INSTITUTO SUPERIOR
DE TECNOLOGIAS
AVANÇADAS DE LISBOA

Métodos de Autenticação em Cloud Computing

Manuley dos Santos Neto

Dissertação para obtenção do Grau de Mestre em

INFORMÁTICA

Presidente: Professor Doutor Paulo André Reis Duarte Branco

Arguente: Professor Especialista Pedro Fernando Morais Martins Crispim

Orientador: Professor Doutor Pedro Ramos dos Santos Brandão

Junho, 2023

Índice

Índice de Figuras

Dedicatória

Dedico este trabalho aos meus colegas, amigos, familiares, em particular à minha companheira, e aos Professores Pedro Brandão, Paulo Duarte, Pedro Crispim e Nuno Mingatos.

Agradecimento

Agradeço aos meus familiares e ao Inocêncio Barros, pela força ao longo desta caminhada, aos professores pelo método implementado, para nos obrigar a estarmos preparados para esta fase da dissertação, que é a mais exigente, ao meu orientador, pelo apoio ao longo deste percurso exigente e, em simultâneo, interessante, não esquecendo a minha companheira, a minha mãe, bem como os meus amigos e familiares, que sempre me deram um apoio incondicional.

Índice de abreviaturas e acrónimos

2FA – Two Factor Authentication

AWS – Amazon Web Service

DNA - Deoxyribonucleic Acid

ECG - Electrocardiogram

FaaS - Function as a Service

GaaS – Gaming as a Service

IaaS -Infrastructure as a Service

ISP - Internet Service Provider

MFA – Multiple Factor Authentication

PaaS – Platform as a Service

SaaS – Software as a Service

SFA – Single Factor Authentication

SLA - Service Level Agreement

XaaS – Anything as a Service

AD – Active Directory

Resumo

Este trabalho tem como objectivo, documentar e demonstrar de modo prático, a importância dos métodos de autenticação em *Cloud Computing* e determinar, de uma forma concreta, as diferenças entre os fornecedores Microsoft Azure e Amazon AWS.

Neste projecto, serão abordados os conceitos dos métodos de autenticação no nosso dia-a-dia e, comparados de uma forma eficiente, bem como a segurança que podemos encontrar e os tipos de métodos utilizados pelo Microsoft Azure e Amazon AWS.

Palavras-chave: Computação em Nuvem, Métodos de Autenticação, Azure, AWS.

Abstract

The aim of this work is to document and demonstrate in a practical way the importance of authentication methods in Cloud Computing and to determine, in a concrete way, the differences between the providers Microsoft Azure and Amazon AWS.

This project will cover the concepts of authentication methods in our daily lives, and will compare, efficiently, the security we can find and the types of methods used by Microsoft Azure and Amazon AWS.

Keywords: Cloud Computing, Authentication Method, Azure, AWS

1 Introdução

1.1 Enquadramento e Motivação

A computação em nuvem é uma tecnologia emergente, que nos permite solicitar serviços e recursos aos fornecedores de serviços num ambiente, a pedido. Isto é, uma infra-estrutura complexa, que economiza recursos para as necessidades de negócios modernos e fornece os meios, pelos quais os serviços são entregues aos utilizadores finais, via Internet. No ambiente de nuvem, os utilizadores podem aceder aos serviços, com base nas suas necessidades, sem saber como os serviços são entregues e onde o serviço se encontra hospedado [1].

Os serviços em nuvem, são fornecidos em três modelos fundamentais [2]: Infra-estrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). O IaaS é o nível mais baixo e que está mais próximo dos dispositivos de hardware, enquanto o SaaS é o nível mais alto no fornecimento de serviços aos utilizadores finais. O serviço da Web da Amazon, é um tipo de IaaS amplamente utilizado desde 2006, enquanto o sistema CRM Salesforce.com é um exemplo de SaaS. O nível de PaaS fornece uma plataforma de aplicativos na nuvem [2].

A plataforma Microsoft Azure, é um exemplo de PaaS que permite aos desenvolvedores criar, hospedar e dimensionar os seus aplicativos nos *data centers* da Microsoft. Recentemente, um novo conceito, denominado de *Everything as a Service* (XaaS)" foi adoptado como a nova tendência na computação em nuvem. Vários fornecedores, como a Microsoft e a Hewlett Packard, foram associados ao mesmo, conforme indicado [2].

A Autenticação Biométrica como Serviço (BioAaaS) foi definida como uma abordagem para autenticação forte, em ambientes web, baseada no modelo SaaS. Aquando da autenticação pelo utilizador pela Internet, a credencial será enviada pelo principal (utilizador, máquina ou serviço solicitante de acesso). Se as credenciais corresponderem, o utilizador terá permissão para aceder aos serviços que subscreveu aos fornecedores de serviços. Nesta dissertação, consideramos o "utilizador" a pessoa principal que envia as suas informações de login, para se autenticar na nuvem. Existem diferentes tipos de informações de login, denominadas de credenciais, que os utilizadores podem enviar, como forma de comprovar quem são.

A chave compartilhada é normalmente utilizada nos protocolos de senha, como o *Password Authentication Protocol* (PAP) e o *Challenge Handshake Authentication Protocol* (CHAP) [3]

O objectivo de um protocolo de autenticação é fornecer o acesso seguro, troca de dados e comunicação entre todas as entidades, com recurso a regras criptográficas digitais. Um método de autenticação fornece a garantia de acordos importantes, não divulgados, de compartilhamento, métodos de não negação e computação multipartidária [4].

Tais protocolos visam fornecer total sigilo e preservar a segurança na presença de um invasor. É altamente irrelevante que um adversário deva seguir regras específicas de ataque, padrões de ataque [4].

O certificado digital é o segundo tipo de credencial que pode fornecer uma autenticação robusta no ambiente de nuvem. É um documento electrónico que utiliza uma Autoridade de Certificação (CA) confiável para ocultar a chave de criptografia com uma identidade. A chave de desencriptação é a única maneira de validar o certificado assinado.

Outro tipo de credencial é a senha de uso único (OTP) frequentemente utilizada. O utilizador final obtém o OTP do *token* (hardware ou software) durante o tempo de login. O *token* pode gerar uma sequência de senha aleatória, com base num complexo algoritmo, em tempo real. Visto que a senha gerada é única e só pode ser utilizada uma vez, OTP pode ser utilizado no ambiente de nuvem. Por exemplo, a *Amazon Web Services* (AWS) utiliza um *token* OTP para uso com contas da AWS [4].

1.2 Metodologia de Investigação

A metodologia utilizada será do tipo misto, com métodos quantitativos e qualitativos. Utilizar-se-á uma metodologia de investigação teórica e desenvolvimento prático no dia-a-dia das empresas, com diferentes instrumentos de análise como metodologia, análise documental, entre outros.

1.2.1 Questões e Contributos de Investigação

P1: Quais são os Métodos de Autenticação utlizados em Computação na Nuvem?

P2: Quais as diferenças entre os métodos de autenticação utilizados pelo Microsoft Azure e Amazon AWS?

C1: O primeiro contributo desta dissertação, consiste em dar a conhecer aos leitores um entendimento sobre a privacidade dos dados e de como os dados podem ser protegidos através de vários métodos de autenticação existentes. Esta entidade foi implementada, com o intuito de controlar a forma como os dados dos utilizadores podem ser autenticados.

C2: O modo como se aplica a privacidade e a protecção dos dados nos fornecedores Azure e AWS; cada fornecedor de serviço de computação em nuvem utiliza métodos distintos, esta dissertação irá fazer uma comparação na vertente da autenticação e apresentar aos leitores as especificidades e a credibilidade de cada método existente. Cada entidade tem a sua forma de processar e proteger os dados dos cidadãos/clientes, com definições extensivas de informações pessoais, concedendo aos clientes/consumidores/cidadãos, direitos sobre as suas informações pessoais e exigindo que as empresas cobertas facultem um aviso transparente, acerca das suas práticas.

C3: Neste contributo introduzimos, finalmente, a metodologia comparativa, com que iremos comparar através de uma metodologia, os métodos mais utilizados nas empresas e determinar quais os métodos da preferência dos utilizadores das empresas, e a forma como se aplica a privacidade dos dados pessoais.

1.2.2 Método de Pesquisa

Estas são as etapas que foram levadas a cabo na pesquisa descrita nesta dissertação:

- Na primeira etapa da investigação, foi realizado um estudo exaustivo e preliminar da literatura apropriada, que abrangeu os tópicos relevantes, como a computação em nuvem, métodos de autenticação, Azure e AWS.
- Na segunda etapa da investigação, fez-se uma comparação na forma como os métodos de autenticação se distinguem uns dos outros, verificando os seus conceitos e a vantagem de cada método de autenticação existente no mercado.

- Na terceira e última etapa da investigação, interligaram-se os resultados do estudo comparativo entre os métodos de autenticação utilizados pelos

fornecedores Azure e AWS, efectuando uma comparação de como funciona em cada fornecedor e, após isso, foi elaborado um questionário para as empresas, para validar quais os fornecedores que utilizam, quais os métodos que estão a actualizar, qual dos métodos garante a melhor segurança dos dados e qual é o mais fácil de implementar, em termos dos custos para as empresas, ou seja, qual garante a melhor rentabilidade em termos de qualidade/custo.

1.3 Estrutura da Dissertação

O capítulo dois contém um estudo aprofundado acerca da computação em nuvem, no qual se abordaram temas tais como a definição proveniente de diferentes investigadores, tipos de serviços, modelos de implementação e benefícios em aderir, sem esquecer as suas características essenciais.

No capítulo três, realizou-se uma descrição sobre os tipos de métodos de autenticação existentes no mercado, os seus conceitos, como funcionam, e quais as vantagens de utilizar cada um desses métodos.

O capítulo quatro contém uma revisão sobre o Azure, os seus conceitos, como funciona a plataforma, os termos de responsabilidade da plataforma do Azure e dos clientes, quais os métodos de autenticação utilizados e como funciona cada método de autenticação na plataforma Azure.

O capítulo cinco contém uma descrição completa da AWS, os seus conceitos, como funciona a plataforma, os termos de responsabilidade da plataforma AWS e dos clientes, quais os métodos de autenticação utilizados e como funciona cada método de autenticação na plataforma AWS.

No capítulo seis, fez-se uma comparação entre métodos de autenticação utilizados pela plataforma Azure e AWS.

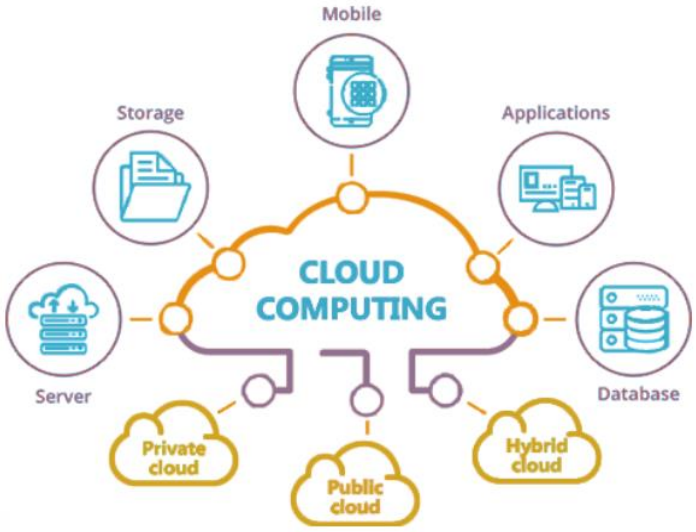
No capítulo sete, realizou-se um inquérito de interligação entre os métodos de autenticação utilizados pelas empresas na plataforma Azure e AWS, de forma a validar o método de autenticação mais utilizado e qual as empresas consideram mais credível.

2 Cloud Computing

Este capítulo, é uma visão geral da computação em nuvem, incluindo cenários habituais de computação em nuvem no nosso dia-a-dia, as características, definições, origens e desenvolvimento de computação em nuvem, as vantagens e classificação da computação em nuvem, várias tecnologias de suporte à computação em nuvem [7]. O modelo de computação e a implementação da computação em nuvem, nas perspectivas para apoiar as empresas ou particulares a compreender qual a melhor solução para as suas necessidades de negócio. Conforme havia proposto neste capítulo, espero que obtenham uma compreensão geral da computação em nuvem e estabeleçam as bases para o estudo aprofundado dos capítulos seguintes.

2.1 O que é?

É um termo, normalmente, utilizado pelas entidades que fornecem serviços de nuvem. Estes serviços são normalmente divididos em três categorias: Infra-estrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). O nome computação em nuvem surgiu na simbologia da nuvem que representa a Internet e diagramas [9], conforme pode confirmar na Fig. 1, a composição da *Cloud Computing* e os 3 tipos de *nuvem*.



1) Figura 1 Conceito de Cloud Computing e a sua especificação, fonte: [1]

2.2 Características

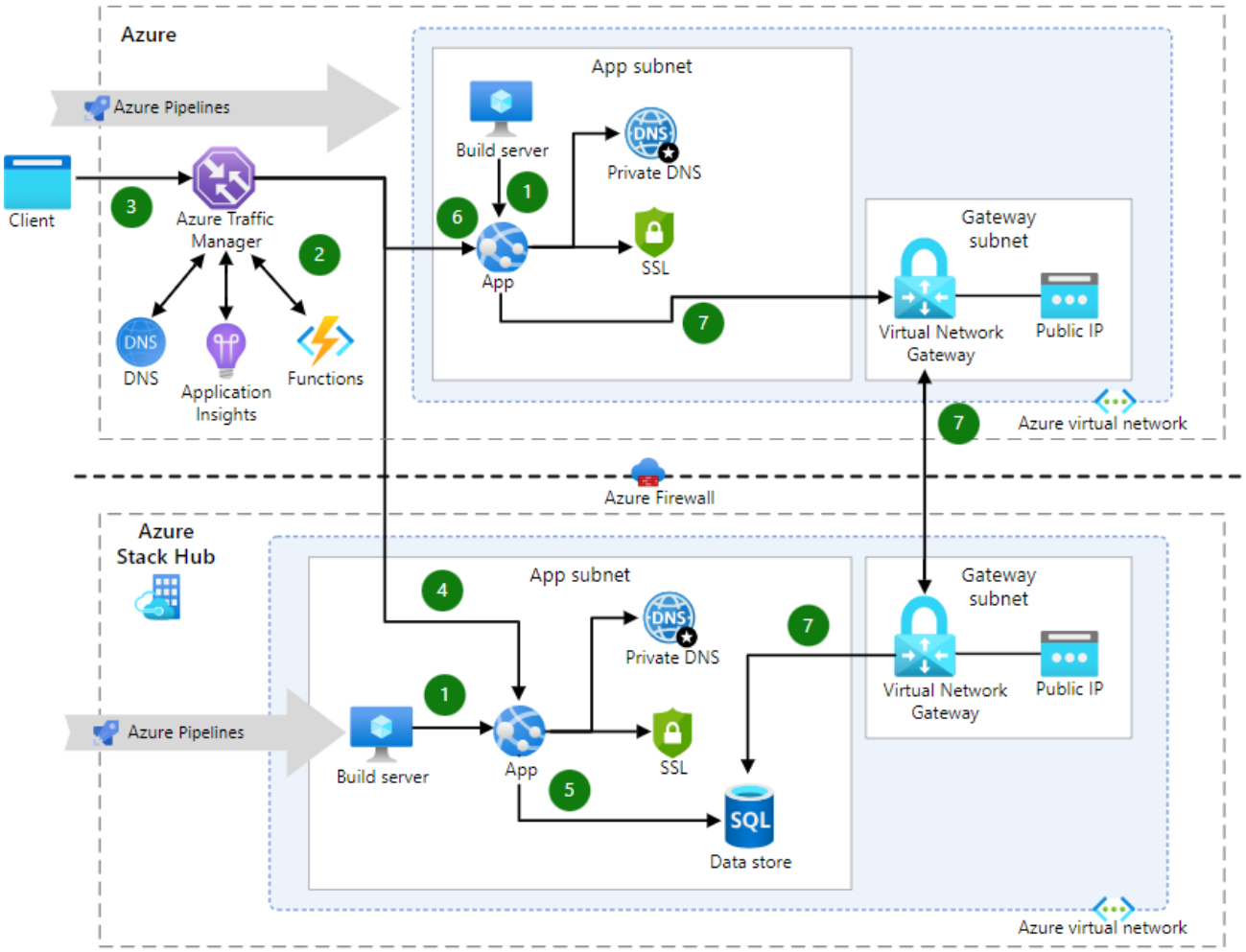
Existem 5 características que definem a computação em nuvem, as quais passamos citar:

2.2.1 On-Demand Self-Service

No *On-Demand Self-Service*, o cliente pode aderir aos serviços de computação em nuvem de acordo com suas necessidades de negócio. O *On-Demand Self-Service* é uma das principais características dos modelos de funcionamento em nuvem. De seguida, apresentaremos os modelos da Infra-estrutura como um serviço (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS) [8]. Com esta característica o utilizador tem a possibilidade de escolher entre um desses modelos, com base nas suas necessidades de negócio e, depois de seleccionar o modelo de implementação, tendo diferentes configurações à escolha.

Os processos são, geralmente, efectuados por gestão própria e não requerem a intervenção de terceiros, a menos que ocorra uma situação de problema que requeira intervenção [1]. Conforme apresentado na Fig. 2, no fornecedor Azure, as especificações do servidor para nuvens públicas têm muitas configurações, várias opções de instâncias de servidor por opção. Geralmente, é implementada no seu repositório e em qualquer local, a principal restrição na escolha de uma máquina virtual (VM) é conseguir obter a máquina que cumpre com os requisitos das suas necessidades diárias.

O *On-Demand Self-Service* tem como premissa ir ao encontro das necessidades do cliente e dos produtos que irá necessitar. Obviamente, são necessárias as experiências de utilização da nuvem dos utilizadores que irão implementar este serviço. Os utilizadores que não têm o conhecimento e os recursos para utilizarem serviços em nuvem, podem contratar técnicos especializados para implementar os serviços, de acordo com a necessidade do seu negócio [7].



2) Figura 2 - Especificações do servidor para nuvens públicas Azure, fonte: [1]

2.2.2 Extensive Network Access (Amplo Acesso à Rede)

É outra das características fundamentais da computação em nuvem, dado que os recursos da nuvem devem ser acedidos através da rede de Internet, desta forma todas as nuvens devem contar com disponibilidade a conectividade de rede. Podemos presumir que a base da computação em nuvem é a rede, especialmente a Internet, a nuvem é sempre inseparável da Internet. A conectividade à rede de Internet pode fornecer acesso remoto, a qualquer hora e em qualquer lugar, aos recursos de TI. A computação em nuvem pode ser interpretada como a "Internet mais recursos de computação", e o acesso à rede de Internet é uma propriedade intrínseca da computação em nuvem [9].

Apesar de o conceito de computação em nuvem ser interpretado como tendo acesso pela Internet, existem várias formas de poder aceder a um recurso na nuvem. Imaginemos uma empresa que tem serviços de nuvem Híbrida, estes acessos à nuvem podem ser efectuados

através de uma VPN ou de uma linha dedicada com ISP´s (Internet Service Provider) para ter exclusividade de rede e largura de banda, desta forma a segurança sai reforçada. O nível de serviço da rede de conectividade entre utilizadores de nuvem e fornecedores de serviços de nuvem, a qualidade de serviço (QoS) depende do fornecedor de serviços de Internet (ISP) que fornece o acesso à rede [9].

Actualmente, a Internet faz parte do nosso dia a dia e, com isso, temos acesso aos recursos de rede a qualquer momento, uma grande variedade de terminais digitais, como computadores e telemóveis, o que facilita e torna mais acessível qualquer necessidade de aceder à nuvem.

Assim sendo, podemos dizer que o amplo acesso à rede é um dos recursos da computação em nuvem de grande importância, tanto para a nossa vida quotidiana, quanto para a disponibilidade de serviço. Pode ser uma rede com fios ou uma rede sem fios, como a Wi-Fi. Em suma, sem uma rede de Internet não haveria serviços de computação em nuvem [7].

2.2.3 Resource Pooling

O pool de recursos é uma terminologia utilizada na área de TI, para os ambientes de computação em nuvem, para descrever uma situação na qual os fornecedores prestem serviços ao em simultâneo a vários clientes “host” com serviços fiáveis e escaláveis. Esta característica da computação pode ser ajustada para cumprir as necessidades de cada cliente, sem que o utilizador final sinta qualquer alteração do seu lado [8].

Geralmente, as plataformas de computação em nuvem são acedidas pela Internet, e podem ser plataformas compartilhadas, geridas ou desenvolvidas para oferecer serviços dedicados, exclusivamente, à necessidade de um cliente. Estas são tecnologias de alto nível, que ajudam os clientes a desfrutar da flexibilidade e escalabilidade do serviço. No modelo de pool de recursos da computação em nuvem, o fornecedor de serviços disponibiliza vários serviços e a vários clientes em simultâneo. Utilizam um modelo multilocatário “multi-inquilinos” para conseguir partilhar e gerir vários clientes, em simultâneo.

Por isso, esta característica da computação contém recursos de TI, tais como: núcleos, dispositivos de armazenamento e memória RAM, etc. E todos esses recursos são considerados e tratados como um só, para obter flexibilidade na prestação dos serviços. Estes tipos de serviços possuem várias rotas, o que proporciona rapidez na sua execução, tanto para serviço de alojamento como de processamento dos dados.

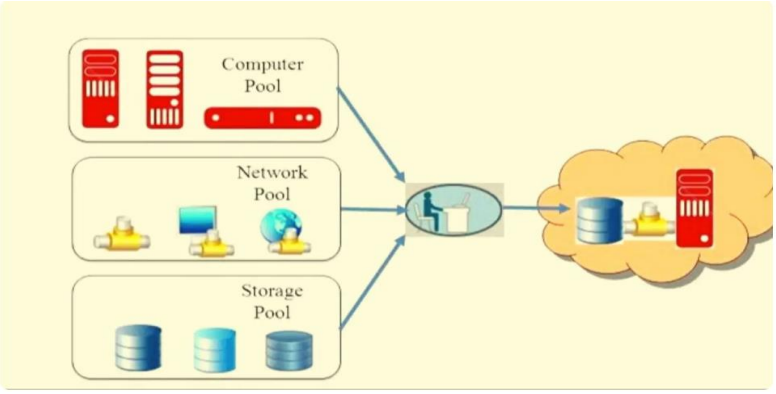
Resumindo, no modelo multilocatário “multi-inquilinos” utilizado na área de TI, o fornecedor do serviço, fornece a vários tipos de clientes o mesmo tipo de serviço como, por exemplo, empresas que gerem alojamentos de sites partilham o mesmo tipo de serviço, a vários clientes sem que os clientes sintam que os recursos estão a ser partilhados.

Outras das características de um pool de recursos é a de poder filtrar as diferenças entre os vários recursos e conseguir partilhar esses recursos conforme a utilização de cada inquilino.

