CIÊNCIAS EMPRESARIAIS
ESCOLA SUPERIOR
POLITÉCNICO SETÚBAL

Rui Carlos Pereira da Silva Durão de Sá

Cloud Computing – Prática Organizacional

Orientadora:

Doutora Leonilde Reis

Data: outubro 2024

Dedicatória

Este trabalho só foi possível ser realizado com o apoio incondicional da minha família, a todos, o meu muito obrigado.

Agradecimentos

Quero começar por agradecer à doutora Leonilde Reis pelo seu grau de exigência e pelo apoio ao longo do trabalho, possivelmente teria sido mais difícil ou mesmo impossível.

Ao doutor Manuel Landum pela sua experiência, disponibilidade e apoio. Na parte mais complicada do trabalho, ambos me apoiaram de uma forma notável.

A todos os meus professores do Instituto Politécnico de Setúbal por todo o conhecimento transmitido e muitas vezes foram mais além.

Resumo

A adoção da *cloud computing* implica a proteção de dados sensíveis, conformidade com regulamentos de privacidade, legislação nacional e conformidade dos serviços oferecidos, assim como a migração de dados, desta forma, quais as políticas que foram adotadas e qual a legislação que uma autarquia se rege para salvaguardar a segurança dos dados.

A *Cloud Computing* pode ser uma solução para a autarquia armazenar, processar e aceder a informações pertinentes no seu dia a dia.

O objetivo geral deste trabalho consiste em analisar os Sistemas de Informação e as Tecnologias de Informação e Comunicação de uma autarquia local, respondendo às seguintes questões: Quais as vantagens e desvantagens no uso da *Cloud Computing*? Benefícios de *datacenters* próprios? Poderá usar *datacenters* próprios e beneficiar de alguns serviços de *cloud* em simultâneo?

A virtualização é um processo cada vez mais importante e crucial, oferecendo à autarquia local maior eficiência, flexibilidade e contribuindo para uma abordagem mais ecológica na gestão de recursos computacionais, indo de encontro ao *Green IT.*

Desta forma, será crucial saber se a autarquia utiliza tecnologia de virtualização, numa arquitetura de microserviços ou monolíticos e qual a política de segurança, nomeadamente *Zero Trust*.

A elaboração do trabalho será realizada através da recolha e tratamento de informações junto da autarquia bem como na análise documental e possíveis estudos realizados.

A pesquisa qualitativa é uma abordagem que se centra na compreensão profunda e contextual de fenómenos, permitindo uma análise rica e detalhada.

A análise permitiu concluir que a autarquia beneficia financeiramente a longo prazo, no uso de *datacenters* próprios e na utilização da *cloud computing* a nível de *backups* e segurança.

Podendo, em conjunto com outras autarquias, optar pelo uso de uma *cloud* comunitária, favorecendo a partilha de informações, segurança da informação e de *backups* entre as mesmas.

Palavras-chave: *Cloud Computing,* Virtualização, *Datacenters,* Segurança.

Summary

The adoption of cloud computing implies the protection of sensitive data, compliance with privacy regulations, national legislation and compliance of the services offered, as well as data migration, so what policies have been adopted and what legislation does a municipality follow to safeguard data security?

Cloud computing can be a solution for local authorities to store, process and access relevant information in their day-to-day work.

The general aim of this work is to analyse the Information Systems and Information and Communication Technologies of a local authority, answering the following questions: What are the advantages and disadvantages of using Cloud Computing? Benefits of own datacentres? Can you use your own datacentres and benefit from some cloud services at the same time?

Virtualisation is an increasingly important and crucial process, offering the local authority greater efficiency, flexibility and contributing to a greener approach to managing computing resources, in line with Green IT.

It will therefore be crucial to know whether the local authority uses virtualisation technology in a microservices or monolithic architecture and what its security policy is, namely Zero Trust.

The work will be carried out by collecting and processing information from the local authority, as well as analysing documents and possible studies.

Qualitative research is an approach that focuses on a deep and contextual understanding of phenomena, allowing for a rich and detailed analysis.

The analysis led to the conclusion that the municipality benefits financially in the long term from using its own datacentres and from using cloud computing for backups and security.

Together with other municipalities, it could opt to use a community cloud, favouring the sharing of information, information security and backups between them.

Key words: Cloud Computing, Virtualisation, Datacenters, Security.

Índice Geral

Figuras

Tabelas

Lista de Siglas/Acrónimos

ACL- Access Control List

APIs- Application Programming Interfaces

ASPM- Application Security Posture Management

B2B- Business-to-Business

CA- Central Authority

CapEx- capital Expenditure

CD- Continuous Deployment

CDR- Cloud Detection and Response

CFR- Carta dos Direitos Fundamentais da União Europeia

CI- Continuous Integration

CIEM- Cloud Infrastructure Entilement Management

CMB- Câmara Municipal do Barreiro

CNPD- Comissão Nacional de Proteção de Dados

CS- Cloud Server

CSPM- Cloud Security Management

CWP- Cloud Workload Protection

DO- Data Owner

DPO- Data Protection Officer

DU- Data User

DevOps- Development and Operations

IA- Inteligência Artificial

IaaS- *Infrastructure as a Service*

IDA- Ideal Distribution Algorithm

IP- Internet Protocol

LLMs- Large Language Models

MTA- Multi-Tenancy Architecture

MPLS- Multiprotocol Label Switching

NIST- *National Institute of Standards and Technology*

NID- Network Intrusion Detection

NZIA- Net-zero industry act`

OpEx- Operational Expenditure

PaaS- *Platform as a Service*

RGPD- Regulamento Geral sobre a Proteção de Dados

SaaS- *Software as a Service*

SCCs- Clausulas contratuais padrão da União Europeia

SGSI- Sistema de Gestão de Segurança da Informação

SIEN- *Security Information and Event Management*

SOC- Security Operation Center

SLA- Service Level Agreement

TFUE- Tratado sobre o Funcionamento da União Europeia

TIC- Tecnologias de Informação e Comunicação

2FA- *Two-Factor Authentication*

UE- União Europeia

VCE- Virtual Computing Environment

VMs- Virtual Machine

VPN- Virtual Private Network

ZT- Zero Trust

Introdução

A *cloud computing* tem vindo a crescer desde 2006, sendo atualmente uma tecnologia relevante das Tecnologias de Informação e Comunicação (TIC), oferecendo armazenamento e *software* a baixo custo.

Nos dias de hoje a era digital é caracterizada por um conjunto de tecnologias como a virtualização, serviços digitais e inteligência artificial. Sendo a virtualização um elemento crucial para a *cloud*, tendo vantagens como agilidade, escalabilidade e controlo de custos.

