CONTINUIDADE DE NEGÓCIO EM CLOUD[1]

Rafael Krause Ferrão

Resumo: Um grande tema presente nas empresas é referente à jornada de transformação digital com maior adoção de *clouds* públicas como Azure e Amazon. Este fato se concentra na necessidade que o mercado está impondo as empresas atualmente de maior agilidade, disponibilidade e confiabilidade nos serviços prestados. A demora no lançamento de um novo produto ou a disponibilidade das aplicações de uma empresa pode causar impacto na sua imagem no mercado, perda de clientes ou até mesmo o encerramento das atividades da empresa. Este artigo apresentará formas sobre como garantir a adoção do melhor modelo de proteção em nuvem para o negócio, que garantam a resiliência adequada para as aplicações, além de como analisar e definir as métricas para um plano de continuidade de negócio em Nuvem pública.

Palavras-chave: Disponibilidade. Cloud. Palavra. DRP. Continuidade de Negócio.

1 INTRODUÇÃO

Com o grande crescimento do uso da internet nos últimos anos e a grande adesão das pessoas ao uso de plataformas digitais, se torna cada vez mais importante que as organizações busquem a disponibilidade de suas aplicações como premissa de qualidade do serviço prestado. Uma falha na prestação de um serviço em dias atuais pode impactar inclusive na rentabilidade da empresa, na sua imagem e ainda acarretar perda de clientes para os seus concorrentes.

Como afirma Oliveira (2011). “A medida em que aumentamos a dependência por serviços de tecnologia da informação, devemos aumentar nossos planos para

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Curso de Especialização em Datacenter: projeto, operação e serviços, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Datacenter: projeto, operação e serviços.

continuidade desses serviços em caso de interrupções graves, que podem, em muitos casos, decretar a morte da empresa."

Em meio a este tema temos ainda há a oferta de serviços de nuvem para hospedar as aplicações de negócio e assim diminuir a complexidade dos serviços de TI. Porém somente a utilização de um serviço em nuvem não garante a continuidade de serviço de TI se não forem feitas análises adequadas. Algumas métricas são necessárias para garantir que as aplicações estejam protegidas conforme a necessidade do negócio.

Diante da necessidade de proteção do ambiente em nuvem é necessário definir o melhor modelo de continuidade de negócio, com planos de recuperação bem definidos, os quais devem ser baseados nos níveis de disponibilidade esperados pela organização.

Segundo Softline (2018), "A continuidade operacional refere-se à capacidade que uma empresa tem de manter seus equipamentos e sistemas funcionando normalmente mesmo diante de um evento crítico, como um desastre. Já o plano, descreve como retomar os negócios após uma interrupção desse tipo. A intenção é agir de forma preventiva, em vez de reativa, reduzindo os impactos negativos gerados."

Neste trabalho iremos usar como modelo o serviço da Microsoft de nuvem, chamado Azure, este serviço é uma plataforma de computação em nuvem que roda nos Datacenters da Microsoft e que oferece serviços como maquinas virtuais, banco de dados e aplicações sem a necessidade que a empresa necessite se preocupar com o gerenciamento dos ativos de infraestrutura.

Para isso iremos abordar a seguir como desenvolver uma análise de impacto no negócio para determinar qual a métrica de disponibilidade requerida para cada ambiente, quais são os modelos ofertados em nuvem e suas características em comparação com um ambiente tradicional utilizando um serviço de *colocation*[2], além de exemplificar quais são os modelos de proteção disponíveis no serviço de nuvem da Azure e como

[2] Colocation: Serviço de disponibilização de infraestrutura para hospedar servidores de sua empresa em um Data Center alugado

implementamos as métricas acordadas usando o modelo que garanta a disponibilidade deseja pela organização, áreas de negócio e acionistas.

Outro ponto abordado refere-se às limitações do ambiente em nuvem da Azure no Brasil e como isso impacta no nível de disponibilidade ofertado e como o serviço de Recuperação de Desastres da Azure atua neste cenário.