Com os recursos de armazenamento, que podem ser um disco rígido mecânico ou SSD agrupados, o utilizador pode solicitar uma certa quantidade de espaço de armazenamento, que corresponde ao disco rígido mecânico ou SSD, que é disponibilizado na sua área de cliente [7]

Geralmente, os utilizadores não têm a visibilidade ou o conhecimento de onde os recursos são fornecidos, apesar de poderem controlar onde quer estes dados sejam localizados, a um nível altamente abstracto [9].

Na computação em nuvem, os recursos que podem ser agregados e agrupados incluem a computação, armazenamento e rede, serviços de base de dados, etc. Os recursos de computação incluem o CPU e a memória. Se a CPU estiver agrupada, a menor unidade da CPU que o utilizador vê, pode ser um núcleo virtual e não são indicados mais atributos físicos, como o fabricante da CPU sendo a AMD ou a Intel. Conforme mostrado na Fig. 3, a implementação de uma *Pooling* de Recursos



3) Figura 3 - Implementação de uma Resource Pooling, fonte: [8].

2.2.4 Fast and Elastic Scaling

O Fast and Elastic Scaling como característica da computação em nuvem, é normalmente citado como uma das principais razões de conquista dos utilizadores, para "abraçar" a

computação em nuvem. Na Nuvem, existe a possibilidade dos utilizadores escalarem, de forma automática e transparente os seus recursos, em função das suas necessidades de negócio. Por exemplo, para estar à vontade com o súbito incremento do tráfego em eventos mais frequentes, os utilizadores da plataforma podem adquirir, automaticamente e temporariamente, um grande número de recursos virtuais, para expandir a capacidade.

Isso quer dizer que os utilizadores podem utilizar os recursos da plataforma, de forma assertiva, para suas necessidades de negócio, quando têm mais eventos expandem o recurso, e quando têm menos evento de negócio, voltam a reduzir o recurso [6].

A escalabilidade pode incluir vários tipos de recursos desde servidores, recursos de redes, base de dados, armazenamento, entre outros. Esta característica da computação permite que a empresa consiga gerir melhor o seu negócio e gerir os custos a ter com a computação, por não serem recursos caros, que podem ser utilizados apenas quando necessário e quando o negócio precisa, ao contrário dos recursos privados, nos quais não existe essa possibilidade.

Na computação em nuvem, o maior benefício do dimensionamento elástico rápido para os utilizadores é o custo económico, enquanto mantêm o seu negócio ou a aplicação a funcionar sem problemas. As empresas podem adquirir pequenas quantidades de recursos quando estão na época de menor procura do seu negócio e, gradualmente, aumentar o seu investimento em recursos. À medida que a empresa vai ganhando mercado e necessita de mais investimento justificável, ou de concentrar os recursos adquiridos no uso comercial prioritário, durante períodos de maiores eventos, e se estes recursos não forem suficientes, pode e deve solicitar mais recursos e, após a baixa do evento, pode libertar os recursos adquiridos, sendo que assim apenas paga pelo tempo em que utilizou estes novos recursos. Qualquer cenário é conveniente para o utilizador [9].

2.2.5 Measurable Services

Medir não é mesma coisa que facturar, embora esteja na base de uma facturação. Entre os vários serviços disponibilizados pela computação em nuvem, a maior parte destes serviços são pagos; também existem serviços gratuitos, que os utilizadores podem utilizar para testes ou mesmo para produção. O utilizador também tem a possibilidade de ter um crédito para utilizar os serviços gratuitamente, e para experimentar se vão de encontro às suas necessidades de negócio. [9].

A metrologia utiliza a tecnologia e outros meios para alcançar a unidade, precisão e medição confiável. Pode afirmar-se que os serviços de computação em nuvem são todos mensuráveis, alguns desses serviços baseiam-se no tempo, outros baseiam-se em quotas de

recursos utilizados e alguns baseiam-se no tráfego. O serviço de medição ajuda os utilizadores a controlar e a optimizar a alocação de recursos, com precisão, de acordo com seu próprio negócio e o seu custo mensal com os serviços.

Na computação em nuvem, habitualmente, o sistema que gere a facturação, serve, especificamente, para recolher e processar dados de utilização, envolvendo a liquidação dos fornecedores de serviços e a facturação dos recursos dos utilizadores da nuvem.

Os sistemas de gestão de preços são desenvolvidos com vários critérios e regras de preços, e podem também personalizar e optimizar o modelo de preços, consoante cada utilizador de nuvem ou para cada recurso de TI, conforme indica [2].

Na facturação, os utilizadores têm a opção de escolha no modelo de pagamento, podendo assim escolher entre utilização pré-paga ou o pagamento após a utilização. Este último tipo de pagamento é dividido em limites predefinidos e tem uso ilimitado. Se o limite for definido, geralmente, aparecem na forma de quota. Isso quer dizer que existe uma quota definida, e se estes limites foram ultrapassados o sistema pode rejeitar qualquer utilização de recursos adicionais, logo implica risco para empresas que utilizam ou fornecem serviços críticos.

Imaginemos que um utilizador dispõe de uma quota de memória de 500 GB, quando a capacidade de armazenamento do utilizador na computação em sistema de nuvem atingir os limites definidos de 500 GB, novas solicitações de armazenamento serão rejeitadas [8].

A computação em nuvem, permite aos utilizadores adquirirem os serviços de acordo com suas necessidades de negócio, fazendo assim a sua gestão de custos e podem visualizar, a utilização dos seus serviços adquiridos. Para utilizadores contratados, o tipo de produto utilizado consiste em serviços com requisitos de qualidade, com custo por unidade de tempo ou custo por solicitação de serviço, que são geralmente especificados no contracto [9].

A Figura 4 apresenta os padrões de preço das instâncias do *Amazon Elastic Cloud Server*, mostra os padrões de precificação de instâncias de servidor virtual, com diferentes configurações, e pode não estar actualizada dado que as tabelas de preços das plataformas podem ser alteradas no momento em que adquirimos os serviços. Neste exemplo, são cobrados mensalmente.

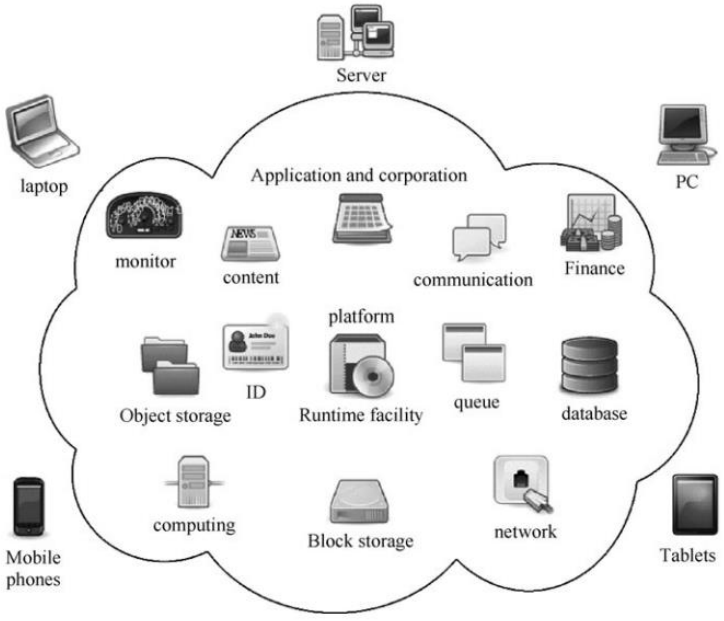
General computing-plus c7n	c7n.xlarge.4	4 vCPUs	16 GiB	Intel Ice Lake 2.6GHz	1.6 / 8 Gbit/s	800,000 PPS
General computing-plus c7n	c7n.2xlarge.2	8 vCPUs	16 GiB	Intel Ice Lake 2.6GHz	3 / 15 Gbit/s	1,500,000 PPS
General computing-plus c7n	c7n.2xlarge.4	8 vCPUs	32 GiB	Intel Ice Lake 2.6GHz	3 / 15 Gbit/s	1,500,000 PPS
General computing-plus c7n	c7n.3xlarge.2	12 vCPUs	24 GiB	Intel Ice Lake 2.6GHz	5 / 17 Gbit/s	2,000,000 PPS

Selected specifications **General computing-plus | c7n.large.2 | 2 vCPUs | 4 GiB**

4) Figura 4 - Pricing standards for Huawei Elastic Cloud Server Instances, adaptado de: [8].

2.3 Modelos de Serviços

As plataformas de computação em nuvem podem oferecer diversos modelos de serviço de nuvem, como: IaaS, PaaS e SaaS, GaaS, XaaS FaaS, entre outros. Diferentes camadas de nuvens fornecem diferentes serviços. A Figura 5 mostra a composição de um típico sistema de computação em nuvem.



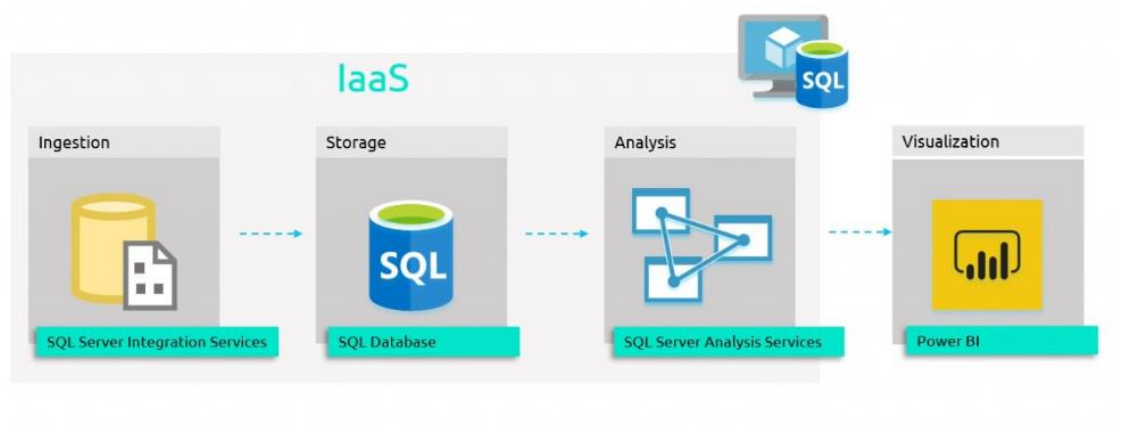
5) Figura 5 Modelos de Cloud Computing, fonte: [8].

2.3.1 IaaS

Na composição do modelo de computação em nuvem, a IaaS situa-se na parte inferior do serviço da computação em nuvem, e é a base estrutural coberta pela definição restrita de

computação em nuvem. A IaaS fornece a infra-estrutura de TI aos utilizadores, sob a forma de serviços como água e electricidade, e aos recursos de TI altamente escaláveis e conforme as necessidades dos utilizadores, com base no hardware, recursos como servidores e armazenamento na forma de serviços. Geralmente é cobrado de acordo com o custo dos recursos consumidos [8].

A camada de serviços fornecidos pela IaaS fornece recursos básicos de computação e armazenamento. Pode fornecer diversos recursos de computação, tais como, a unidade básica: o servidor virtual, incluindo CPU, memória, sistema operacional e alguns softwares, conforme indicado na Fig. 6. A instância específica é a Azure VM [8]

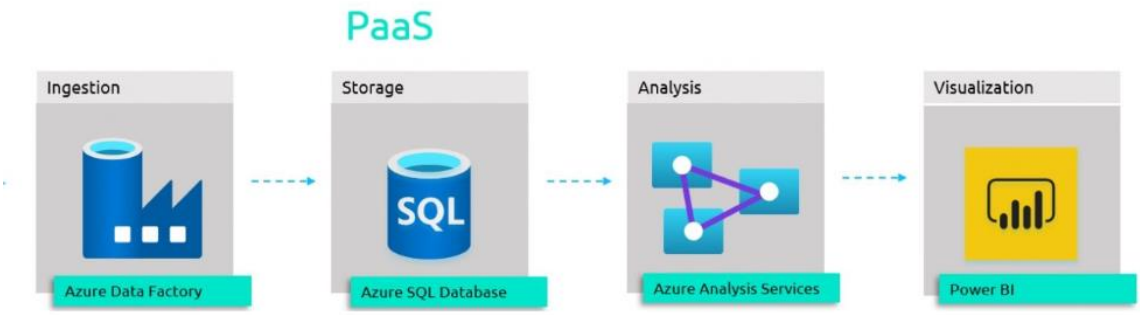


6) Figura 6 Modelos de Cloud Computing (Iaas, fonte: [8].

2.3.2 PaaS

Dos modelos da computação em nuvem, o PaaS situa-se no meio do serviço da computação em nuvem, e é, por diversas vezes, referido como um "sistema operacional em nuvem", conforme mostrado na Figura 7. Fornece aos utilizadores finais um ambiente baseado na Internet, incluindo interfaces de programação de aplicações e plataformas de sistemas operacionais e suporta imensos recursos de software/ hardware, bem como as ferramentas necessárias para todo ciclo de vida de uma aplicação, desde a sua criação até à operação [1].

No modelo PaaS, os fornecedores de serviços oferecem serviços de TI encapsulados em capacidades ou nalguns recursos lógicos, como bases de dados, sistemas de arquivos e ambientes operacionais, como o software. Exemplos de produtos PaaS incluem a nuvem de desenvolvimento de software da Azure [9].



7) Figura 7 Modelos de Cloud Computing (Paas), fonte: [8]

O modelo de computação PaaS é, geralmente, destinado a desenvolvedores de software. Era um problema que o desenvolvedor enfrentava, o de escrever e executar programas num ambiente de computação em nuvem, por meio de rede. Com a possibilidade de aumento gradual da largura de banda da rede, o surgimento de duas tecnologias resolveu esse problema. Uma delas são as ferramentas de desenvolvimento online [2].

Os desenvolvedores podem utilizar navegadores, consolas remotas (executando ferramentas na consola) que é muito comum na actualidade e outras tecnologias, para desenvolver 14 aplicações remotamente, sem a necessidade de instalar ferramentas de desenvolvimento no dispositivo local, e o outro são as ferramentas de desenvolvimento local e a tecnologia integrada de computação em nuvem, ou seja, implementar uma aplicação desenvolvida no ambiente de computação em nuvem, por meio de ferramentas de desenvolvimento local, enquanto habilita a depuração remota [8].

2.3.3 SaaS

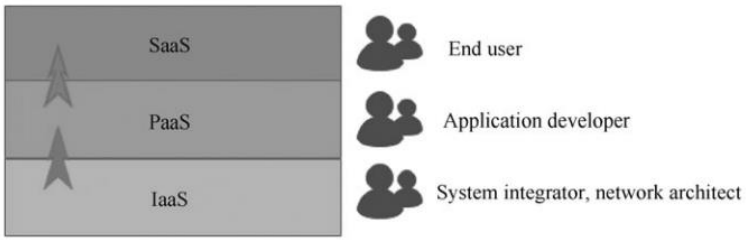
É no modelo SaaS, que existe o serviço de computação em nuvem mais comum, desde os sites que acedemos, aplicações, Office 365 e muito mais, localizado no topo do serviço de computação em nuvem, conforme mostrado na Figura 2.8. Permite ao utilizador utilizar o software na Internet, por meio de um navegador da Web padrão. Os fornecedores de serviços em nuvem são responsáveis por manter e gerir o software, o hardware, as instalações e fornecer serviços aos utilizadores finais, para serviços gratuitos ou sob contracto [8].

Esses serviços são para utilizadores em geral, como o Office 365 e G-suite, e para grupos empresariais, para auxiliar no processamento dos dados do pagamento, na gestão de recursos humanos, na colaboração, na gestão de relacionamento com os clientes e parceiros de negócio [8].

Essas aplicações de SaaS fornecidas reduzem o tempo para os utilizadores instalarem e manterem o software, os seus requisitos de hardware e podem reduzir as taxas de licença de software através do pagamento por utilização, na modalidade "*pay as you go*".

Cada um dispõe de suporte técnico, correspondente ao fornecimento do serviço desta camada, ou seja, o fornecedor de serviços disponibiliza vários suportes técnicos e o cliente escolhe de acordo com a sua necessidade e complexidade de serviço adquirido, com características de computação em nuvem, como o dimensionamento elástico e a implementação automática. Cada camada de serviços em nuvem pode ser independente numa nuvem, ou com base nos serviços fornecidos pelos modelos de nuvens anteriores.

Cada tipo de nuvem pode ser fornecido, directamente, aos utilizadores finais para utilização ou pode ser utilizado para oferecer suporte a serviços disponibilizados na camada superior. Os três tipos de modelos de serviço têm, geralmente, utilizadores de diferentes grupos [8], conforme demonstrado na Fig. 8, para que servem os 3 principais modelos da computação em nuvem.



8) Figura 8 - Modelos de Cloud Computing (Saas), fonte: [8]

2.3.4 GaaS (Gaming-as-a-Service)

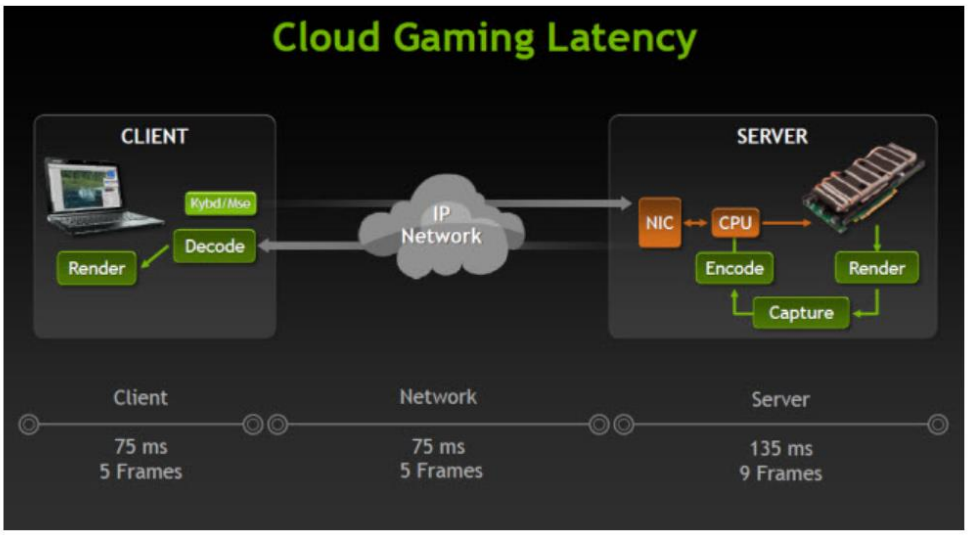
Gaming as a Service refere-se a jogos que operam sem custos iniciais de compra e, em vez disso, lucram com assinaturas ou compras no jogo [11].

O modelo *gaming as a Service* possibilita que os jogos de computador sejam rentabilizados mesmo depois de serem lançados, e foi comprovado que mantêm os jogadores mais empenhados por mais tempo. Em vez de vencer um nível, perder o interesse e esquecer o jogo no fundo do armário, este tipo de modelo possibilita às plataformas manter os jogadores envolvidos e motivados em vários ciclos do jogo, os jogadores são constantemente trazidos de volta, com a promessa de conteúdo novo e actualizado.

Os *Gaming as a Service* (GaaS) geralmente, podem ser transmitidos directamente da nuvem para um dispositivo do utilizador, permitindo acesso aos mesmo em qualquer lugar e em qualquer momento. Esta abordagem também facilita a funcionalidade de plataforma cruzada, um aspecto crucial para se manter competitivo na indústria dos jogos [12].

Essa estratégia possibilita a actualização regular dos jogos, podendo ocorrer semanal, mensal ou até diariamente, com o intuito de manter os utilizadores entusiasmados e envolvidos. A introdução de novo conteúdo muitas vezes é anunciada por meio de "drops" ou lançamentos, seguindo uma técnica semelhante à estratégia de marketing de produtos de luxo [2].

Os *Gaming as a Service* também são conhecidos como "jogos em nuvem", "jogos a pedido", " *Gaming as a Service* ao vivo" ou "streaming de jogos". Alguns exemplos populares de Gaming as a Service incluem o Candy Crush, Fortnite, Destiny e Overwatch [12], conforme ilustrado na Figura 9, que mostra como o serviço de jogos é oferecido aos utilizadores finais.



9) Figura 9 - Modelos de Cloud Computing (Gaas), fonte: [8]

2.3.5 Function as a Service (FaaS)

O FaaS é uma das maiores tendências da computação em nuvem para os próximos anos. A sua adopção no mercado tem vindo a ocorrer em razão dos benefícios que oferece, em comparação com o PaaS — modelo do qual o FaaS se tornou uma alternativa.

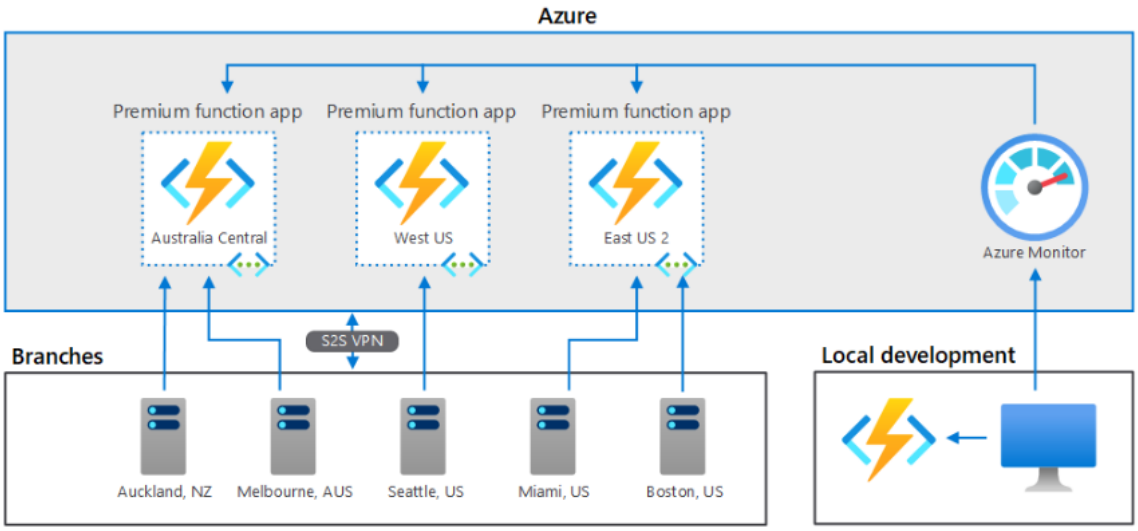
O FaaS emerge como uma das principais tendências da computação em nuvem nos próximos anos. A sua adopção no mercado tem crescido, devido aos benefícios que oferece em comparação com o PaaS (Plataforma como Serviço), do qual o FaaS se tornou uma alternativa [8].

Um dos factores mais convincentes para líderes de negócios é a redução de custos proporcionada pelo FaaS. Enquanto o PaaS oferece vantagens nesse sentido, o potencial de economia do FaaS é ainda maior, uma vez que é uma solução de nuvem desprovida de gestão de infra-estrutura.

