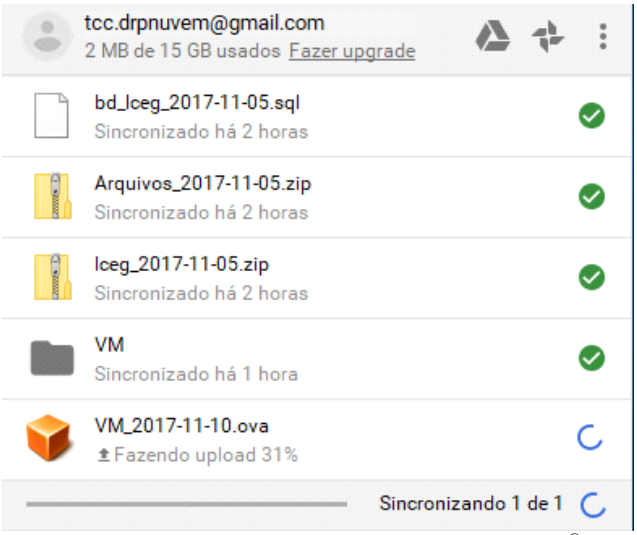

Figura 8 - Painel de status de atualização de arquivos do *Google Drive*® (Fonte: Próprio autor).

A ferramenta de análise de pacotes e protocolos *WireShark*® monitorou os processos de *backup* e restauração, analisando o *upload* e *downloads* dos arquivos, como mostra a Figura 9. Para que não houvesse problemas na identificação dos protocolos utilizados foi desligado todos os outros recursos do computador hospedeiro mantendo somente os programas de armazenamento em nuvem utilizados.

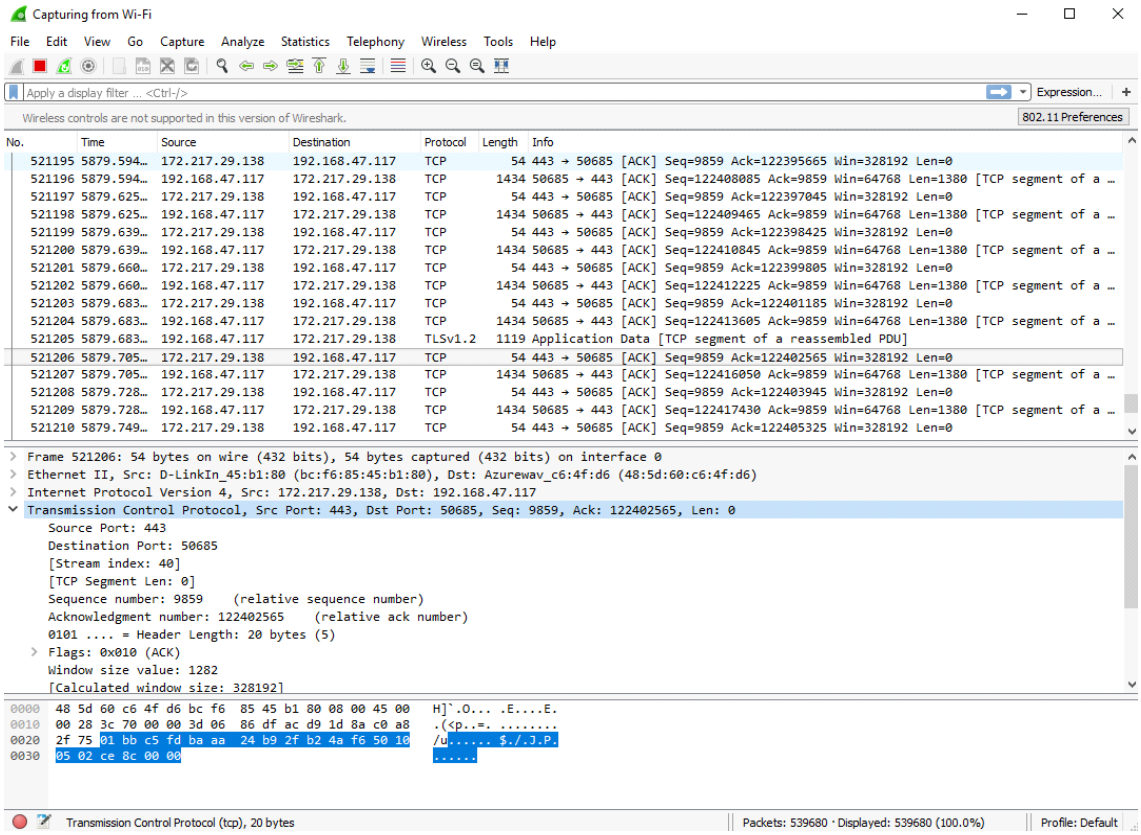

Figura 9 - Processo de análise dos protocolos de rede (Fonte: Próprio autor).