2 SERVICOS DE NUVEM

Para implementação de um modelo de serviço que atenda às necessidades de disponibilidade e proteção da organização devemos primeiro, entender qual o nível de disponibilidade requerida para aplicação, estas necessidades são encontradas através de uma análise do impacto no negócio, pelo uso das métricas de Objetivo do tempo de recuperação (RTO). A métrica RTO mede qual o tempo esperado para recuperação do serviço após uma falha.

Com essas métrica estabelecida, é possível calcular o nível de disponibilidade esperado e implementar o modelo adequado de recuperação para desastres e interrupções não planejadas.

2.1 ANÁLISE DE IMPACTO NO NEGÓCIO

Antes de começarmos a desenvolver um plano de continuidade de negócios em Cloud para uma companhia devemos primeiramente mapear o que devemos proteger e quais os níveis de disponibilidade que a organização necessita para cada componente ou área. Uma grande ferramenta e de extrema importância para isto é o BIA (*Business Impact Analysis*).

Segundo Tres (2019), “A BIA tem como objetivo a identificação e análise de processos e ou atividades de negócios, com o objetivo de compreender o impacto do tempo de inatividade, levando em consideração a priorização sobre as atividades “Core Business” da organização e ativação dos planos de recuperação.”

Antes de seguir para um modelo de arquitetura desejado, coletamos o nível de resiliência esperado pela área de negócio através das entrevistas e informações sobre as

necessidades de Tempo de recuperação (RTO) e Ponto de recuperação (RPO) para a confecção do BIA.

Com auxílio das respostas coletadas é gerado o nível de disponibilidade esperado e serve de premissa para desenhar a melhor arquitetura para o ambiente.

Segundo a Microsoft (2020), "Uma plataforma é considerada altamente disponível de acordo com o contrato e as expectativas dos clientes e participantes. A disponibilidade de um sistema pode ser expressa por meio deste cálculo: Tempo de atividade real/tempo de atividade esperado X 100%"

Abaixo temos uma tabela de exemplo que será usada de guia para elaboração da arquitetura.

Tabela 1: Cálculo o nível de disponibilidade e RTO esperados no período de um mês.

Aplicação	RTO Mínimo Desejado (Mês)	RPO Mínimo Desejado (Mês)	Cálculo de Disponibilidade Total
Sistema de Pagamento	2 Horas	2 Horas	99.72%
Sistema de Remessa	12 horas	2 Horas	98.33%
Sistema de Vendas	15 minutos	0	99.97%
Sistema Financeiro	2 Horas	0	99.72%

Fonte: Rafael Ferrão (autor, 2020)

Como podemos ver na tabela, para o Sistema de Vendas é necessário implementar uma estrutura que nos garanta 99,97% de disponibilidade por mês.

Por meio da ferramenta do BIA, também é possível analisar e determinar o impacto financeiro por tempo de inatividade de cada aplicação. Este impacto pode ser maior ou menor dependendo da atividade da empresa, função da aplicação impactada, valor da empresa no mercado e outras variáveis.

2.2 PLANO DE CONTINGÊNCIA

O plano de contingência segue como premissa o processo de gerenciamento de disponibilidade, para garantir a disponibilidade e confiabilidade do sistema. O plano de contingência não se limita na análise de um componente de infraestrutura de forma individual, mas sim no ecossistema do serviço que esses componentes fazem parte.

Sendo assim, após a definição da disponibilidade do ecossistema é necessário ter um plano de contingência para se proteger de paradas totais de serviço que impactem na operação da empresa.

Segundo OLIVEIRA, (2014), “Plano de Continuidade de Negócios, mais conhecido como PCN, refere-se a um conjunto de estratégias e planos de ação preventivos que garantem o pleno funcionamento dos serviços essenciais de uma empresa durante quaisquer tipos de falhas, até que a situação seja normalizada.”

Como falado anteriormente o plano de contingência é baseado nas métricas de Objetivo para o Tempo de Recuperação (RTO) e o Objetivo para o Ponto de Recuperação (RPO).

Teclogica (2017) define RTO como, “...é um indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após uma falha.”