Para entender essa comparação, o PaaS fornece uma plataforma composta por infra-estrutura e software geridos pelo utilizador, resultando em recursos computacionais disponíveis 24/7, mesmo quando não está a ser utilizado esse mesmo recurso. Isso leva à activação do modo *standby* do servidor e gera desperdício de recursos [1].

No caso do FaaS, os recursos são consumidos apenas quando uma função ou código da aplicação é executado. Os servidores respondem a eventos isoladamente, são "descartáveis" e não mantêm relações entre si. Dessa forma, a execução e a tarefa têm o mesmo ciclo de vida, como exemplo no mercado temos o “Azure Functions” [7].

O cálculo do consumo de FaaS é feito de maneira diferente do convencional. Em vez de os utilizadores pagarem pelo consumo mensal, o cálculo é realizado para cada execução ou tempo de execução. Essa abordagem mais precisa permite que os administradores optimizem melhor o orçamento e desenvolvam estratégias de redução de custos, como ilustrado no exemplo das “Azure Functions” na Figura 10.



10) Figura 10 - Modelos de Cloud Computing (Faas), fonte: [21]

2.3.6 XaaS (Everything as a Service)

Com o desenvolvimento da computação em nuvem, é evidente que a tendência para os próximos anos será a disponibilização de qualquer tipo de serviço computacional pelos fornecedores de computação em nuvem.

O uso comum do acrónimo XaaS na área, indica que os modelos de nuvem apresentados representam apenas a ponta do iceberg, onde o "X" simboliza a "infinitude" de serviços que a nuvem pode oferecer.

Perante esse cenário, a capacidade para trabalhar com essa tecnologia torna-se um diferencial para o profissional do futuro. Para aqueles que desejam iniciar esse caminho, a sugestão é escolher entre áreas que tendem a gerar maior procura nos próximos anos, como a Segurança da Informação, Arquitectura de Computação em Nuvem, Big Data, Inteligência Artificial e Internet das Coisas [11].

Além disso, é esperado o surgimento de vários outros modelos de computação em nuvem, semelhantes aos que já se estão a disseminar no mercado, incluindo o Content as a Service (CaaS), Energy Storage as a Service (ESaaS), Database as a Service (DBaaS), Backup as a Service (BaaS), Game as a Service (GaaS), Robots as a Service (RaaS), entre muitos outros.

Essa diversidade de serviços indica a expansão contínua e a adaptação da computação em nuvem para atender às diversas necessidades do mercado.

2.4 Modelos de implementação de Cloud Computing

2.4.1 Nuvem Pública

A nuvem pública refere-se a um ambiente de nuvem que está acessível publicamente através da Internet e, geralmente, é propriedade de um fornecedor de serviços de nuvem terceirizado. O termo "pública" é utilizado porque esse tipo de nuvem pode ser acedido pelo público em geral, sem restrições. Os fornecedores de serviços de nuvem pública oferecem uma gama completa de serviços, desde a infra-estrutura física até à instalação de aplicativos e ambientes operacionais de software.

Nesse modelo, os utilizadores finais alcançam os seus objectivos por meio de recursos compartilhados e pagam apenas pelos recursos que utilizam, seguindo o modelo conhecido como "pay-as-you-go". Essa abordagem permite que as empresas paguem apenas pelos serviços que realmente necessitam, e desta forma diminuem despesas [11].

No entanto, na nuvem pública, os utilizadores não têm conhecimento sobre com quem estão a partilhar os recursos e como esses recursos subjacentes são implementados. Eles também não têm controle sobre a infra-estrutura física. Portanto, é responsabilidade do fornecedor de serviços em nuvem garantir a segurança e confiabilidade dos recursos fornecidos, bem como assegurar os outros requisitos não funcionais [7].

A qualidade desses serviços não funcionais também influencia o nível de serviço do fornecedor de serviços em nuvem. Para serviços em nuvem que precisam de cumprir rigorosamente a segurança e conformidade regulamentares, são necessários níveis de serviço mais elevados e maduros. Exemplos de nuvens públicas incluem o Google App Altice Cloud, Amazon EC2, IBM Developer, Microsoft O365, Tencent Cloud, Alibaba Cloud, Cloud Huawei, Ucloud, etc, podemos verificar na Fig. 11, a distinção entre vários tipos de implementação de Cloud Computing [8].

2.4.2 Nuvem Privada (On-premises)

As empresas e outras organizações sociais, não são abertas à nuvem pública. Serviços que são geridos e implementados pela própria entidade ou empresas, para fornecer serviços a funcionários da própria empresa, são chamados de nuvens privadas [7].

Empresas e outras organizações sociais que não optam por utilizar a nuvem pública, muitas vezes, recorrem a serviços geridos e implementados internamente para fornecer serviços aos seus funcionários. Esses serviços são conhecidos como nuvens privadas [11].

Em comparação com as nuvens públicas, os utilizadores de nuvens privadas têm controle total sobre as instalações centrais da nuvem, podendo decidir onde os programas são executados e quais os utilizadores que têm permissão para aceder aos serviços em nuvem.

Os serviços de nuvem privada são direccionados para empresas ou organizações e podem estar sujeitos a menos restrições do que aquelas que precisam ser consideradas em nuvem públicas, como limitações de largura de banda, questões de segurança e condições de regularização. Além disso, as nuvens privadas podem oferecer garantias adicionais de segurança e privacidade, proporcionando um controlo rigoroso sobre as restrições de rede aos utilizadores.

Os tipos de serviços oferecidos por nuvens privadas são diversificados. Elas não se limitam apenas a fornecer serviços de infra-estrutura de TI, mas também oferecem suporte a serviços em nuvem, como aplicações e ambientes operacionais de *middleware*, incluindo serviços em nuvem do sistema interno de informações de administração (IMS), [9], conforme podemos ver na Fig. 11, que apresenta vários tipos de implementação da computação em nuvem.

2.4.3 Nuvem Híbrida

A nuvem híbrida é uma combinação da nuvem pública e privada, permitindo que os utilizadores possuam e compartilhem serviços de nuvem de ambas as formas e de uma maneira controlada. As empresas podem tirar proveito dos custos mais baixos das nuvens públicas para executar aplicações menos críticas, enquanto fornecem serviços através da nuvem privada interna para aplicações mais essenciais, com requisitos de segurança mais altos e críticos [7].

Existem várias razões para optar por uma nuvem híbrida, sendo as principais:

- Compromisso de Múltiplas Considerações: algumas organizações desejam aproveitar os benefícios da nuvem pública, mas devido a regulamentações, requisitos de confidencialidade ou restrições de segurança, não podem migrar todos os seus recursos para a nuvem pública. Nesses casos, parte dos recursos de TI é implementada no local da empresa, formando uma nuvem híbrida, conforme podemos ver na Fig. 11, que apresenta vários tipos de implementação da Cloud Computing [11]
- Transição da Nuvem Privada para a Nuvem Pública: a transição gradual da nuvem privada para a nuvem pública é outra razão para a adopção de nuvens híbridas. Algumas organizações podem começar com a nuvem privada e, ao longo do tempo,

migrar gradualmente para a nuvem pública à medida que se tornam mais confortáveis com a tecnologia e superam obstáculos regulamentais ou de segurança.

A nuvem pública é considerada a principal corrente de desenvolvimento na computação em nuvem, devido à sua eficiência na utilização de recursos. No entanto, a coexistência de nuvens privadas e públicas é esperada por um longo período, seguindo uma trajectória de desenvolvimento comum [8].

A analogia com serviços bancários é mencionada, onde a transferência de dinheiro para custódia bancária é mais segura e conveniente, mas algumas pessoas optam por manter o controlo dos seus recursos [8].

11) Figura 11 - Métodos de implementação de Cloud Computing, Bmc blogs, fonte: [34]

2.5 Vantagens

Certamente, a implementação e inovação de qualquer tecnologia tem o foco de colmatar as necessidades específicas de determinados grupos de pessoas ou empresas. A computação em nuvem não foge a essa regra. Ela tem gradualmente penetrado em todas as áreas da vida e produção, proporcionando comodidade e benefícios tanto para pessoas quanto para

empresas. As vantagens da computação em nuvem são diversas, podemos ver na Fig. 12 os benefícios da computação em nuvem, mas vamos citar as seguintes [7]:

1. Baixo custo

Na computação em nuvem, as empresas podem minimizar ou cortar completamente o investimento, porque não precisam de implementar centros de dados ou criar software/ plataformas de hardware por conta própria, nem precisam de contratar profissionais para o desenvolvimento, operação e manutenção. É muito mais barato utilizar serviços de computação em nuvem, do que comprar software/ hardware, para construir o sistema requerido.

2. Os dados podem ser acedidos, instantaneamente, a qualquer hora, em qualquer lugar.

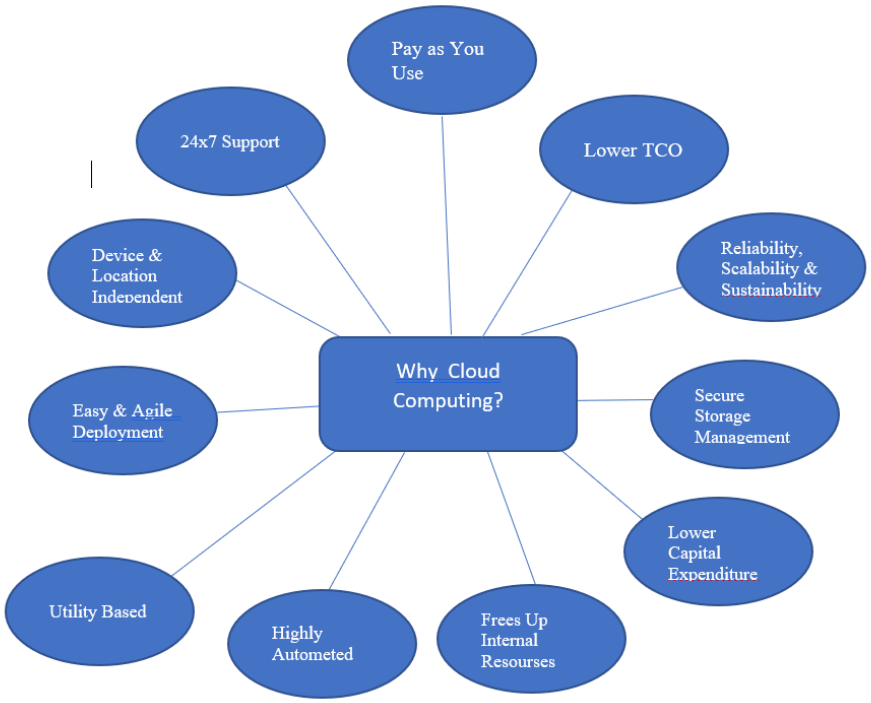
A "*Nuvem*" traz maior flexibilidade e mobilidade. Ao utilizarem a computação em nuvem, as empresas podem aceder, instantaneamente, às suas contas através de qualquer dispositivo, a qualquer hora e em qualquer lugar; os dados podem ser armazenados, transferidos, restaurados ou processados facilmente, economizando muito tempo e esforço.

3. Melhorar a adaptabilidade e expandir de forma flexível as necessidades, na maioria dos casos, a capacidade do sistema de TI não corresponde às necessidades do empreendimento. Se uma empresa configura equipamentos de TI de acordo com o volume necessidade (*demand*), estes ficarão ociosos em horários normais, resultando em desperdício de investimento.

Se uma empresa configura equipamentos de TI de acordo com a sua necessidade média, tal não será suficiente durante o pico de utilização. No entanto, com os serviços em nuvem, as empresas podem fazer escolhas mais flexíveis e aumentar, diminuir ou libertar os recursos que solicitarem, a qualquer momento.

4. Plataforma unificada

As empresas podem executar diferentes tipos de plataformas e dispositivos, em simultâneo.



12) Figura 12 - Vantagens da Cloud Computing, adaptado de: [1]

2.6 Desvantagens

A adopção da computação em nuvem também apresenta desafios e preocupações relacionados com a segurança e a confiabilidade. Algumas das principais desvantagens que podemos elencar incluem:

- Impossibilidade de acesso a informações e aplicações, caso não haja uma ligação ao Wi-Fi, ou na eventualidade de uma falha;

- Possibilidades de falhas do servidor ou saturações pontuais, que impedem ou atrasam o trabalho;

- Perda de controlo directo sobre as informações armazenadas;

- O uso de servidores e recursos partilhados, por diferentes empresas e utilizadores, favorece a possibilidade de falhas de acesso, que geram acesso não autorizado;

- Se as transferências de dados não forem criptografadas, representam um ponto adicional para possíveis fugas de informação;

- Possibilidade de alterações dos locais dos servidores de dados, com desconhecimento da empresa, para países fora do Espaço Económico Europeu (EEE), nos quais não há legislação que garanta os níveis de protecção de dados das empresas [7].

3 Métodos de autenticação e Gestão de identidades

3.1 Conceito

Desde o início da computação ou dos sistemas computacionais, percebeu-se que eram dispositivos compartilhados que não tinham meios de garantir a segurança ou confidencialidade dos dados criados e armazenados, entre os computadores ou dispositivos compartilhados na mesma rede.

Na década de 1960, o MIT desenvolveu o Sistema de Compartilhamento de Tempo Compatível (CTSS), permitindo que vários terminais compartilhassem os recursos de um computador central.

No entanto, surgiu uma preocupação de segurança nos sistemas de arquivos compartilhados. Para abordar esse problema, em 1961, Fernando Corbató, do MIT, introduziu senhas como método de autenticação, para os utilizadores acederem a dados e arquivos específicos [13].

No entanto, Allan Scherr, pesquisador do MIT, descobriu que os sistemas baseados em servidor, armazenavam senhas de forma fácil e acessível num arquivo mestre de senhas, permitindo o acesso a qualquer arquivo protegido por senha.

Na década de 1970, o pesquisador dos Bell Labs, Robert Morris, desenvolveu uma técnica para proteger o arquivo mestre de senhas do sistema operacional Unix. Morris aplicou uma técnica criptográfica chamada "função hash", que tornava uma senha ilegível ao olho humano, mas não para o sistema computacional. Esse conceito básico foi logo adoptado pela maioria dos outros sistemas operacionais [17].

De forma a obter acesso a dados ou serviços, é necessário primeiro verificar a identidade de um utilizador por meio de métodos de autenticação, como senhas, MFA, etc.

A **autenticação** é um processo de validação da identidade e confiabilidade de uma pessoa ou dispositivo [13].

Um exemplo, seria ao usar um cartão bancário para fazer uma compra, em que nos autenticamos, possuindo o cartão e conhecendo o *Personal Identification Number* (PIN). Com a modernização, digitalização e a dependência crescente das pessoas nos dispositivos computacionais, a autenticação tornou-se essencial.

A personificação do utilizador representa um risco crítico de segurança para qualquer sistema computacional. O primeiro mecanismo de defesa contra esse tipo de ataque é permitir que o utilizador se autentique, estabelecendo assim a confiabilidade de quem está a utilizar o sistema [13].

Podemos confirmar a identidade de um utilizador em três dimensões:

• Baseado em conhecimento, o que inclui senhas e PINs;

• Baseado em posse, que inclui cartões inteligentes e *tokens*;

• Baseado em herança, como a biometria, que inclui impressões digitais, faciais, etc.

Ao longo do tempo, à medida que os invasores aprenderam a explorar algoritmos de *hash* por "força bruta", a indústria teve de aprimorar as funções de *hash*, adicionando uma randomização extra. O método de armazenamento de senhas baseado em *hash* desenvolvido por Morris, na década de 1970, contribuiu para melhorar a segurança dos sistemas de autenticação [13].

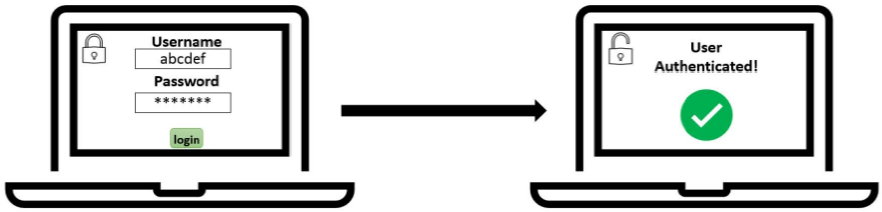
Além do *hashing*, existem outras abordagens criptográficas eficazes para autenticação. A criptografia de chave pública ou assimétrica é uma dessas tecnologias. No início dos anos 1970, foram adoptadas a criptografia assimétrica e as chaves públicas/privadas, para mitigar e corrigir vulnerabilidades nos sistemas de segurança e autenticação.

Na década de 1990, as técnicas de criptografia, especialmente as relacionadas com a chave assimétrica, tornaram-se mais públicas. No final dos anos 1970, pesquisadores começaram a explorar essa tecnologia, resultando no desenvolvimento do popular algoritmo RSA. Certificados e assinaturas digitais tornaram-se cruciais para a autenticação.

Ao mesmo tempo, pesquisadores e cibercriminosos desenvolveram novas abordagens para explorar senhas, já que os sistemas digitais dependiam delas para segurança. Isso levou a uma constante busca por inovações na indústria, para fortalecer a autenticação do sistema, evidenciando a necessidade contínua de melhorias na segurança [13].

Os sistemas de senha permanente apresentam uma vulnerabilidade significativa: se as credenciais de alguém forem obtidas, podem ser reproduzidas. Para combater isso, os pesquisadores desenvolveram estratégias para tornar as senhas únicas em cada login, implementando mudanças frequentes nas senhas, a partir da década de 1990.

Essas estratégias incluem técnicas como o CAPTCHA, um teste automatizado para diferenciar humanos de computadores. Embora o CAPTCHA não autentique directamente os utilizadores, é eficaz na prevenção de ataques automatizados à autenticação.



13) Figura 13 - Single factor authentication, fonte: [13]

A Autenticação Multifactorial (MFA), ganhou destaque desde os anos 2000, surgindo como resposta às limitações das senhas tradicionais. Apesar de as senhas serem amplamente utilizadas, são susceptíveis a roubo e requerem práticas rigorosas de segurança, para serem eficazes.

Muitas pessoas e empresas não seguem essas práticas, resultando em inúmeros vazamentos de dados e várias evidências de insuficiência das senhas para proteger as identidades online. A MFA surge como uma solução para reforçar a autenticação, embora a implementação de alguns sistemas e alternativas possa ser dispendiosa ou desafiadora.

A disponibilidade generalizada de smartphones, na década de 2010, tornou tecnologias como biometria, a autenticação de dois factores (2FA) e a MFA mais acessíveis ao público em geral.

3.2 Factor de autenticação

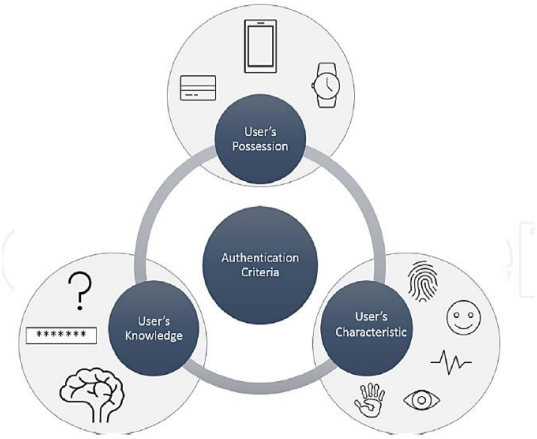
A autenticação é o processo de verificar a identidade de uma pessoa, geralmente através de um nome de utilizador e senha. Este procedimento confirma se a pessoa é quem diz ser.

É importante destacar que a autenticação, por si só, não determina os direitos de acesso dessa pessoa; essa função é desempenhada pela autorização. A autorização é responsável

por conceder acesso a objectos específicos do sistema, com base na identidade autenticada e na gestão dos privilégios de acesso [14].

3.2.1. Autenticação de factor único (SFA)

A técnica de autenticação mais utilizada é uma combinação de nome de utilizador e senha, conforme pode verificar na Fig. 14.



14) Figura 14 - Autenticação de factor único (SFA), fonte: [13]

3.2.1.1. Vantagens

A autenticação de factor único (SFA), ou autenticação de um único factor, refere-se ao método de autenticação que requer apenas um tipo de evidência, para verificar a identidade de um utilizador. As vantagens da autenticação de factor único, incluem a simplicidade e facilidade de utilização, pois os utilizadores precisam de fornecer apenas uma forma de identificação, como uma senha [13].

3.2.1.2. Desvantagens

A autenticação de factor único (SFA), que envolve apenas um método de autenticação, geralmente uma senha, tem várias desvantagens associadas [16]:

Menor Segurança: oferece uma única camada de segurança, tornando-se mais susceptível a ataques, como tentativas de força bruta ou roubo de credenciais.

Vulnerabilidade a Ataques de Senha: como a autenticação depende apenas de uma senha, a exposição ou comprometimento dessa senha, pode resultar em acessos não autorizados.

Falta de Redundância: em caso de esquecimento ou perda da senha, pode ser necessário recorrer a processos de recuperação que, se não estiverem adequadamente protegidos, podem ser explorados por atacantes.

Limitações na Verificação de Identidade: a autenticação baseada num único factor pode ser insuficiente, para verificar efectivamente a identidade, especialmente quando comparada co, métodos mais avançados, como a autenticação multifactorial (MFA).

Facilidade de Ataques de Engenharia Social: ataques de engenharia social, nos quais os utilizadores são enganados, para divulgarem as suas senhas, podem ser mais eficazes em ambientes de SFA.

Risco de Reutilização de Senhas: os utilizadores podem ser tentados a reutilizar senhas em vários serviços, aumentando o risco de comprometimento, caso uma senha seja descoberta.

Conformidade Limitada: certos regulamentos e padrões de segurança podem exigir a implementação de métodos de autenticação mais robustos do que a SFA.

Falta de Adaptabilidade: num mundo em que os métodos de autenticação evoluem, a SFA pode tornar-se obsoleta, comparativamente com opções mais avançadas, como a MFA ou a autenticação baseada em biometria [16].

3.2.2 Autenticação de dois factores (2FA)

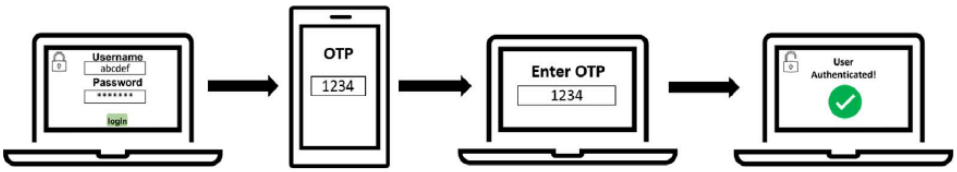
O uso exclusivo da *Single Factor Authentication* (SFA) representa riscos significativos de segurança. A abordagem mais segura é o uso da *Two-Factor Authentication* (2FA), que combina a tradicional combinação de nome de utilizadores/senha como forma de identificação, como um *token* seguro ou uma *One Time Password* (OTP).

