Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Física

Gabriel Donizeti Candido

Uma revisão de melhores práticas de segurança na Azure

São Carlos
27 de Março de 2023

Universidade Federal de São Carlos
Centro de Ciências Exatas e Tecnológicas
Departamento de Física

Uma revisão de melhores práticas de segurança na Azure

Trabalho de Conclusão de Curso apresentado à Coordenação do curso de Engenharia Física da Universidade Federal de São Carlos como requisito para obtenção do título de Bacharel em Engenharia Física.

Orientador: Prof. Dr. Fernando Manuel Araújo Moreira

São Carlos
27 de Março de 2023

Resumo

O texto trata sobre conceitos de segurança da informação do ponto de vista de nuvem (*cloud*) e utiliza a Azure como provedora de exemplo. São contextualizadas as definições de serviços de infraestrutura, plataforma e software, com exemplos com base na provedora escolhida, como máquinas virtuais, bancos de dados SQL e serviços de aplicativo Web. Também são apresentados conceitos introdutórios sobre segurança da informação, como os *frameworks* de segurança e os principais tipos de ataques cibernéticos seguindo a lista do OWASP, uma organização mundial para segurança de aplicações. E juntando os conceitos de nuvem com os de segurança, são ilustrados alguns recursos oferecidos pela Azure para proteger aplicações em nuvem.

Como aplicação dos conceitos, é apresentado uma arquitetura de um projeto real e sua descrição "*as is*". O projeto trata de um fluxo de dados envolvendo *Azure Data Factory*, *Azure Databricks*, *Azure Storage Account*, *SQL Server*, *APP Service* e outros recursos de nuvem. É realizada uma análise do ponto de vista da segurança, e então é apresentada uma proposta de solução para a resolução dos pontos falhos.

Os principais pontos apresentados como solução são a utilização de redes virtuais isoladas, com exposições estratégicas na internet através do Azure Application Gateway e do Azure VPN Gateway, bem como a utilização de *firewall* como o *Web Application Firewall* (WAF), a utilização de ferramentas de gestão da identidade como o *Azure Active Directory* (AAD), e de controle de segredos como o *Azure Key Vault*.

Por fim, conclui-se que a redundância de políticas de segurança contribui para a criação de uma solução em nuvem mais segura, e que isolar o ambiente da internet utilizando redes virtuais e aplicando políticas de *Firewall* e políticas de acesso mínimo dificulta o acesso de invasores. Conclui-se também que ao provisionar uma solução em nuvem, grande parte da responsabilidade é compartilhada com a provedora, que já possuí soluções muito bem testadas e validadas de segurança e, portanto, diminui os riscos de ações de *hackers*.

Conteúdo

1 Introdução

1.1 Motivações

Um ataque cibernético é uma tentativa de roubo ou sequestro de informação bem como de prejudicar o fornecimento de determinados serviços por sistemas computacionais de pessoas ou organizações. Os objetivos por trás do ato envolve a obtenção de informações sigilosas, sequestro de dados (*ransomware*) cruciais sob controle de empresas mediante o pagamento de resgate, ataques de negação de serviço (DDoS, do inglês *Distributed Denial-of-Service*), entre outros. Alguns casos recentes (2021) são os ataques de *ransomware* na *CNA Financial*, que custou à empresa cerca de US$ 40 milhões; e os roubos de criptomoedas no valor de US$ 15,6 milhões da *Inverse Finance* e US$ 625 milhões da *Ronin Network*. No Brasil, os dados também são preocupantes. [1]

Segundo dados da Fortinet, empresa de soluções de segurança cibernética, o Brasil registrou um total de 31,5 bilhões de tentativas de ataques cibernéticos no primeiro semestre de 2022. Este número é 94% maior em comparação com o mesmo período do ano anterior e torna o Brasil o segundo país da América Latina a receber mais ataques, ficando atrás somente do México, com 85 bilhões. No Brasil, pode-se citar o ataque às Lojas Renner e ao CVC, impedindo o fornecimento dos serviços por algumas horas e por cerca de 12 dias, respectivamente; e o roubo de dados pessoais de mais de 200 milhões de brasileiros sob o controle da *Serasa Experian*. [2, 3]

Neste cenário de tendência de ataques cibernéticos, a melhora das tecnologias de computação através das ferramentas de Big Data e processamento em paralelo pode atuar como catalisador. Recentemente, a *Google Cloud Platform* (GCP), registrou um ataque DDoS a um de seus clientes de 46 milhões de requisições por segundo (RPS, *request per second*). A fim de comparação, este número de requisições é o equivalente ao que a *Wikipedia* recebe em um dia, porém no período de 10 segundos. [4]

Faz-se necessário a contínua melhoria, entendimento e aplicação das ferramentas de segurança, e em especial, das ferramentas de segurança de e para soluções desenvolvidas em nuvem, onde a fácil escalabilidade de recursos pode ser um fator de risco para a segurança da informação.

1.2 Microsoft Azure

Segundo o último relatório anual (2021) publicado pelo *Gartner*, que é uma das maiores referências em tecnologia do mundo, as três maiores empresas provedoras de nuvem do mercado são a *Amazon Web Services* (AWS), a *Microsoft Azure* e a *Google Cloud Platform* (GCP). Este estudo levou em consideração critérios como habilidade de execução (do inglês, *ability to execute*) e completude da visão (*completeness of vision*), para classificar provedoras de nuvem em quatro categorias: líderes (*leaders*), visionárias (*visionares*), atuantes em um nicho específico (*nishe players*) e desafiantes (*chalengers*). [5]

É importante destacar que como a Azure é tema deste texto, sempre que possível os conceitos serão ilustrados através de figuras e recursos encontrados na documentação da própria *Microsoft*. Porém, também é válido dizer que muitos destes recursos possuem seus semelhantes em outras provedoras de nuvem, como a AWS ou a GCP. Por exemplo, a Azure possui um recurso para Armazenamento de *Blob*, que seria o armazenamento de arquivos em geral. Este serviço é ofertado pela Azure através de uma conta de armazenamento (do ingês, *Storage Account*), que possuí seu similar na AWS sob o nome de S3 e na GCP de *Google Storage*.

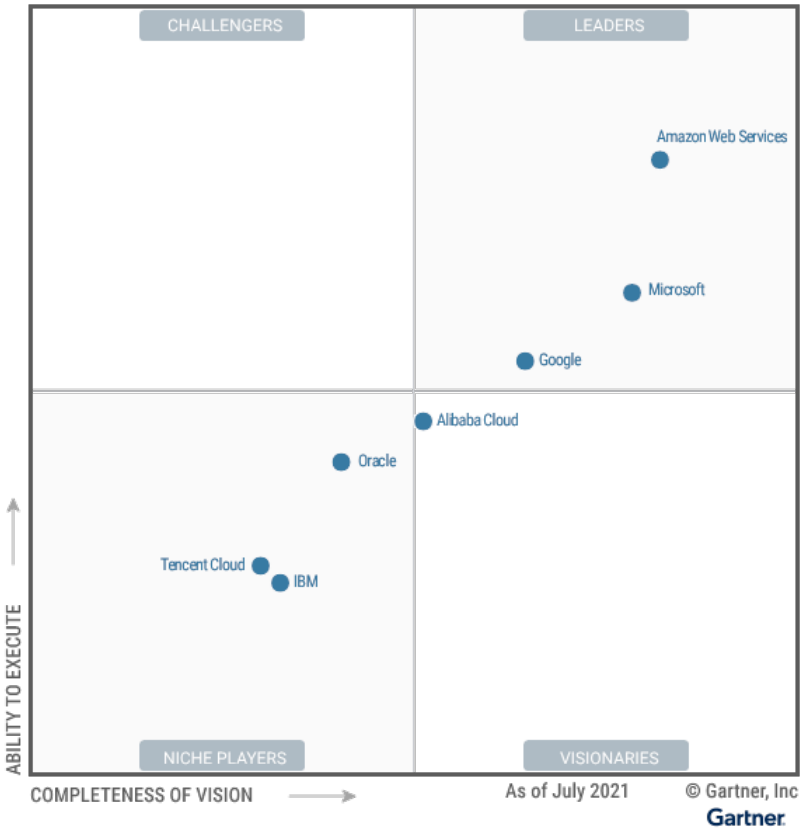

Figura 1: Quadrante Mágico para Infraestruturas em Nuvem e Serviços de Plataformas[5]

Observa-se pelo quadrante da imagem 1 que a Microsoft é uma das principais provedoras de nuvem do mercado, ficando atrás somente da AWS. A seguir serão explanados os conceitos de computação em nuvem com exemplificações no ambiente da Azure.

2 Fundamentos Teóricos

2.1 Fundamentos de Computação em Nuvem

O termo computação em nuvem é utilizado em um contexto onde recursos computacionais como *hardwares* e *softwares* são administrados por uma provedora e contratados por um usuário final. Este usuário não tem acesso físico aos recursos, porém é capaz de interagir através da internet por meio de assinaturas, onde a mais comum é no formato pague conforme o uso (do inglês, *pay as you go*), podendo haver também contratos específicos dependendo das necessidades da empresa contratante. A figura a seguir ilustra os tipos de recursos computacionais que uma provedora, no caso a Microsoft, pode ofertar. [6, 7]

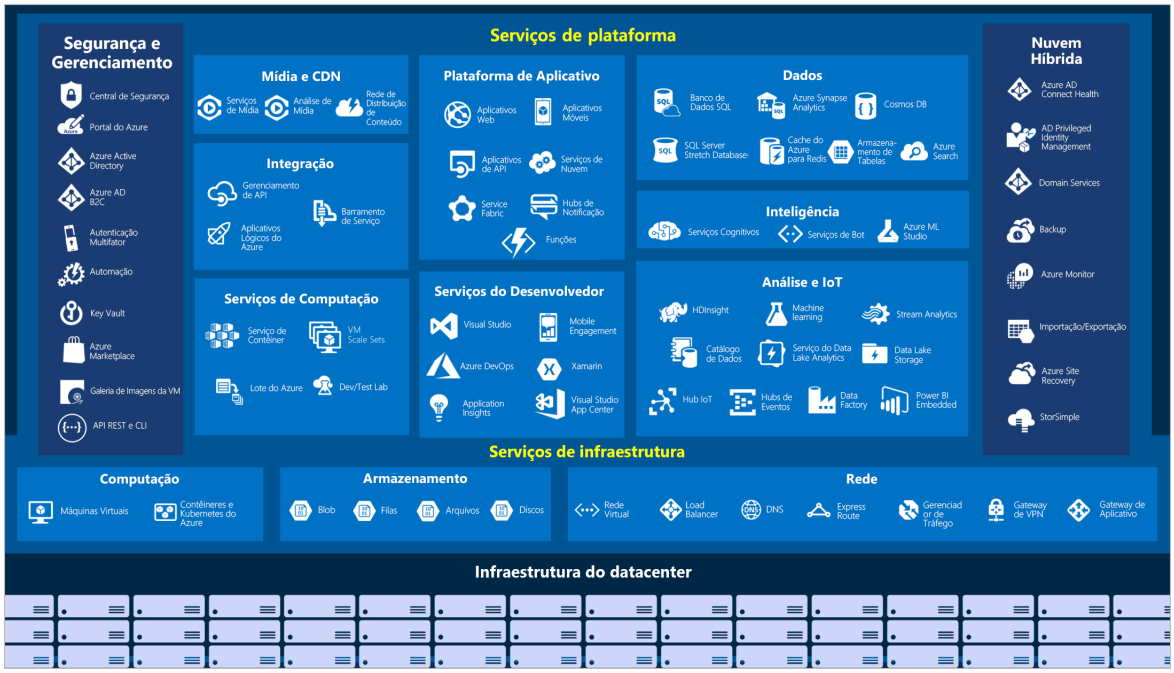

Figura 2: Soluções de IaaS, PaaS e SaaS, oferecidas pela *Microsoft*. [6]