A compreensão da utilização da *cloud computing* em prol dos tradicionais datacenters, bem como as suas vantagens e desvantagens é um dos objetivos deste trabalho. Perceber a vantagem na utilização de datacenters próprios no dia-a-dia, criando apenas *backups* na *cloud,* pagando apenas pelo que se usa ou, migrar toda a operação.

A adoção bem-sucedida pode ser avaliada por métricas como a produtividade, ou seja, tirar o máximo partido com a máxima rentabilidade.

A segurança da informação é crucial para a sobrevivência de qualquer organização, neste caso, uma autarquia. Desta forma, para salvaguardar a segurança, terão de ser alocados muitos recursos, nomeadamente colaboradores com capacidades técnicas para suportar possíveis ataques. A *cloud computing* poderá neste caso, oferecer ferramentas para salvaguardar os dados, libertando a autarquia de um encargo, ou não.

Entender quais as opções mais lucrativas, a sua burocracia e a sua legislação.

A elaboração desta dissertação terá três capítulos.

No primeiro capítulo, Enquadramento Teórico, será descrito a definição de *cloud computing*, as suas características, os seus serviços, benefícios, operacionalidade, legislação e segurança, baseados em pesquisa bibliográfica, metodologia definida, objetivos gerais e específicos.

No segundo capítulo será enunciado a Metodologia de Estudo, fomentando a escolha do método baseado em autores de referência.

No terceiro capítulo, Caracterização da Organização, entender como a autarquia faz uso dos seus recursos de SI/TIC e perceber as razões da utilização, ou não ou em parte, da *cloud computing.*

Por último, Conclusões e Perspetivas de Trabalho Futuro, neste ponto será enunciado quais as conclusões retiradas bem como os obstáculos encontrados durante a realização do trabalho. Será proposto uma realização de investigação de um futuro trabalho, tendo em

consideração os obstáculos encontrados, como melhorar e tendo sempre em consideração os avanços tecnológicos, em particular o uso da inteligência artificial.

1 Enquadramento Teórico

Será enunciado o conceito de *cloud computing,* as suas características e seus serviços, bem como os seus benefícios, operacionalidade, segurança e legislação em vigor.

1.1 Conceito de *Cloud Computing*

A evolução dos SI e das TIC transformou radicalmente a forma como as organizações operam, otimizam os seus processos e interagem com o mercado. Observando uma constante evolução na transformação digital, proporcionando novos modelos de negócio e melhorando a eficiência bem como a competitividade.

Com o surgimento da *Internet* constatou-se a uma revolução na comunicação, reduzindo barreiras tando de distância como de tempo. As organizações agora expandem-se a nível global.

O cientista *Ramnath Chellappa* utilizou o termo *cloud computing* pela primeira vez em 1997 aquando da publicação de um artigo científico, descrevendo o paradigma emergente de fornecimento de serviços de computação através da *Internet.* Em meados da década de 2000, com o aumento da virtualização e o desenvolvimento dos serviços *Web*, o termo *cloud computing* começou a ganhar importância e a ser adotado pelas organizações ou por particulares (Islam et al., 2023).

A *cloud computing* é uma das invenções mais poderosas que despertou a curiosidade dos tecnólogos do mundo inteiro (Pallathadka et al., 2022).

Os autores Mell & Grance (2011), do *National Institute of Standards and Technology* (NIST), descrevem *cloud computing* como um modelo que permite o acesso à rede ubíquo, conveniente e a pedido de um conjunto partilhado de recursos informáticos configuráveis. Afirmam que o modelo de nuvem é composto por cinco características essenciais (Tabela 1), três modelos de serviço (Tabela 2) e quatro modelos de implantação (Tabela 3).

Esta tecnologia permite o armazenamento de dados e programas, substituindo os discos rígidos dos computadores. Sendo possível o seu acesso de qualquer dispositivo de qualquer lugar através da *Internet.*

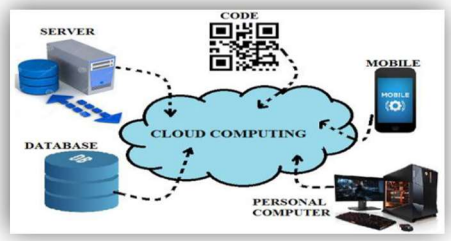
Permitindo pagar apenas pelo que se usa, escalabilidade dos recursos computacionais (servidores, armazenamento) e elasticidade (capacidade de ajustar os recursos automaticamente em tempo real) dos recursos oferecidos, conforme as necessidades do cliente, sendo a sua manutenção e atualizações geridas pelo fornecedor de serviço.

A *cloud computing* permite aos seus clientes desenvolver as suas próprias aplicações, fornecendo todas as ferramentas, tendo a particularidade de os utilizadores e as organizações, poderem aceder aos seus serviços a partir de qualquer lugar.

Para tirar partido das vantagens da *cloud computing*, as organizações recorrem ao *Cloud Sourcing*, sendo definido como um processo através do qual a implementação e a manutenção das TIC são asseguradas por um ou vários fornecedores de serviços de nuvem, podendo assim ser considerado como uma variante específica da externalização dos recursos de TIC (Muhic et al., 2023).

A Figura 1, exemplifica o funcionamento, de uma forma simplista, de *cloud computing*, sendo necessário um centro de dados, base de dados, computador, telemóvel, *tablet* ou qualquer dispositivo com ligação à *Internet* para aceder a qualquer informação.

Figura 1- Noção de cloud computing



Fonte: “Cloud computing an overview” (Shilpashree et al., 2018, p. 1)

Conforme a Figura 1, entende-se que a facilidade de acesso não só amplia as possibilidades de uso, mas também elimina barreiras geográficas e limitações de *hardware*, permitindo que profissionais e organizações operem eficientemente em ambientes dinâmicos e móveis.

Podendo ser um fator determinante para a adoção da *cloud computing* por parte da autarquia local.

1.2 Caracterização e Serviços

A tabela 1 apresenta as características essenciais, de uma forma sucinta, pela NIST.