Teclogica (2019) define RPO como. “Ele é utilizado em políticas de backup de dados e, nesse cenário, auxilia na definição do tempo entre a replicação de cada informação que é salva nos backups.”

O sucesso do plano de continuidade de negócio depende de uma construção assertiva da análise impacto, a escolha da melhor estratégia para cada aplicação e um plano de gerência de crise para uma rápida resposta durante uma situação de parada.

Segundo Teclogica (2019), “O plano de gerenciamento de crises, como o próprio nome revela, deve existir antes mesmo que a crise aconteça. Ele é importante porque ajuda você e sua equipe a seguirem estratégias que foram pensadas em momentos apropriados, com análises e estudos realizados longe do clima de caos e da urgência que as crises carregam consigo.”

Para elaboração de um plano de contingência ainda é necessário fazer testes programados para garantir a assertividade do plano, corrigir erros e melhoras os tempos de resposta.

2.3 MODELOS DE CONTINUIDADE EM NUVEM

Para exemplificar os modelos de continuidade em nuvem foi escolhido o provedor AZURE, ofertado pela Microsoft, sendo um provedor de grande adoção mundialmente, que está presente em diversos países e contém uma Região de disponibilidade no Brasil, localizada em São Paulo.

Para provisionar serviços em nuvem, primeiro devemos escolher qual estratégia iremos seguir, já que podemos implementar recursos com diferentes graus de interação e responsabilidades. Existem três tipos de modelos principais que oferecem uma camada de abstração diferente se adequando a necessidade da empresa e aplicação em questão e diminuindo a complexidade das operações de serviços.

Os três modelos ofertados são *IaaS*[3], *PaaS*[4] *e SaaS*[5]: O modelo IaaS é basicamente a oferta de infraestrutura como serviço sem necessidade de ter que manter o hardware desses ambiente, já o modelo PaaS, é a oferta de plataforma como serviço, neste modelo não é necessário manter o sistema operacional e os aplicativos instalados, já no modelo SaaS este já se trata de um produto pronto para o usuário final, neste exemplo podemos citar a plataforma do O365.

Na Figura 1 abaixo, podemos ver de forma gráfica a diferença para cada um dos modelos ofertados.

[3] IaaS: Modelo de provisionamento que oferece Infraestrutura como serviço.
[4] PaaS: Modelo de provisionamento que oferece Plataforma como serviço.
[5] SaaS: Modelo de provisionamento que oferece Sofware como serviço