A 2FA abrange três grupos de factores para aumentar a segurança, conforme indicado na Fig 15:

1. Factor de propriedade - algo que o utilizador possui, como telemóveis, tablets, portáteis, etc.;

2. Factor de conhecimento - algo que o utilizador conhece, como uma senha (password);

3. Factor biométrico - um facto sobre a biometria ou comportamento do utilizador.



15) Figura 15 Autenticação de dois factores (2FA), fonte: [13]

A implementação deste método de identificação requer um mecanismo adicional, como um dispositivo electrónico, como um telemóvel, tablet ou computador, ou outro componente físico, conforme indicado na figura 15. Após a conclusão da primeira etapa de autenticação, o segundo mecanismo solicita ao utilizador a apresentação de uma *One-Time Password* (OTP), que pode ser enviada por e-mail, SMS ou através de outro dispositivo [13].

3.2.2.1. Vantagens

A autenticação 2FA é um método melhorado para a identificação do utilizador, envolvendo dois ou mais factores para aumentar a segurança. O segundo mecanismo de autenticação, escolhido pelo utilizador, impede o acesso não autorizado, mesmo se as credenciais primárias forem comprometidas.

Isso é conseguido através de dispositivos inteligentes, como senhas e *tokens* gerados, cartões RFID, proporcionando uma experiência de utilizador mais segura e de fácil utilização.

3.2.2.2. Desvantagens

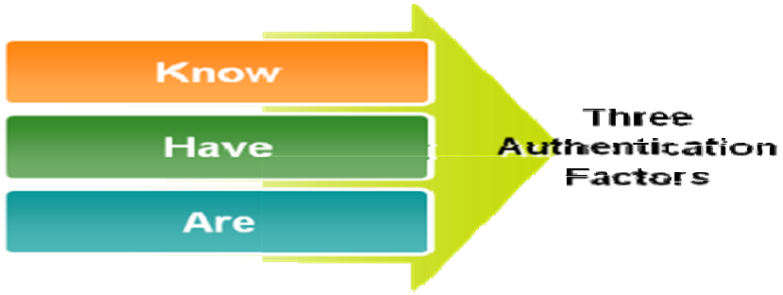
O uso de múltiplos mecanismos de autenticação, como na 2FA, pode complicar o processo, aumentando os custos e reduzindo a acessibilidade. A dependência de ambos os mecanismos pode ser uma desvantagem e a conectividade com esses dispositivos pode apresentar desafios, como a ausência de conectividade do dispositivo, que é um desafio crítico.

3.2.3. Autenticação Multifactorial (MFA)

A autenticação multifactorial é um método de autenticação que envolve três elementos: algo que o utilizador sabe (por exemplo, uma senha), algo que possui, (como um *token*) e

uma característica do utilizador (como uma característica biométrica). Para ser autenticado, cada um desses factores tem de ser confirmado aquando do processo [14].

O uso desses factores aumenta a segurança, tornando mais provável que a identidade seja verdadeira em diversos contextos. Além do número de factores, outros elementos, como senhas, cartões ou características biométricas, contribuem para a garantia da identidade [14].



16) Figura 16 - Autenticação multifactorial (MFA), fonte: [14]

3.2.3.1. Vantagens

A autenticação multifactorial (MFA) combina diversos factores como o conhecimento, a posse e a biometria, para fortalecer a identificação do utilizador. A biometria, especialmente a impressão digital nos smartphones, desempenha um papel crucial nesse processo, tornando-o acessível e eficaz. A MFA é valiosa em contextos como cursos online, transacções bancárias e registos de saúde, garantindo uma autenticação segura e consistente.

3.2.3.2. Desvantagens

A utilização de elementos biométricos na MFA, enfrenta desafios relacionados à facilidade de utilização e à precisão. Discrepâncias entre a apresentação biométrica e os dados registados podem ocorrer, especialmente, com equipamentos menos precisos. A Taxa de Aceitação Falsa (FAR) e a Taxa de Falsa Rejeição (FRR) são preocupações críticas, dado que atingir uma precisão total nessas métricas é praticamente impossível [15].

3.2.4. Certificados Digitais

Utiliza chaves criptográficas e certificados digitais para autenticar os utilizadores e dispositivos.

3.2.5. OAuth (Open Authorization)

Trata-se de um protocolo de autorização, que permite que as aplicações acedam a recursos em nome de um utilizador, sem compartilhar as senhas directamente.

3.2.6. OpenID Connect

É um protocolo de autenticação que opera sobre o OAuth 2.0, e que fornece uma autenticação segura em aplicações da web e telemóveis.

3.2.7. SAML (Security Assertion Markup Language)

Trata-se de um protocolo de intercâmbio de informações de autenticação e autorização entre partes, especialmente útil em ambientes de associação de identidade.

3.2.8. LDAP (Lightweight Directory Access Protocol)

É um protocolo padrão, para aceder a directórios de serviços de directório, comumente utilizado para a autenticação em ambientes corporativos.

3.2.9. Kerberos

Trata-se de um protocolo de autenticação, que utiliza tickets para verificar a identidade dos utilizadores, em redes de computadores.

3.2.10. Azure AD (Active Directory) e Single Sign-On (SSO)

Consiste em soluções de autenticação e autorização, disponibilizadas pela Microsoft para a gestão de identidades em ambientes corporativos.

3.3 Técnicas de autenticação

Existem 3 factores, um factor de conhecimento, um factor de posse e um factor de característica de utilizador, que podem ser associados de uma forma individual a várias técnicas e protocolos existentes, conforme indicado na figura 17 [14].

Dependendo dos critérios mencionados anteriormente, agrupamos e relatamos as seguintes técnicas:

Criterion	Technique
Users Possession	Smart Card Cell Phone Password Secure Token
Users Knowledge	Cognitive Password PIN Personal Questions
Users Characteristic	Fingerprints Retina Facial Features Hand Geometry

17) Figura 17 - Técnicas de autenticação, fonte: [13]

O custo da apresentação biométrica é geralmente alto e, por conseguinte, é utilizado em casos especiais e raros. Ao combinar várias técnicas em MFA, é considerada uma boa prática seleccionar critérios de grupos distintos, e combiná-los para criar um processo de autenticação altamente seguro.

Em muitos casos, as informações de localização do utilizador real também são consideradas no processo de autenticação, utilizando o GPS, o endereço IP ou a geolocalização.

A MFA é amplamente utilizada para a identificação e autenticação, no acesso a dados confidenciais.

3.3.1. Segurança de senha

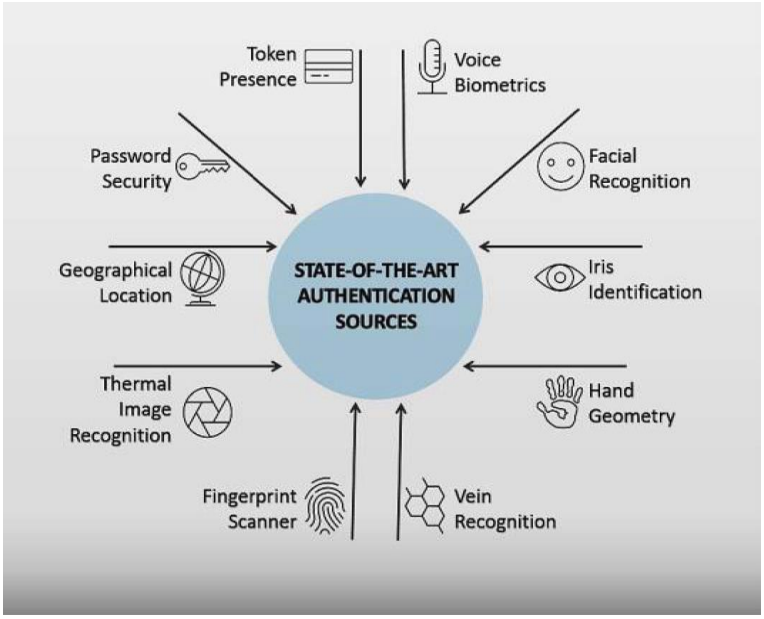
Uma senha é uma chave secreta utilizada para a autenticação do utilizador, sendo o método mais comum. Muitas técnicas de autenticação de dois factores baseiam-se na senha como um dos factores [14].

3.3.2. Cartões Inteligentes e Tokens

A autenticação pode ser aumentada com um *token* tangível, como forma de provar a propriedade.

Exibir códigos dinâmicos em telas LCD ou *e-ink* que proporcionam a autenticação, sem a necessidade de uma ligação electrónica.

O número gerado criptograficamente a partir de um segredo compartilhado, evita a dedução do segredo a partir da sequência de números, este tipo de método utiliza, geralmente, um programa único (OTP) para gerar esses tipos de códigos [14].



18) Figura 18 - Fontes de autenticação de última geração, fonte: [13]

3.3.3. Biometria de Voz

O reconhecimento da fala visa verificar a identidade do locutor em relação a um padrão de voz armazenado, sem compreender o conteúdo falado [14].

3.3.4. Reconhecimento facial

A tecnologia de reconhecimento facial utiliza características distintivas da face, tais como os contornos oculares, as maçãs do rosto e a posição do nariz e dos olhos.

No entanto, depender exclusivamente de uma única característica biométrica, como a impressão digital ou rosto, apresenta desvantagens, como a variação na qualidade das impressões digitais, distorção elástica da pele devido a métodos de detenção por toque e problemas potenciais com a higiene e limpeza do sensor, que podem interferir com a tecnologia.

3.3.5. Reconhecimento visual

A tecnologia de reconhecimento visual, que inclui a digitalização da retina e da íris, apresenta desafios próprios. O hardware é caro e especializado, e a utilização é lenta e inconveniente, podendo causar desconforto aos utilizadores.

Esta tecnologia já existe há mais de 20 anos, por ser uma tecnologia de elevado custo, o seu crescimento tem sido gradual, distinto das outras que existem no mercado.

3.3.6. Geometria da mão

Estamos habituados a impressões digitais, mas raramente pensamos na mão inteira como um identificador individual. Este método depende de dispositivos que medem o comprimento e os ângulos de cada dedo. Embora seja mais fácil de utilizar que as varreduras de retina, ainda assim é complicado [14].

3.3.7. Scanner de Impressão Digital

As impressões digitais são reconhecidas como únicas e são facilmente acessíveis, necessitando de pouco espaço físico para o hardware de leitura ou armazenamento de dados [14].
A autenticação por impressão digital, é comumente utilizada em dispositivos móveis e até mesmo em cartões de cidadão. No entanto, esse método simples pode ser explorado por meio da recolha de impressões digitais de objectos tocados. Embora tenha potencial de integração, não é recomendado como um mecanismo de autenticação autónomo [13].

3.3.8. Reconhecimento de Imagem Térmica

Os sensores térmicos são utilizados para construir uma imagem térmica única do sangue de um indivíduo, da estrutura do vaso sanguíneo na face, conforme indicado por Velásquez I, Caro A, Rodríguez A. Tal é particularmente útil, em situações onde níveis baixos de luz podem ser um problema [15].

No entanto, o desempenho na apresentação pode ser afectado, como resultado do estado de bem-estar do utilizador, que pode alterar as suas características [13].

3.3.9. Localização Geográfica

Esta técnica permite identificar logins ou acesso a partir de uma localização especifica, vamos dar um exemplo que de certeza ocorre no nosso dia a dia, a utilização da VPN, como sabemos, há países nos quais não é possível aceder a redes sociais especificas do IP publico do pais; para contornar essa situação, a população utiliza uma VPN que escolhe um IP doutro pais e logo mascara a localização para aceder a essas redes, isso quero dizer que esta tecnologia permite restringir ou adicionar um determinado acesso, com base na localização do utilizador.

3.3.10. Técnicas Beam-forming

Referem-se a métodos utilizados no processamento de sinais para direccionar ou concentrar sinais numa direcção específica. Essas técnicas são frequentemente aplicadas em sistemas de comunicação sem fio, radar, sonar e *arrays* de microfones.

Podem ser analógicas, ajustando fase e amplitude, ou digitais, envolvendo o processamento de sinais após a recepção. O objectivo principal é o de melhorar a qualidade do sinal, reduzir interferências, oferecer filtragem espacial e ampliar o alcance em diversas aplicações [13].

3.3.11. Sistemas de Classificação de Ocupantes (OCS)

Os sistemas de OCS em veículos, utilizam sensores para reconhecer as características dos ocupantes, como o peso ou a postura, ajustando automaticamente as configurações do veículo para proporcionar um maior conforto personalizado, a cada utilizador.

3.3.12. Dados Electrocardiográficos (ECG)

O ECG capturados a partir de um dispositivo computacional, podem ser analisados para um padrão específico, sendo uma possível via biométrica de difícil falsificação de dados, proporcionando precisão e benefícios significativos para a autenticação.

3.3.13. Dados Electroencefalográficos (EEG)

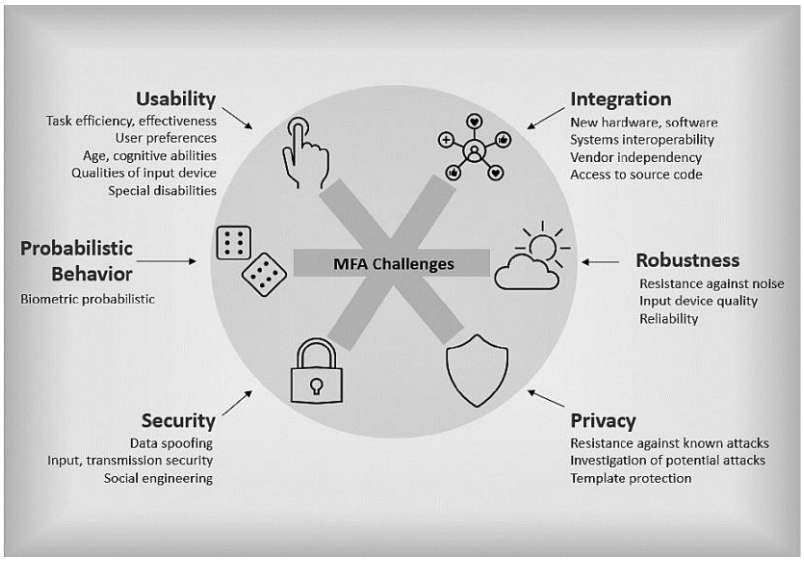
Os dados electroencefalográficos (EEG) envolvem a análise da função cerebral, permitindo a recolha de padrões individuais de actividade cerebral. Anteriormente limitada a contextos clínicos, a recolha de dados EEG é agora possível com dispositivos comercialmente acessíveis, como auriculares [15].

3.3.14. Reconhecimento de Ácido Desoxirribonucleico (DNA)

Este produto químico orgânico do interior do corpo, contém informações genéticas únicas, e é individual, tal como as impressões digitais e é altamente preciso na determinação da identidade do utilizador.

Envolve a utilização do material genético único no corpo, como outros tipos de técnicas biométricas, para determinar a identidade do utilizador.

É uma técnica que tem um custo elevado e é um processo demorado, desta forma é utilizada para casos específicos e muito sensíveis, conforme indicado na Fig. 19.



19) Figura 19 - Fontes de autenticação de última geração, fonte: [13]

3.3.15. Comparação de Factores de MFA

A MFA é um sistema de segurança, que utiliza duas ou mais formas de autenticação para garantir a legitimidade de um acesso. Este método cria camadas de defesa, dificultando o acesso não autorizado a sistemas ou redes. Utiliza os 3 factores, conhecimento (PIN), posse (*token* ou cartão inteligente) e as características biométricas do utilizador [15].

As técnicas de autenticação podem ser avaliadas na MFA, com os seguintes princípios fundamentais de características biométricas [13], conforme pode verificar na figura 20:

- Universalidade: o que está presente em cada indivíduo;
- Unicidade: capacidade de distinguir um indivíduo do outro;
- Colheita: facilidade de recolher dados para processamento;
- Desempenho: precisão, eficiência e robustez alcançáveis;
- Aceitabilidade: aceitação na vida quotidiana;
- *Spoofing*: dificuldade em recolher e falsificar uma amostra;

Factor	Universality	Uniqueness	Collectability	Performance	Acceptability	Spoofing
Password	Unavailable	Low	High	High	High	Low
Token	Unavailable	Medium	High	High	High	Low
Voice	High	Medium	Medium	Low	High	Medium
Facial	High	Medium	Medium	Low	High	Medium
Eye	High	High	Medium	Medium	Low	High
Hand geometry	High	Medium	Medium	Medium	Medium	Medium
Fingerprint	High	High	Medium	High	Medium	High
Thermal image	High	High	Low	Medium	High	High
Location	Unavailable	Low	High	High	Medium	Medium
Beam-forming	Unavailable	Medium	Low	Low	Low	High
OCS	High	Low	High	Low	Low	Medium
ECG	High	High	Low	Medium	Medium	Medium
EEG	High	High	Low	Medium	Low	High
DNA	High	High	Low	High	Low	High

20) Figura 20 - Comparação de factores de MFA, fonte: [13]

3.4 Gestão de Identidades

A gestão de identidades consiste no conjunto de processos e tecnologias utlizadas para controlar e gerir as identidades digitais de utilizadores numa organização, garantindo o acesso seguro aos recursos e informações, conforme a autorização e políticas definidas [17]:

Vamos citar alguns dos mais utilizados tipos de gestão de identidades utilizados pelos fornecedores da nuvem:

1. Utilizador e Senha: A autenticação tradicional com nome de utilizador e senha é comumente usada para aceder a serviços e plataforma da nuvem;

2. Chaves de Acesso: Com o surgimento do APIs ou o acesso a serviços na nuvem por meio de programação, as chaves de acesso, como as chaves de acesso da plataforma e as chaves secretas, são frequentemente utilizadas na autenticação;

3. 2FA /Autenticação Multifator (MFA): Suporta a autenticação com vários factores, o que adiciona uma camada adicional de segurança, exigindo um segundo factor de autenticação para além das credenciais padrão;

4. Assinaturas e *Tokens*: Para interacções seguras entre os serviços, as plataformas utilizam assinaturas e *tokens* para efeitos de autenticação e autorização.

5. *Identity and Access Management* (IAM): é um serviço fundamental que permite gerir o acesso a recursos de maneira segura;

6. Federação de Identidade: A federação de identidade permite que as organizações integrem os seus sistemas de identidade existentes com a AWS ou Azure, por exemplo;

7. *Single Sign-On* (SSO): é um serviço que facilita a gestão do acesso a várias contas e aplicações. Com um único acesso, os utilizadores acedem a diversos recursos, sem a necessidade de uma password para cada recurso, permite a utilização de um único conjunto de credenciais;
8. *Active Directory* (AD): O AD é o serviço de gestão de identidades da Microsoft baseado na nuvem. Fornece recursos tais como a autenticação do utilizador, a autorização e a gestão de directórios. É amplamente utilizado para autenticar utilizadores e controlar o acesso a recursos;

9. AD B2C (*Business to Consumer*): Este serviço estende as capacidades do AD para permitir a gestão de identidades para clientes externos. É direccionado para o consumidor, oferecendo recursos como o registo e login social, a recuperação de senhas, etc.;

10. AD *Domain Services*: Este serviço fornece serviços de domínio compatíveis com o Active Directory em ambientes da nuvem. Facilita a migração de aplicações locais e tradicionais que dependem de controladores de domínio do Active Directory local;

11. *Multi-Factor Authentication* (MFA): Fornece uma camada adicional de segurança exigindo mais de uma forma de autenticação. Para além de utilizador e senha, são solicitados outros factores, que reforçam a segurança da autenticação;

12. AD *Privileged Identity Management* (PIM): Ajuda a gerir, controlar e monitorizar o acesso dentro de uma organização, garantindo que só é dado acesso às pessoas certas e permitidas pela organização;

13. *Managed Identity*: Oferece identidades que são geridas de uma forma automática pelo Azure. Estas identidades podem ser utilizadas para se autenticar em serviços disponibilizados pelo Azure;

14. *Azure Key Vault*: Não é bem considerada uma ferramenta de gestão de identidades, mas contribui para a segurança ao permitir o armazenamento e a gestão das chaves, segredos e certificados utilizados pelas aplicações e serviços do Azure;
15. Estes são apenas alguns dos principais serviços de gestão de identidades oferecidos pela plataforma Azure. A escolha do método depende das necessidades específicas da aplicação e do contexto do cliente;

3.5 SLA

SLA - *Service Level Agreement* – ou Acordo de Nível de Serviço é um documento do nível de serviço, em que tanto o fornecedor de serviço como o cliente se comprometem a assegurar a responsabilidade deste mesmo acordo.

O SLA no Azure e AWS refere-se a um compromisso formal assumido pela Microsoft e pela Amazon como fornecedores de serviço, em relação à disponibilidade e desempenho dos serviços [37]:

1. Compromissos de Disponibilidade:

O SLA do Azure e AWS geralmente especifica os compromissos de disponibilidade de serviços. Por exemplo, um SLA típico pode garantir uma disponibilidade de 99,9% ou mais.

2. Cálculo de Tempo de Inactividade:

O tempo de inactividade dos serviços disponibilizados pelos fornecedores é calculado com base numa fórmula específica definida no SLA. Esse mesmo cálculo leva em consideração o tempo total do mês, excluindo períodos de manutenção programada e eventos inesperados.

3. Créditos de Serviço:

Caso os fornecedores não cumpram com os compromissos de disponibilidade estabelecidos no SLA, os clientes podem ter direito a créditos de serviço. Esses créditos são proporcionais ao tempo de inactividade, além dos limites especificados.

4. Detalhes Específicos por Serviço:

Cada serviço do Azure e AWS pode ter o seu próprio SLA, com termos específicos. Por exemplo, o SLA para o Azure Virtual Machines pode ser diferente do SLA para o Azure Blob Storage [37].

5. Monitorização Contínua:

Os fornecedores monitorizam, continuamente, o desempenho e a disponibilidade dos serviços de forma a assegurar o SLA. As métricas e os relatórios de desempenho são frequentemente disponibilizados aos clientes.

6. Compromisso com a Transparência:

Os fornecedores têm um compromisso com a transparência e fornecem informações detalhadas sobre o estado do serviço, eventos passados e futuros de manutenção, e *logs*, para que os clientes estejam cientes de qualquer potencial impacto que possa ocorrer com os seus serviços.

7. Contractos Individuais:

Os SLAs são parte integrante dos contractos de serviço. Os clientes podem especificar ou solicitar termos contratuais para cada serviço que adquirirem.

8. Manutenção Programada:

O SLA normalmente exclui o tempo de inactividade causado pela manutenção programada, tais manutenções devem ser comunicadas aos clientes com alguns dias de antecedência, para que os clientes estejam cientes e consigam mitigar qualquer impacto crítico.

O SLA é muito importante, desta forma é necessário que os clientes conheçam os SLA contratados e compreendam os mesmos, dado que cada serviço pode ter condições e detalhes de SLA específicos.
O SLA é uma parte crucial do contracto de serviço, que estabelece as expectativas e responsabilidades entre o fornecedor do serviço e os utilizadores da plataforma.
Recordamos que o SLA varia de serviço para serviço e, desta forma, os clientes ou utilizadores da plataforma devem estar a pardas condições do SLA, de forma a salvaguardar os seus serviços e dados, desde a manutenção da plataforma até à segurança dos dados.