Na parte inferior da Figura 2, é ilustrado como infraestrutura física os datacenters responsáveis por atender às demandas computacionais. Quado estes datacenters são compartilhados pelos clientes da provedora, a nuvem é chamada de Nuvem Pública. Caso o cliente possuí regulamentações específicas de segurança e necessite de um ambiente dedicado, a nuvem é chamada de Nuvem Privada. É possível também haver uma mesclagem entre estes dois níveis de funcionamento, chamando-se Nuvem Híbrida. O leitor pode verificar na parte superior direita da Figura 2 que a Azure possuí alguns serviços específicos para este nicho, como serviços de *backup*, de exportação e importação de arquivos. [8]

Ainda analisando a Figura 2, é possível notar também as categorias Serviços de Infraestrutura (IaaS, *Infrastructure as a Service*) e Serviços de Plataforma (PaaS, *Platform as a Service*). Essas categorias, mais os Serviços de Softwares (SaaS, *Software as a Service*) são os tipos de implantações de soluções em nuvem e a diferença entre elas se dá principalmente pelo compartilhamento da responsabilidade. A figura a seguir ilustra a divisão de responsabilidade entre a empresa contratante e a provedora. [9]

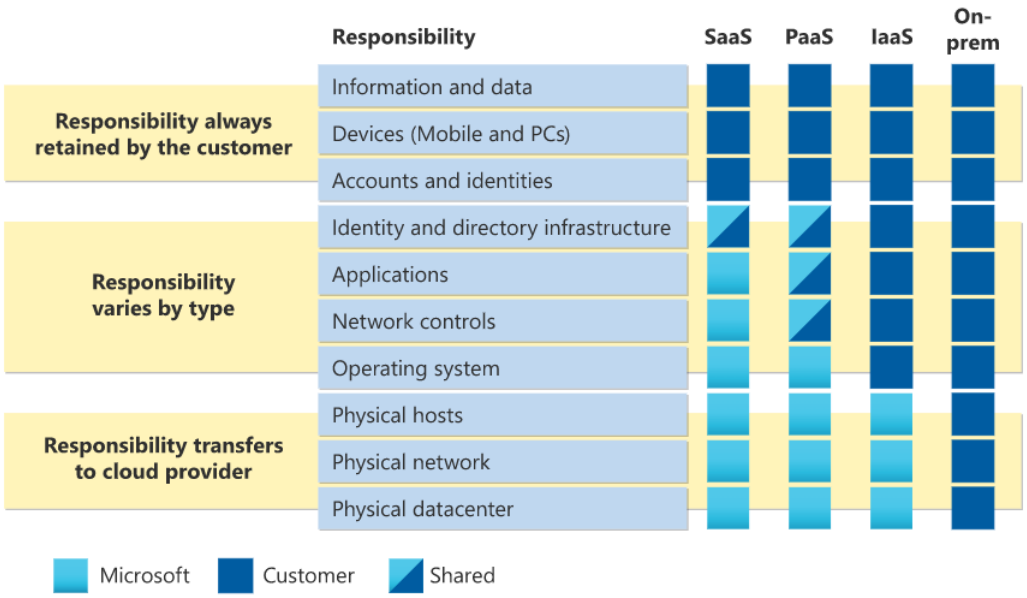

Figura 3: Divisão da responsabilidade sobre os serviços contratados de acordo com suas classificações em IaaS, PaaS e SaaS. [9]

Observe na figura acima que quando o ambiente está totalmente *On-premise*, isto é, no *datacenter* local do cliente e sem auxílios de nuvem, toda a responsabilidade sobre os serviços e dados é do cliente. Porém, quando algumas soluções passam a ser migradas para a nuvem, seguindo os níveis de infraestrutura (IaaS), plataforma (PaaS) e até mesmo *softwares* (SaaS), parte da responsabilidade passa a ser compartilhada com a provedora. Isso é importante do ponto de vista da segurança da informação, pois o cliente precisa saber que somente parte da responsabilidade é compartilhada, e não toda ela. Por exemplo, se um SQL Server, que é um banco de dados relacional, é provisionado na Azure na configuração de PaaS, a Azure irá fornecer a infraestrutura com os datacenters, o gerenciamento do servidor e a atualização dos *patches* de segurança para que ele fique ligado de acordo com o contrato de nível de serviço (SLA, *Service Level Agreements*). Porém, se o cliente criar um usuário para este servidor e disponibilizá-lo publicamente na internet, dependendo das regras de *Firewall* para acessar este banco, a solução ficará vulnerável. [6]

O tema de segurança será abordado com mais profundidade nos próximos capítulos. Agora, trataremos de conceitualizar os termos IaaS, PaaS e SaaS, bem como exemplificar, para que o leitor se familiarize com os tipos de serviços que são ofertados por uma provedora de nuvem, em especial pela Azure.

2.1.1 Infraestrutura como Serviço (IaaS)

Os serviços de infraestruturas fornecidos pela Azure são categorizados principalmente em três tipos: Computação, Armazenamento e Rede. Através destes tipos de serviço, os clientes da provedora acessam recursos básicos de computação e são cobrados de acordo com o uso destes recursos.

Por se tratarem de recursos de infraestrutura, grande parte da responsabilidade é compartilhada com o cliente. E a principal responsabilidade da provedora é garantir os recursos físicos,

como os datacenters e as redes. As responsabilidades decorrentes de controle de tráfego, identidade de acesso e tratamento de dados, por exemplo, é compartilhada com o cliente. [9]

A seguir serão abordados alguns exemplos de recursos de computação, armazenamento e rede.

Computação

Alguns exemplos de serviços de infraestrutura de computação oferecidos pela Azure são as Máquina Virtuais (VMs, *Virtual Machines*), o *Azure Kubernetes Service* (AKS) e o *Azure Functions*. Tratam-se de recursos de infraestrutura escalonáveis sob demanda e pagos conforme o uso. [6]

Imagine que você, leitor, executará um certo trabalho em seu computador pessoal. Este trabalho será realizado em um *software* considerado "pesado", isto é, que ocupa bastante espaço da memória. Imagine que o seu computador tenha 8 GB de memória RAM e que ao executar o *software*, ele trava por um tempo indeterminado. Então, você entra no site do fabricante do *software* e descobre que a configuração mínima para execução é de 64 GB de RAM. O que você faz? Você pode comprar um computador de 64 GB de RAM e pagar algo em torno de R$ 10.000,00 para executar uma atividade de algumas horas e depois ter um computador muito bom porém sem muita utilidade, ou contratar uma VM de 64 GB de RAM na Azure, por exemplo, por umas 3 horas, executar a sua tarefa e depois eliminar o recurso. Neste caso, o custo seria de aproximadamente R$ 21,65, conforme mostra a imagem abaixo. [10]

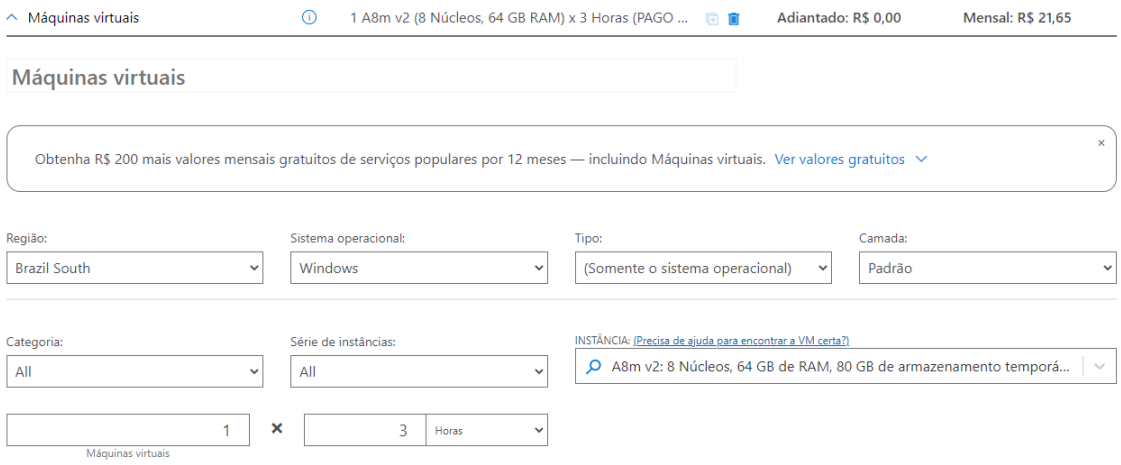

Figura 4: Estimativa de custo de uma VM do tipo A8m V2 para 3 horas de uso, realizado na calculadora de preços da Azure. [10]

O caso descrito acima é um dos exemplos de uso de uma VM, não só na Azure mas em qualquer outra provedora de nuvem. Mas agora imagine que você é um desenvolvedor e está construindo uma aplicação escalonável para uma loja que fará uma grande promoção na inauguração. Você percebe que o caso descrito no parágrafo anterior não seria uma solução adequada pois apesar do escalonamento vertical (de 8 para 64 GB de RAM) você calcula que o número de requisições seria tão alto que o sistema ficaria sobrecarregado do mesmo jeito. Então, você decide provisionar uma solução mais robusta para a sua aplicação, que não utiliza somente um

recurso de computação, porém vários. Ou melhor, vários nós de computação gerenciados por um nó central. Aqui, entramos no caso do *Azure Kubernetes Service*. [11]

O Kubernetes é um serviço de orquestração de contêineres que automatiza o dimensionamento, implantação e gerenciamento de aplicativos em container. O Kubernetes pode ser implantado em máquinas locais e utilizar os recursos instalados localmente para escalar a aplicação conforme necessário. Porém, o diferencial de provisionar um recurso desse tipo em uma provedora de nuvem é justamente o poder de escalonar rápido e fácil sem a necessidade de construir e gerenciar um *data center* físico. Por tanto, no exemplo do parágrafo anterior, após a promoção, os recursos podem ser desalocados e a fatura cobrada somente pela quantidade de recursos consumidos. [12]

O último exemplo mencionado para recursos de computação do tipo IaaS é o *Azure Functions*. Neste caso, o desenvolvedor trabalha somente com o bloco de código que precisa ser executado e a Azure aloca os recursos computacionais necessários seguindo a politica de escalonamento definida. [13]