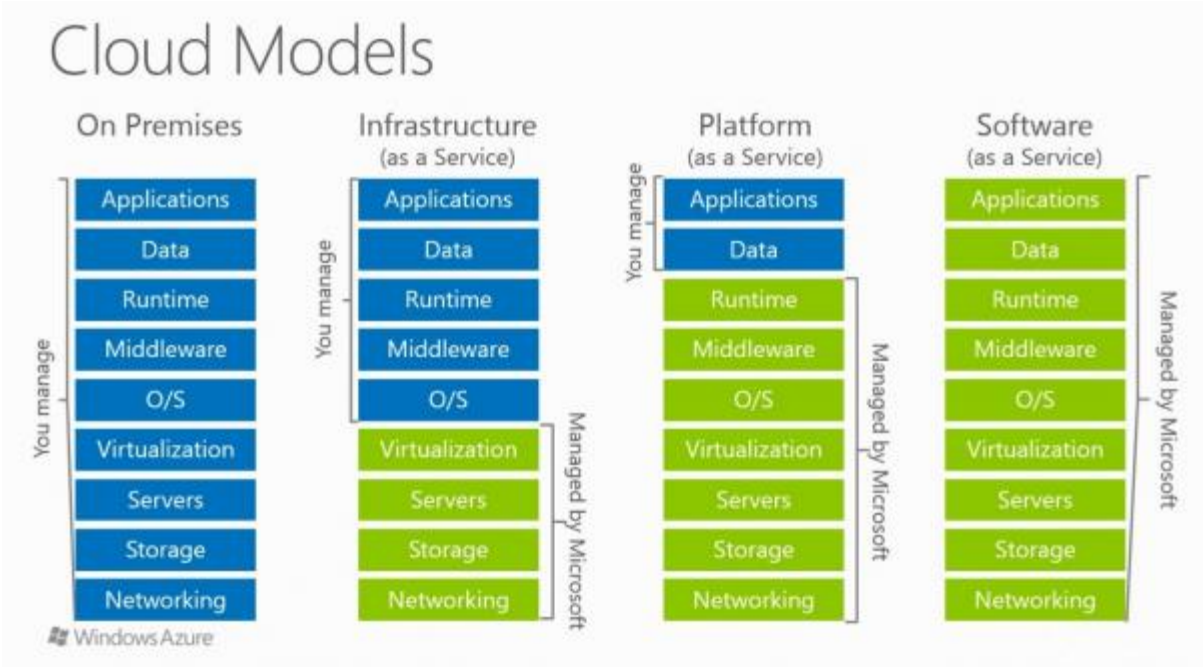


Figura 1: Exemplo de modelos ofertados.

Fonte: Amorim (2017)

A escolha do modelo é seguida usando vários aspectos, como por exemplo, se a aplicação existente na empresa, tem o seu modelo ofertado na Azure, ou se tratar de uma aplicação desenvolvida internamente que exige diversos tipos de subcomponentes instalados.

O estudo realizado aqui adota um conceito de *lift-and-shift*, ou seja, migrar as aplicações para a nuvem no mesmo estado atual, sem considerar mudanças de componentes ou desenho da aplicação. O que nos leva a escolha da Infraestrutura como Serviço (*IaaS*).

Baseado em modelo de *IaaS* a Microsoft oferece um nível de disponibilidade dependendo de como a estrutura for provisionada.

Segundo Azure (2020), “Para qualquer Máquina Virtual de Única Instância que usa Discos Gerenciados por HDD Padrão para os Discos de Sistema Operacional e Discos de Dados, garantimos que você terá Conectividade de Máquinas Virtuais pelo menos 95% do tempo.”

Se nos basearmos em um cálculo de disponibilidade em que um período de um mês, que compreende 30 dias e cada dia tem 24 horas, diremos que em 720 horas (24x30), teremos 5% de indisponibilidade do serviço no mês. Isso corresponderá a 36 horas de disponibilidade no mês. Se nos basearmos na indisponibilidade por dia, esta seria de 1 hora e 12 minutos por dia. Um número bastante elevado para aplicações consideradas críticas.

Segundo Azure (2020), “Para todas as Máquinas Virtuais com duas ou mais instâncias implantadas em duas ou mais Zonas de Disponibilidade na mesma região, garantimos que você terá Conectividade de Máquinas Virtuais, no mínimo, a uma instância, pelo menos, 99,99% do tempo”

Já neste modelo de implementação teríamos uma indisponibilidade mensal de 7 horas e 12 minutos. O que se torna um modelo bem mais factível para aplicações críticas.

Porem no Brasil a segunda zona de disponibilidade ainda está em construção então não é possível implementar um serviço com 99,99% de disponibilidade, sendo assim é necessário o uso do serviço *Azure Site Recovery*, que é a implementação de um serviço de continuidade em outra região.

Na figura 2 encontramos de forma mais ilustrativa os modelos de disponibilidade presentes na Azure atualmente para cada tipo de solução.