3.6 Módulo de Segurança de Hardware (HSM)

Trata-se de um serviço na plataforma de nuvem que oferece um ambiente seguro para gerir chaves criptográficas. Esse serviço utiliza módulos de hardware dedicados, proporcionando um espaço isolado para realizar operações criptográficas importantes. Os utilizadores da plataforma dispõem de controlo total sobre as chaves, e o serviço é projectado para corresponder a requisitos rigorosos de segurança e conformidade.
O *Hardware Security Module* inclui os seguintes pontos [21, 22]:

- ✓ **Gestão de Chaves Criptográficas:** Permite que os utilizadores façam a gestão das chaves criptográficas, de forma segura num ambiente dedicado;

- ✓ **Hardware Dedicado:** O *Dedicated HSM* oferece módulos de hardware dedicados para operações criptográficas, proporcionando um isolamento físico para melhorar a segurança;

- ✓ **Controlo Administrativo Total**: Os utilizadores têm o controlo administrativo total, sobre as chaves armazenadas na plataforma. Tal significa que o fornecedor do serviço na nuvem não tem acesso directo às chaves do cliente;

- ✓ **Conformidade e Certificações**: É projectado para fornecer requisitos rigorosos de conformidade, e os fornecedores procuram certificações reconhecidas para a validação da segurança do serviço;

- ✓ **Uso em Nuvem Privada Virtual (VPC**): É implementado numa Nuvem Privada Virtual (VPC), proporciona isolamento e controlo sobre o ambiente em que o serviço é executado;

- ✓ **Segurança Física e Lógica**: O serviço aborda preocupações de segurança em níveis físicos e lógicos, e assegura a protecção contra ameaças em ambos os aspectos;

- ✓ **Hardware Validado pelo FIPS**: A utilização de hardware validado pelo FIPS assegura que a AWS Nuvem HSM disponibilize os padrões de segurança estabelecidos pelos Padrões Federais de Processamento de Informações (FIPS);

- ✓ **Instâncias de HSM Dedicadas**: Os clientes têm acesso a instâncias dedicadas de HSM, proporcionando um ambiente isolado, para a gestão de chaves criptográficas;

- ✓ **Locação Única e de Propriedade do Cliente:** A Nuvem HSM permite que as instâncias de HSM sejam de locação única, garantindo que uma instância de HSM específica seja atribuída a apenas um cliente. Além disso, as instâncias podem ser de propriedade do cliente, proporcionando um maior controlo sobre o hardware;

- ✓ **Execução em Nuvem Privada Virtual (VPC):** O AWS Nuvem HSM opera numa VPC, permitindo a criação de uma nuvem privada virtual isolada para o armazenamento seguro das chaves;

- ✓ **Segurança e Conformidade:** O serviço é projectado para atender a rigorosos requisitos de segurança e conformidade, sendo adequado para casos de utilização que exija níveis elevados de protecção para chaves criptográficas;

Estes são alguns dos mais importantes módulos de segurança de hardware utilizados pela plataforma na nuvem, de forma a garantir uma segurança mais robusta e segura para os seus clientes. Existem vários benefícios, tais como a combinação da segurança física e lógica, bem como a conformidade com os padrões reconhecidos, para proteger informações sensíveis e garantir a integridade dos seus dados na nuvem.

3.7 Modelo de Responsabilidade Partilhada na nuvem

O modelo de responsabilidade partilhada é já bastante conhecido, mas muita gente desconhece o que isso representa, ou como pode afectar a computação em nuvem.

Analisando um *datacenter* corporativo tradicional, a empresa é responsável por manter o espaço físico, garantir a segurança e manter ou substituir os servidores, caso algo aconteça. O departamento de TI é responsável por assegurar que as infra-estruturas e softwares necessários para manter o *datacenter* a funcionar estão activos, e também serão responsáveis por manter todos os sistemas funcionais e na versão correcta [23, 24].

Este modelo é um conceito fundamental na computação em nuvem, que determina como as responsabilidades de segurança são repartidas entre o fornecedor de nuvem e o cliente. Para percebermos isso, vamos comparar com um *datacenter* corporativo tradicional.

Considerando num *datacenter* tradicional, a empresa é responsável por cuidar do espaço, garantir a segurança, e manter ou substituir os servidores conforme haja necessidade. O departamento de TI lida com toda a infra-estrutura e software para manter o *datacenter* operacional, assegurando que todos os sistemas estejam funcionais e actualizados [19].

Com o modelo de responsabilidade compartilhada na nuvem, essas responsabilidades são divididas entre o fornecedor de nuvem e o consumidor. O fornecedor de nuvem é responsável pela segurança física, energia, arrefecimento e ligação de rede, dado que o consumidor não está fisicamente no *datacenter* e, portanto, não faz sentido que ele cuide desses aspectos [10].

O consumidor é responsável pelos dados e informações armazenados na nuvem. Isso é decisivo, principalmente, porque os clientes, de maneira geral, não querem que o fornecedor de nuvem tenha acesso aos seus dados. Para além disso, o consumidor é responsável pelo acesso e pela sua segurança, o que significa que deve gerir quem pode aceder às informações, garantindo que apenas as pessoas autorizadas tenham acesso a esses dados [20, 21].

Conclui-se que o modelo de responsabilidade compartilhada varia em função da situação e do tipo de serviço em nuvem utilizado. Vamos analisar um exemplo para entender melhor:

- **Base de Dados SQL em Nuvem:**

  Utilizando uma base de dados SQL em nuvem, o fornecedor de serviço será responsável por manter a infra-estrutura real da base de dados. No entanto, o cliente ainda é responsável pelos dados específicos que são inseridos nessa base de dados. Isso significa que precisa de garantir a segurança e a integridade dos dados que armazena.

- **Máquina Virtual com Base de Dados SQL:**

  Se implementou uma máquina virtual e instalou uma base de dados SQL, tornou-se responsável por mais elementos. Além de manter a máquina virtual, também terá de lidar com correcções e actualizações da base de dados, assim como garantir a segurança e a integridade dos dados armazenados

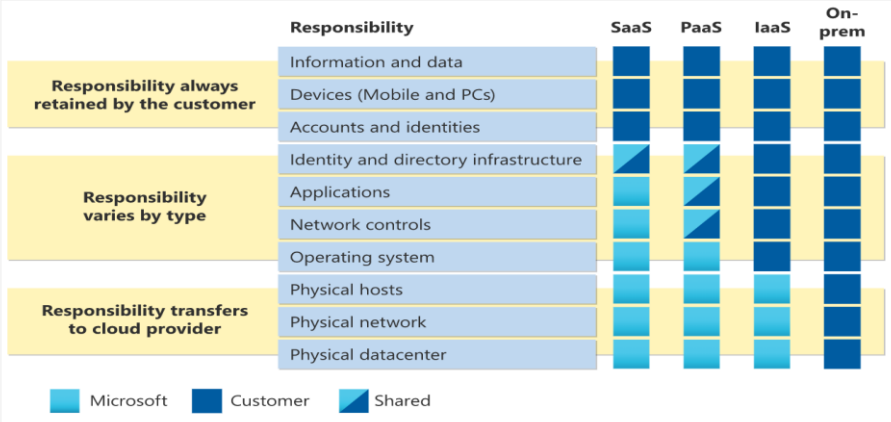
- **Datacenter Local:**

  Num *datacenter* local, a empresa é responsável por todos os aspectos, desde a infra-estrutura física até à manutenção de dados e informações.

O modelo de responsabilidade compartilhada está directamente relacionado com os tipos de serviços em nuvem: Infra-estrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). A responsabilidade varia de acordo com estes modelos. A IaaS coloca mais responsabilidade no consumidor, enquanto que a SaaS coloca a maior parte da responsabilidade no fornecedor do serviço de nuvem. A PaaS fica no meio, repartindo a responsabilidade de maneira equitativa entre o fornecedor e o consumidor.

O diagrama, abaixo representado, destaca visualmente como o Modelo de Responsabilidade Compartilhada funciona, mostrando como são repartidas as responsabilidades nos diferentes tipos de serviços em nuvem [10].

Resumindo, este modelo de responsabilidade compartilhada esclarece quem é o responsável por cada elemento da nuvem. O fornecedor cuida da infra-estrutura física, enquanto o consumidor zela pela segurança e controlo de acesso aos seus próprios dados na nuvem.



21) Figura 21 - Modelo de responsabilidade compartilhada, fonte: [23].

4 Azure

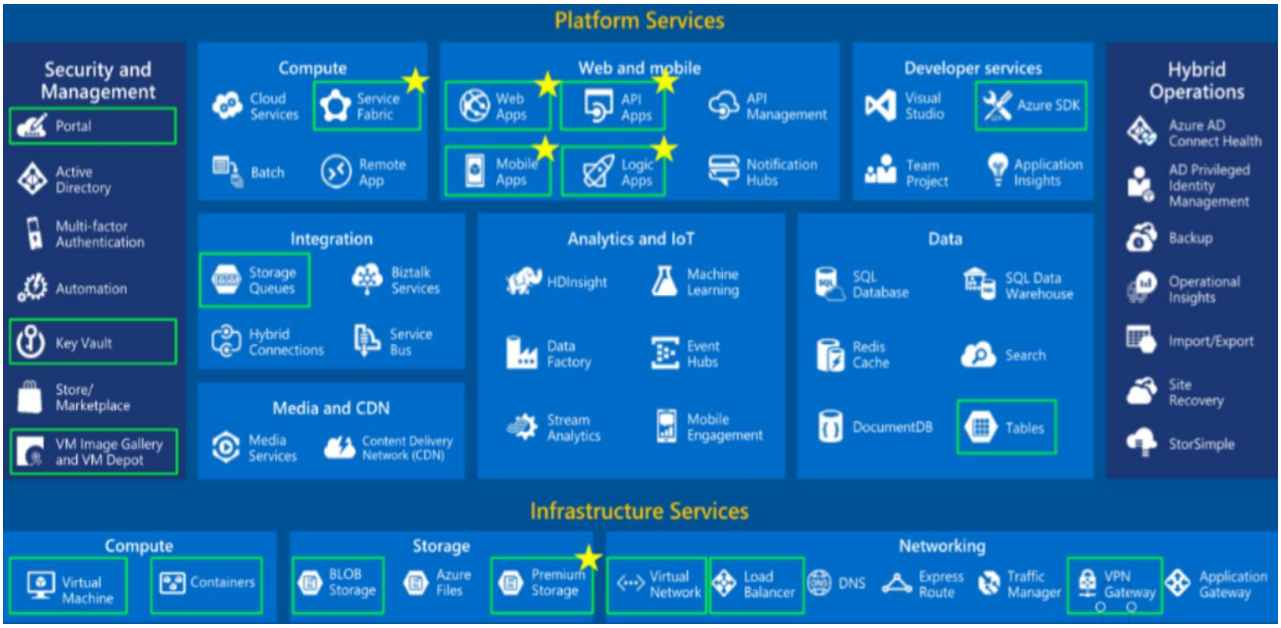
4.1 Conceito

A Azure é uma plataforma de computação em nuvem projectada pela Microsoft, que permite às empresas criar, implementar e gerir as suas aplicações e serviços à escala global. Essa plataforma proporciona uma vasta gama de serviços, como o armazenamento em nuvem, alojamento de sites, base de dados em nuvem, análise de dados em nuvem, serviços de inteligência artificial, Internet das Coisas (IoT) e mais [10].

A Azure foi concebida para ser altamente escalável e flexível, possibilitando que as empresas encontrem vantagens, que vão ao encontro das suas necessidades de negócios, de forma apropriada. Esta plataforma oferece diferentes modelos de implementação, como nuvem pública, nuvem privada e nuvem híbrida, para que as empresas possam fazer opções, conforme as suas necessidades.

A Azure fornece, também, uma variedade de recursos de segurança e de privacidade, incluindo a criptografia de dados, a autenticação de utilizadores, a gestão de identidade e acesso, entre outros. Esses recursos procuram ajudar as empresas a cumprir as regulamentações governamentais e do sector [24].

Concluindo, a Azure é uma plataforma bastante flexível e dimensionável, que auxilia as empresas a controlar e administrar os seus procedimentos de negócios, de forma rápida e eficiente, assegurando segurança e a conformidade com as regulamentações.



22) Figura 22 - conceito Azure, fonte Azure learning, fonte: [23]

4.2 Como funciona a Azure

A Azure, da Microsoft, actua como uma robusta infra-estrutura de computação em nuvem, que permite às empresas criar, implementar e gerir aplicações e serviços na nuvem. A Azure é composta por uma variedade de componentes e serviços, que colaboram para oferecer uma solução altamente escalável e flexível.

Seguem-se alguns dos principais elementos e serviços da Azure e de como estes funcionam:

- **Datacenters:**

A Azure opera em *datacenters* distribuídos globalmente, onde as empresas podem armazenar os seus dados e implantar aplicações. Esses *datacenters* são altamente seguros e confiáveis, com recursos, tais como a energia redundante e sistemas de arrefecimento para garantir a disponibilidade contínua dos serviços [10].

- **Recursos de Computação:**

  A Azure disponibiliza uma variedade de recursos de computação, incluindo máquinas virtuais, *containers* e funções sem servidor. Esses recursos permitem que as empresas executem as suas aplicações na nuvem, com flexibilidade para escolher com base na capacidade, desempenho e escalabilidade.

- **Armazenamento em Nuvem:**

  Oferece diversos tipos de armazenamento em nuvem, como o armazenamento de *blobs*, arquivos, tabelas e *streaming*. Esses serviços possibilitam às empresas armazenar e aceder a dados de maneira escalável e segura.

- **Base de Dados em Nuvem:**

  Disponibiliza serviços de base de dados em nuvem, incluindo o SQL Server, MySQL, PostgreSQL e Cosmos DB. Esses serviços possibilitam às empresas implementar e gerir as suas bases de dados na nuvem, com grande disponibilidade, escalabilidade e segurança.

- **Serviços de Aplicações:**

  Fornece serviços para alojar e gerir aplicações web, móveis e empresariais na nuvem, tais como Azure App Service, Azure Functions e Azure Logic Apps, etc.

- **Serviços de Análise:**

  Oferece diversos serviços de análise de dados em nuvem, como Azure Data Factory, Azure Stream Analytics e Azure Machine Learning. Estes serviços permitem às empresas processar, analisar e visualizar os seus dados na nuvem [10].

  Estes são apenas alguns dos principais componentes e serviços do Azure. A plataforma é altamente flexível e fiável, possibilitando às empresas escolher os serviços mais adequados

às suas necessidades de negócios e os integrá-los nas suas aplicações e processos existentes, conforme detalhado no conceito Azure.

4.3 Método de Autenticação e Gestão de Identidades utilizado pelo Azure

Dos vários métodos disponíveis no mercado, a plataforma Azure utiliza os seguintes, para disponibilizar segurança na sua plataforma e serviços aos seus clientes:

1. Nome de utilizador e senha: Os utilizadores fornecem um nome de utilizador e uma senha, para se autenticarem no Azure;

2. Autenticação 2FA/ multifactorial: adiciona uma camada adicional de segurança à autenticação do utilizador. Os utilizadores precisam de fornecer um segundo factor de autenticação, além do nome de utilizador e a senha, como um código enviado por SMS ou gerado por uma aplicação de autenticação;

3. Certificados digitais: são utilizados para autenticar os utilizadores, aplicações ou serviços no Azure. São baseados em criptografia assimétrica, o que significa que o certificado contém uma chave pública, que pode ser utilizada para verificar a identidade do utilizador ou da aplicação;

4. Chaves de acesso: são utilizadas para autenticar aplicações ou serviços no Azure. São um conjunto de credenciais exclusivas para cada assinatura do Azure, que permitem que os aplicativos se liguem aos recursos do Azure.

5. *Tokens* de segurança: Os *tokens* de segurança são utilizados para autenticar os utilizadores em aplicações baseadas na nuvem. O Azure utiliza o protocolo OAuth 2.0 para autenticação baseada em *token*, conforme indicado no conceito Azure.

6. Azure Active Directory: O Azure Active Directory (AD) é um serviço da Microsoft de gestão da identidade e acesso baseado em nuvem. Permite que os utilizadores se autentiquem, utilizando as suas credenciais corporativas ou escolares, no caso do ensino.

7. Autenticação federada: A autenticação federada permite que os utilizadores externos se autentiquem em aplicações baseadas no Azure, utilizando as credenciais da sua organização. O Azure suporta vários padrões de autenticação federada, incluindo SAML, WS-Federation e OpenID Connect, segundo o conceito Azure.

A plataforma Azure utiliza vários serviços para a gestão de identidades, garantindo a segurança e controlo de acesso aos seus recursos. Alguns dos principais métodos de gestão de identidades no Azure incluem [24]:

1. Azure Active Directory (Azure AD): O Azure AD é o serviço de gestão de identidades da Microsoft baseado na nuvem. Fornece recursos, tais como a autenticação de utilizador, autorização e gestão de directórios. É amplamente utilizado para autenticar utilizadores e controlar o acesso aos recursos do Azure;

2. Azure AD B2C (*Business to Consumer*): Este serviço estende as capacidades do Azure AD para permitir a gestão de identidades para clientes externos. É direccionado para o consumidor, oferecendo recursos como o registo e o login social, recuperação de senha, etc.;

3. Azure AD Domain Services: Este serviço fornece serviços de domínio compatíveis com o Active Directory em ambientes do Azure. Facilita a migração de aplicações locais e tradicionais, que dependem de controladores de domínio do Active Directory local;

4. Azure Multi-Factor Authentication (MFA): Fornece uma camada adicional de segurança exigindo mais de uma forma de autenticação. Para além de utilizador e senha, são solicitados outros factores que reforçam a segurança de autenticação;

5. Azure AD Privileged Identity Management (PIM): Ajuda a gerir, controlar e monitorizar o acesso dentro de uma organização, garantindo que só é dado acesso às pessoas certas e permitidas pela organização;

6. Azure Managed Identity: Oferece identidades, que são geridas de uma forma automática pelo Azure. Estas identidades podem ser utilizadas para se autenticar em serviços disponibilizados pelo Azure;

7. Azure Key Vault: Não é bem considerada uma ferramenta de gestão de identidades, mas contribui para a segurança ao permitir o armazenamento e gestão das chaves, segredos e certificados utilizados pelas aplicações e serviços do Azure.

   Estes são apenas alguns dos principais serviços de gestão de identidades oferecidos pela plataforma Azure. A escolha do método depende das necessidades específicas da aplicação e do contexto do cliente.

4.4 Como funcionam os métodos de autenticação e gestão de identidades no Azure?

Os métodos de autenticação e gestão de identidades no Azure funcionam de maneira integrada, para fornecer um melhor controlo de acesso seguro aos recursos da plataforma. Vamos abordar como funcionam esses métodos [25]:

1. Azure Active Directory (Azure AD): Autenticação de Utilizador: No Azure AD gere a autenticação e autorização dos utilizadores. Suporta a autenticação multifactorial, senha única (SSO), e fornece *tokens* de acesso.

Controlo de Acesso: O Azure AD controla o acesso a aplicativos e serviços, garantindo que só os utilizadores autorizados tenham permissões atribuídas;

2. Azure Multi-Factor Authentication (MFA): Camada adicional de Segurança: A MFA exige uma verificação adicional, além das credenciais padrão (como senha), como um código enviado por mensagem de texto, notificação *push* ou autenticação biométrica;
3. Azure AD Privileged Identity Management (PIM): Gestão de Privilégios: O PIM ajuda a gerir as permissões dos utilizadores, garantindo que os privilégios elevados (como de administrador) sejam temporários e somente concedidos quando necessário [26];
4. Azure Managed Identity: Gestão de Identidades: são atribuídas de forma automática aos recursos do Azure, como máquinas virtuais, permitindo que se autentiquem a outros serviços, sem a necessidade de credenciais explícitas [26];
5. Azure Key Vault: Armazenamento Seguro de Chaves e Segredos: Ajuda a gerir e a proteger segredos, chaves de criptografia e certificados, garantindo um armazenamento seguro e controlado dessas informações;
6. Azure AD B2C: Gestão de Identidade para Clientes Externos: Com foco nas aplicações do consumidor, o Azure AD B2C tem o seu foco em funções como registo, autenticação social e recuperação de senha para clientes externos;

7. Azure AD Domain Services: Compatibilidade com Active Directory: Este serviço possibilita a facilidade da migração das aplicações que dependem do Active Directory local, fornecendo serviços de domínio compatíveis;
8. Autenticação para Serviços Azure: *Tokens* e Certificados: Para autenticação entre serviços Azure, são utilizados *tokens* e certificados, garantindo uma comunicação segura entre os recursos;
9. Integração com Outros Serviços (Azure Services Integration): Métodos de autenticação e gestão de identidades são integrados em muitos serviços Azure, proporcionando segurança em várias camadas [25]:
10. Monitorização e Auditoria: Azure Monitor e Azure Security Center: são serviços que fornecem monitorização e auditoria, para identificar e responder a ameaças de segurança em tempo real.

Estes métodos garantem que apenas utilizadores que foram permitidos pelo administrador, possam ter acesso aos recursos disponibilizados e aos dados e serviços no Azure, permitindo um ambiente de segurança e controlado.

5 AWS

5.1 Conceito

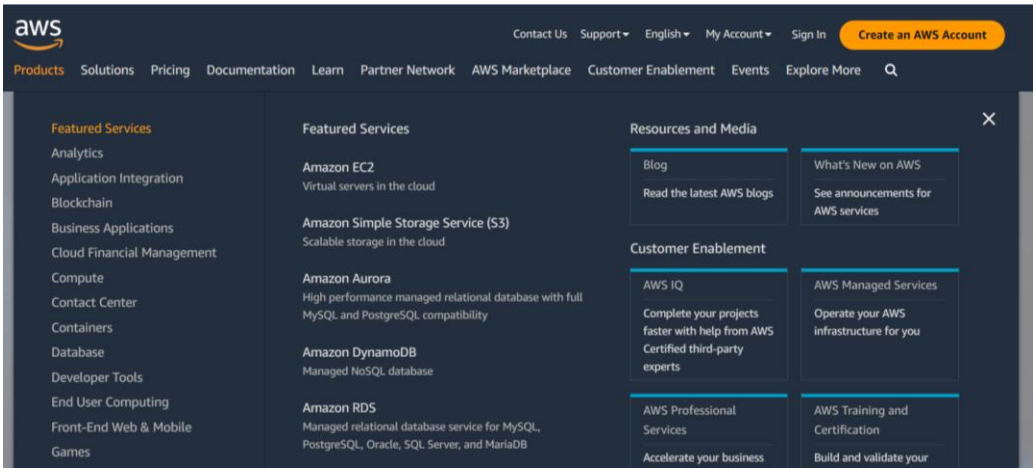
A Amazon Web Services (AWS) é uma plataforma de serviços em nuvem oferecida pela Amazon, que proporciona recursos computacionais, armazenamento e serviços de rede através da Internet.