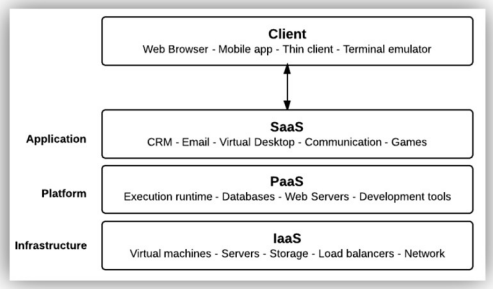
Tabela 1- Características da *cloud*

Característica	Descrição
Autosserviço a Pedido	Um consumidor pode aumentar o armazenamento em rede sem a necessidade de interação humana com o fornecedor.
Acesso Alargado à Rede	Os dados estão em rede, podendo ser acedidos através de um telemóvel, *tablet*, computadores portáteis ou outros dispositivos com ligação à *Internet*.
Agrupamento de Recursos	Os recursos informáticos do fornecedor são agrupados de modo a servir vários utilizadores com diferentes recursos físicos e virtuais. Existe uma sensação de independência da localização, ou seja, o cliente não tem controlo ou conhecimento sobre a localização exata dos recursos fornecidos. Exemplos de recursos: armazenamento, memória e largura de banda de rede.
Elasticidade Rápida	As capacidades podem ser aprovisionadas e libertadas de forma elástica, sendo, em alguns casos, de uma forma automática, para se expandirem rapidamente em função da procura. Isto dá a ideia ao utilizador de que as capacidades são ilimitadas.
Serviço Medido	Os sistemas de *cloud computing* controlam e otimizam automaticamente a utilização dos recursos, tirando partido de uma capacidade de medição a um nível de abstração adequado ao tipo de serviço (armazenamento, processamento, largura de banda e contas de utilizador ativas).

Fonte: Adaptado de "*The NIST definition of cloud computing"* (Mell & Grance, 2011).

A Figura 2 apresenta alguns exemplos de serviços de *SaaS, PaaS e IaaS.*

Figura 2- SaaS, PaaS e IaaS



Fonte: "What is Cloud? It is time to update the NIST definition?" *(Miyachi, 2018, p. 2)*

Conforme apresentado na Figura 2 e apresentando a *IaaS,* esta poderá oferecer à autarquia uma infraestrutura de virtualização, servidores e armazenamento, permitindo pagar apenas pelo que usa, transformando *Capital Expenditure (*Capex) em *Operational Expenditure* (Opex), tendo em consideração à escalabilidade e à sua flexibilidade. Podendo desta forma usufruir das últimas tecnologias inovadoras sem a necessidade de adquirir em definitivo, nem de recursos humanos para as criarem, pois, as mesmas estão prontas a ser usadas.

A tabela 2 descreve os três modelos de serviço, pela NIST *IaaS, PaaS e SaaS.*

Os modelos de serviço a adotar por parte da autarquia podem ir de encontro às suas necessidades e objetivos.

Se, no caso da CMB e tendo em consideração o trabalho em questão e sendo possível ser adotado por qualquer organização, pode apenas usufruir de um modelo de serviço ou dois.

Isto quer dizer que a CMB poderá optar por usar apenas do modelo de serviço de *SaaS* ou de *IaaS,* caso não tenha uma arquitetura de virtualização.

A escolha do ou dos modelos de serviço vai depender das necessidades específicas de cada organização e da sua dimensão.

Esta análise terá de ser realizada minuciosamente, não podendo muitas vezes ser feita a realização de comparação.

A comparação pressupõe que terá de ter as mesmas características bem como os mesmos objetivos.

Tabela 2- Modelos de serviço

Modelo de Serviço	Descrição
***Software* como um Serviço (SaaS)**	A capacidade oferecida ao consumidor é a de utilizar as aplicações do fornecedor que funcionam numa infraestrutura de nuvem. As aplicações são acessíveis a partir de vários dispositivos através de uma interface simples, como um navegador *Web* ou de uma interface de programa.
Plataforma como um Serviço (PaaS)	A capacidade fornecida ao consumidor é a de implantar na infraestrutura de nuvem aplicações criadas pelo consumidor ou adquiridas. As aplicações são geridas e controladas pelo consumidor, que pode utilizar linguagens, bibliotecas, serviços e ferramentas suportadas pelo fornecedor.
Infraestrutura como um Serviço (IaaS)	A capacidade fornecida ao consumidor é a de fornecer processamento, armazenamento, redes e outros recursos computacionais fundamentais onde o consumidor pode implantar e executar software arbitrário, que pode incluir sistemas operativos e aplicações.

Fonte: Adaptado de "*The NIST definition of cloud computing"* (Mell & Grance, 2011)

Após análise da tabela 2, podemos concluir que os 3 modelos de serviço podem facilitar o trabalho dos técnicos e especialistas da divisão de informática da Câmara Municipal do Barreiro (CMB).

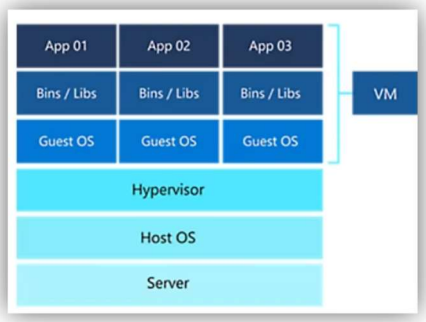
No caso de uma organização optar por ter *datacenter* próprio com arquitetura de virtualização, não existe a necessidade de recorrer de *IaaS*, pois já tem uma infraestrutura de servidores, armazenamento e de redes.

No entanto, poderá usufruir dos serviços de *PaaS e SaaS.* A relação entre vários *softwares* é possível através de interfaces de programação de aplicações (APIs).

No caso da virtualização de servidores, permitindo a criação de máquinas virtuais, torna-se necessário um hipervisor, sendo este um *software* responsável tanto por criar como para gerir as máquinas virtuais.

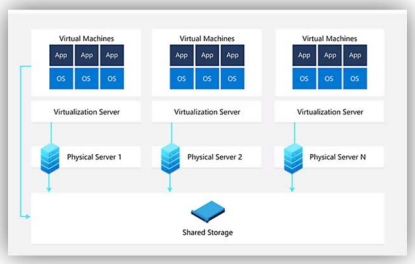
A Figura 3 mostra a arquitetura de máquinas virtuais individuais num único servidor através de um hipervisor e a Figura 4 expande o conceito para múltiplos servidores demonstrando como um ambiente de *datacenter* ou *cloud* podem hospedar inúmeras máquinas virtuais num servidor diferente, utilizando um armazenamento partilhado para os dados.