Armazenamento

Os recursos IaaS de armazenamento, como o próprio nome sugere, é focado em armazenar dados e programas de um cliente Azure. Por exemplo, a VM que comentamos na seção de recursos de computação é provisionada junto com um disco gerenciado (*Azure Managed Disks*). Esse disco, por sua vez, é a abstração de um disco físico e pode ser do tipo SSD (unidades de estado sólido) *Premium*, *SSDs Standard* e HD (unidades de disco rígido). Ele pode ser utilizado como o disco da VM, e tambem como um *backup* caso o usuário decida restaurar essa VM em um momento futuro. [14]

Outro exemplo de recurso de armazenamento muito utilizado em nuvem é o Blob (*Binary large object*) (vide a parte de Armazenamento da figura 2). Trata-se de uma conta de armazenamento (*Storage Account*) utilizada para armazenar arquivos em geral. No caso da Azure, as contas de armazenamento de uso geral do tipo v2 permitem a gestão destes blobs em um sistema de diretórios, muito utilizados na estrutura de *Datalakes*. A figura a seguir ilustra uma conta de armazenamento para um projeto típico de engenharia de dados, onde os arquivos (blobs) são estruturados nas camadas de *staging* (dados sem tratamento), *int* (dados com um certo nível de tratamento) e *report* (dados prontos para consumo). [15]

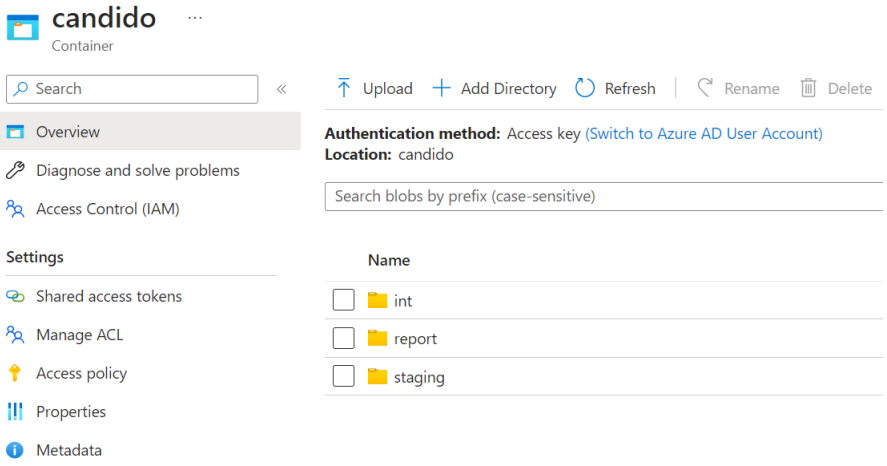

Figura 5: Estruturação de um Datalake utilizando Storage Account. Fonte: o autor.

A figura acima apresenta a visão de um container ("candido") de um *Storage Account* visto do Portal da Azure. Dentro deste container é possível estruturar os dados em diretórios como se fosse um sistema de arquivos local.

Os dados podem ser armazenados nessas contas de armazenamento nos níveis de acesso *hot*, *cool*, e *archive*. No *hot*, costuma-se armazenar dados que são consultados e atualizados com frequência. O custo de acesso é menor e o de armazenamento é maior. No *cool*, costuma-se armazenar dados pouco acessados. Neste nível, o custo para acesso é maior e o de armazenamento é menor. E o *archive* é utilizado para armazenar dados que são raramente consultados. [16]

Rede

Os serviços de rede da Azure são outro tipo de soluções IaaS. Na imagem 2, pode-se notar recursos como Rede Virtual, *Load Balancer, Express Route, Gateway de VPN*, entre outros, que exemplificam esse tipo de serviço.

A Rede Virtual do Azure (Vnet) é um serviço de rede privada na nuvem que permite uma comunicação segura entre outros recursos. Ela permite o isolamento destes recursos de forma a evitar ataques cibernéticos. Porém, muitas vezes é importante que estes recursos isolados acessem objetos fora da rede. Estes objetos podem ser, por exemplo, a própria internet, um computador local ou até mesmo uma outra rede virtual. Por padrão, os recursos de uma rede podem se comunicar com a internet na saída, ou seja, se você estiver logado em uma máquina virtual que está associada a uma rede, por padrão você conseguirá acessar a internet com essa máquina. Porém, para que ocorra o tráfego de entrada é necessário a criação de um IP público ou de um *Load Balancer* (Balanceador de Carga) público. Estes últimos podem também ser utilizados para gerenciar as configurações de saída dessa rede. [17]

O tema de redes é extremamente importante do ponto de vista de segurança da informação, e por esse motivo, alguns recursos de rede como Redes Virtuais Privadas (VPN), *Express Route*, e pontos de extremidade de serviço de rede virtual, serão melhor tratados no capítulo seguinte.

2.1.2 Plataforma como Serviço (PaaS)

Os serviços de plataforma também utilizam a infraestrutura da provedora de nuvem porém oferece algumas funcionalidades a mais. Por exemplo, imagine que você precisa implantar um banco *SQL Server* para armazenar alguns dados de negócios de uma empresa qualquer, porém você está cogitando implantar esse banco utilizando a nuvem. Uma das opções seria utilizar uma VM da Azure, que é um IaaS. Você logaria nessa VM utilizando *Secure Shell* (SSH) ou RDP (*Remote Desktop Protocol*) e então instalaria um servidor SQL. Então você instalaria também o SSMS (*Sql Server Management Studio*) para fazer a gestão dos bancos no novo servidor instalado. De tempos em tempos, você precisaria fazer manutenção neste servidor para garantir que ele continue funcionando com um certo nível de segurança. Porém, existe um caminho um pouco mais simples, que seria instanciar um *Azure SQL Server*. Ao invés de criar uma VM e então instalar o servidor, você instância o próprio servidor. Agora, a responsabilidade por manter o servidor funcionando é da provedora de nuvem. Você só precisa configurar um usuário administrador e fazer a gestão de negócio em si dos seus bancos de dados. Além disso, não seria nem necessário um SSMS, você poderia acessar as funcionalidades dos bancos através do próprio portal da provedora. Essa é a vantagem de um serviço de plataforma com relação ao IaaS. [18]

Na Azure existem vários serviços de plataforma, como pode ser observado na imagem 2. Outro exemplo bastante interessante é o *Azure App Service* (Aplicativos Web, na figura). Com ele, é possível realizar a publicação de um site e escalar sob demanda, por exemplo. O cliente poderia desenvolver todo o site no próprio computador e ao publicar, ele garante que independente da quantidade de usuários que haverá no site, ele terá capacidade computacional suficiente para atender essa demanda, o que não ocorreria se ele utilizasse o próprio computador para essa publicação. Além disso, ele abstrai grande parte da gestão do tráfego para a provedora e pode focar o seu tempo em outras atividades. Aqui, do ponto de vista da segurança, cabe uma ressalva. A escalabilidade de uma aplicação não pode ser ilimitada. No caso de um ataque de negação de serviço (DDOS), por exemplo, onde inúmeros robôs acessam a página simultaneamente, a página pode não suportar e cair, e o site não atender os usuários reais, ou a página pode suportar e escalar de forma desnecessária, podendo fazer com que a empresa tenha um enorme prejuízo. [19]

2.1.3 Software como Serviço (SaaS)

Os serviços do tipo SaaS são os mais comuns no dia a dia das pessoas. Neste caso, toda a infraestrutura e gerenciamento da plataforma é abstraída do usuário e o que ele contrata é um aplicativo em si. Muitos serviços SaaS são ofertados gratuitamento, como as ferramentas de email e o Microsoft Office 365. Algumas outras ferramentas são pagas, como sitemas de gerenciamento de clientes (CRM), sendo um dos mais populares o SAP, e sistemas de gerenciamento empresarial (ERP), onde podemos citar o *SalesForce*. Nos serviços SaaS, a principal responsabilidade de segurança a nível de cliente, é restringir o acesso utilizando a política de acesso mínimo, isto é, o usuário poder acessar somente o que ele precisa para realizar as suas atividades. Outras configurações, como o isolamento dos recursos em uma rede, serão tratadas de maneira geral no decorrer do texto.

2.2 Fundamentos em Segurança da Informação

2.2.1 Frameworks de Segurança e Lei Geral de Proteção de Dados

Um *framework* de segurança da informação é uma ferramenta que ajuda uma empresa a atender os princípios básicos da segurança da informação. Os três princípios básicos são:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Estes princípios garantem que a informação seja acessada somente por pessoas autorizadas (confidencialidade), que seja alterada somente por pessoas autorizadas (integridade) e que esteja sempre disponível pelas pessoas autorizadas (disponibilidade). [20]

Existem vários *frameworks* disponíveis no mercado e também certificações para que as empresas comprovem publicamente que estão aplicando as políticas de segurança definidas nesses *frameworks*. Alguns exemplos de *frameworks* de segurança da informação são a ISO 27001, que é uma referência internacional para a Segurança da Informação; o CIS (*Center of Internet Security*) *Controls*, uma organização sem fins lucrativos que possui um conjunto de 20 controles tecnológicos e de processos de segurança da informação; e também podemos citar o *NIST Cyber Security Framework*, voltado para empresas privadas dos Estados Unidos. [21, 22]

Do ponto de vista de nuvem, e mais especificamente da Azure, somente alguns recursos disponibilizados atendem totalmente ou parcialmente às definições de segurança impostas pelos principais *frameworks* do mercado, como o CIS e o NIST cidados acima. Porém, isso não garante a adequação completa a elas, visto que seria necessário um processo de certificação interno da empresa. [23]

Este texto não tem por objetivo passar por todos pontos necessários para a certificação nos *frameworks*, porém estabelecer um caminho inicial de melhores práticas utilizando ferramentas da Microsoft para garantir a segurança da informação de soluções provisionadas na Azure.

Do ponto de vista de segurança da informação, mais precisamente em relação a dados, em 2018 entrou em vigor no Brasil a Lei Geral de Proteção de Dados (LGPD) que regulariza o processo de tratamento de dados pessoais em território nacional ou que foram extraídos em território nacional. A lei tem por objetivo garantir ao titular dos dados direitos como o acesso aos dados, à alteração destes dados caso seja necessário, e que exista uma finalidade pautada na lei para o tratamento dos dados, como a finalidade legítima da empresa para oferecer seus serviços, cumprimento de obrigação legal, proteção da vida, entre outros. [24]

Dentre as obrigações de uma empresa que controla dados de pessoas físicas, destaca-se a importância de garantir que os dados não sejam expostos a pessoas não autorizadas, logo a aplicação de políticas de segurança além de evitar ataques de infraestrutura e de negócios às empresas, é uma medida de garantir o cumprimento da LGPD.

2.2.2 Tipos de Ataques Cibernéticos

A imagem a seguir ilustra os 10 principais tipos de ameaças cibernéticas listadas pelo OWASP (*Open Worldwide Application Security Project*), uma organização sem fins lucrativos dedicada

a segurança de aplicativos Web. [25].