Reconhecida como uma das principais plataformas no mercado de computação em nuvem, a AWS disponibiliza uma variedade extensa de serviços, incluindo servidores virtuais (EC2), armazenamento em nuvem (S3), bases de dados (RDS), serviços de análise de dados (Redshift), serviços de rede (VPC), segurança e mais [27].

A AWS também disponibiliza recursos para automatização, gestão e monitorização, facilitando aos utilizadores o controlo e optimização dos seus recursos na nuvem.

Empresas de todas as dimensões, desde pequenas *startups* até grandes corporações de tecnologia em todo o mundo, utilizam a AWS para alojar aplicações, armazenar e processar grandes volumes de dados, realizar análises e muito mais.

Além disso, a plataforma é adoptada por governos e organizações sem fins lucrativos para diversas finalidades [28], conforme demonstrado na Figura 23, que apresenta vários serviços oferecidos pela plataforma AWS.



23) Figura 23 - AWS conceito, fonte AWS plataforma, fonte: [29].

5.2 Como funciona a AWS

A Amazon Web Services (AWS) é uma plataforma de serviços em nuvem da Amazon, que opera por meio de uma infra-estrutura global de *datacenters* e que oferece uma ampla variedade de serviços, desde o armazenamento, bases de dados, computação, redes, inteligência artificial e *machine learning*, entre outros, conforme indicado em *Computação em nuvem com a AWS [*29].

O funcionamento da AWS pode ser resumido em vários componentes e princípios-chave:

1. Data Centers Globais: possui uma rede de *datacenters* distribuídos globalmente. Esses *datacenters* armazenam e processam dados, permitindo que os utilizadores acedam aos serviços em nuvem, em qualquer lugar do mundo;

2. Modelo de Serviços: oferece uma variedade de serviços, incluindo a computação, armazenamento, banco de dados, inteligência artificial, *machine learning*, análise de dados, segurança, entre outros;

3. Modelo de Pagamento por Uso “Pay As You Go”: A AWS opera num modelo de pagamento em função da utilização, o que significa que os utilizadores pagam apenas pelos recursos que consomem, no que difere de uma nuvem privada.

4. Escalabilidade: Um dos principais princípios da AWS é a capacidade de escalabilidade. Os utilizadores podem aumentar ou diminuir, dinamicamente, os recursos conforme as suas necessidades, permitindo lidar com picos de negócio;

5. Elasticidade: a AWS oferece elasticidade, permitindo que os recursos se ajustem, automaticamente, à necessidade de cada cliente. Isso significa que os clientes podem escalar, para cima ou para baixo de forma automática, com base nas condições de utilização;

6. Serviços Geridos: Muitos serviços da AWS são totalmente geridos, o que significa que a Amazon cuida da manutenção e operação dos serviços. Isso liberta os utilizadores, para se concentrarem no desenvolvimento de aplicações e na lógica de negócios, enquanto a AWS cuida da infra-estrutura.

7. Segurança e Conformidade: A AWS coloca uma forte ênfase na segurança. A empresa fornece várias ferramentas e recursos de segurança, além de permitir que os utilizadores implementem práticas de segurança personalizadas. Além disso, a AWS esforça-se para estar em conformidade com várias regulamentações e padrões de segurança;

8. Serviços de Apoio: oferece serviços adicionais, tais como ferramentas de automatização, gestão e monitorização, para ajudar os utilizadores a administrar de forma eficiente os seus recursos.

Em suma, podemos afirmar que a AWS funciona como uma infra-estrutura de nuvem globalmente distribuída, que fornece uma ampla gama de serviços e recursos que podem ser consumidos de acordo a necessidade de cada cliente, com um modelo de pagamento flexível e com o foco na escalabilidade, elasticidade e segurança [29].

5.3 Método de autenticação e Gestão de Identidades utilizado pela AWS

Dos vários métodos disponíveis no mercado, a plataforma AWS utiliza os seguintes para disponibilizar segurança na sua plataforma e serviços aos seus clientes [19]:

1. Utilizador e Senha: A autenticação tradicional com nome de utilizador e senha é comumente utilizada para aceder aos serviços e à plataforma da AWS;

2. Chaves de Acesso: Com o surgimento das APIs ou serviços da AWS por meio de programação, as chaves de acesso, como chaves de acesso da AWS e chaves secretas são frequentemente utilizadas na autenticação;

3. 2FA /Autenticação Multifator (MFA): A AWS suporta a autenticação com vários factores, o que adiciona uma camada adicional de segurança, exigindo um segundo factor de autenticação, além das credenciais padrão;

4. Assinaturas e Tokens: Para interacções seguras entre os serviços, a AWS utiliza assinaturas e *tokens* para efeitos de autenticação e autorização.

5. AWS Identity and Access Management (IAM): é um serviço fundamental na AWS, que permite gerir o acesso a recursos de maneira segura;

6. Federação de Identidade: A AWS suporta a federação de identidade, permitindo que as organizações integrem os seus sistemas de identidade existentes com a AWS;

7. AWS Single Sign-On (SSO): é um serviço que facilita a gestão de acesso a várias contas e aplicações. Com um único acesso, os utilizadores acedem a diversos recursos, sem a necessidade de uma password para cada recurso, a AWS permite a utilização de um único conjunto de credenciais;

   Citamos alguns dos métodos de autenticação disponíveis na AWS, e a escolha depende dos requisitos específicos de segurança e do contexto de utilização de cada cliente.

   A plataforma AWS utiliza vários serviços para a gestão de identidades, garantindo a segurança e o controlo do acesso aos seus recursos. Alguns dos principais métodos de gestão de identidades no AWS são [30]:

8. AWS Identity and Access Management (IAM): é um serviço central para o controlo de acesso aos utilizadores e serviços/ recursos da AWS, desde a criação e administração de utilizadores e grupos, atribuição de permissões e políticas, autenticação dos utilizadores e aplicação;

9. Amazon Cognito: é um serviço que facilita a adição de autenticação, autorização e gestão de utilizadores das aplicações na web e móveis, incluindo a autenticação de utilizadores com serviços de identidade federados, sincronização de dados do utilizador entre dispositivos e o suporte à autenticação multifactorial;
10. AWS Single Sign-On (SSO): Descrição: é um serviço que permite aos utilizadores acederem a várias contas e aplicações no AWS, apenas com uma senha ou credenciais; tem como funcionalidade a autenticação única para várias contas e aplicações, e integração com a Microsoft Active Directory;

11. AWS Directory Service: Descrição: permite a integração da Cloud AWS com directórios existentes, como o Microsoft AD, como por exemplo, na implementação de directórios administrados na AWS, na autenticação de utilizadores em máquinas Windows e aplicações;

12. AWS Organizations: possibilita consolidar várias contas na plataforma AWS, numa organização que se cria e controla, desde o agrupamento de contas numa estrutura hierárquica e a aplicação de políticas de controlo de acesso às contas.

5.4 Como funcionam os métodos de autenticação e Gestão de identidades na AWS?

A AWS utiliza vários métodos de autenticação e oferece várias possibilidades de gestão de identidades, para permitir que os utilizadores acedam aos seus serviços de forma segura [31].

Nos métodos de Autenticação temos:

1. IAM (Identity and Access Management):

   Funcionamento: permite criar e gerir identidades na AWS, como utilizadores, grupos e políticas.

   Autenticação: Os utilizadores com IAM podem autenticar e utilizar credenciais de segurança, incluindo o nome de utilizador e senha.

2. Amazon Cognito:

Funcionamento: permite a autenticação de utilizadores, em aplicações web ou móveis, oferecendo serviços de identidade federada e gestão de utilizadores.

Autenticação: Suporta a autenticação com fornecedores de identidade federada, como Google, Facebook e Amazon, além de permitir a autenticação directa dos utilizadores.

3. AWS Single Sign-On (SSO):

Funcionamento: simplifica o acesso a várias contas e aplicações, permitindo à AWS utilizar um único conjunto de credenciais.

Autenticação: Oferece autenticação única (SSO) e suporte à MFA para fortalecer a segurança.

Na gestão de Identidades temos:

1. IAM (Identity and Access Management) [29]:

Funcionamento: Além da autenticação, o IAM permite a gestão de credenciais e autorizações das permissões específicas a cada utilizador, grupo e função.

Gestão: Permite atribuir políticas especificas, o controlo das permissões que cada identidade pode fazer em recursos específicos.

2. Amazon Cognito:

Funcionamento: possibilita a gestão de perfis dos utilizadores, bem como sincronizar dados entre dispositivos.

Gestão: Permite a gestão de utilizadores, incluindo perfis e oferece opções de sincronização de dados.

3. AWS Organizations:

Funcionamento: permite o agrupamento das contas AWS, numa única hierarquia organizacional, simplificando a gestão das mesmas.

Gestão: possibilita a criação de unidades organizacionais, aplicação de políticas e delegação de controlo.

4. AWS Directory Service:

Funcionamento: permite a integração com vários directórios já existentes, como o Microsoft AD, para autenticação e gestão dos utilizadores.

Gestão: fornece serviços de directório geridos na AWS, possibilitando a integração com os sistemas legados.

Além desses métodos de autenticação e gestão de identidades, a AWS também oferece outros recursos de segurança, como o *AWS Web Application Firewall* (WAF), que pode proteger aplicações web contra os ataques mal-intencionados "malware", e o *AWS Shield*, que pode ajudar a proteger as aplicações contra os ataques DDoS [31].

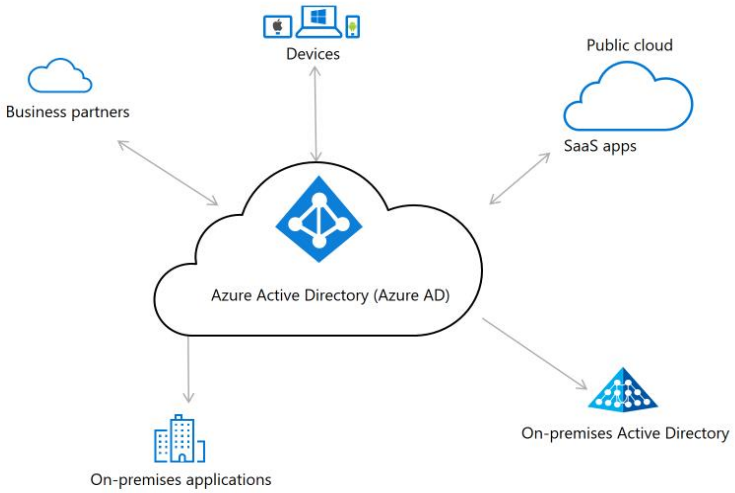
6 Comparação entre os Métodos de Autenticação/ Gestão de Identidades utilizados pela Plataforma Azure e AWS

6.1 Métodos utilizados e as diferenças de métodos de autenticação utilizado no Azure e AWS.

A plataforma Azure e a plataforma AWS utilizam vários métodos de autenticação disponíveis no mercado para proteger recursos e dados de *Cloud Computing* [28].

Métodos de autenticação suportados pela plataforma Azure:

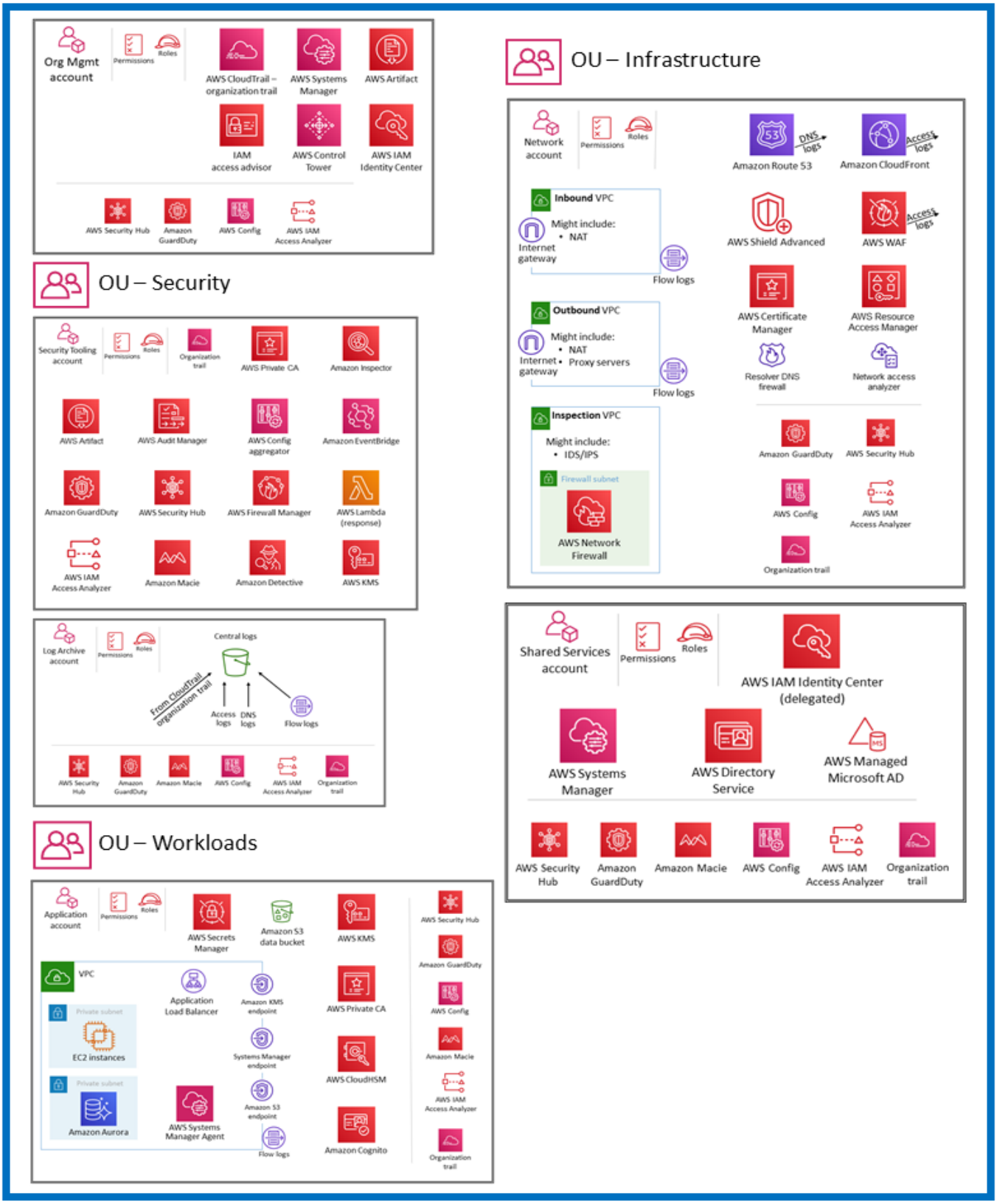
- ✓ Nome de utilizador e senha: Permite o login com credenciais padrão;
- ✓ Multifactorial (MFA): Exige informações extra, além do nome de utilizador e senha, incluindo opções como aplicativo, SMS e chamada de voz;
- ✓ Federada: Permite utilizar credenciais de identidade corporativa ou de um fornecedor para aceder aos recursos do Azure;
- ✓ Baseada em certificado: Utiliza certificados digitais para autenticar os utilizadores;
- ✓ Baseada em *token*: Permite o uso de *tokens* de fornecedores de identidade para autenticação no Azure.



24) Figura 24 - Arquitectura de identidade da plataforma Azure, fonte: [28].

Métodos de autenticação suportados pela plataforma AWS:

- ✓ Nome de utilizador e senha, é um método padrão;
- ✓ Autenticação multifactorial (MFA), que exige informações adicionais além da senha;
- ✓ Autenticação federada, que permite utilizar credenciais de login existentes de uma identidade corporativa;
- ✓ AWS Identity and Access Management (IAM), é um serviço que ajuda a controlar o acesso aos recursos da AWS, permitindo aos administradores criar, gerir identidades e definir políticas de acesso específicas a cada grupo ou utilizador.



25) Figura 25 - Arquitectura de identidade da plataforma AWS, fonte: [29].

Tanto o Azure quanto o AWS oferecem diversas opções de autenticação, para atender a diferentes necessidades de segurança. A escolha do método de autenticação dependerá dos requisitos específicos e das preferências do utilizador ou da organização [30].

Apesar de disponibilizarem quase os mesmos serviços de nuvem, existem modos de implementação diferentes, e os mesmos não diferem na implementação dos métodos de autenticação. Vamos destacar alguns deles:

- ✓ O Azure utiliza o Azure Active Directory (AD) como serviço de directório padrão, enquanto o AWS usa o AWS Identity and Access Management (IAM) para gerir as identidades e acessos;
- ✓ Ambas as plataformas oferecem autenticação multifactorial, sendo o Azure por meio do Azure AD e a AWS pelo AWS IAM podendo integrar outras soluções MFA;
- ✓ Ambas suportam a autenticação baseada em certificado, para garantir o acesso seguro aos recursos
- ✓ Tanto o Azure quanto o AWS oferecem suporte à autenticação baseada em *tokens*, como OAuth 2.0 e Security Assertion Markup Language (SAML);
- ✓ O Azure suporta a autenticação integrada do Windows, para aplicações em máquinas virtuais, assim como a AWS.

Essas diferenças reflectem as abordagens distintas, mas também as semelhanças, na oferta de métodos de autenticação em ambas as plataformas [30].

Logo, podemos resumir que as duas plataformas trabalham com toda a dedicação, e utilizam tecnologias de ponta para garantir a segurança e disponibilidade dos serviços aos seus clientes, e para assegurar as suas responsabilidades com os SLA definidos.

6.2 As diferenças entre a Gestão de Identidades oferecida pela Azure e AWS.

Entretanto, na gestão de identidades, as duas plataformas oferecem métodos específicos, com o objectivo de os utilizadores e as empresas gerirem melhor os seus dados e políticas de segurança, vamos citar algumas diferenças entre a Azure e a AWS:

- ✓ Serviço de Directório Padrão:

  Azure: Utiliza o Azure Active Directory (AD) como o seu serviço de directório padrão [31].

AWS: Utiliza o AWS Identity and Access Management (IAM) para gerir as identidades e acessos [32].

- ✓ Autenticação Multifatorial (MFA):

  Azure: Oferece a MFA por meio do Azure AD;

  AWS: Proporciona a MFA através do AWS IAM;

Ambas permitem a integração com outras soluções MFA.

- ✓ Autenticação Baseada em Certificado:

  Azure e AWS: oferecem a autenticação baseada em certificado, para garantir o acesso aos recursos.

- ✓ Autenticação Baseada em *Tokens*:

  Azure e AWS: oferecem suporte para a autenticação baseada em *tokens*, incluindo o OAuth 2.0 e SAML.

- ✓ Autenticação Integrada do Windows:

  Azure e AWS: Suportam a autenticação integrada do Windows, para aplicações em máquinas virtuais.

- ✓ Serviços de Gestão de Identidade Específicos:

  Azure: Além do Azure AD, possui serviços específicos para a gestão de identidade, como por exemplo o Azure B2C (Business-to-Consumer).

  AWS: O IAM é o serviço central, mas podem ser utilizados outros tipos de ferramentas, conforme a necessidade do cliente.

Nas abordagens de gestão de identidade entre o Azure e AWS, podemos afirmar que reflectem as suas filosofias e estratégias individuais, na entrega de serviços de autenticação e de controlo de acesso.

Cada plataforma tem as suas próprias características e opções, para disponibilizar de acordo com as necessidades específicas dos utilizadores e organizações. A escolha entre o Azure e AWS dependerá dos requisitos específicos, preferências e integração com outros serviços ou infra-estruturas que podem já existir. Como os dados e a tecnologia são sempre actualizados, é recomendável estar sempre ao corrente das actualizações que possam ocorrer em ambas as plataformas.

6.3 Comparação: Soluções de Segurança em AWS e Azure

Nesta comparação, vamos abordar algumas soluções obtidas com as informações que tivemos oportunidades de recolher, sobre as plataformas Azure e AWS [33].

6.3.1. AWS

É possível encontrar na plataforma AWS as soluções necessárias para cumprir os padrões de segurança. Nesta secção forneceremos uma breve descrição dessas soluções.

Category	Pattern title	Solutions in AWS	Solutions in Azure
Compliance and Regulatory	**Data Citizenship**	Use AWS location tags to designate the location for data processing	Azure information protection and location tag. Azure frontdoor service
	Cryptographic Erasure	Use AWS KMS	Use Azure Key Vault
	Shared Responsibility Model	AWS provides different services to ensure protection of data and system. It is upto client to use it or not. However, AWS is responsible for only the vailability and basic security of cloud platform.	Azure provides different security tools to ensure protection of data and system. It is upto client to use it or not. However, Azure is responsible for only the vailability and basic security of cloud platform
	Compliant Data Transfer	AWS locaton tags	Azure location tag
	Data Retention	The data retention policies can be defined and executed by AWS. For example Lambda	Azure provides option to define data retention policy in Database system
	Data Lifecycle	AWS data lifecycle manager	Azure blob storage lifecycle
	Intentional Data Remanence	database (e.g. DynamoDB)	database (e.g. Azure backup)
Identification, Authentication and Authorisation	**Multi-Factor Authentication**	AWS Cognito	Azure active directory : multi-factor
	Federation (Single Sign-On)	AWS SSO (Single Sign-On)	Azure AD Seamless Single Sign-On
	Access Token	AWS security token service	Azure active directory : Token service
	Mutual Authentication	Use AWS TLS/SSL certificate, Certificate feature of API Gateway (AWS client VPN)	Azure App service
	Secure User Onboarding	AWS customer on boarding	Azure security center
	Identity and Access Manager	AWS IAM and Cognito	Azure IAM
	Per-request Authentication	AWS Signing and Authenticating REST Requests	Azure API management & REST API authentication
	Access Control Clearance	AWS cloud watch and AWS Cognito/IAM	Azure access control service
Secure Development, Operation and Administration	**Bastion Server**	AWS bastion host	Azure Bastion host
	Automated Threat Detection	AWS GuardDuty	Azure advanced threat protection
	Durable Availability	AWS cloud watch, AWS WAF	Azure web access firewall & firewall application gateway
	Economic Durability	AWS cloud watch	Azure Monitor
	Vulnerability Management	AWS vulnerability scanning	Vulnerability scan in Azure security center
Privacy and Confidentiality	**End-to-End Security**	AWS KMS, Certificate manager	Azure Key Vault
	Computation on Encrypted Data	N/A	N/A
	Data Anonymisation	Algorithms can be defined and ran by AWS module (e.g. lambda)	Azure provides Dynamic Data Masking on SQL database
	Processing Purpose Control	N/A	N/A
Secure Architecture	**Virtual Network**	AWS Virtual Private Cloud	Azure Virtual Network
	Web Application Firewall	AWS WAF	Azure application firewall gateway
	Secure Element	AWS IoT Device Management	Azure IoT Hub & IoT Suit
	Secure Cold Storage	AWS Glacier	Azure Coldblob storage
	Certificate and Key Manager	AWS Certificate and Key manager (AWS KMS)	Azure Key Vault
	Hardware Security Module	AWS CloudHSM	Azure Dedicated HSM
	Secure Auditing	AWS Auditing Security Checklist	Azure Monitor, Stream, Network Watcher

26) Figura 26 - Soluções de segurança SaaS em AWS e Microsoft Azure, fonte: [33]

1. **Conformidade e Regulamentação**. A AWS disponibiliza ferramentas para apoiar o processamento e a gestão da conformidade reguladora de dados.