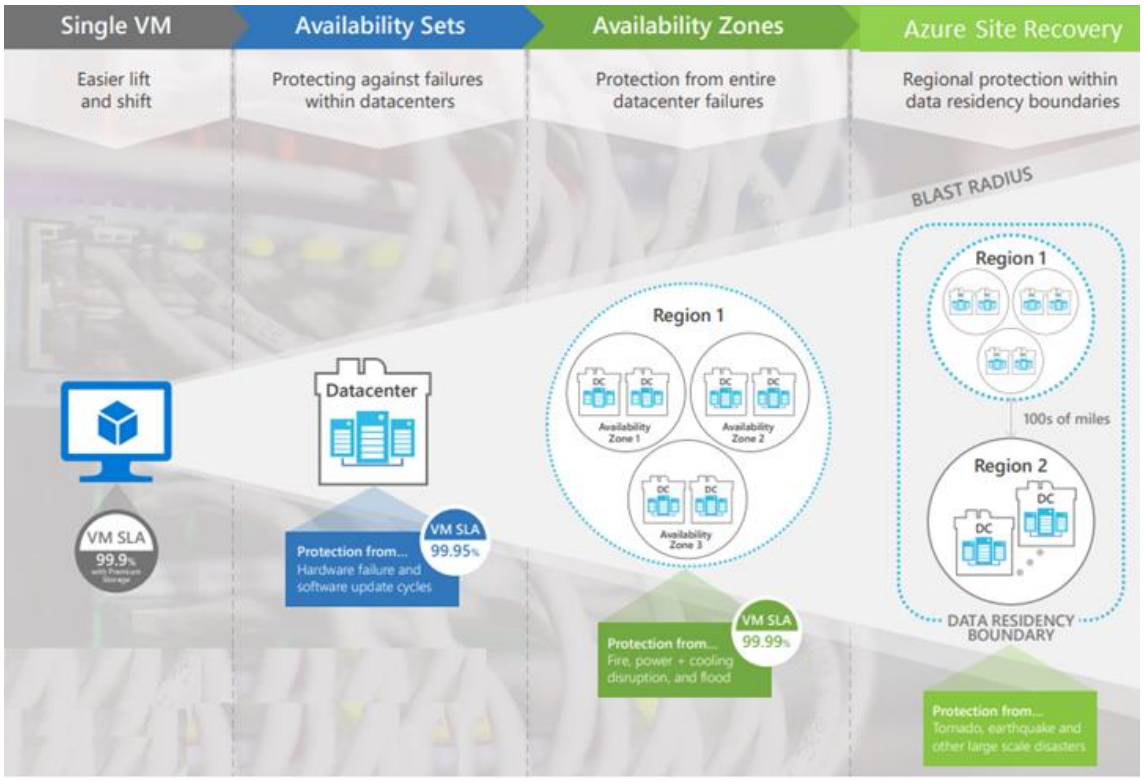


Figura 2: Exemplo de modelos de proteção ofertados.

Fonte: Weyn (2018)

2.4 ANALISE DA SOLUÇÃO

As premissas que foram analisadas neste projeto para implementação do melhor modelo em nuvem foram as seguintes.

- Serviço de Recuperação na Azure

- Regiões com transferência de arquivos em baixa latência.

- Política de proteção de dados em território estrangeiro.

O serviço de recuperação na Azure funciona em regiões, no que são chamados de Cluster geográficos. Segundo Microsoft (2020), “Clusters geográficos são definidos mantendo a latência de dados e a soberania em mente.”

A implementação da nuvem usara a região localizada no Sul do Brasil para o ambiente produtivo da empresa e a latência entre as regiões deve ser considerado para

que a cópia de dados entre as regiões seja rápida e apresente pouca latência. Isso serve para garantir que não haja um alto RPO (Objetivo do Ponto de Recuperação), garantindo assim que não ocorro perda de dados durante um evento de interrupção de serviço.

Segundo a Microsoft (2020), “Para a região Sul do Brasil, você pode replicar e fazer failover para estas regiões: Centro-Sul dos EUA, Centro-Oeste dos EUA, Leste dos EUA, Leste dos EUA 2, Oeste dos EUA, Oeste dos EUA 2 e Centro-Norte dos EUA.”

Para realizar a implementação na empresa foi escolhido a região Oeste dos EUA 2 que garante baixa latência com a região do Brasil onde estará localizado a estrutura de serviço principal da empresa.

Falando sobre proteção de dados e as novas diretrizes da LGPD e considerando que a empresa avaliada trabalha no segmento financeiro e deve seguir normas de regulamentações do BACEN é necessário a haja a garantia que os dados possam ser hospedados nos Estados Unidos.