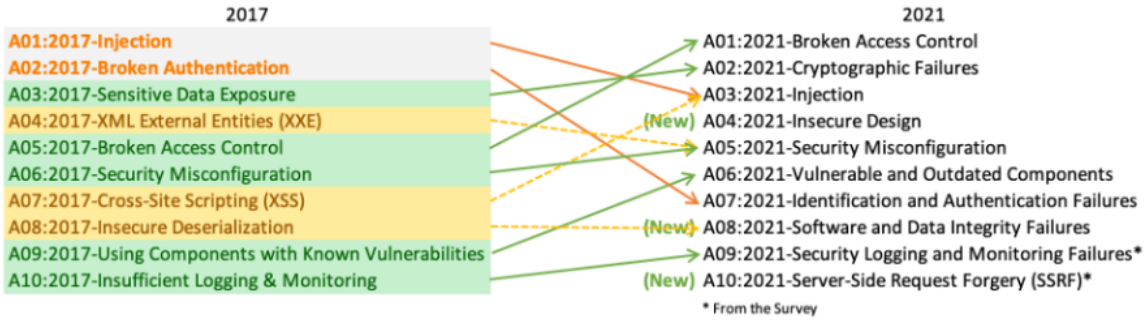

Figura 6: Evolução dos 10 maiores riscos cibernéticos entre os anos de 2017 e 2021 segundo o OWASP. [25]

Observe que muitos dos ataques listados na imagem 6 ocorrem do lado do servidor e do gerenciamento de softwares (A02, A08 e A10). Porém, é importante notar que o principal risco ocorre a nível de acesso (A01 - *Broken Access Control*). Neste caso, soluções e dados estão sendo acessados por pessoas não autorizadas. Muitos são os fatores que contribuem para isso, como por exemplo, a regra do privilégio mínimo. Destaca-se também na figura que um dos principais ataques é o de injeção SQL. Neste ataque, o *hacker* insere através de *inputs* de dados da aplicação *scripts* SQL maliciosos que podem alterar dados do banco, corromper ou trazer informações confidenciais.

Outro ataque bastante comum que está listado na imagem 6 como *Cryptographic Failures*, é o de sequestro de dados. Neste ataque, o invasor acessa o ambiente e aplica uma criptografia que somente ele possui acesso à chave. Os fatores de riscos aqui são dois. Os dados podiam já estrar criptografados e o invasor não conseguiu entender o significado destes dados e somente impediu a vítima de utilizá-los, ou os dados não estavam criptografados e o invasor obteve acesso total aos dados, o que além de ser muito mais perigoso do ponto de vista de negócio, pois os dados podem conter informações confidenciais de negócio da vítima, viola a LGPD e pode trazer consequências sérias à empresa.

Para descrever melhor os principais riscos de segurança listados pelo OWASP, analisemos uma imagem retirada de um relatório de segurança para implantação de uma arquitetura em duas provedoras de nuvem, a Azure e AWS.

ATAQUE	DESCRIÇÃO	COMO PREVENIR?	SEVERIDADE	Recurso
Ataque de Negação de Serviço (DoS)	Realiza inúmeras solicitações ilegítimas a um site de modo que este seja incapaz de processar as solicitações legítimas.	Firewall para detectar solicitações ilegítimas.	Alta	AWS WAF; MFA.
Ataque de Negação de Serviço Distribuído (DDoS)	Semelhante ao DoS, porém os ataques são realizados a partir de várias máquinas hosts.	Firewall para detectar solicitações ilegítimas.	Alta	AWS WAF; MFA.
Ataques man-in-the-middle (MITM)	Intercepta mensagens entre pessoas/redes/computadores e as modificam de modo que as partes envolvidas (emissor/receptor) não tenham consciência disto.	Criptografia nos pontos de acesso e Rede Virtual Privada (VPN)	Alta	VPC Gateway; impor HTTPS.
Ransomware	O alvo faz o download de um Ransomware (malware) criado para explorar as vulnerabilidades e fica como refém até que concorde em pagar ao invasor um resgate.	Atentar-se aos sites visitados e utilizar firewalls do tipo NGFW.	Alta	Utilizar ferramentas de detecção de vulnerabilidades, como o Amazon Inspector; Implementar Política de Acesso Mínimo.
Ataques de Injeção de SQL	São consultas indevidas que ocorrem em bancos de dados utilizados por sites para atenderem seus clientes.	Utilizar modelos de privilégios mínimos.	Alta	VPC Gateway; AWS WAF.
Interpretação de URL	O invasor sabe a ordem em que as informações são inseridas na URL de um site e utiliza isso para acessar páginas que à priori não teria acesso.	Utilizar métodos de autenticação em páginas confidenciais do site bem como exigir Autenticação Multifator (MFA)	Alta	AWS Route 53; Tableau.
Falsificação de DNS (DNS Spoofing)	O invasor altera os endereços DNS para que os usuários do site enviem suas informações confidenciais para o endereço fraudulento.	Manter os endereços DNS atualizados.	Alta	AWS Route 53; Digital Certificate (AWS Certificate Manager).
Ataques de Força Bruta	É um tipo de ataque em que o invasor utiliza bots para tentar adivinhar usuários e senhas para invadir o sistema.	Não criar senhas triviais, utilizar protocolos criptográficos e bloqueios de senhas.	Média	WAF; AWS CloudWatch; MFA.
Web Attacks	Os hackers utilizam vulnerabilidades em aplicativos baseados na web para interceptar parâmetros enviados como requisição pelos usuários e os utilizam, por exemplo, em ataques de injeção de SQL.	Identificar e corrigir vulnerabilidades.	Alta	WAF; MFA; VPC Gateway.
Ameaças Internas	Ataques originados por pessoas que fazem parte da própria empresa e conhecem a arquitetura e têm credenciais de acesso aos vários ambientes.	Utilizar modelos de privilégios mínimos e MFA.	Alta	AWS CloudWatch; AWS Key Management Service; AWS IAM; Política de Acesso Mínimo.
Cavalos de Tróia	Trata-se de um programa malicioso escondido dentro de um programa legítimo. Este malware pode ser usado para abrir um backdoor para que os invasores acessem o sistema.	Não baixar e instalar pacotes de origens desconhecidas e utilizar firewall do tipo NGFW.	Alta	AWS WAF; VPC Gateway; Criptografia de duas camadas; MFA.
Ataques Drive-by	Um malware é inserido em um site não seguro de modo que quando um usuário acessa o site, já fica exposto ao ataque.	Garantir que as versões dos softwares estejam atualizadas.	Alta	
Cross-Site Scripting (XSS)	O ataque ocorre por meio da criação de um conteúdo clicável no navegador alvo, de modo que se o usuário clicar neste conteúdo o script do invasor é executado.	Criar uma lista de permissões de entidades permitidas.	Alta	Digital Certificate (AWS Certificate Manager).
Ataques de Espionagem	São ataques MITM em que o hacker intercepta o tráfego de uma rede de forma passiva (observa os dados) ou ativa (coleta os dados).	Criptografia nos pontos de acesso e Rede Virtual Privada (VPN)	Alta	VPC Gateway; AWS IAM; Comunicação SSL e HTTPS; Política de Acesso Mínimo.
Birthday	Tipo de ataque em que o invasor tenta identificar o hash utilizado pelo usuário para substituir a mensagem enviada ao servidor.	Utilizar hashes mais longos para verificação.	Média	AWS WAF; VPC Gateway.
Malware	É um software malicioso instalado em um computador alvo que altera o seu funcionamento, destrói dados, observa o comportamento do usuário ou do tráfego de rede.	Utilizar firewalls e verificar a integridade da origem do software.	Alta	AWS WAF; Serviços de Detecção de Vulnerabilidade (Amazon Inspector).
Spyeye	Invade navegadores de internet inserindo/alterando campos e registrando/pressionando teclas para coletar informações confidenciais dos usuários.	Identificar e corrigir vulnerabilidades.	Alta	Digital Certificate; Digital Certificate (AWS Certificate Manager).
Criptojacking	Roubo da capacidade de processamento através de scripts maliciosos executados no navegador do usuário. Geralmente utilizados para mineração de criptomoedas.	Visitar sites confiáveis e utilizar firewalls.	Alta	Aplicar criptografia de duas camadas.
Ataque DMA (Direct Memory Access)	Utilização de um meio periférico para acessar os dados de memória RAM de um servidor.	Utilizar proteções contra DMA como a fornecida pelo Windows.	Alta	Aplicar criptografia de duas camadas.

Figura 7: Descrição de um dos principais ataques cibernéticos e como prevení-los através de recursos em nuvem. Fonte confidencial.

Na imagem 7, apesar deste texto tratar especificamente de melhores práticas de segurança de nuvem no ambiente da Azure, os recursos da AWS foram mantidos para fins de comparação do leitor. A lista aborda os principais ataques cibernéticos que ocorrem hoje em dia, como prevenir no contexto de nuvem, qual a severidade e qual recurso pode ser utilizado para combater o ataque. Vale ressaltar que muitos dos ataques são prevenidos por padrão por alguns recursos das provedoras. Por exemplo, dificilmente um invasor conseguirá utilizar um *ransomware* para roubar dados de um *Storage Account*, visto que os dados são criptografados por padrão utilizando uma chave AES de 256 bits gerenciada pela Microsoft. Isto significa que mesmo que os dados sejam sequestrados, os sequestradores não conseguirão acessar esses dados pois eles estariam criptografados. E para eles sequestrarem a ponto do cliente não ter acesso, eles teriam que invadir a própria Microsoft. Caso as configurações de acesso por parte do cliente estiverem bem definidas, isto seria uma tarefa bem difícil. Aqui entra também a questão da responsabilidade compartilhada. Para um *storage* com criptografia em repouso, isto é, para os dados armazenados, a Azure gerencia uma chave e é de responsabilidade dela garantir a segurança dessa chave. É possível aplicar uma dupla camada de criptografia, ou seja, além da criptografia padrão, é possível criptografar novamente os dados através de uma chave gerenciada pelo cliente. Para um sequestrador de dados conseguir ler dados criptografados desta maneira, ele precisaria quebrar a chave do cliente e a chave da Azure. [26]

Na imagem 7 destaca-se também o ataque de negação de serviço. Neste tipo de ataque, vários *hosts* tentam acessar uma aplicação instanciada na nuvem e umas das maneiras de se evitar isso é através do *Multifactor Authentication* (MFA) habilitado no *Azure Active Directory* (AAD) e de um *Firewall*, como o *Web Application Firewall* (WAF). Neste caso, para o usuário logar na aplicação, é necessário passar por um segundo fator de autenticação, uma mensagem de texto no celular, por exemplo, para validar a sua identidade e só então acessar o serviço. Isso garante que a solução esteja sendo acessada somente por usuários autorizados e também evita ataques do tipo DDoS. Além disso, a Azure oferece serviços específicos para combater ataques DDoS, como o *Azure DDoS Protection*. Este é um recurso que pode ser aplicado em redes virtuais do Azure e fornecer uma proteção maior para a aplicação. É importante destacar que em termos de segurança, é preferível errar por redundância do que por escassez. [27, 28]

2.2.3 Princípios de Design de Segurança

Como observado na lista do OWASP para os principais riscos de segurança cibernética, um dos principais fatores é a não adoção dos princípios de Design de Segurança. Estes princípios descrevem como arquiteturas locais ou na nuvem devem ser implementadas de modo a minimizar os riscos envolvidos. De acordo com a Microsoft, estes princípios são [29]:

- Planejar recursos e como protegê-los;
- Automatizar e usar privilégios mínimos;
- Classificar e criptografar dados;
- Monitorar a segurança do sistema, planejar a resposta a incidentes;
- Identificar e proteger pontos de extremidade;

- Proteger contra vulnerabilidades de nível de código;
- Modelar e testar contra possíveis ameaças.