- ***Data Citizenship* (Cidadania de Dados).** É uma ferramenta de *tags* de localização, também conhecida como restrição geográfica ou bloqueio geográfico, para gerir o acesso do utilizador, com base na localização geográfica. O CloudFront, na AWS, permite limitar ou permitir o acesso ao conteúdo com base em listas brancas ou negras de países aprovados ou banidos. Também é possível utilizar serviços de geolocalização de terceiros, para um controlo mais granular, considerando parâmetros como a cidade, o Código Postal, a latitude e a longitude [33].

- ***Cryptographic Erasure* (Apagamento criptográfico).** Disponibiliza o serviço KMS (Key Management Service) que serve para criar, gerir e controlar o uso de criptografia em vários serviços e aplicações da plataforma [33].

- ***Shared Responsibility Model* (Modelo de Responsabilidade Partilhada).** Disponibiliza uma variedade de serviços e ferramentas para garantir a segurança dos dados e do sistema, com algumas opções gratuitas e outras pagas. A principal responsabilidade da AWS é garantir a disponibilidade e a segurança básica da plataforma de nuvem [33].

- ***Compliant Data Transfer* (Transferência de dados compatível).** É utilizada para controlar a transferência de dados dentro de limites geográficos, sendo semelhante ao conceito de cidadania de dados.

- **Data Retention (Retenção de dados).** Disponibiliza uma variedade de ferramentas de armazenamento e backup de dados, como o DynamoDB, que permite uma configuração flexível para backup, proporcionando uma protecção contra exclusões acidentais e ataques intencionais aos dados.

- ***Data Lifecycle* (Ciclo de vida dos dados).** Oferece uma automatização, para operações específicas em recursos e dados das aplicações na plataforma AWS, utilizando políticas de ciclo de vida configuráveis.

- ***Intentional Data Remanence* (Remanência intencional de dados).** Disponibiliza serviços de backup, para garantir que os dados permanecem seguros mesmo em casos de exclusão acidental ou intencional. Um exemplo é o serviço de backup do DynamoDB, que permite que os utilizadores definam as

suas próprias políticas de backup, oferecendo assim uma camada adicional de protecção avos dados armazenados. Essas ferramentas visam preservar a continuidade e a integridade dos dados na plataforma AWS.

2. **Identificação, Autenticação e Autorização (AAA – Accounting, Authorization and Authentication).** É um sistema que permite a identificação, autenticação e autorização seguras de dispositivos e utilizadores na plataforma AWS. Todos os utilizadores ou dispositivos devem passar nesses 3 estágios de segurança.

   - ***Multi-factor Authentication*** **(Autenticação multifactorial).** A AWS disponibiliza uma gama de ferramentas e serviços, para garantir a identificação, autenticação e autorização seguras dos dispositivos e utilizadores na sua plataforma. Isso inclui o AWS Cognito, uma ferramenta de controlo de acesso que suporta autenticação padrão e multifactorial para utilizadores e APIs de aplicação. Também fornece serviços de backup para proteger dados contra exclusões acidentais e ataques deliberados. A plataforma também oferece soluções de restrição geográfica para controlar o acesso, com base na localização geográfica. A gestão de chaves criptográficas (KMS) é outra ferramenta importante para controlar o uso de criptografia em vários serviços da AWS. Essas medidas garantem a segurança e protecção dos dados na plataforma [33].

   - ***Federation (single sign-on)*** **Federação (*logon* único).** É um método que a AWS utiliza para facilitar a gestão unificada do acesso a diferentes contas e aplicações de negócios na AWS. Permite que os utilizadores façam login uma única vez para aceder a várias contas e aplicações, simplificando a administração de identidades e controlo de acesso.

   - ***Access Token*****.** É um método online, que permite que os utilizadores solicitem credenciais temporárias com privilégios limitados. Essas credenciais temporárias podem ser utilizadas para autenticar o utilizador ou a API da aplicação na AWS. AWS [27].
   - ***Mutual Authentication*** **(Autenticação Mútua).** A AWS Client VPN realiza uma autenticação mútua, o que significa que tanto o cliente quanto o servidor são autenticados durante a ligação. Utiliza certificados gerados pelo AWS Certificate Manager, para garantir uma verificação de identidade em ambas as extremidades da ligação [33].

- ***Secure User On-boarding*** **(Integração segura do utilizador).** É um serviço que assegura a protecção do conteúdo, que impede a sua utilização não autorizada. Esse processo é alcançado através da implementação de uma gestão de direitos digitais (DRM), denominada Secure Packager and Encoder Key Exchange (SPEKE) [33].

- ***Identify and Access Manager*****.** Ajuda a controlar quem pode aceder aos serviços e recursos dentro da AWS. Basicamente, permite criar e gerir utilizadores e grupos, nos quais podemos definir as acções que esses utilizadores e grupos podem realizar nos diversos serviços da AWS. É uma parte fundamental, para garantir a segurança e a gestão eficaz da sua infra-estrutura na nuvem AWS [33].

- ***Per-request Authentication*****.** Disponibiliza o serviço "Signing and Authenticating REST Requests" para gerir o acesso e as operações com base na identidade do solicitador. Significa que diferentes grupos de utilizadores têm permissões específicas, como a criação de blocos ou de objectos dentro de um bloco. Essa funcionalidade visa garantir a segurança e o controlo efectivos sobre as acções realizadas na AWS.

- ***Access Control Clearance*** **(Liberação de controle de acesso).** A AWS disponibiliza vários métodos e serviços projectados para assegurar e gerir, com segurança o acesso a dados e recursos do sistema. O IAM e o Cognito são utilizados para a autenticação e administração de utilizadores, enquanto o AWS Cloud Watch é responsável por monitorizar tanto os utilizadores como os recursos [33].

3. ***Secure Development,*** A plataforma AWS disponibiliza uma variedade de ferramentas, para gerir a segurança aquando do desenvolvimento, operação e administração dos sistemas implementados na plataforma.

- ***Bastion Server*****.** É uma solução projectada para fornecer acesso seguro a uma rede privada a partir de uma rede externa, como a Internet. A sua função principal é a de reduzir as possibilidades de sucesso de possíveis ataques, para assegurar uma camada adicional de segurança, aquando do acesso remoto à rede privada.
- ***Automated Threat Detection*** **(Detecção automatizada de ameaças).** É um serviço de segurança, que está sempre atento a actividades suspeitas e

comportamentos não autorizados para proteger as contas, cargas de trabalho e recursos na plataforma AWS. Age como um guardião que alerta sobre possíveis ameaças e ajuda a manter um ambiente seguro na nuvem da AWS.

- ***Durable Availability*** **(Disponibilidade durável).** São diversas e variáveis as ferramentas que a AWS disponibiliza para garantir a segurança de acesso e o bom funcionamento das aplicações alojadas na plataforma. Estas incluem serviços como IAM (Identity and Access Management) para gerir identidades e permissões, CloudWatch para monitorizar, WAF (Web Application Firewall) para protecção contra ataques, e GuardDuty para detenção de ameaças. Além disso, a AWS fornece serviços de autenticação, backup e criptografia para proteger os dados e recursos. Essas medidas visam assegurar um ambiente seguro e estável para as aplicações que utilizam a infra-estrutura da AWS [33].

- ***Economic Durability*** **(Durabilidade económica).** O CloudWatch utilizado pela AWS desempenha um papel crucial na supervisão das aplicações na plataforma, para assegurar que não ocorram situações em que invasores consumam excessivamente os recursos, como a capacidade de processamento disponível. Monitoriza de perto o comportamento, a utilização e os recursos, para manter um desempenho eficiente e seguro.

- ***Vulnerability Management*** **(Gestão de Vulnerabilidades).** Existem ferramentas de terceiros, como o AlienVault USM, que podem ser implementadas, para identificar vulnerabilidades no software disponibilizado na plataforma AWS. Essas ferramentas desempenham um papel crucial na avaliação contínua da segurança, ajudando a identificar e corrigir potenciais pontos fracos no sistema.

4. ***Privacy and Confidentiality*** **(Privacidade e Confidencialidade).** Existem vários serviços e ferramentas para ajudar na protecção da privacidade e na confidencialidade dos dados. Contudo, há requisitos específicos que podem não ser totalmente cobertos por esses serviços, exigindo que os desenvolvedores implementem soluções personalizadas. Essas soluções podem incluir práticas como a anonimização de dados, a utilização de criptografia em dados sensíveis e o controlo rigoroso sobre a finalidade do processamento, para garantir a conformidade com as normas de privacidade e segurança necessárias.

- ***End-to-end Security*** **(Segurança de ponta a ponta).** A AWS disponibiliza serviços que visam assegurar a segurança dos dados transmitidos entre diferentes componentes de uma aplicação, como o *back-end* e o *front-end.* O AWS Certificate Manager é uma ferramenta que simplifica o processo de obtenção, gestão e implementação de certificados SSL/TLS, tanto para uso público quanto privado. Esses certificados são fundamentais para garantir a integridade e a segurança das comunicações, entre várias partes de uma aplicação ou sistema alojado na AWS [33].

- ***Computation on Encrypted Data*** **(Computação em Dados Criptografados).** A capacidade de realizar a computação em dados criptografados, ainda não está prontamente disponível na plataforma AWS. Isso significa que os dados criptografados têm, geralmente, de ser descriptografados antes de serem processados, o que pode introduzir considerações adicionais de segurança e privacidade na gestão desses dados.

- ***Data Anonymisation*** **(Anonimização de Dados).** Esta solução não se encontra disponível na AWS.

- ***Processing Purpose Control*****.** Esta solução não se encontra disponível na AWS.

5. ***Secure Architecture*** **(Arquitectura Segura).** Um conjunto de ferramentas e serviços de arquitectura segura está disponível na AWS.

    - ***Virtual Network*** **(Rede Virtual).** A Nuvem Privada Virtual (VPC) da AWS oferece a capacidade de criar uma área isolada e lógica dentro da Nuvem AWS. O que permite que os utilizadores configurem e executem recursos da AWS numa rede virtual própria, mantendo um controlo total sobre o ambiente, como a definição de intervalos de endereços IP, criação de sub-redes e configuração de rotas de rede. Uma VPC proporciona uma forma personalizada e segura de estruturar a infra-estrutura na AWS.

    - ***Web Application Firewall*****.** A AWS WAF é uma espécie de "guarda-costas" digital para aplicações web. Actua como uma barreira de protecção, impedindo ataques comuns, que poderiam prejudicar a segurança, o desempenho ou a

disponibilidade de uma aplicação online. Em essência, é uma camada de defesa que mantém as aplicações web seguras contra ameaças da Internet [33].

- ***Secure Element* (Elemento Seguro).** O AWS IoT Device Management torna fácil integrar, monitorizar e gerir dispositivos IoT com segurança, em grande escala. Com essa ferramenta, podemos registar os dispositivos ligados individualmente ou em grupos, facilitando a administração de permissões para manter a segurança dos dispositivos após o envio.

- ***Secure Cold Storage*** Para uma fácil recuperação e eficiência de dados é recomendado armazenar os dados menos acedidos numa localização específica. A AWS oferece o serviço Glacier para armazenar os dados que são acedidos com menor frequência, contribuindo para optimizar o tempo de recuperação quando necessário.
- ***Certificate and Key Manager* (Certificado e Gestor de Chaves)**. A AWS disponibiliza dois serviços essenciais para a gestão de segurança: o AWS Key Management Service (KMS) e o AWS Certificate Manager. O KMS permite criar e gerir chaves criptográficas para proteger os dados, enquanto o Certificate Manager facilita a utilização e a gestão de certificados TLS/SSL para garantir ligações seguras. Esses serviços desempenham um papel crucial na segurança das operações na nuvem [33].

- ***Hardware Security Module* (Módulo de segurança de hardware).** O CloudHSM é uma ferramenta na nuvem, que oferece uma camada extra de segurança na vertente hardware. Permite criar chaves criptográficas ou configurar as próprias chaves, para serem utilizadas em diferentes aplicações e serviços na AWS [33].
- ***Secure Auditing* (Auditoria Segura).** A AWS criou uma lista de verificação para auditorias de segurança, que ajuda os clientes a avaliar quão bem os serviços da AWS cumprem os requisitos de segurança da informação específicos dos seus sectores industriais e governamentais. Esta lista fornece um guia, para garantir que os controlos de segurança necessários estejam em vigor e indicação dos pontos a melhorar, se assim for necessário.

6.3.2. Azure

O Azure, similar à AWS, oferece a maioria das ferramentas necessárias para lidar com os padrões de segurança. Podemos evidenciar, na figura 26 como esses padrões se relacionam com as opções de segurança disponíveis no Azure. Oferecemos nesta sessão uma descrição sucinta das soluções específicas do Azure para esses padrões de segurança (consulte a Figura 26).

1. ***Compliance and regulatory*** **(Conformidade e regulamentação).** Diversas ferramentas e serviços disponíveis na plataforma Azure podem ser fornecidos, para ajudar no processamento e na administração da conformidade regulamentar dos dados. Abaixo, fornecemos uma descrição de como funciona cada uma dessas soluções.

    - ***Data Citizenship*** **(Cidadania de Dados).** Pode ser utilizado para controlar, com base na localização geográfica, o acesso aos dados e aplicações. A Firewall de Aplicativo da Web (WAF) no Front Door permite que o utilizador defina uma política, com recurso a regras de acesso personalizadas, para um caminho específico no ponto de extremidade, determinando se o acesso de países específicos deve ser permitido ou negado. Como exemplo, temos vários países que não permitem acesso ao seu IP público para ter acesso a algumas redes sociais, com base na localização do IP. Os utilizadores não conseguem, desta forma; podem, contudo, contornar esse bloqueio, com a utilização de uma VPN (Virtual Private Network), com localização de outro país e IP desse outro país para ter acesso; concluímos que este serviço restringe ou permite um acesso específico, baseado na localização [33].

    - ***Cryptographic Erasure*** **(Apagamento criptográfico).** A funcionalidade de "Cryptographic Erasure" no Azure Key Vault possibilita que o utilizador faça a gestão da sua chave criptográfica com segurança, permitindo operações como a exclusão ou remoção da chave. O Azure Key Vault não se limita apenas a isso, também inclui outros serviços, como a gestão de segredos e certificados, e oferece um armazenamento seguro para segredos respaldados por módulos de segurança de hardware.

    - ***Shared Responsibility Model*** **(Modelo de Responsabilidade Compartilhada).** Assim como a AWS, o Azure disponibiliza uma variedade de serviços e

ferramentas para assegurar a protecção de dados e sistemas. Entretanto, é importante notar que nem todos esses serviços e ferramentas são gratuitos. A utilização fica a critério do cliente, que deve escolher de acordo com as suas necessidades específicas. A responsabilidade legal do Azure inclui garantir a disponibilidade e a segurança fundamental da plataforma de nuvem [33].

- ***Compliant Data Transfer*** **(Transferência de dados compatível)**. O serviço Azure Front Door (AFD) pode ser utilizado para gerir e regular a transferência de dados entre diferentes fronteiras geográficas, como temos no nosso dia-a-dia o conceito de Cidadania de Dados.

- ***Data Retention*** **(Retenção de dados).**
  A plataforma Azure fornece diversas formas de armazenamento de dados e ferramentas de backup, como o armazenamento de Blob, armazenamento de arquivos e armazenamento de tabela. Esses recursos são utilizados para salvaguardar dados contra exclusões acidentais e ataques intencionais. Por exemplo, o Azure Cosmos DB é um serviço de base de dados distribuído multimodelo [33], e oferece uma alternativa, que garante a gestão segura dos dados.

- ***Data Lifecycle*** **(Ciclo de vida dos dados).** Possibilita supervisionar a evolução dos dados na plataforma. Essa funcionalidade oferece uma política abrangente e fundamentada em regras, que os utilizadores podem implementar para orientar os dados desde a sua origem, durante a utilização e até à conclusão do seu ciclo de vida.
- ***Intentional Data Remanence*** **(Remanência intencional de dados).** Na plataforma Azure, este serviço é utilizado para guardar dados de forma a que possam ser mantidos, mesmo em situações de tentativas de exclusão ou remoção. Proporciona capacidades de backup para todos os recursos presentes na plataforma Azure Cloud.

2. ***Identification, Authentication and Authorisation*** (**Identificação, Autenticação e Autorização).** O Azure disponibiliza inúmeras ferramentas para garantir a identificação, autenticação e autorização seguras de utilizadores, aplicações e dispositivos na plataforma, assegurando assim o cumprimento da sua responsabilidade e SLAs.

- ***Multi-factor Authentication* (Autenticação multifator)**. Disponibiliza diversos serviços para a gestão de acesso dos utilizadores e dados, incluindo a autenticação multifactorial [27]. No Azure, é utilizada uma abordagem de verificação em duas etapas, que inclui o método tradicional, com nome de utilizador e senha, além de uma autenticação adicional, como um factor de posse.

- ***Federation (single sign-on)* Federação (logon único).** Possibilita ao utilizador usar apenas uma senha, para aceder a várias contas ou serviços disponibilizados ou contratados, e utilizando o acesso já disponibilizado pela empresa, caso a empresa já tenha o mesmo utilizador criado e senha do domínio da organização.

- ***Access Token* (Símbolo de acesso).** Permite que o utilizador crie um código que pode ser usado com segurança, para solicitar informações das APIs protegidas pelo Azure.

- ***Mutual Authentication* (Autenticação Mútua)**. Oferece uma funcionalidade de autenticação mútua, que pode ser utilizada para controlar o acesso a aplicações e recursos específicos no ambiente do Azure.

- ***Secure User On-boarding* (Integração segura do utilizador**). É composto por vários serviços de segurança projectados para salvaguardar aplicações, recursos e dispositivos na rede. O serviço de Integração Segura é implementado para adicionar dispositivos externos à rede, de forma segura [33].

- ***Identity and Access Manager* (administrador de Identidade e Acesso**). Tem como principal objectivo a gestão de política de segurança, desde a gestão de utilizadores, gestão de grupos, políticas de autenticação, utilizando o método AAA (Accounting, Athentication and Authorization), com estes 3 métodos o utilizador é validado, autenticado e é-lhe depois autorizado apenas o acesso que lhe foi atribuído.

- ***Per-request Authentication* (Autenticação por solicitação)**. A gestão de API do Azure e a Autenticação da API REST [33] permite que o utilizador crie o *token* de acesso essencial, para efectuar chamadas nas APIs do Azure.

- ***Access Control Clearance*** **(Liberação de controle de acesso)**. O Serviço de Controle de Acesso do Azure (ACS) tem como finalidade as mesmas características do Azure IAM possibilitando a gestão de políticas de acesso, e a autenticação dos utilizadores e grupos.

3. ***Secure Development, Operation and Administration*** **(Desenvolvimento, Operação e Administração Seguros).** O Azure disponibiliza de uma forma segura diversas ferramentas para assegurar o desenvolvimento, operação e administração dos sistemas que operam na plataforma.
   - ***Bastion Server*****.** Serve como um ponto de entrada único que habilita os utilizadores a acederem aos recursos implantados no ambiente do Azure. Esse *host bastion* estabelece uma ligação segura aos recursos, autorizando apenas o tráfego remoto de endereços IP públicos que estão numa lista permitida [33].

   - ***Automated Threat Detection*** **(Detecção automatizada de ameaças)**. É uma solução de segurança que possibilita a identificação, detecção e investigação de ameaças sofisticadas e avançadas, identidades comprometidas e acções internas maliciosas.
   - ***Durable Availability*** **(Disponibilidade durável).** Para garantir a qualidade do serviço e a disponibilidade das aplicações, a plataforma Azure disponibiliza um serviço de firewall para acesso à Web (WAF) que actua como uma firewall, protegendo contra ataques externos, enquanto o Azure Application Gateway funciona como um balanceador de carga de tráfego web, para gerir eficientemente o tráfego de aplicativos da web [33].

   - ***Economic Durability*** **(Durabilidade Económica).** O Azure Monitor [33] tem como foco auxiliar os administradores a compreender o desempenho dos seus serviços, caso precisem de melhoria, se está a utilizar muitos recursos ou se está a ter um mau desempenho, de forma a melhorar a eficiência e a não desperdiçar recursos, que têm seu custo financeiro.
   - ***Vulnerability Management*** **(Gestão de Vulnerabilidades).** A análise de vulnerabilidades no Azure Security Center pode ser utilizada para monitorizar ataques, impedir acessos não autorizados e identificar falhas de segurança no sistema como a CloudWatch na AWS.

4. ***Privacy and Confidentiality (Privacidade e Confidencialidade).*** A segurança completa, que inclui todo o processo, é garantida pelas ferramentas como o Key Vault no Azure. Contudo, alguns recursos relacionados com a preservação da privacidade ainda não são totalmente integrados no Azure. Nesses cenários, os desenvolvedores da plataforma precisam de criar as suas próprias soluções para suportar serviços, como computação em dados criptografados e o controlo do propósito do processamento [33].

    - ***End-to-end Security*** **(Segurança ponta a ponta). O**ferece serviços separados para a gestão de chaves e gestão de certificados, incluindo o aprovisionamento e a implantação de SSL/TLS tanto público quanto privado;

    - ***Computation on encrypted data***. O Azure disponibiliza serviços, como a computação confidencial, para proteger dados durante a utilização, mas actualmente não suporta a capacidade de realizar cálculos, directamente, em dados criptografados na plataforma;

    - ***Data Anonymisation*** **(Anonimização de Dados).** Com o mascaramento de dados dinâmicos na Base de Dados SQL do Azure [33], é possível limitar a exposição dos dados sensíveis, ocultando-os a utilizadores não privilegiados. Esse recurso permite ao administrador monitorizar e evitar acessos não autorizados a informações confidenciais, dando-lhe um controlo sobre a quantidade de dados sensíveis a serem revelados;

    - ***Processing Purpose Control*****. A**inda não está disponível na plataforma Azure.

5. ***Secure Architecture*** **(Arquitectura Segura)**. São várias ferramentas de arquitectura segura que se encontram disponíveis no Azure, variando entre rede privada virtual a auditoria segura.