Segundo a Grosmann (2018), “O Conselho Monetário Nacional aprovou a Resolução 4568/18, pela qual estabelece que todas as instituições financeiras do país tenham políticas de segurança cibernética. Além disso, a nova norma regula o uso de computação em nuvem no mercado financeiro, com liberdade para armazenamento de dados fora do Brasil desde que o acesso do Banco Central às informações seja garantido já nos termos contratuais.”

Isso garante que usar o serviço de recuperação hospedado nos Estados Unidos segue as regulamentações vigentes.

2.5 ESTRUTURA DO AMBIENTE

Visando garantir o nível de disponibilidade esperado, o primeiro passo se trata dos níveis de acordo de serviço presentes na nuvem da Azure para a Região do Brasil. A Microsoft garante um nível de disponibilidade de serviço de 99.99% utilizando duas zonas de disponibilidade dentro da mesma região. Porem atualmente hoje no Brasil a Azure só dispõe de uma zona para região do Brasil, que garante hoje 99.95% de disponibilidade, se para o sistema de vendas necessitamos de 99,97%, sendo assim é

necessário a implementação de um serviço de DR entre zonas, no qual permite a replicação de dados entre duas regiões no ambiente da nuvem e o uso de um sistema de balanceamento dos dados de entrada entre elas.

Segundo Microsoft (2020), “O sul do Brasil é exclusivo porque está emparelhado com uma região fora de sua geografia. A região secundária do Sul do Brasil é EUA Central do Sul.”

Diante destas premissas e analisando a estrutura necessária para as aplicações a estrutura implementada na Azure contém os seguintes componentes:

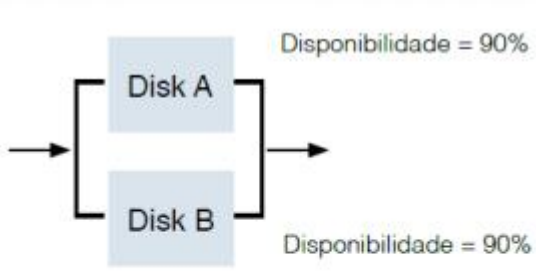
Firewall da Azure: O serviço de Firewall visa garantir melhor segurança na proteção dos componentes da aplicação e garantir a proteção de dados do ambiente.

Máquinas virtuais (*IaaS*): Ambiente virtualizado na Azure que oferece diversos sistemas operacionais como Windows e Linux.

Banco de Dados SQL (*PaaS*): Banco de dados utilizado para armazenagem das informações de forma estruturada.

Balanceador de carga: Permite balancear o tráfego interno entre os componentes como máquinas virtuais e bancos de dados, por exemplo.

Usamos o cálculo presente na figura 3 abaixo para chegar na disponibilidade total para o ambiente proposto, calculando a redundância em caso de falha para ambientes ligados em paralelo.



Disponibilidade = I - não disponível
I - ambos não disponível =
I - (A não disponível) x (B não disponível) =
I - 0.1 * 0.1 = 0.99 ou 99%

Figura 3: Cálculo de disponibilidade para ambientes em paralelo.

Fonte: Rosário (2018)

Usando o cálculo proposto e usando duas regiões da Azure com disponibilidade por zona de 99.93% a disponibilidade total para ambientes ligado em paralelo de 99.99% de disponibilidade esperada, cumprindo assim a disponibilidade esperada pelos acionistas, diretores e líderes de negócio da organização.

A topologia do ambiente está apresentada a seguir demostrando os componentes e regiões utilizadas para cumprir o a arquitetura, desenho e disponibilidade esperados para o ambiente de aplicações. Para balanceamento da entrada de dados foi utilizado o serviço de gerenciamento de tráfego da Azure para garantir o redirecionamento de dados em caso de virada para o ambiente secundário.