Gostaria de destacar o segundo item da lista acima, "Automatizar e usar privilégios mínimos". A quebra de acesso por pessoas não autorizadas em aplicações não ocorre somente por terceiros, ela pode ocorrer internamente dentro da própria empresa. A política de acesso mínimo específica que os usuários de um serviço devem acessar somente os recursos necessários para a execução de suas atividades. Por exemplo, se uma empresa aleatória utiliza um sistema interno para gerir a folha de pagamento dos seus funcionários, somente os usuários do RH, e talvez apenas alguns funcionários do RH, devem ter acesso a essa funcionalidade do site. Os outros usuários não deveriam poder acessar.

Da lista acima, destaque também para a criptografia de dados. Quando uma provedora de nuvem é contratada, muitos serviços que ela oferece já contém a criptografia de repouso por padrão e a em trânsito também. A criptografia em repouso já foi discutida neste texto. E por outro lado, a criptografia em trânsito garante que caso os dados sejam interceptados enquanto estão sendo movidos de um servidor a outro, o interceptador não conseguirá interpretá-los. Na criptografia de trânsito é necessário uma chave que apenas o emissor e o receptor conhecem. [30]

A identificação e proteção de pontos de extremidade de serviço é outro tema extremamente importante do ponto de vista de segurança da informação, em especial para proteção contra os ataques do tipo DDoS já comentados neste texto. Ao utilizar uma rede virtual por exemplo, o ambiente que foi provisionado na nuvem é isolado na internet. Os usuários que estão navegando na internet não conseguem nem visualizar os recursos internos da rede, tornando quase que impossível um ataque direcionado. Porém, neste caso nem mesmo as pessoas autorizadas conseguiriam acessar estes recursos, visto que o ambiente está completamente isolado. Porém, a utilização de IPs públicos podem abrir portas estratégicas, porém ainda com vários níveis de proteção, para que estes recursos possam ser acessados. Isto de certa maneira expõem o ambiente, porém de forma controlada.

No capítulo seguinte falaremos de alguns recursos da Azure que são utilizados por padrão ou que podem ser contratados para garantir que os requisitos de segurança sejam cumpridos em um nível confiável. Será falado também sobre como expor redes na internet com segurança na Azure.

2.3 Segurança da Informação na Azure

2.3.1 Controle de acesso aos dados

Um dos principais serviços da Azure que ajuda a garantir o controle de acesso aos recursos instanciados é o *Azure Active Directory* (AAD). Ele é um serviço de identidade que gerencia os usuários que estão acessando a plataforma e garante que eles são quem dizem ser e que estão acessando o que deveriam acessar. O AAD é usado não somente para recursos provisionados na Azure, mas também pode ser entendido como uma ferramenta externa para controlar acesso a aplicações externas à Azure.

Para que uma pessoa com um endereço de email tenha acesso a recursos instanciados na Azure, é necessário que ela seja convidada a fazer parte da organização que controla a assinatura. Ela então poderá acessar o serviço como usuário convidado ou usuário interno à organização. Após isso, outro usuário que tem privilégios para delegar funções pode aplicar funções específicas a este novo usuário. Estas funções definem o que o usuário pode fazer dentro da nuvem. A figura a seguir ilustra algumas dessas funções.

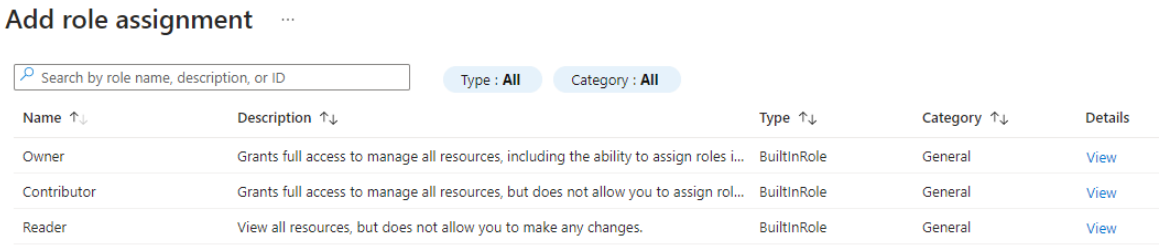

Figura 8: Lista parcial de funções aplicáveis a um usuário na Azure. Fonte: o autor.

De um modo geral, as funções podem ser aplicadas a nível de assinatura, de grupos de recursos ou de recursos. Se for aplicada a nível de assinatura, por exemplo, todos os grupos de recursos e recursos pertencentes à assinatura herdam a função aplicada. Se for aplicada a nível de grupo de recurso, os recursos internos do grupo herdam a função e se for aplicada a nível de recurso, somente o recurso recebe a função. Por exemplo, se em um grupo de recursos foi instanciada uma VM e um servidor SQL, e a função *Reader* for aplicada a um usuário qualquer ao grupo de recurso, este usuário poderá visualizar os dois recursos porém não poderá alterar nada. Se a função aplicada foi de Contribuidor, ele terá todos os acessos de *Owner* com a excessão de que não poderá aplicar acessos a outros usuários. A única diferença entre *Owner* e *Contributor*, a nível de grupo de recurso, é que o *Owner* permite a atribuição de funções a outros usuários, fora isso, o Contribuidor pode realizar qualquer coisa, como deletar recursos ou criar novos. [31]

Uma função que é interessante citar é a *SQL Security Manager*. Com essa função o usuário pode controlar a segurança do servidor instanciado, criando regras de exceção no *Firewall*, por exemplo. O caso do SQL ilustra outro ponto importante com relação a níveis de acesso para os recursos instanciados na Azure. Quando um servidor SQL é criado, também é criado um usuário administrador. Dependendo do nível de função do usuário que está acessando o banco, é possível trocar o usuário administrador. Porém, para acessar o banco, é necessário uma função dentro do próprio banco que é além da função do AAD. Por exemplo, caso eu seja um usuário não

administrador e eu desejo logar no banco, é necessário que eu tenha um usuário específico para o banco com funções do banco. Neste sentido, imagine que o departamento de física da UFSCar tenha uma assinatura na Azure (@*df.ufscar.br*), e que eu seja um usuário com permissões de *Reader* global, ou seja, eu posso ler todos os recursos criados na organização do departamento. Para que um usuário possa me dar acesso a um banco SQL, basta que ele entre neste banco e execute o comando da imagem a seguir.

```
CREATE USER [gabrielcandido@df.ufscar.br] FROM EXTERNAL PROVIDER;

ALTER ROLE [db_ddladmin] ADD MEMBER [gabrielcandido@df.ufscar.br];
ALTER ROLE [db_datareader] ADD MEMBER [gabrielcandido@df.ufscar.br];
ALTER ROLE [db_datawriter] ADD MEMBER [gabrielcandido@df.ufscar.br];
```

Figura 9: Comando para criar acesso através de usuário externo. Fonte: autor.

Na imagem 9, o parâmetro *"from external provider"* significa que o usuário no banco está sendo criado a partir de um provedor externo ao banco, que no caso é o AAD. E ao atribuir as funções *db_ddladmin, db_datareader e db_datawriter* para o meu usuário do banco recém criado, ele permite que eu possa criar tabelas, ler e escrever dados. [32]

Este tipo de recurso pode ser acessado por usuários próprios fora da nuvem sem que este usuário saiba, inclusive, que o serviço foi instanciado na nuvem. Outros exemplos disso é o *Azure Databricks* (ferramenta de engenharia de dados). Nele, é necessário que o usuário tenha acessos específicos da *workspace* criada para o recurso.

2.3.2 Criptografia de dados

Como comentado em seções anteriores, a criptografia de dados na Azure pode ser realizada para dados em repouso e dados em trânsito. Existem recursos que permitem que os dados sejam criptografados na própria criação do recurso através de uma chave gerenciada pela Azure, como o *Azure Storage Account* e o *Azure Synapse Analytics*. E há ainda a opção de ter chaves gerenciadas pelo cliente ou através de uma aplicação do cliente onde ele faz a gestão dessa chave, ou através de um *Key Vault*. [30]

O *Azure Key Vault* é uma ferramenta de gestão de segredos, senhas e certificados onde é possível armazenar chaves criptográficas que somente o cliente tem acesso. Ele possui níveis de acesso a nível do AAD e também a níveis de políticas de acessos internas. Por exemplo, para que uma aplicação dentro da própria Azure consiga visualizar os segredos que estão armazenados no *Key Vault*, é necessário que uma política de acesso seja criada para essa aplicação. Um exemplo deste caso é o *Azure Data Factory* (ADF) acessando a senha de um usuário de serviço de um banco *SQL Server*. [33]

Tanto o *Storage Account* quanto o *Azure Synapase Analytics* permitem a dupla criptografia. E existem outras opções como a criptografia de discos, utilizados em VMs, criptografia em repouso do *SQL Server*, Cosmos DB (ferramenta de banco de dados não relacional), entre outros recursos.

2.3.3 Ambiente Isolado

Como comentado em seções anteriores, uma das maneiras de proteger um ambiente de ameaças externas é isolando este ambiente para usuários que de fato precisam acessá-lo. Uma das maneiras de fazer isso, também como comentado, é através de redes virtuais. Neste texto, não vamos entrar em detalhes em como uma faixa de rede é configurada ou como as subredes (*subnets*, redes menores dentro das redes virtuais) são configuradas. Trataremos apenas dos conceitos básicos e de como esses recursos podem ser utilizados para proteger as aplicações de nuvem.