***Figura 3*- Máquina Virtual**



Fonte: “Azure” (Microsoft, 2024)

Figura 4- Máquinas Virtuais em servidores físicos diferentes



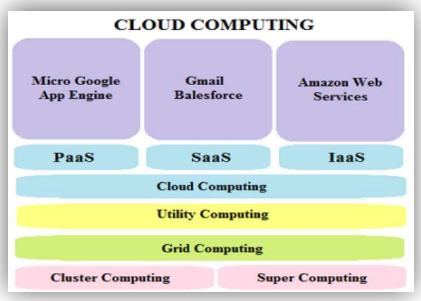
Fonte: “Azure” (Microsoft, 2024)

Virtual Machine Manager, permite executar vários sistemas operacionais em diferentes máquinas virtuais em simultâneo, tais como *Linux* num sistema operacional *Windows* (Microsoft, 2024). As máquinas virtuais funcionam de maneira similar a qualquer outro computador físico (possui CPU, memória, armazenamento) ligando-se à *Internet* sempre que necessário, sendo vistas como computadores virtuais ou definidos por *software,* existindo apenas como código em servidores físicos (Microsoft, 2024).

A Figura 5, é um exemplo de serviços de *cloud computing*, nomeadamente de *SaaS*, *PaaS* e de *IaaS*.

Representando uma hierarquia.

Figura 5- *Cloud Computing*



Fonte: "*Cloud computing an overview"* (Shilpashree et al., 2018, p. 2)

A Figura 5 representa uma hierarquia para relacionar os modelos de computação, indicando a computação em *cluster* e a supercomputação são tecnologias fundamentais que levam a serviços mais complexos e específicos, como *PaaS, SaaS* e *IaaS.* A descrição sugere que cada modelo ou serviço se baseia no anterior, ilustrando não apenas a progressão dessas tecnologias, mas também a forma como se acumulam para formar uma gama mais ampla de opções para utilizadores e organizações.

1.3 Tipos de *Cloud*

A tabela 3 descreve e enuncia, de uma forma sucinta, pela NIST, os quatro tipos de nuvem. De salientar que a autarquia poderá optar por um tipo de nuvem, dependendo da fragilidade e da importância da informação a ser mantida ou se pretende apenas combinar um dos modelos de implementação com um *datacenter* próprio.

Esta combinação permite à autarquia local um maior controlo dos custos bem como da informação.

O controlo da informação significa que sabe sempre aonde está a mesma, reforçando que um dos fatores pela não adoção da *cloud* é não ter plenamente conhecimento aonde está a informação e qual o real nível de segurança.

Salientando que cada *cloud* apresenta características diferentes conforme descrito na tabela 3.

Como já salientado, a escolha do tipo de *cloud* caberá à CMB, sendo o mais comum recair pela pública.

Tabela 3- Modelos de implementação

Tipo de *Cloud*	Descrição
***Cloud* Privada**	A infraestrutura de *cloud* é para uso exclusivo de uma única organização que inclui vários consumidores. Pode ser propriedade, gerida e operada pela organização, por um terceiro ou por alguma combinação deles, e pode existir dentro ou fora das instalações.
***Cloud* Comunitária**	A infraestrutura de *cloud* é para uso exclusivo por uma comunidade específica de consumidores de organizações que têm preocupações comuns, missão e requisitos de segurança, política e considerações de conformidade.
***Cloud* Pública**	A infraestrutura de *cloud* é para uso aberto pelo público em geral. Pode pertencer, ser gerida e operada por uma organização empresarial, académica ou governamental, ou por uma combinação destas.
***Cloud* Híbrida**	A infraestrutura de *cloud* é uma composição de duas ou mais infraestruturas de *cloud* distintas (privada, comunitária ou pública) que continuam a ser entidades únicas, mas estão ligadas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicações.

Fonte: Adaptado de "*The NIST definition of cloud computing"* (Mell & Grance, 2011)

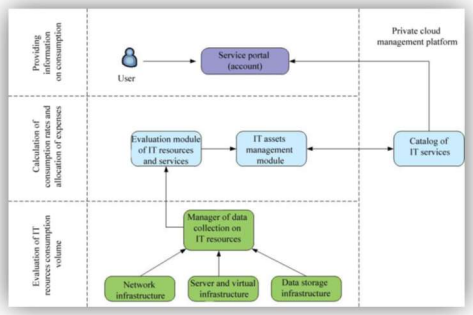
1.3.1 *Cloud* Privada

A Figura 6 apresenta um diagrama de gestão da *cloud* privada em que se avalia o volume de consumo de recursos informáticos, cálculo das taxas de consumo e afetação das despesas e informações sobre o consumo.

É imperativo que as organizações mantenham controlados e atualizados os custos que estão a ter. A sua ausência poderá encarecer ainda mais e podendo estar a usar recursos desnecessários.

Sendo o objetivo principal da CMB a redução do *Capex.*

Figura 6-Diagrama de Gestão da *cloud* privada



Fonte: “Types of cloud deployment” (Tavbulatov et al., 2020, p. 3)

Na Figura 6 constata-se três camadas, em que a primeira representa a interação do utilizador com a plataforma através do portal de serviço, a segunda será responsável pelo cálculo de consumo e gestão de ativos e a última na recolha e avaliação dos dados de uso das infraestruturas de rede, servidores e armazenamento.

A *cloud* privada necessita de investimento em *hardware* e *software* licenciado, custos iniciais de configuração, mas permite reduzir despesas de manutenção e energia, sendo gerida por terceiros. Tornando a sua gestão simples e reduz a necessidade de ter equipas internas na sua gestão. A longo prazo é mais rentável para a autarquia obter um *datacenter* próprio do que migrar para a *cloud* privada, perdendo, no entanto, a nível de flexibilidade e escalabilidade. A tabela 4 apresenta algumas soluções de implementação

Tabela 4- Tipos de implementação da *cloud* privada.

Nome	Descrição
Dell Active System	Família de sistemas integrados para implementação e virtualização de uma *cloud* privada.
VCE vBlock	Infraestrutura de *cloud* "pronta para uso".
Hewlett Packard Enterprise OpenStack Helion	Complexo para a criação de um ambiente de *cloud* privada.
VMware vCloud Suite, VMware Integrated OpenStack	*Suite vCloud da VMware, VMware Integrated OpenStack.*

Fonte: Adaptado de “*Types of cloud deployment”* (Tavbulatov et al., 2020, p. 3)

Salientando que no caso de a autarquia ter aplicações que requerem um processamento intensivo ou acesso em tempo real, a proximidade física dos servidores no *datacenter* próprio poderá oferecer um desempenho superior.