    - ***Virtual Network*** **(Rede Virtual).** A infraestrutura de Rede Virtual permite que diferentes recursos, como Máquinas Virtuais, SQL Server, se comuniquem em segurança. O administrador tem a opção de criar múltiplas redes virtuais em cada assinatura e região do Azure;

- ***Web Application Firewall* (Firewall das aplicações Web).** A Firewall de Aplicativos Web (WAF), uma funcionalidade incorporada no Azure Application Gateway, oferece uma camada centralizada de protecção para aplicações web, defendendo contra ataques e vulnerabilidades comuns, como a injecção de SQL "SQL injection" e *scripts* entre sites [33];

- ***Secure Element* (Elemento Seguro).** O Azure IoT Hub e Suite [33] disponibilizam serviços de Internet das Coisas (IoT) que facilitam a integração de dispositivos com a nuvem;

- ***Secure Cold Storage*.** É uma solução económica para armazenar dados que são raramente acedidos. Por exemplo, para dados que são acedidos para consulta de tempos a tempos, não existe a necessidade de os colocar agregados com dados que são consultados diariamente, desta forma coloca-se em armazenamento menos frequente a utilização que tem um custo de utilização mais baixo;

- ***Certificate and Key Manager* (Certificado e Gerenciador de Chaves).** É um serviço projectado para auxiliar na administração de chaves criptográficas e certificados. Capacita o utilizador da plataforma a criar, gerir e fornecer chaves criptográficas, assim como certificados TLS/SSL [33];

- ***Hardware Security Module* (Módulo de segurança de hardware).** O Azure Dedicated HSM proporciona ao utilizador a capacidade de gerir e ter controlo absoluto, tanto em termos administrativos quanto criptográficos, sobre as chaves. É importante destacar que a Microsoft não tem acesso às chaves armazenadas no Módulo de Segurança de Hardware (HSM);

- ***Secure Auditing* (Auditoria Segura)**. O Azure oferece serviços específicos para realizar auditorias seguras no uso de recursos e operações das aplicações. O Azure Monitor pode ser utilizado para verificar a utilização de recursos, enquanto o Azure Network Watcher é utilizado para diagnosticar problemas de conectividade na rede.

Observação: a AWS e o Azure oferecem soluções abrangentes, para a maioria dos padrões de segurança definidos, mas há algumas lacunas que os desenvolvedores da plataforma precisam abordar por meio do desenvolvimento das suas próprias soluções (ver notas na Figura 26).

Após estas comparações demonstradas, já podemos ter uma noção abrangente da importância dos métodos da autenticação na "cloud computing", e vamos especificar algumas:

Os métodos de autenticação são importantes porque garantem:

- ✓ Protecção Contra Acessos Não Autorizados
- ✓ A Integridade dos Sistemas
- ✓ Conformidade com Regulamentações e Normas
- ✓ Experiência do Utilizador e Utilidade
- ✓ Mitigação de Riscos de Segurança
- ✓ Facilitação da Gestão de Identidades e Acessos
- ✓ Protecção de Infra-estrutura e Aplicações, entre outros.

Os métodos de autenticação na computação em nuvem são essenciais, para garantir a segurança, integridade e conformidade dos serviços e dados na nuvem. Estes métodos não protegem apenas contra acessos não autorizados, mas também melhoram a experiência do utilizador, facilitam a gestão de identidades e asseguram que a organização cumpre os requisitos regulatórios. Escolher e implementar métodos de autenticação apropriados é um passo crítico para qualquer organização que utilize a computação em nuvem.

No próximo capítulo, será apresentado um inquérito, no qual foram formuladas 5 questões, tendo sido inqueridas 33 pessoas, através da plataforma Google Forms, direccionados a 2 empresas, para percebermos como as empresas em Portugal encaram a segurança da computação em nuvem e para determinar quais as suas preocupações, relativamente a estes serviços que são acedidos directamente via Internet.

As 5 questões visam perceber a importância dos métodos de autenticação na computação em nuvem, e qual a sua finalidade e contributo na segurança dos dados para empresas.

7 Inquérito aos utilizadores das empresas que utilizam Azure ou AWS

Neste inquérito, foram feitas 5 perguntas, citadas no ponto 7.1, dirigidas a utilizadores de várias empresas, para perceber qual o fornecedor ou fornecedores de *Cloud Computing* que

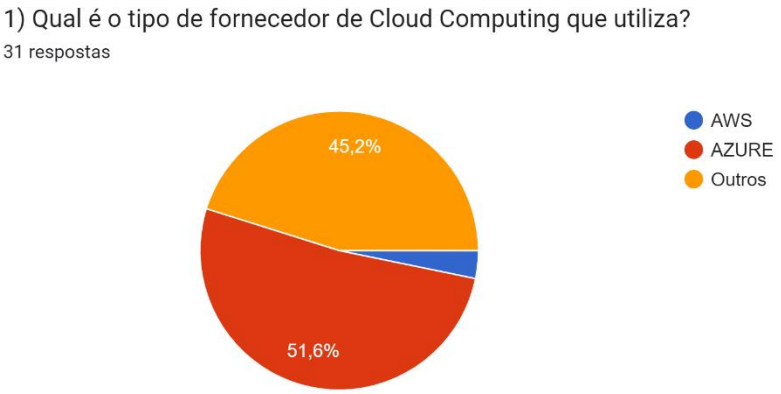
utilizam, e quais os métodos de autenticação utilizados, para segurança dos seus sistemas e dados.

Deste modo, iremos documentar cada questão na sua percentagem, na vertente geral e para cada empresa.

7.1 Questões?

No inquérito, foram efectuados e recolhidos dados sobre as seguintes questões:

i. Questão 1:



27 – Gráfico 1 - Qual o tipo de fornecedor de Cloud Computing que utiliza?

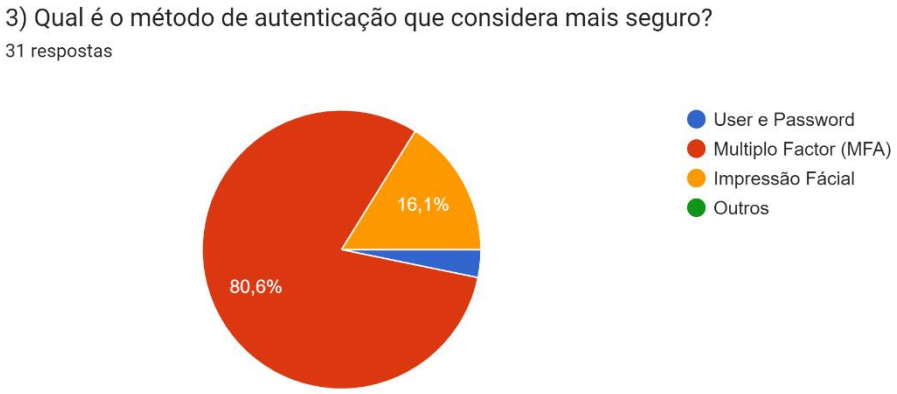
Na questão 1 do inquérito, após 33 respostas, verificamos que 51,6% utilizam o fornecedor de serviço *nuvem Azure*, 45,2% utilizam a AWS e os restantes utilizam outros fornecedores de serviço *nuvem*, como por exemplo, a *Google Cloud*, *IBM Cloud*, entre outros.

ii. Questão 2:

28 – Gráfico 2 - Que método de autenticação utiliza para se autenticar?

Após o inquérito, constatamos que 74,2% dos inquiridos utilizam métodos de autenticação de múltiplos factores, 22% utilizam um factor de autenticação simples, por "*user* e *password*" e os restantes utilizam a impressão facial "Face ID". Com esta informação, podemos validar o facto de que as empresas têm tido preocupação com uma autenticação robusta, que garanta a segurança do utilizador e dos dados.

iii. Questão 3:

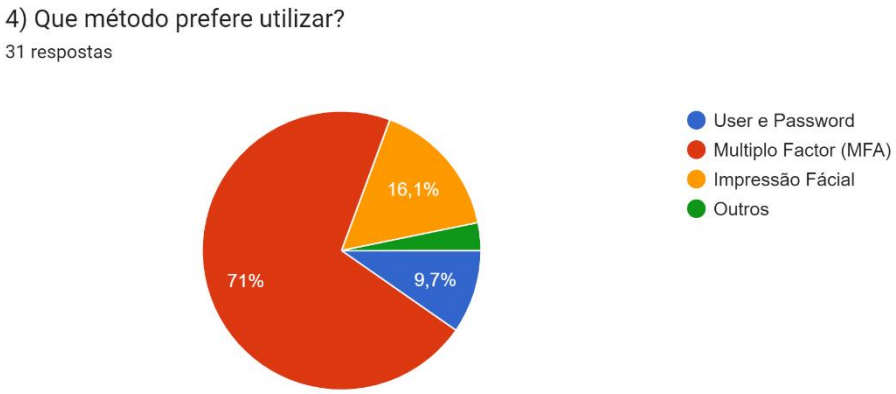


29 – Gráfico 3 - Qual o método de autenticação que considera mais seguro?

Após as respostas dos inquéritos, podemos concluir que 80,6% considera mais segura a autenticação por múltiplo factor, 16,1% considera o método de autenticação impressão facial (face ID) mais seguro, e os restantes consideram o método de autenticação com *user*

e *password*. Desta forma, podemos validar que os utilizadores estão mais informados e têm conhecimento da importância da segurança dos dados.

iv. Questão 4:



30 – Gráfico 4 - Que método prefere utilizar?

Após as respostas aos inquéritos, verificamos que 71% preferem utilizar a autenticação por múltiplo factor, 16,1% preferem utilizar a autenticação por impressão facial (Face ID), 9,7% preferem utilizar a autenticação por *User* e *Password* e os restantes preferem outros métodos de autenticação.

v. Questão 5:

Em relação à questão número 5, procuramos perceber qual importância de um método de autenticação e qual a sua finalidade para a empresa e utilizadores.
Nesta questão de resposta aberta, obtivemos diferentes pontos de vista dos inquiridos, dos quais citamos algumas respostas:

- "A autenticação deverá ter sempre um segundo método de autenticação forte, por forma a garantir a segurança dos dados armazenados em nuvem".
- "A meu ver a autenticação de múltiplos factores é a mais segura, pois reduz o risco de, por exemplo, palavras-passe comprometidas e permite a possibilidade de usar várias camadas de autenticação, resultando num maior controlo de segurança."
- "Aumentar a segurança das nossas contas e dados pessoais."
- "Fundamental para garantir a confidencialidade dos dados"
- "Para proteger dados/ informação"

Na questão 5, foi feita uma pergunta aberta, onde os inquiridos puderam dar o seu ponto de vista sobre qual a importância dos métodos de autenticação e a sua finalidade. Podemos validar que os utilizadores sabem da sua importância, tanto para a protecção dos dados pessoais como também, para a protecção dos dados das empresas.

Podemos considerar, segundo os inquéritos, que a maioria das empresas em Portugal utiliza o fornecedor de serviço *Azure Cloud*, que as empresas e utilizadores têm tido mais consciência da importância do método de autenticação, do quão importante é para a protecção e segurança dos dados, e que a segurança é de todos, tanto utilizadores como empresas.

Com este inquérito foi possível compreender como as empresas têm abordado a segurança em Portugal, e qual nível de importância que a segurança está a ter para as empresas actualmente. Deste modo, salientamos que as empresas em Portugal têm alterado a forma de abordagem, antes muitos consideravam a segurança como uma despesa, porém, actualmente, temos vindo a ser considerada como um investimento, dado que a segurança dos dados e serviços, é o ponto prioritário para as empresas.

8 Conclusão

Com as informações recolhidas acerca da computação na nuvem, podemos observar que esta tecnologia tem um papel bastante importante, na forma como as empresas de pequena dimensão sobrevivem face às empresas de grande dimensão, começando pelos inúmeros serviços disponibilizados. Mas o foco desta dissertação centra-se na comparação entre os métodos de autenticação em computação em nuvem utilizados pelas empresas. Quando uma empresa escolhe o seu fornecedor de serviço *nuvem*, deve considerar, além dos serviços utilizados, as disponibilidades, e um factor muito importante que é a fiabilidade, bem como quais os métodos de autenticação utilizados pelo fornecedor de serviço *nuvem*, para garantir a segurança dos seus serviços e dados.

A segurança dos dados e serviços, são pontos que as empresas têm em comum e continuam a ser uma preocupação, tanto para as empresas como para os fornecedores da nuvem. Como os dados são acedidos pela Internet, a ameaça à integridade dos dados é maior, isto porque estes ficam mais expostos aos ataques dos hackers ou de outras pessoas mal-intencionadas; logo, tanto o cliente como o fornecedor da nuvem, têm uma responsabilidade partilhada nesse campo, dependendo do tipo do serviço que as empresas contratam.

Efectuámos uma descrição dos métodos que as empresas podem utilizar, para a protecção dos seus dados e serviços e a importância de cada um; é verdade que, actualmente, existem vários métodos de autenticação, mas as empresas devem considerar qual é mais eficiente e que garante a protecção dos seus dados em cada cenário.

A comparação realizada entre os métodos de autenticação utilizados pelos fornecedores de *nuvem* Azure e o AWS, a respeito de quem é protegido e as informações a serem protegidas, leva-nos à conclusão de que ambas as entidades têm estes dois pontos em comum, mas com uma abordagem ligeiramente diferente uma da outra. Pode observar-se ainda, que ambas se centram na disponibilidade de serviços, na segurança de informação e em como os serviços chegam às empresas, da forma como os serviços chegam aos seus clientes e a sua funcionalidade, em termos de procura e segurança dos dados.

Foi efectuado um inquérito para validar como as empresas e utilizadores estão a considerar a segurança dos dados, na vertente dos métodos de autenticação, qual a sua importância e finalidade e como podemos proteger os dados e garantir a segurança nas organizações.

Podemos responder as duas questões efectuadas neste trabalho e o seu contributo o seguinte:

P1: Quais são os Métodos de Autenticação utlizados em Computação na Nuvem?

Com as informações documentadas neste trabalho, leitura e investigação, podemos concluir que a computação em nuvem utiliza requisitos rigorosos de segurança, para cumprir os SLAs acordados com os clientes, assegurando a disponibilização, fiabilidade e segurança da plataforma de nuvem e dos dados dos clientes.

Esses métodos são amplamente utilizados para proteger o acesso a recursos e dados em ambientes de computação na nuvem. A escolha do método adequado depende das necessidades específicas de segurança e conveniência da organização.

P2: Quais as diferenças entre os métodos de autenticação utilizados pelo Microsoft Azure e Amazon AWS?

Relativamente a esta questão, podemos concluir que, tanto a plataforma Azure como a AWS, utilizam tecnologias de ponta, para garantir a melhor segurança e serviços aos seus utilizadores, os serviços podem distinguir uma da outra na sua abordagem ou conceito, mas a finalidade é a mesma, de garantir segurança dos dados e serviços. Apresentamos uma breve comparação entre os métodos utilizados pelas duas plataformas:

Método de Autenticação	Microsoft Azure	Amazon AWS
Senha	Azure AD, Azure Managed Identities	AWS IAM, AWS Cognito
Autenticação Multifactorial (MFA)	Azure AD MFA (SMS, chamadas, push)	AWS IAM MFA (dispositivos físicos, apps)
Autenticação Sem Senha	Biometrics, Windows Hello, FIDO2, Authenticator App	N/A (dependente de integrações externas)
Single Sign-On (SSO)	Azure AD	AWS Cognito, Federated Identity
Certificados e Smart Cards	Azure AD	Suporte limitado via políticas de IAM
Autenticação Federada	Azure AD	AWS IAM, AWS Cognito

Assinaturas de API e Tokens de Sessão	N/A	AWS IAM
Biometrica	Windows Hello, Authenticator App	AWS Cognito (via integrações externas)
Gestão de identidades	Azure Managed Identities	N/A

A Azure AD é uma solução abrangente que oferece diversas opções de autenticação e é bem integrada com o ecossistema Microsoft.

Já o AWS IA e AWS Cognito fornecem flexibilidade e um suporte robusto para integrações e *federated identities*, com forte ênfase em MFA e *tokens* de sessão para segurança de APIs.

Ambas as plataformas possuem pontos fortes específicos, e a escolha entre elas pode depender das necessidades específicas da sua organização, e do ecossistema tecnológico em que opera.

Como referimos anteriormente, muitas das tecnologias de autenticação são utilizadas pelas ambas as empresas, e apesar das abordagens e modo de implementação serem diferentes, o objectivo e a finalidade são os mesmos, de garantir segurança da plataforma, serviços e dados.

a. Trabalho Futuro

Como trabalho futuro, sugere-se acompanhar o processo de métodos de autenticação utilizados por outros fornecedores de serviço, uma vez que o Azure e AWS estão há mais tempo no mercado, e perceber o que vão fazer para melhorar a segurança dos serviços e dados dos seus clientes.

b. Limitações

As limitações encontradas, ao longo deste processo de investigação, foram o excesso de documentação encontrada e seleccionar e recolher a mais adequada a esta dissertação. Também foi complexo na vertente da aplicação do inquérito, para recolher as informações e opiniões dos funcionários das empresas, para perceber como consideram e valorizam, no contexto dos métodos de autenticação, a segurança dos serviços e dados.

9 BIBLIOGRAFIA

1. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Institute of Standardization and Technology (2009).
2. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud Computing and Emerging IT Platforms: Vision, Hype, Fashion and Reality for Providing Computing as the Fifth Utility. Future Generator. Comput. Sist. 25, 599–616 (2009);
3. Neuman, B.C., Ts'o, T.: Kerberos: An Authentication Service for Open Network Systems;
4. Recordon, D., Reed, D.: OpenID 2.0: a platform for user-centric identity management, Alexandria (2006);
5. Lenk, A., Klems, M., Nimis, J., Tai, S., Sandholm, T.: What's inside the cloud? An architectural map of the cloud landscape. In: Actas do 2009;
6. ClearSale, Consultado no dia 22 de Janeiro de 2023 em: https://blogbr.clear.sale/metodos-de-autenticacao-conheca-os-principais
7. Business School, consultado no dia 22 de Janeiro de 2023 em: https://fia.com.br/blog/computacao-em-nuvem/
8. Business school, Ltd. Huawei Technologies Co, consultado no dia 8 de Fevereiro em: researchgate.net/publication/364180107_Introduction_to_Nuvem_Computing_Computing
9. Data flair, Features of Cloud Computing – 10 Major Characteristics of Cloud Computing
10. Azure concept, consultado no dia 14 de Março de 2023 em: https://learn.microsoft.com/en-us/training/modules/describe-nuvem-compute/1-introduction-microsoft-azure-fundamentals?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.microsoft-azure-fundamentals-describe-nuvem-concepts
11. Profissionais Linux, Consultado no dia 12 de Fevereiro de 2023 em: https://e-tinet.com/nuvem/4-modelo-servico-de-computacao-em-nuvem
12. NeilPatel, Jr Kashyap, Consultado no dia 12 de Fevereiro de 2023 em: https://neilpatel.com/blog/gaas/
13. Maria PapathanasakiTai, S., Leandros Maglaras: Modern Authentication Methods: consultado a 06 de Março de 2023
14. Tamara Saad Mohamed, Security of Multifactor Authentication Model to Improve Authentication Systems, 2014.

15. Velásquez I, Caro A, Rodríguez A. Authentication schemes and methods: A systematic literature review. In: Information and software technology. Chile: Chillán; 2018.
16. Khan academy, Consultado no dia 29 de Dezembro de 2023 em: https://pt.khanacademy.org/college-careers-more/internet-safety/xef9bb6e081c9f4ff:online-data-security/xef9bb6e081c9f4ff:user-authentication-methods/a/multi-factor-authentication
17. Authentication Method, consultado no dia 29 de Dezembro de 2023 em: https://docs.aws.amazon.com/singlesignon/latest/APIReference/API_AuthenticationMethod.html
18. Azure Dedicated HSM, consultado no dia 02 de Janeiro 2024 em: https://azure.microsoft.com/en-us/products/azure-dedicated-hsm
19. Microsoft Learn, Consultado no dia 15 de Março de 2023 através: https://azure.microsoft.com/
20. AWS NuvemHSM, Consultado no dia 02 de Janeiro de 2024 em: https://aws.amazon.com/pt/nuvemhsm/
21. AWS Modelo de responsabilidade compartilhada, fonte datada no dia 19 de Março de 2023 em: https://aws.amazon.com/pt/compliance/shared-responsibility-model/
22. Microsoft Learn, Consultado no dia 14 de Março de 2023 em: https://learn.microsoft.com/en-us/azure/nuvem-adoption-framework/get-started/how-azure-resource-manager-works
23. Tipos de gestão de identidades no Azure, consultado no dia 28 de Dezembro de 2023 em: https://learn.microsoft.com/pt-br/azure/security/fundamentals/identity-management-overview
24. Introdução ao Servidor Multi-Factor Authentication do Azure, consultado no dia 28 de Dezembro de 2023 em: https://learn.microsoft.com/pt-pt/entra/identity/authentication/howto-mfaserver-deploy,
25. K. Swedha; Tanuja Dubey: Analysis of Web Authentication Methods Using Amazon Web Services (2018).
26. Pooja Pandit. Case Study on AWS Identity and User Management. August 2021.
27. Computação em nuvem com a AWS, fonte datada no dia 19 de Março de 2023 em: https://aws.amazon.com/pt/what-is-aws/
28. Documentação do AWS Identity and Access Management, consultado no dia 29 de Dezembro de 2023 em: https://docs.aws.amazon.com/pt_br/iam/
29. AWS Identity and Access Management (IAM)" e "Multi-Factor Authentication (MFA), fonte datado no dia 19 de Março de 2023 em: https://aws.amazon.com/iam/ e https://aws.amazon.com/iam/features/mfa/

30. Amazon Web Services identity and authentication, fonte datada no dia 19 de Março de 2023 em: https://aws.amazon.com/pt/identity/authentication/
31. Comparação entre métodos utilizado por Azure e AWS, Consultado no dia 02 de Abril de 2023 em: https://docs.microsoft.com/pt-br/azure/security/fundamentals/authentication-authorization e https://aws.amazon.com/pt/identity/authentication/
32. Victor Recuero, Sergio Medina, Alberto López e David Marin: Protección integral frente a las amenazas, Seguridad en un Mundo móvil, MicrosoftSecure.
33. Amazon, Consultado no dia 30 de Dezembro de 2023 em: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
34. Rath, A., Boucart, N., Thiran, P., & Spasic, B. (2019). Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure. computers, (28), Artigo Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure.
35. Bmc blogs, Public vs Private vs Hybrid: Nuvem Differences Explained, Consultado no dia 23 de Março de 2023 através: https://www.bmc.com/blogs/public-private-hybrid-nuvem/
36. Service Level Agreements (SLA) for Online Services, consultado no dia 29 de Dezembro de 2023 em: https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1
37. AWS Service Level Agreements (SLAs), consultado no dia 02 de Janeiro de 2024 através: https://aws.amazon.com/legal/service-level-agreements/
38. Identidades gerenciadas para recursos do Azure, consultado no dia 28 de Dezembro de 2023 através: https://learn.microsoft.com/pt-br/entra/identity/managed-identities-azure-resources/overview
39. AWS NuvemHSM, Consultado no dia 02 de Janeiro de 2024 em: https://aws.amazon.com/pt/nuvemhsm/
40. AWS Service Level Agreements (SLAs), consultado no dia 02 de Janeiro de 2024 em: https://aws.amazon.com/legal/service-level-agreements/
41. Azure Dedicated HSM, consultado no dia 02 de Janeiro 2024 em: https://azure.microsoft.com/en-us/products/azure-dedicated-hsm
42. Azure Access Token. Available online: https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens (acedido 04 de Abril 2023).