Quando criamos uma rede virtual e associamos recursos da Azure a essa rede, estes recursos ficam livres para se comunicar entre si, porém a sua comunicação com a internet fica restrita. Uma das maneiras mais seguras de acessar essas redes é através de uma conexão do tipo *Express Route*. Com ela, a comunicação acontece por cabeamento entre a empresa local e o próprio *datacenter* da Azure. Não há pontos de exposição na internet e a comunicação é extremamente rápida. Porém, hoje em dia, muitas empresas estão adotando modelos de trabalho híbridos ou de *home office*. Com isso, os seus colaboradores precisam acessar o ambiente em nuvem da empresa de uma forma segura e através de suas casas. Se a empresa possui recursos isolados em uma rede, uma das maneiras de fazer isso é utilizando uma VPN (*Virtual Private Network*). Observe a figura a seguir. [17, 34, 35]

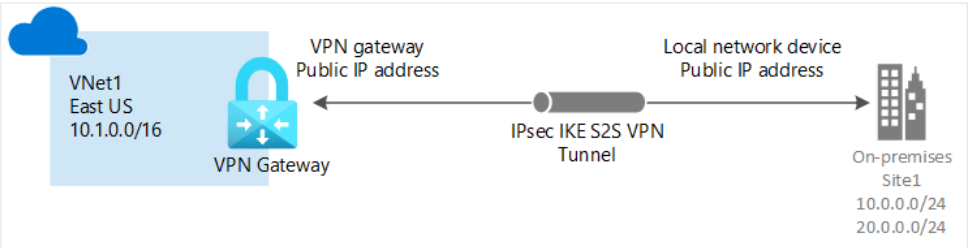

Figura 10: Ilustração do funcionamento de um gateway VPN na Azure. [35]

No canto esquerdo da figura 10, percebe-se que existe uma Vnet, isto é, uma rede virtual na Azure à qual o ambiente local (*On-premises*) deseja se conectar. Para estabelecer essa conexão, é necessário a criação de um *VPN Gateway*, que conterá um IP Público para que a rede seja visualizada na internet. A partir deste *gateway* de VPN, é criado um *gateway* de rede local, que possuí as informações necessárias para conexão partindo do ambiente *On-premises*. As configurações são instaladas no ambiente local e então a conexão é estabelecida de maneira segura através de um túnel criptografado IPsec IKE S2S. Assim, os usuários do ambiente local conseguem "visualizar"os recursos que estão na Vnet. Perceba que esta configuração é apenas para expor a rede que está na nuvem para o ambiente local. Todos as outras configurações de acesso como funções do AAD, funções de banco de dados e etc precisam ser estabelecidas para que o usuário que está acessando a nuvem localmente consiga realizar modificações no ambiente. [35]

Dentro da Azure, ainda é possível outros cenários, como por exemplo criar subredes dentro de uma rede e também emparelhar redes em si, onde são aplicados os mesmos conceitos de isolamento descritos acima. Para controlar acesso às redes, ainda é possível criar grupos de

segurança de redes (NSGs, *Network Security Group*), onde as regras e políticas de acesso de recursos e IPs ficam centralizadas em um único serviço. [36]

Do ponto de vista da criação de ambientes isolados, vale comentar a utilização de dois recursos da Azure em conjunto: o *Application Gateway* (AppGW) e o *Web Application Firewall* (WAF), apresentado na figura 10. Estes dois recursos aplicados em uma rede permite com que o tráfego de rede seja gerenciado e ao mesmo tempo detecta e ataca possíveis invasões de *hackers*. A utilização do WAF será melhor comentada na seção a seguir. [27]

2.3.4 Monitoramento de Ataques Cibernéticos

Para recursos da Azure que não estão associados a uma rede virtual, existe uma configuração padrão de proteção contra ataques do tipo DDoS. Por outro lado, para recursos que pertencem a uma rede, é possível habilitar o *Azure DDoS Protection*, que é um serviço pago de acordo com o SKU (para proteção de IP Público ou proteção de rede), que funciona 7 dias por semana e 24 horas por dia. Ele atua detectando se existe alguma ameaça de DDoS e caso a ameaça seja verificada, ele a ataca automaticamente. [37] A imagem ilustra a configuração do *Azure DDoS Protection*.

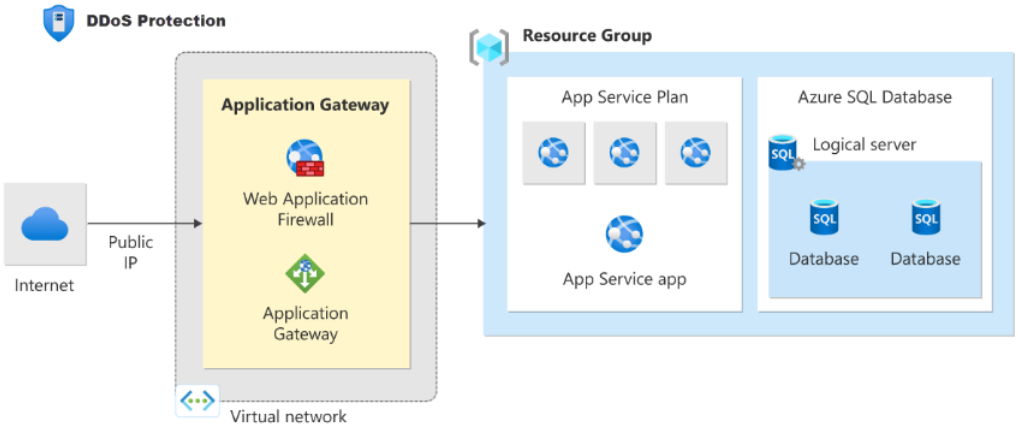

Figura 11: Ilustração do funcionamento do Azure DDoS Protection [37]

Na figura acima, observe que a comunicação de entrada ocorre por meio de um IP Público. E além disso, existe um *Firewall* (WAF), que vasculha o tráfego de entrada e protege contra os principais ataques. Uma vez que a requisição passa pelas verificações, o *gateway* distribui o tráfego pelos recursos internos da rede.

O WAF (*Web Application Firewall*) é um serviço da Azure que oferece proteção contra os principais ataques cibernéticos. Ele pode ser deployado junto com o *Azure Application Gateway* (AppGW), *Azure Front Door*, e junto com o *Azure Content Delivery Network* (CDN). A figura a seguir ilustra a arquitetura para o caso em que o WAF é configurado junto com o AppGW. [38]

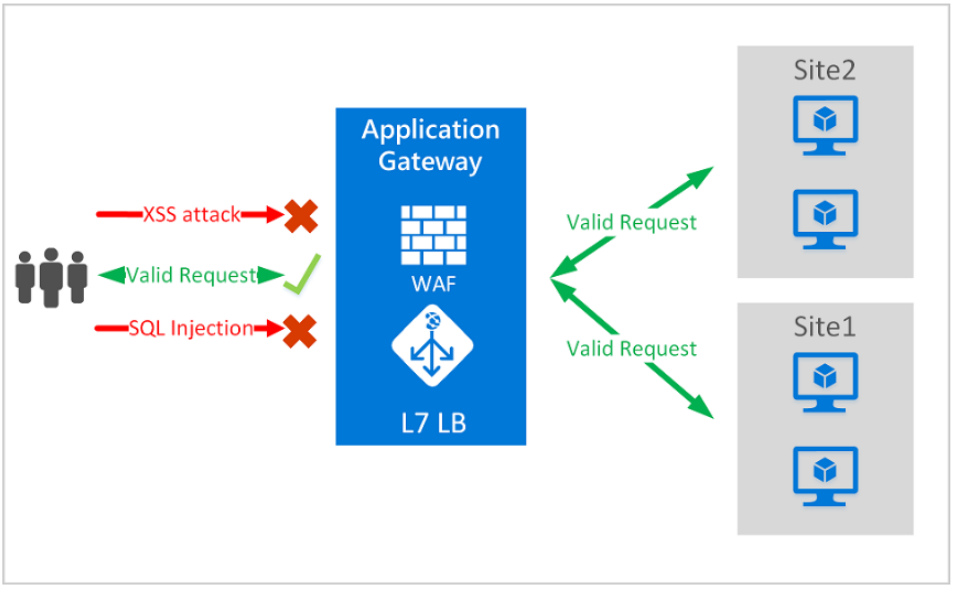

Figura 12: Ilustração do funcionamento do WAF junto com o Application Gateway [38]

Como ilustrado na figura 12, o WAF ajuda a identificar os ataques do tipo SQL Injection, por exemplo, onde o *hacker* tenta inserir um código corrompido para ser executado no banco da aplicação e impede que a requisição seja direcionada pelo *Application Gateway*. Uma das principais vantagens de utilizar o WAF é, assim como em muitos outros casos de utilização de serviços de nuvem, o compartilhamento da responsabilidade. O WAF já foi desenhado para combater os principais ataques cibernéticos, e caso ele não seja utilizado em uma aplicação suscetível a esses ataques, o time de desenvolvimento da aplicação deverá tomar todas as medidas necessárias, e essa tarefa não é nada trivial.

Algumas das ações possíveis com o WAF são [38]:

- *Allow* (permitir a requisição);
- *Block* (bloquear a requisição);
- *Log* (registrar a ocorrência);
- *Redirect* (redirecionar a requisição para uma URL em específico);
- *Anomaly Score* (para gestão de anomalias detectadas).

A principal diferença entre o *Application Gateway* e o *Azure Front Door* ao qual o WAF pode ser configurado, é que o primeiro funciona como um *load balancer* (gerenciador de carga) regional, dividindo as requisições entre VMs e contêineres, por exemplo. E o segundo funciona como um *load balancer* não regional e o seu tráfego pode ser roteado para todas as regiões do mundo. [39]

Outro recurso de segurança da Azure para monitoramento de ataques cibernéticos é o *Azure Sentinel*, que funciona como um gerenciador geral de toda a segurança da nuvem em si e pode ser integrado inclusive com o WAF. A figura a seguir ilustra as principais funcionalidades do *Azure Sentinel*.

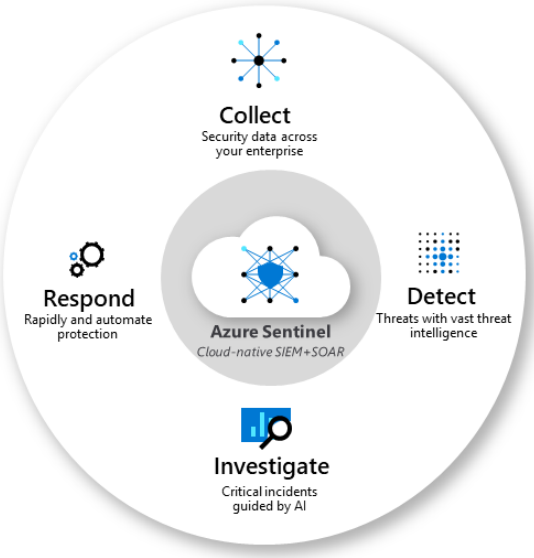

Figura 13: Principais funcionalidades do Azure Sentinel [40]

Como ilustrado na figura 13, a ferramenta permite a coleta de logs de recursos da Azure de forma integrada, detectar ataques, investigar e também responder aos ataques cibernéticos. Com o *Azure Sentinel*, os logs do WAF também podem ser centralizados.

3 Desenvolvimento

Agora, com base nos recursos da Azure introduzidos nos capítulos anteriores e aos conceitos de segurança apresentados, iremos analisar a arquitetura de uma solução real implementada no ambiente da Azure. Por motivos de confidencialidade e para respeitar a Lei Geral de Proteção de Dados, todos os nomes serão anonimizados.

3.1 Descrição do Problema

Considere a arquitetura representada na figura a seguir.