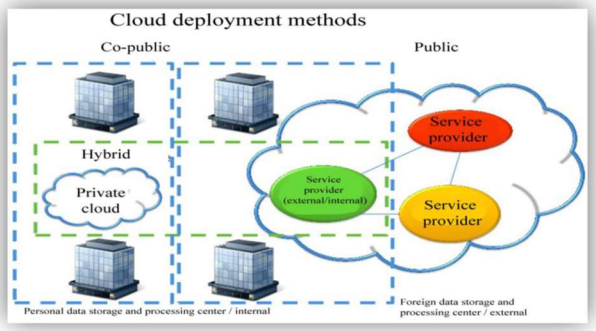
A CMB pode aproveitar uma das soluções apresentadas na tabela 4 para implementar numa *cloud* privada.

1.3.2 *Cloud* Comunitária

A Gartner (2024) refere-se à *cloud* comunitária como um ambiente de serviço de *cloud computing* partilhado que se destina a um conjunto limitado de organizações ou colaboradores (como bancos e no caso deste trabalho de uma partilha por parte das câmaras nacionais). O princípio de organização da comunidade pode variar, mas os membros da comunidade geralmente partilham requisitos semelhantes de segurança, privacidade, desempenho e conformidade. Os membros da comunidade podem querer invocar um mecanismo que é frequentemente gerido por eles próprios (e não apenas pelo fornecedor) para analisar os que pretendem entrar na comunidade.

A NIST (2024) identifica a *cloud* comunitária como uma infraestrutura para uso exclusivo por uma comunidade específica, partilhando preocupações como requisitos de segurança, políticas, missão e considerações de conformidade.

Figura 7- *Cloud* Comunitária



Fonte: “Types of cloud deployment” (Tavbulatov et al., 2020, p. 6)

Através da *cloud* comunitária, ilustrada pela Figura 7, é possível a partilha de vários servidores pela comunidade.

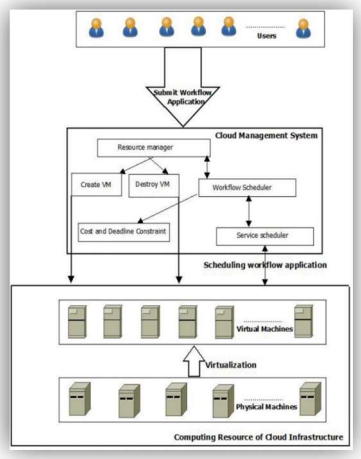
Quando múltiplas organizações necessitam de infraestrutura idêntica e desejam compartilhar, uma *cloud* comunitária é formada. Ao reunir recursos, as empresas podem colher os benefícios. Reconhecendo como um dos benefícios a redução de custos, oferecendo uma

nova abordagem de gestão, tendo sido criado um algoritmo de escalonamento, *Ideal Distribution Algorithm* o IDA (Aldahwan & Ramzan, 2022).

A *cloud* comunitária poderá ser útil para todas as câmaras municipais do território português, pois partilham de preocupações de segurança, missão, considerações de conformidade, políticas e são uma comunidade específica.

A Figura 8, ilustra a arquitetura comum utilizada para o agendamento de fluxos de trabalho numa nuvem comunitária.

Figura 8- Arquitetura do fluxo de trabalho na *cloud* comunitária



Fonte: "A Management System for Servicing Multi-Organizations on Community Cloud Model in Secure Cloud Environment" (Dubey et al., 2019, p. 2)

A Figura 8, ilustra um sistema de gestão da *cloud* para agendar fluxos de trabalho, destacando as interações entre os vários utilizadores, mas também a interação entre a virtualização e a infraestrutura de *cloud* na sua gestão e agendamento, tendo em consideração os possíveis constrangimentos de custo e tempo.

A possível utilização da *cloud* comunitária pelas câmaras nacionais do território português, facilitaria a comunicação entre as câmaras e agilizava a partilha de informações bem como os seus custos.

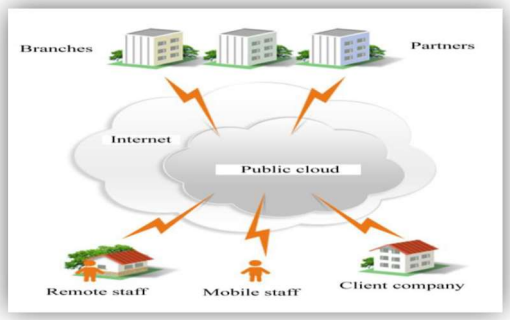
A dificuldade inerente à sua implementação poderá estar nos diferentes partidos políticos das diversas câmaras, sendo de conhecimento público a ausência de entendimento entre os mesmos.

Tendo em consideração ao facto das várias eleições, pois as mesmas originam mudanças na presidência camarária.

1.3.3 *Cloud* Pública

A Figura 9, representa o funcionamento de uma *cloud* pública.

Figura 9-*Cloud* Pública



Fonte: "Types of cloud deployment" (Tavbulatov et al., 2020, p. 4)

A *cloud* pública apresenta algumas vantagens que tornam a adoção pela CMB mais atrativa sendo a sua utilização mais simples e eficiente e com recursos informáticos ilimitados. Requerendo apenas e como já foi referido anteriormente aquando da definição de *cloud computing,* ligação à *Internet.*

Tabela 5- Soluções prontas para implementação numa *cloud* pública.

Nome	Descrição
Windows Azure	Infraestrutura de *cloud* que opera com várias aplicações, serviços e tarefas de negócio numa *cloud*, permitindo criar, implementar e gerir aplicações sob o controle da *Microsoft*.
Google Cloud	Serviço de *cloud* gratuito com uma vasta gama de configurações que funciona perfeitamente em *smartphones* com sistema operativo *Android*.
AWS	A *cloud* mais conhecida que utiliza diversos centros de processamento de dados localizados em diferentes regiões.

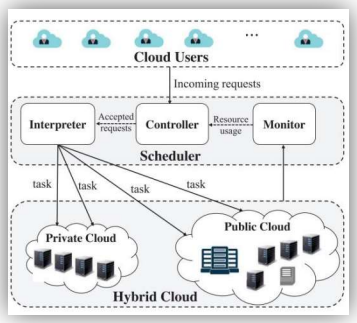
Fonte: Adaptado de "*Types of cloud deployment"* (Tavbulatov et al., 2020, p. 5)

A CMB poderá solicitar os serviços de *cloud* a um ou a mais de um prestador de serviços, sendo uma opção a ser tida em consideração.

1.3.4 *Cloud* Híbrida

A Figura 10, representa uma *cloud* híbrida que combina recursos de *cloud* privada e pública para melhorar a eficiência e a escalabilidade. Neste tipo de *cloud*, tanto os dados como as aplicações podem migrar da *cloud* privada para a *cloud* pública e vice-versa, desta forma obtém-se maior flexibilidade. A migração é feita através de um programador que controla, interpreta e monitoriza as credenciais dos utilizadores.