Todo o procedimento ocorreu através da placa de *WiFi* do computador hospedeiro, todo o tráfego de arquivos e seus protocolos foram monitorados.

Foi gerado também um arquivo de *log* do tráfego de rede com apenas os programas abertos e o computador em estado ocioso, como é demonstrado no gráfico 1, garantindo assim que pudéssemos analisar somente o tráfego utilizado no momento do *backup* e da restauração:

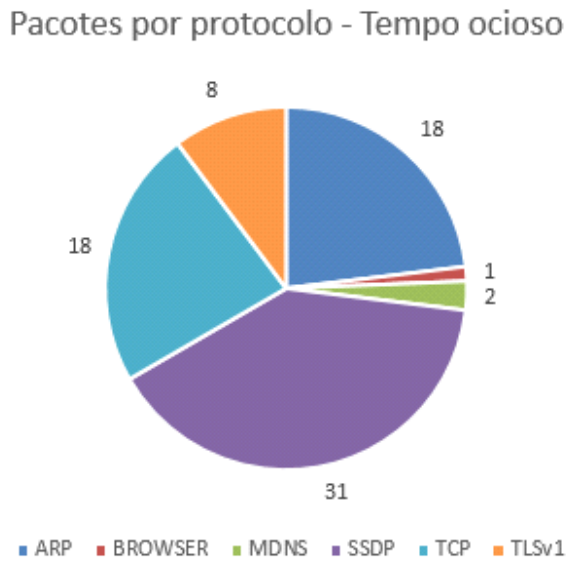

Figura 10 - Pacotes por protocolo no computador ocioso (Fonte: Próprio autor).

Foram salvos e analisados os dados extraídos do programa *WireShark*®, separando o tráfego referente ao *Google Drive*® e *Microsoft OneDrive*®. Com os dados extraídos com o

computador em tempo ocioso e o auxílio de um *site* para localização de *IPs* (*https://www.localizaip.com.br/*) foi possível separar somente o tráfego dos softwares de armazenamento.

Os dados capturados durante a utilização do *Microsoft OneDrive*® com os *IPs* de Origem e Destino, e os protocolos estão apresentados na Tabela 1.

Tabela 1 – Tabela *IP* e protocolos *OneDrive*® (Fonte: Próprio autor).

Destination	***Source***	***Protocolo***
192.168.47.117	204.79.197.213	*TCP* *TLS*v1.2
	40.117.100.83	*TCP* *TLS*v1.2
204.79.197.213	192.168.47.117	*TCP* *TLS*v1.2
40.117.100.83	192.168.47.117	*TCP* *TLS*v1.2

E os dados capturados durante a utilização do *Google Drive*® com os *IPs* de Origem e Destino, e os protocolos estão apresentados na Tabela 2.

Tabela 2 – Tabela *IP* e protocolos *Google Drive*® **(**Fonte: Próprio autor).

Destination	***Source***	***Protocolo***
192.168.47.117	172.217.29.138	*TCP* *TLS*v1.2
172.217.29.138	192.168.47.117	*TCP* *TLS*v1.2

Observamos que os dois *softwares* utilizaram igualmente o protocolo *TCP* para transferência dos pacotes e *TLS*V1.2 para a criptografia desses pacotes.

Uma das dificuldades enfrentadas com este modelo de *DRP* foi a velocidade da *internet*, que interferiu diretamente no tempo de realização dos *backups* e restaurações.

Foi utilizado um pacote de dados com baixa taxa de transferência, porém foi possível completar as tarefas exigidas pelo modelo de *DRP* imposto com sucesso. Ainda assim, este fato está diretamente relacionado com a qualidade do *DRP* exigindo uma boa qualidade do pacote de dados.