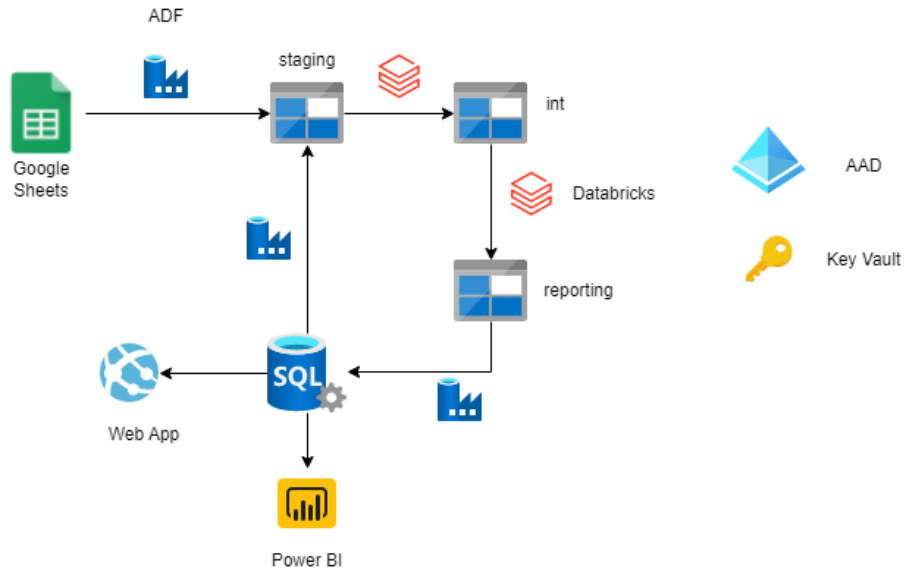

Figura 14: Arquitetura atual (as is). Fonte: o autor.

A arquitetura da imagem acima descreve o seguinte projeto. Dados são coletados de um banco de dados SQL e de uma planilha do *Google Sheets* através de um serviço orquestrador de dados que é o *Azure Data Factory*. Ele se conecta com o *Google Sheets* por meio de um token de acesso à API do Google que é armazenado no *Key Vault*. O *Key Vault* possui uma política de acesso que permite à Identidade Gerenciada do ADF (um identificador do ADF na Azure) ler os segredos. E também o ADF se conecta ao *SQL Server* através de um usuário de serviço cujas credenciais estão armazenadas no Azure *Key Vault*. A conexão do ADF ao *storage* (*Datalake*) ocorre por meio de um SAS Token que possui um prazo de validade de um ano e que também está armazenado no *Key Vault*. Os dados são trazidos primeiro para uma camada de *staging* do *storage*, e depois à medida que passa pelos processos de harmonização e agregação é migrado para as camadas de integração e *reporting*. Além disso, uma aplicação Web utiliza um *SQL Server* como banco e apresenta no formato de site web os dados desse banco, permitindo ao usuário inserir, deletar e alterar informações nele. Todos os registros de negócio do APP ficam disponibilizados no *SQL Server* através de uma *view* que é consumida por um *Power BI*. A arquitetura não possui redes virtuais na Azure, porém o acesso dos usuários é realizado via AAD e todos eles fazem o loging utilizando o MFA (*Multifactor Authentication*). O objetivo de negócios é centralizar a entrada de horas da empresa por projeto e ter uma visão generalizada

do faturamento por consultor e por projeto.

Outro ponto que é importantes destacar é que a empresa que utiliza a arquitetura proposta possui políticas de privilégios mínimos, isto é, somente os engenheiros de dados possuem acesso ao ADF, os analistas de BI possuem acesso somente de leitura à *view* consumida pelo Power BI, e os desenvolvedores possuem acesso somente ao Web APP e ao banco SQL. Além disso, os dados dos *storages* são criptografados por chaves gerenciadas pela Azure.

3.2 Análise da Segurança

A arquitetura apresentada na seção anterior atende muitos dos principais requisitos de segurança como a política de privilégio mínimo e a criptografia dos dados. Porém, não existe nenhuma solução específica que faz o monitoramento das requisições ao *Web App*. Mesmo que para acessar os dados nele seja necessário um login via AAD, o site em si está exposto na internet e por tanto está suscetível a ataques de *SQL Injection* e de *DDoS*, por exemplo. Como o objetivo do site é para uso interno na empresa, a exposição do mesmo na internet não é necessária. Além disso, o mesmo vale para o *end point* do *SQL Server* para o BI. Ao se conectar com um banco de dados *SQL Server* através do *Power BI*, uma das primeiras configurações é o endereço deste servidor na internet, que é o *host*. Este *host* está visível para toda a internet, visto que não está especificado na arquitetura atual uma política de *Firewall* que impeça o acesso de pessoas não autorizadas.

Vale destacar também que o acesso do time de BI ao banco *SQL Server* não é necessário. Do ponto de vista de dados, seria preferível criar um *delta lake* na camada *reporting* do *storage* e utilizar o *hive* do Databricks para fazer o consumo do *Power BI*. Desta maneira, o banco de dados transacional da aplicação ficaria exposto somente pela aplicação.

Por outro lado, um ponto positivo da arquitetura é a utilização do *Key Vault* para gerenciamento de segredos da aplicação. Para configurar as fontes de dados no ADF é necessário passar explicitamente as credenciais ou apontar para as credenciais no *Key Vault*. Como o *Key Vault* possui uma política de acesso para o ADF, este apontamento é possível. Além disso, o colaborador do ADF não precisa nem ter acesso de leitura do segredo no *Key Vault*, pois quem na verdade está lendo este segredo é o ADF e não o seu usuário.

3.3 Proposta de Solução

Com o objetivo de deixar a arquitetura atual mais redundante a ataques cibernéticos, sugere-se o seguinte *design*.

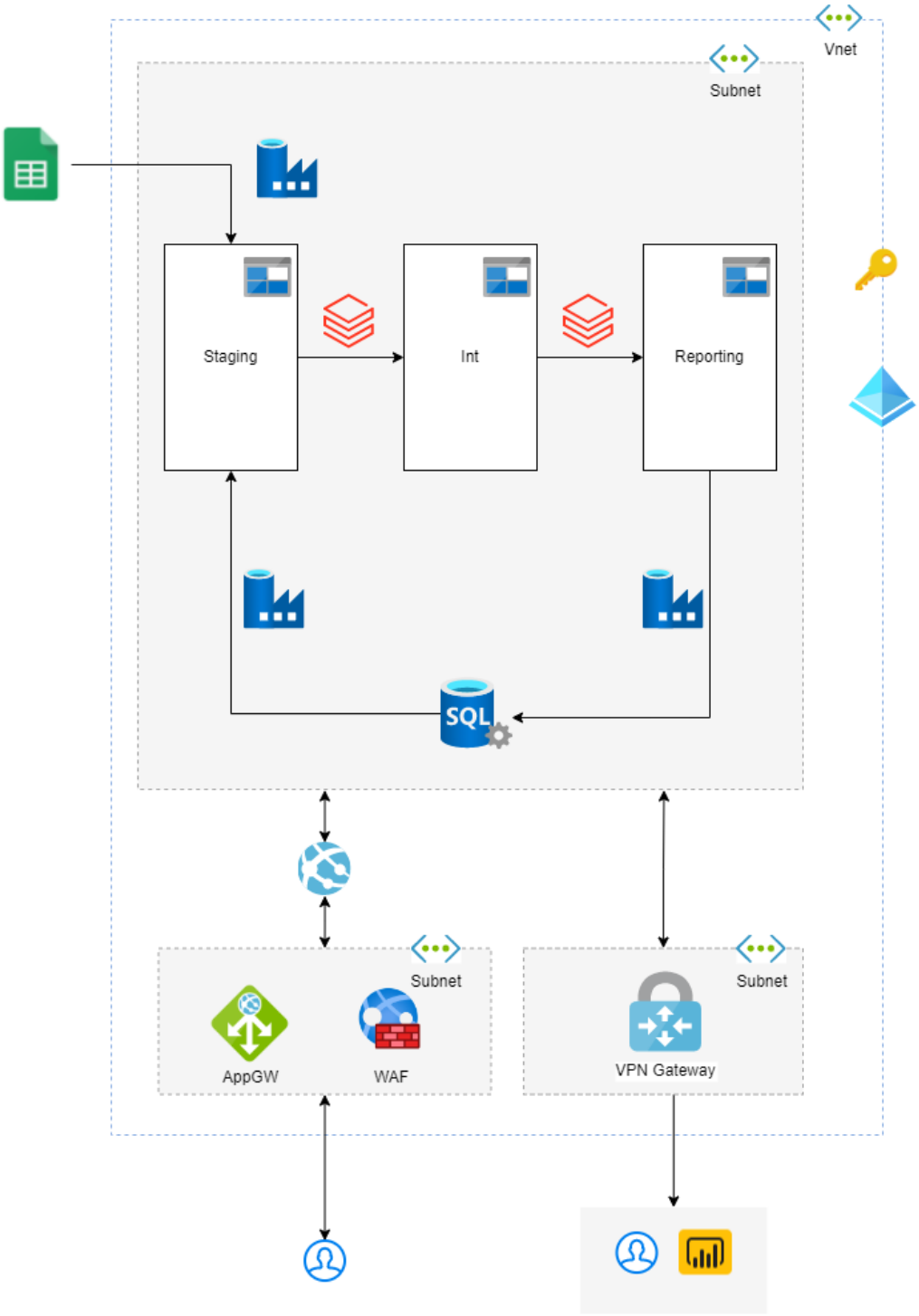

Figura 15: Proposta de arquitetura que atende melhor aos requisitos de segurança. Fonte: o autor.

Na figura acima, pode-se observar que alguns componentes foram acrescentados. O primeiro ponto que se destaca é que todos os recursos da Azure foram encapsulados por uma rede virtual

(Vnet), desta maneira, estes recursos só ficam expostos caso haja IPs Públicos criados para eles ou caso haja regras de exceções em NSGs (*Network Security Group*). Como não há a necessidade de exposições desse tipo, não foram considerados NSGs na arquitetura. [41]

Além disso, para expor somente pontos estratégicos à internet, os recursos internos da rede principal foram encapsulados em subredes de forma que existe uma subrede que não está exposta à internet, que é onde estão os *storages, o Data Factory, o Databricks* e o *SQL Server*, e existem subredes expostas à internet porém com o objetivo exclusivo de dar acesso e controlar o tráfego de entrada.

É importante notar que a planilha do *Google Sheets* está completamente fora da rede, pois ela é uma fonte externa de dados e cujas informações serão consumidas internamente utilizando o *Data Factory*. Não entraremos em detalhes sobre como configurar a API do Google no *Google Cloud Platform* (GCP), que é a provedora de nuvem do Google, pois fugiria do objetivo deste texto. Porém, assume-se que a API esteja devidamente configurada e que somente pessoas autorizadas possuam acesso a ela e aos dados inseridos no *Google Sheets*.

O *Application Gateway* (AppGW) junto com o WAF estão instanciados em uma subrede isolada para aumentar o nível de redundância com relação ao acesso da aplicação, visto que a responsabilidade para impedir ataques do tipo *SQL Injection* fica compartilhada agora com a Azure. O usuário acessa o AppGW, a requisição é verificada pelo WAF e caso seja uma requisição verdadeira, o AppGW direciona para a aplicação. Só então, a aplicação utiliza os recursos da subrede interna. Caso o WAF detecte que a requisição não seja legítima, ela é bloqueada e os recursos internos não são consumidos.