Figura 10- *Cloud* Híbrida



Fonte: "Cost and makespan-aware workflow scheduling in hybrid clouds" (Zhou et al., 2019, p. 2)

Para a *Microsoft* as *clouds* híbridas combinam as *cloud* privadas e *datacenters* no local com *cloud* públicas. Desta forma, as organizações conseguem obter uma maior flexibilidade de utilizar novas tecnologias. Segundo a mesma organização; "assim como uma rede no local multilocal tradicional pode precisar de ligar múltiplas sucursais a uma sede, também a rede de *cloud* híbrida envolve a utilização de tecnologias apropriadas para interligar diretamente os utilizadores, as aplicações e os dados no local a aplicações e dados alojados na cloud*"* (Microsoft, 2024).

1.4 Adoção da *cloud computing*

A *cloud computing* permite às organizações aumentar ou diminuir os seus recursos de TIC de uma forma rápida e fácil, evitando as atualizações dispendiosas de *hardware e software*.

Para a autarquia que procura tirar o máximo partido da tecnologia atualmente utilizada a custos possíveis, tendo em consideração a aquisição de *hardware* e *software* e as suas licenças de utilização, com menor risco, a *cloud computing* é a melhor solução.

A sua utilização na totalidade ou combinada com *datacenters* próprios ainda levanta muitas questões, nomeadamente no conhecimento da localização dos seus dados e em caso de vir

a querer prescindir desta tecnologia o que acontecerá aos seus dados, qual o grau de certeza que o fornecedor eliminará todos as informações.

A dúvida poderá estar relacionada também com o simples facto de pensarem que é mais um custo do que um investimento e a possível ausência de literacia quanto à sua tecnologia.

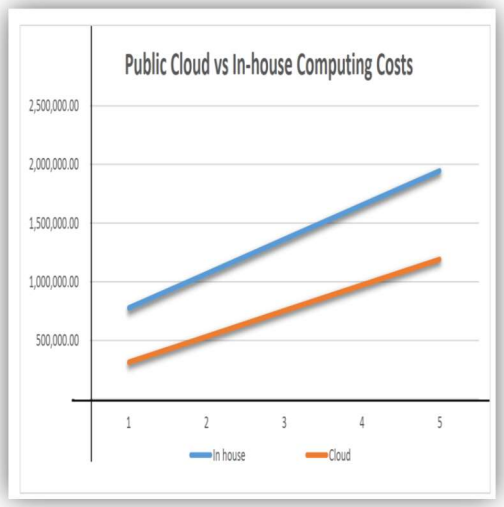
1.4.1 Benefícios

A grande maioria dos clientes não tem conhecimento da localização real dos dados, podendo estes escolher as aplicações na nuvem mais adequadas às suas necessidades, bastando para isso executá-las com os seus dados e pagar apenas pela quantidade de horas de utilização.

As organizações que utilizem os serviços de nuvem poderão reduzir significativamente o *Capex,* tendo em consideração que as mesmas não necessitam de investir em *hardware* ou em instalações, utilizando as infraestruturas oferecidas pela *AWS, Google Cloud* ou *Azure.* Logo, os serviços em nuvem transformam muitos custos que poderiam ser *Capex* em *OpEx.*

Num estudo elaborado pelos autores Abdulle et al. (2022) e fazendo cálculos para cinco anos, consideram que a nuvem pública ficaria mais barato, conforme ilustra a Figura 11.

Figura 11-Análise para um período de cinco anos



Fonte: "*Cost-benefit analysis of public cloud versus in house computing"* (Abdulle et al., 2022, p. 6)

Os autores Bello et al. (2021) no seu estudo sobre a contribuição da *cloud computing* na área da construção, destacam que a área de atividade em questão, tem uma utilização intensiva de dados, uma vez que os dados heterogéneos são continuamente gerados à medida que os projetos avançam nas suas diferentes fases, necessitando de serem armazenados para

serem utilizados pelas suas diversas equipas, sempre que tenham necessidade, em diferentes dispositivos. A tabela 6 apresenta algumas vantagens da *cloud computing.*

A segurança da informação continua a ser deveras importante para a sobrevivência das organizações, constatando que em muitos casos a violação de dados tem como origem no roubo ou na perda de credenciais dos colaboradores, tornando-se importante a implementação da política de segurança de *Zero Trust*, será pertinente conhecer as práticas instituídas pela autarquia.

O estudo em causa, poderia muito bem ser qualquer outra atividade económica em que se trabalhe com muitos dados e em que vários departamentos necessitam de aceder a diferentes informações, com diferentes dispositivos, em lugares distintos e com as informações atualizadas, sendo possível aplicar à CMB. A tabela 6 apresenta algumas vantagens da *cloud.*

Tabela *6*- Vantagens da *Cloud*

Vantagem	O que significa
Agilidade	Criar/editar rapidamente a infraestrutura, permitindo frequentemente inovação
Redução de custos	Pagar apenas pelo que se usa, reduzindo as despesas iniciais.
Resiliência	Alta disponibilidade em múltiplas regiões e capacidades de automação para recuperação de falhas/desastres.
Elasticidade	Escalar facilmente para cima ou para baixo conforme as necessidades do negócio.
Inovação mais rápido	Focar-se nos diferenciais do negócio, não na infraestrutura.
Globalização	Usar as ferramentas fornecidas pelo fornecedor de serviços em *cloud* e a sua presença global para fornecer serviços ao redor do mundo

Fonte: Adaptado de "*Practical adoption of cloud computing in power systems-drivers, challenges, guidance, and real world use cases"* (Zhang et al., 2022, p. 2392)

A tabela 6 apresenta as vantagens a destacando a capacidade para a redução de custos associada à elasticidade, pois ao reduzir a elasticidade reduz automaticamente o preço.

Nos dias de hoje é crucial para o sucesso e para a inovação das organizações, poderem aceder aos seus dados a toda a hora e o mais fidedigna possível. Esta possibilidade de aceder aos dados atualizados, pode ser um marco de diferenciação em relação à concorrência que está cética na utilização da *cloud*. Tendo em consideração que para adotar a *cloud computing*, é fundamental que a CMB desenvolva uma estratégia sólida em SI, implicando uma compreensão detalhada do modelo de negócio.

1.4.2 Desafios

No estudo apresentado pelos autores Bello et al. (2021), afirmam que a implementação de soluções no local requer uma enorme sobrecarga de energia, arrefecimento, segurança, disponibilidade e atualizações, acarretando um enorme encargo em termos de custos operacionais.