CONCLUSÃO

Com base nos resultados apresentados neste artigo, que teve como objetivo analisar a segurança de uma estrutura de *Disaster Recovery Plan* em *Cloud Computing*, conclui-se que o nível de segurança está diretamente relacionado com o sistema de armazenamento em nuvem utilizado.

Segundo os testes realizados com as plataformas *Google Drive*® e *Microsoft OneDrive*®, pode-se garantir que estas são seguras, devido o fato de ambas utilizarem um padrão de criptografia através dos protocolos *TCP* e *TLS*, responsáveis pela transmissão e segurança do tráfego do pacote de dados.

Outro ponto importante a ressaltar é que os testes nos mostraram que a velocidade e qualidade do pacote de dados contratado é essencial para garantir a eficiência e segurança do *DRP* em nuvem, pois influenciam diretamente no tempo de *backup* e restauração.

Pelo *software* analisador de tráfego *Wireshark*®, conclui-se que não é possível a leitura direta dos dados que trafegam na rede, pois estes dados estão sempre criptografados por ambos os serviços testados.

Por fim, dentro das condições estudadas, e atendendo o objetivo deste trabalho, pode-se afirmar que uma estrutura de *Disaster Recovery Plan* em *Cloud Computing* os dados estão criptografados sem maiores interferências garantindo assim a segurança para as empresas que utilizam essa estrutura.

REFERÊNCIAS

ABNT, NBRISO. IEC 27.002: 2005 (antiga NBR ISO/IEC 17799: 2005) - **Código de Prática para a Gestão da Segurança da Informação.**

ANDRADE, Daniel et al**. Plano de contingência de TI: preparando sua empresa para reagir a desastres e manter a continuidade do negócio**. Texto apresentado na pós-graduação em segurança da informação da FACSENAC/DF, 2011.

FAGUNDES, Eduardo M. ***Disaster Recovery Plan* (*DRP*)**. Disponível em: <http://efagundes.com/artigos/disaster-recovery- plan-*DRP*>; Acesso em: 02/05/2017

FOROUZAN, Behrouz A.; FEGAN, Sophia Chung. **Protocolo *TCP*/IP-3**. AMGH Editora, 2009.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. São Paulo: Person, p. 28, 2006.

MORAES, Eliana M. **Planejamento de Backup de Dados**. Texto base da disciplina de Mestrado em Gestão e Desenvolvimento Regional, 2007. Disponível em: <http://ppga.com.br/mestrado/2007/moraes-eliana_marcia.pdf>. Acesso em: 06/11/2017

NIST (*National Institute of Standards and Technology*) - ***The NIST Definition of Cloud Computing***, *National Institute of Standards and Technology, Information Technology Laboratory – Gaithersburg, Maryland* – USA. Disponível em: <http://www.nist.org> Acesso em: 01/05/2017.

Segurança em *Cloud Computing*: Desafios e Gerenciamentos de Riscos. Disponível em: <http://www.culturacolaborativa.com/wp-content/uploads/2015/01/ebook_seguranca_ _cloud _computing.pdf> Acesso em: 01/05/2017.

SILVA, Edilberto M. **"Políticas de Segurança e Planos de Continuidade de Negócios"**. Texto base da disciplina da Pós-Graduação Segurança da Informação FACSENAC/DF, 2011. Disponível em: <http://www.edilms.eti.br/?cat=44>. Acesso em: 02/05/2017

SOUSA, Flávio R. C.; MOREIRA, Leonardo O.; MACHADO, Javam C. **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios**. In: UNIVERSIDADE FEDERAL DO CEARÁ (UFC). 2010. Disponível em <https://www.researchgate.net/profile/Javam_Machado/publication/237644729_Computacao_em_Nuvem_Conceitos_Tecnologias_Aplicacoes_e_Desafios/links/56044f4308aea25fce3121f3.pdf> Acesso em: 01/05/2017.

TAURION, Cezar. **Cloud Computing: Computação em Nuvem: Transformando o mundo da Tecnologia da Informação**. Rio de Janeiro: Brasport, 2009. ISBN 978-85- 7452-423- 8.