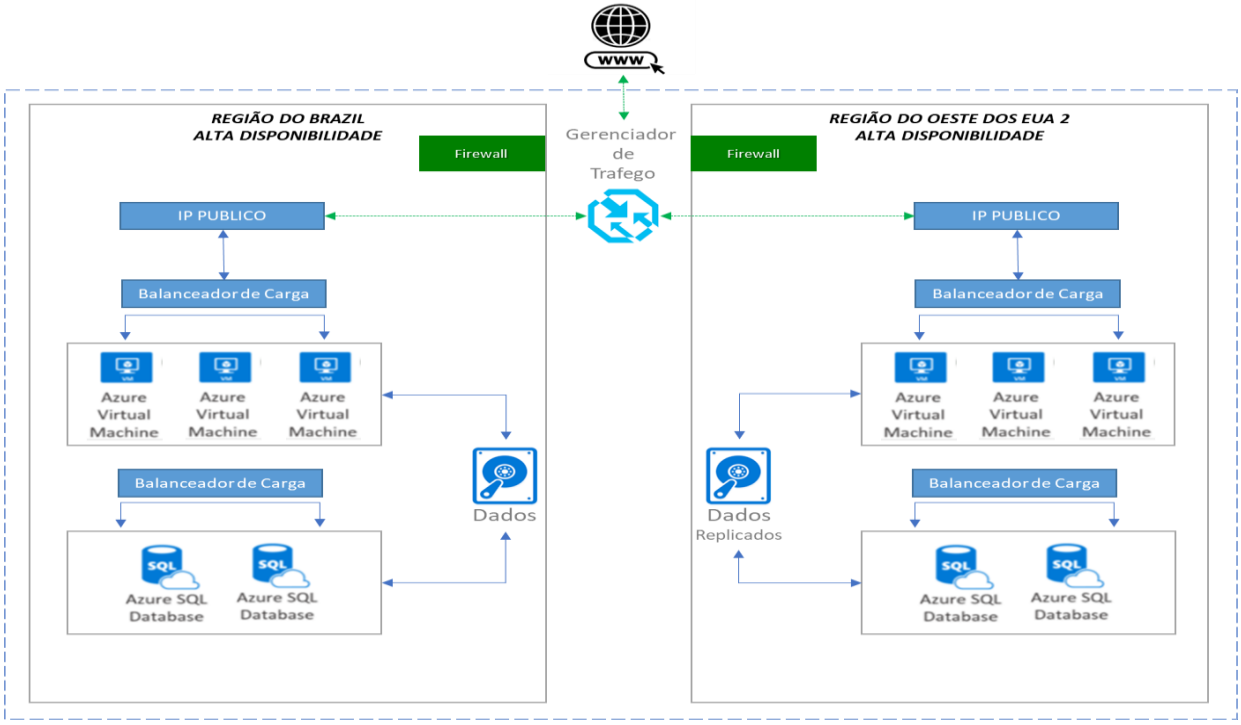


Figura 4: Topologia do Ambiente na Azure

Fonte: Rafael Ferrão (Autor)

3 CONCLUSÕES

Analisando as premissas necessárias para um modelo de alta disponibilidade esperado pela empresa, usando como referência os sistemas abordados neste artigo (Sistemas de Remessa, Pagamento, Financeiro e Vendas) e analisando os serviços de nuvem ofertados pela Microsoft atualmente no Brasil. Podemos concluir que a ausência de uma segunda zona de disponibilidade no Brasil não garante o nível de disponibilidade esperado, sendo necessário a implementação de um serviço de recuperação de serviço entre duas regiões.

Usando de referência a tabela 1 que mostra a disponibilidade exigida para o ambiente, o modelo de recuperação de serviço usando o Serviço de recuperação da Azure apresentado neste artigo garante um nível de disponibilidade esperado para os sistemas mais críticos da companhia, seguindo todas as normas de resiliência, disponibilidade e proteção de dados presentes atualmente hoje no mercado.

A implementação desses serviços traz uma nova camada de complexidade, porque apesar de não haver mais preocupações com a camada física como manutenção de servidores ou compra de novos equipamentos, por exemplo, somente uma migração de serviço sem levar em consideração, qual será a arquitetura implementada, o nível de serviço contratado e a estratégia de cópia de dados, podem não garantir que empresa alcance o nível de serviço esperado e não garantindo a restauração dos serviços em caso de uma eventual indisponibilidade da região onde o serviço está hospedado. Este cenário pode trazer grandes impactos operacionais, afetando a qualidade e a disponibilidade das aplicações.