No entanto, pode-se aceder aos serviços de *cloud* de forma omnipresente e a pedido. Reconhecendo que a utilização da *cloud* pode sofrer de latências de rede a longo prazo.

Considera-se quatro pontos a ter em consideração a nível de desafios, a saber:

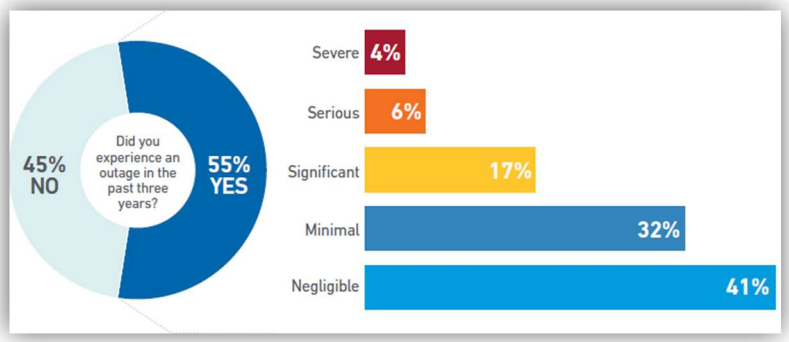
- Necessidade de *Internet* de alta velocidade de apoio em caso de excesso de dados;
- Limitações de tecnologia de base se estiver a utilizar a *cloud* pública;
- Aumento dos custos de manutenção se utilizar a *cloud* privada;

Num estudo anual realizado pela *intelligence*, 2024, mais de metade (55%) dos operadores inquiridos no inquérito de 2023, do *Uptime Institute,* sobre centro de dados, relataram ter tido uma interrupção no serviço nos últimos três anos, 60% em 2022 e 69% em 2021. Perante estes dados do inquérito, o *Uptime Institute,* conclui que existiu uma melhoria de 4 pontos percentuais em relação a 2022 e 10 pontos percentuais em relação a 2021.

A melhoria de 4 pontos percentuais em relação a 2022, a indústria enfrenta novos desafios relacionados coma as mudanças tecnológicas, tais como a instabilidade energética e os efeitos das alterações climáticas, sendo necessário um foco contínuo em resiliência e gestão dos riscos.

A mesma organização e apresentado na Figura 12, solicitou aos operadores que classificassem a falha nos seus centros de dados, numa escala de 1 (insignificante) a 5 (grave), de salientar que os que responderam “não sei” não está incluído.

Figura 12- Qual o impacto na falha nos centros de dados



Fonte: "*Annual outage analysis 2024"* (Intelligence, 2024, p. 4)

Após a análise dos dados constata-se que 55% dos inquiridos afirmaram ter experienciado uma falha de energia nos últimos três anos e 45% afirmaram não ter experienciado nenhuma falha de energia. Apenas uma pequena fração enfrentou falhas graves (4%) ou sérias (6%). De salientar que quatro em cada cinco inquiridos acreditam que as suas falhas mais graves poderiam ter sido evitadas com melhor gestão, processos e configuração.

Constata-se através dos dados que embora a maioria tenha enfrentado falhas de energia, a gravidade tende a ser baixa, com poucas instâncias de impacto grave ou sério.

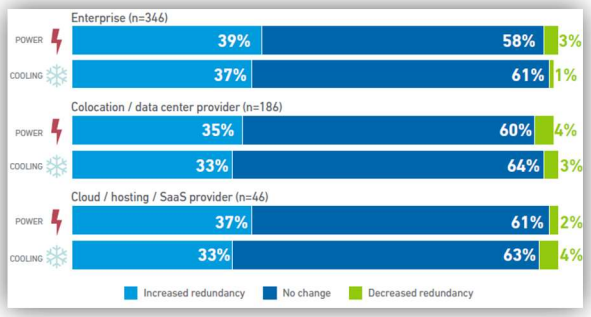
No entanto, 16% relataram custos superiores a $1 milhão de dólares (929.415,00 euros).

A falha nos centros de dados pode causar perdas financeiras e de dados bastante significativas, podendo inclusive colocar toda a operação em risco, tendo em consideração a instabilidade da rede elétrica e os eventos climáticos extremos associados às mudanças climáticas aumentando o risco de falhas.

Estas preocupações devem ser tidas em conta na escolha da *cloud computing* e criar planos para a salvaguarda da informação, pois nada é infalível. Assim sendo, uma boa política de segurança deve estar sempre atualizada para os novos riscos que aparecem.

No mesmo estudo, foi questionado aos operadores qual a mudança nos níveis de redundância, conforme apresentado na Figura 13.

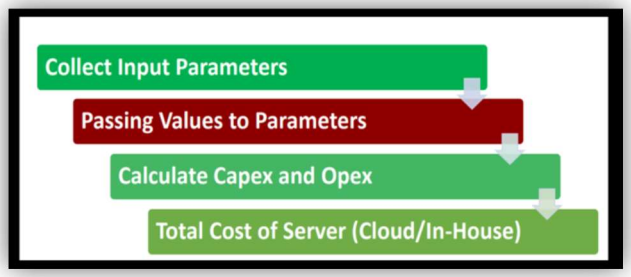
Figura 13- Qual a mudança nos níveis de redundância nos últimos 3 a 5 anos nos centros de dados?



Fonte: "*Annual outage analysis 2024"* (Intelligence, 2024, p. 6)

Nas empresas, a maioria relata sem mudança na redundância tanto para a energia quanto para a refrigeração (58% e 61%, respetivamente) e uma parte significativa aumentou a redundância na energia (39%) e na refrigeração (37%). No caso de provedores de *cloud/ hosting /SaaS* a redundância aumentou 37%, 61% sem qualquer mudança e 2% diminuiu a redundância.

Figura 14-Modelo de processo para calcular Capex e OpEx



Fonte: "*Cost-Benefit analysis of public cloud versus in-house computing"* (Abdulle et al., 2022, p. 4)

Perante a Figura 14 é crucial recolher os parâmetros de entrada, passar valores para parâmetros, calcular *Capex* e *OpEx* e por fim temos os custos totais por servidor.

Torna-se crucial nos dias de hoje, especialmente a CMB, elaborar os seguintes cálculos para entenderem os valores que estão em causa, conforme a tabela 7.