Em outra subrede, está instanciado um *gateway* de VPN. Como comentado na seção de fundamentos, o usuário do ambiente *On-premise* possui instalado em seu ambiente um *gateway* de rede local que o conecta à subrede interna da Azure. E através desta conexão, os recursos internos ficam disponíveis para atualização dos relatórios de *Power BI* ou para acesso ao banco e às ferramentas de engenharia de dados.

Observe também que o AAD foi mantido. Com isso é possível controlar a identidade dos usuários que estão acessando o ambiente e o nível de acesso que cada usuário possui. Outra ferramenta que foi mantida é o *Key Vault*, para gestão de segredos, o que permite granularizar ainda mais o nível de acesso seguindo a regra de privilégio mínimo, visto que agora os usuários não precisam ter acesso aos segredos da aplicação.

4 Conclusões

As soluções em nuvem de modo geral oferecem serviços que podem ser escalados sob demanda e que são pagos conforme o uso. Isso abre uma gama de possibilidades para empresas implementarem os seus problemas de negócio sem precisarem construírem um *datacenter* local. Essa possibilidade transfere para a provedora toda a gestão dos recursos físicos bem como algumas responsabilidades do ponto de vista de gestão de infraestrutura. Com isso, a empresa pode focar nos desafios de negócio, que é o que importa a ela. O compartilhamento de responsabilidade não ocorre somente a nível técnico, como atualização de *patches* de segurança em servidores ou escalabilidade, mas também ocorre a nível de segurança da informação. Hoje em dia, os ataques cibernéticos estão cada vez mais sofisticados, e transferir parte da solução para empresas especializadas pode poupar tempo e dinheiro das organizações.

Existem vários recursos e soluções que a Azure oferece relacionados à segurança da informação, desde para controle de acesso bem como para detecção e combate a ataques cibernéticos, como o SQL Injection, listado como um dos principais riscos cibernéticos pela *Open Worldwide Application Security Project* (OWASP).

Soluções como o *Azure Active Directory* permite à organização controlar o acesso aos recursos instanciados na Azure, tanto a nível de autenticação quanto de autorização. Essa ferramenta vinculada com uma política de privilégios mínimos ajuda a organização a proteger suas soluções e dados de um dos principais riscos cibernéticos, como a quebra do controle de acesso.

Vimos que a Azure oferece outros tipos de soluções que em conjunto ajudam a isolar o ambiente para evitar requisições suspeitas e ataques DDoS. Pode-se isolar os recursos em subredes e redes virtuais, expor portas estratégicas para a internet e ainda aplicar uma política de *firewall* com o *Web Application Firewall* (WAF), um *firewall* que ajuda a detectar e atacar as principais ameaças listadas pelo OWASP. Outros recursos que ajudam a garantir o isolamento das soluções em nuvem é o *Express Route* e os *Gateways de VPN*. No primeiro, a conexão com a rede interna é feita por cabeamento e não há exposição na internet. E no segundo, um gateway local é instalado no servidor local para que o usuário se conecte à nuvem através de um túnel criptografado.

Criptografia é um dos pontos mais importantes em segurança da informação, visto que os ataques de sequestro de dados ocorrem com cada vez mais frequência e geram prejuízos enormes às organizações. A Azure oferece várias opções de criptografia para o armazenamento de dados em nuvem, com chaves gerenciadas por ela e pelo cliente, garantindo que, no pior dos casos, se os dados forem sequestrados por um hacker, a informação de negócio é preservada e a LGPD respeitada.

Além dos recursos que podem ser utilizados para garantir a segurança da informação oferecidos pela Azure, ainda existem *frameworks* que oferecem certificações para as empresas interessadas em provar que os seus ambientes passam de fato por políticas rígidas contra ameaças cibernéticas, como a *ISO 27001* e o *CIS Controls*.

Por fim, conclui-se que do ponto de vista da segurança, a redundância é a melhor opção.

Referências

[1] Microsoft, "What is a cyberattack?." https://www.microsoft.com/en/security/business/security-101/what-is-a-cyberattack. Acesso em 12 de Março de 2023.

[2] L. G. Pacete, "5 ataques cibernéticos no brasil em 2021 que geraram alerta." https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/, 2021. Acesso em 12 de Março de 2023.

[3] Fortinet, "Brasil é o segundo país que mais sofre ataques cibernéticos na américa latina." https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a. Acesso em 12 de Março de 2023.

[4] E. Kiner and S. Konduru, "How google cloud blocked the largest layer 7 ddos attack at 46 million rps." https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps. Acesso em 12 de Março de 2023.

[5] R. Bala, B. Gill, D. Smith, D. Wright, and K. Ji, "Magic quadrant for cloud infrastructure and platform services." https://www.gartner.com/doc/reprints?id=1-26YXE86I&ct=210729&st=sb, 2023. Acessado em 26 de março de 2023.

[6] Microsoft, "Tour of azure services." https://learn.microsoft.com/en-us/training/modules/intro-to-azure-fundamentals/tour-of-azure-services. Acesso em 12 de Março de 2023.

[7] S. Vennam, "O que é cloud?." https://www.ibm.com/br-pt/cloud/learn/cloud-computing, 2020. Acesso em 12 de Março de 2023.

[8] Microsoft, "What are public, private, and hybrid clouds?." https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#benefits. Acesso em 12 de Março de 2023.

[9] T. Lanfear, A. M. Hitchcock, and D. Berry, "Shared responsibility in the cloud." https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility, 2023. Acesso em 12 de Março de 2023.

[10] Microsoft, "Pricing calculator." https://azure.microsoft.com/en-us/pricing/calculator/, 2023. Acesso em 12 de Março de 2023.

[11] C. Nottingham, L. Jackson, M. McKittrick, and other, "Virtual machines in azure." https://learn.microsoft.com/en-us/azure/virtual-machines/overview. Acesso em 12 de Março de 2023.

[12] Microsoft, "Introduction to azure kubernetes service." https://learn.microsoft.com/en-us/training/modules/intro-to-azure-kubernetes-service/. Acesso em 12 de Março de 2023.

[13] G. Gailey, E. Burns, S. Penmatsa, *et al.*, "Introduction to azure functions." https://learn.microsoft.com/en-us/azure/azure-functions/functions-overview. Acesso em 12 de Março de 2023.

[14] J. Borsecnik, J. Richins, J. Mirabal, *et al.*, "Introduction to azure managed disks." https://learn.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview. Acesso em 12 de Março de 2023.

[15] T. Myers, N. Estabrook, D. Callison, *et al.*, "Introduction to azure blob storage." https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction. Acesso em 12 de Março de 2023.

[16] N. Estabrook, T. Myers, L. Schuenemeyer, *et al.*, "Hot, cool, and archive access tiers for blob data." https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview. Acesso em 12 de Março de 2023.

[17] M. Bender, H. A. Kazwini, A. Sudbring, *et al.*, "What is azure virtual network?." https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview. Acesso em 12 de Março de 2023.

[18] R. Downer, R. W. MSFT, W. A. MSFT, *et al.*, "What is azure sql database?." https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql. Acesso em 12 de Março de 2023.

[19] C. Lin, M. Sangapu, E. Fan, *et al.*, "App service overview." https://learn.microsoft.com/en-us/azure/app-service/overview. Acesso em 12 de Março de 2023.

[20] "Framework de politicas de seguranÇa da informaÇÃo." https://bityli.com/74ND5p. Acesso em 12 de Março de 2023.

[21] "Frameworks de segurança da informação." https://documentacao.senior.com.br/seguranca-da-informacao/frameworks.htm. Acesso em 12 de Março de 2023.

[22] "O que é a norma iso 27001?." https://www.27001.pt/index.html, 2023. Acesso em 12 de Março de 2023.

[23] A. Buck, A. Bathini, and M. Baldwin, "Overview of microsoft cloud security benchmark (v1)." https://learn.microsoft.com/en-us/security/benchmark/azure/overview, 2023. Acesso em 12 de Março de 2023.

[24] Brasil, "Lei nº 13.709, de 14 de agosto de 2018." https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, 2018. Acesso em 12 de Março de 2023.

[25] OWASP, "Top 10 web application security risks." https://owasp.org/www-project-top-ten/, 2021. Acesso em 12 de Março de 2023.

[26] T. Myers, S. Savell, and M. Baldwin, "Azure storage encryption for data at rest." https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption. Acesso em 12 de Março de 2023.

[27] D. Au, T. Yao, and Vic, "What is azure web application firewall?." https://learn.microsoft.com/en-us/azure/web-application-firewall/overview. Acesso em 12 de Março de 2023.

[28] J. Hall, T. K, and J. Flores, "How it works: Azure ad multi-factor authentication." https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks. Acesso em 12 de Março de 2023.

[29] S. Wray and G. Moore, "Security design principles." https://learn.microsoft.com/en-us/azure/architecture/framework/security/security-principles. Acesso em 12 de Março de 2023.

[30] S. Gunda, K. Campise, D. Coulter, *et al.*, "Azure encryption overview." https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview. Acesso em 12 de Março de 2023.

[31] J. Flores, J. Grant, R. Lyon, *et al.*, "Azure ad built-in roles." https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference. Acesso em 12 de Março de 2023.

[32] V. To, J. Roth, R. W. MSFT, *et al.*, "Database-level roles." https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver16. Acesso em 12 de Março de 2023.

[33] J. Howell, K. Sharkey, J. Lichwa, *et al.*, "About azure key vault." https://learn.microsoft.com/en-us/azure/key-vault/general/overview. Acesso em 12 de Março de 2023.

[34] D. Lee, D. Coulter, D. Au, *et al.*, "What is azure expressroute?." https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction. Acesso em 12 de Março de 2023.

[35] C. McGuire, G. Sharma, and H. A. Kazwini, "Tutorial: Create a site-to-site vpn connection in the azure portal." https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal, 2023. Acesso em 12 de Março de 2023.

[36] A. Sudbring, H. A. Kazwini, and D. Berry, "Subnet extension." https://learn.microsoft.com/en-us/azure/virtual-network/subnet-extension. Acesso em 12 de Março de 2023.

[37] Microsoft, "What is azure ddos protection?." https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview, 2023. Acesso em 12 de Março de 2023.

[38] J. Downs, R. Downer, J. Basden, *et al.*, "What is azure web application firewall on azure application gateway?." `https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview`. Acesso em 12 de Março de 2023.

[39] D. Au, J. Downs, Jessie, *et al.*, "Frequently asked questions for azure front door." `https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq`. Acesso em 12 de Março de 2023.

[40] R. Mansdoerfer, J. Downs, P. Mandemaker, *et al.*, "What is microsoft sentinel?." `https://learn.microsoft.com/en-us/azure/sentinel/overview`, 2023. Acesso em 12 de Março de 2023.

[41] H. A. Kazwini, E. Enomoto, A. Sudbring, *et al.*, "Network security groups." `https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview`, 2023. Acesso em 12 de Março de 2023.