Neste artigo ainda foi apresentado que hospedar os serviços em outra região, como por exemplo, nos Estados Unidos cumpre com as regulamentações do Banco Central, por haver acordo entre os países para troca de informações.

Pode se concluir então que para a migração de serviços para um ambiente em nuvem, deve ser realizado uma análise dos contratos dos provedores para entender quais são os níveis de disponibilidade ofertados e quais são as estratégias e serviços que podem ser adotados para aumentar os níveis de serviço e garantir que a arquitetura e o desenho do ambiente cumpram com as expectativas esperadas de confiabilidade e segurança.

REFERÊNCIAS

AZURE. **SLA para Máquinas virtuais**, Disponível em: https://azure.microsoft.com/pt-br/support/legal/sla/virtual-machines/v1_9/ , acessado em 05 de setembro de 2020.

AMORIM. Robson Soares. **IaaS, PaaS e SaaS.. Qual a diferença?**, Disponível em: https://www.lambda3.com.br/2017/08/iaas-paas-e-saas-qual-a-diferenca/, acessado em 05 de setembro de 2020.

CHRISTIANINI. **Plano de continuidade operacional: o que é e qual a importância?.** 2018. Disponível em: < https://www.abf.com.br/parceiros-do-franchising/cloud-computing-e-continuidade-de-negocios/ >. Acesso em: 30 de agosto de 2020.

GROSMANN, Luis. **Banco Central autoriza nuvem no exterior, desde que tenha acesso a dados**, Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm, acessado em 17 de setembro. de 2020.

OLIVEIRA, Alexsander. **A importância do Plano de Continuidade** , Disponível em: http://www.itsmnapratica.com.br/a-importancia-do-plano-de-continuidade , acessado em 05 de setembro. de 2020.

OLIVEIRA. Wallace, **O plano de continuidade de negócios garante o funcionamento das empresas em emergências**, Disponível em: https://www.venki.com.br/blog/plano-de-continuidade-de-negocios/ , acessado em 05 de setembro. de 2020.

MICROSOFT, **Matriz de suporte para recuperação de desastre de VM do Azure entre regiões do Azure**, Disponível em: https://docs.microsoft.com/pt-br/azure/site-recovery/azure-to-azure-support-matrix, acessado em 17 de setembro. de 2020.

MICROSOFT, **Conceitos de alta disponibilidade e recuperação de desastre no SharePoint Server**, Disponível em: https://docs.microsoft.com/pt-br/sharepoint/administration/high-availability-and-disaster-recovery-concepts, acessado em 17 de setembro. de 2020.

ROSÁRIO, Djan de Almeida do. **Disponibilidade e qualidade Operacional de Datacenters**: Livro Digital. Unisul Virtual: Palhoça, 2016. 70 p.: il.; 28 cm.

SOFTLINE. **Cloud Computing e continuidade de negócios.** 2014. Disponível em: < https://brasil.softlinegroup.com/sobre-a-empresa/blog/plano-de-continuidade-operacional-o-que-e-e-qual-a-importancia>. Acesso em: 30 de agosto de 2020.

TECLOGICA. **RTO e RPO: entenda o que são e qual a sua importância**, Disponível em: https://blog.teclogica.com.br/rto-e-rpo-qual-a-importancia/ , acessado em 05 de setembro de 2020.

TRES, Carlos Henrique. **BIA (Business Impact Analysis) – Por que ela é tão importante**, Disponível em: https://www.profissionaisti.com.br/bia-business-impact-analysis-por-que-ela-e-tao-importante, acessado em 05 de setembro de 2020.

WEYN, Dandy. **Disaster Recovery Of Zone Pinned Azure Virtual Machines To Another Region**, Disponível em: http://ilikesqldata.com/disaster-recovery-of-zone-pinned-azure-virtual-machines-to-another-region/ , acessado em 05 de setembro de 2020.