Tabela 7- Fórmulas para cálculo dos custos

Item	Fórmula
Custo para servidores	Número de servidores × Custo por servidor
Custo da eletricidade para servidores	Número de servidores × Custo da eletricidade × Consumo de energia por servidor
Custo da eletricidade para ar condicionado	Número de ar condicionados × Custo da eletricidade × Consumo de energia por ar condicionado
Custo de outras eletricidades	Número de horas por dia × Custo da eletricidade × Consumo de energia de outras eletricidades
Custo do sistema operativo	Número de sistemas operativos × Custo por sistema operativo
Custo da base de dados	Número de bases de dados × Custo por base de dados
Custo do antivírus	Número de antivírus × Custo por antivírus
Custo do equipamento de rede	Número de equipamentos de rede × Custo por equipamento de rede
Custo do pessoal	Número de colaboradores × Custo por mês

Custo de espaço alugado	Espaço alugado × Custo por espaço
Manutenção da infraestrutura dos servidores	Número de servidores × Custo por servidor × Custo de proporção
Manutenção de software	Custo de proporção × Custo do software
Custo de largura de banda	Número de linhas alugadas × Custo por linha alugada

Fonte: Adaptado de "*Cost-benefit analysis of public cloud versus in house computing*" (Abdulle et al., 2022)

Os autores consideram que no caso da nuvem pública tem normalmente menos despesa de capital do que *datacenter*, quando se trata de comparar custos iniciais. No caso da imigração cobra em pormenor taxas de subscrição, taxas de consulta e formação de pessoal. Apresentam na tabela 8 os cálculos do *Capex* e do *OpEx* numa *cloud* pública.

Tabela 8- Calcular o Capex e o OpEx da *cloud* pública

Item	Fórmula
Custo de Migração	Taxa de subscrição × Taxas de consultoria × Despesas com colaboradores
Custo de Administração do Sistema	Salário por mês × Número de administradores de sistema
Poder de Computação	Número de utilizadores × Horas por dia × Taxa por hora
Custo de Armazenamento	Uso em GB/hora × Horas por dia × Taxa por hora × GB por hora
Custo de Largura de Banda (ENTRADA + SAÍDA)	Taxa GB/hora ENTRADA × Taxa GB/hora SAÍDA × Horas de trabalho

Fonte: Adaptado de "*Cost-benefit analysis of public cloud versus in house computing*" (Abdulle et al., 2022)

Tendo sido referido anteriormente, a CMB necessita de ter um conhecimento elevado das suas necessidades a nível dos SI e das TIC. A passagem para a utilização de serviços de *cloud computing*, requer que a CMB seja bastante organizada para mover as suas cargas de trabalho. Terá de existir uma boa arquitetura empresarial

1.4.3 Operacionalidade

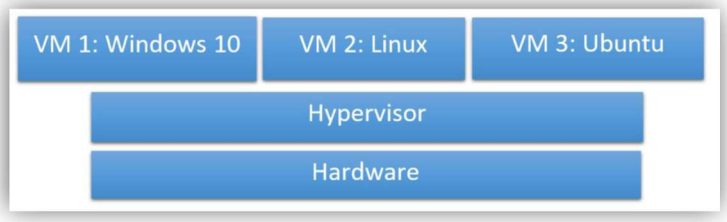
Nos últimos dez anos, os utilizadores têm podido aceder às suas aplicações, dados e serviços através da *cloud*, de qualquer local com ligação à *internet.* A escala dos ambientes de *cloud* heterogéneos está a crescer constantemente, devido ao desenvolvimento de dispositivos inteligentes com uso intensivo de computação.

Com a ajuda das máquinas virtuais, podem ser fornecidos vários serviços de *cloud* aos utilizadores finais, tais como infraestruturas, plataformas e *software.* As máquinas virtuais criam basicamente a ilusão de que o utilizador está a trabalhar numa máquina que lhe é dedicada, fornecendo um sistema operativo completo para trabalhar, podendo usar várias aplicações.

A tecnologia de virtualização permite o uso eficiente dos recursos e reduz os custos de manutenção e segurança para os utilizadores finais e são executadas em hipervisores, que podem ser de dois tipos:

I. O hipervisor de tipo 1, também conhecido como hipervisor "*bare metal"*, opera diretamente no *hardware* físico sem necessidade de um sistema operativo. Exemplos incluem *Citrix XenServer, VMware ESXi e Microsoft Hyper-V.* A arquitetura em camadas deste hipervisor é ilustrada na Figura 15.

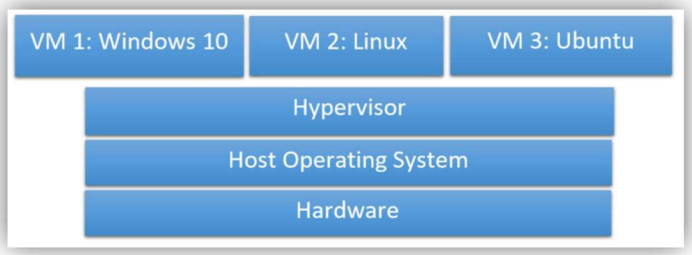
Figura 15 Hipervisor tipo 1



Fonte: "*Disposable Virtual Machines and Challenges to Digital Forensics Investigation"* (Uddin et al., 2021, p. 1)

II. O segundo tipo de hipervisor assenta no sistema operativo e os mais populares são o VMware*, Virtual Box e Parallel Desktop* para *Mac OS*, conforme a Figura 16 (Uddin et al., 2021).

Figura 16- Hipervisor tipo 2



Fonte: "*Disposable Virtual Machines and Challenges to Digital Forensics Investigation"* (Uddin et al., 2021, p. 2)

A *cloud bare metal* fornece um forte isolamento, acesso total e direto ao *hardware* e um desempenho mais previsível. Mas, possui limitações, como fraca escalabilidade, baixa eficiência de custos e pouca adaptabilidade, pois ocorrem porque só podem ser alugados servidores inteiros aos utilizadores e não existe controlo sobre os programas após o servidor ser alugado (Zhang et al., 2020).

Tabela 9- Comparação entre serviços

Serviço	Segurança	Isolamento	Desempenho	Densidade
Nuvem baseada em VM	Ataques side-channel e DoS devido à partilha de recursos	Fraco isolamento devido à partilha de recursos	Sobrecarga de CPU, memória e I/O causada pela virtualização	Densidade muito alta através de sobre provisionamento de servidores
Nuvem bare-metal de inquilino único	Fraca segurança porque um utilizador não confiável tem acesso irrestrito a toda a plataforma	Forte isolamento devido ao acesso exclusivo ao sistema (um ponto discutível devido à fraca segurança)	Desempenho nativo	Densidade muito baixa, um utilizador por servidor, levando a um custo elevado

Fonte: Adaptado de "*High-density multi-tenant bare metal cloud "* (Zhang et al., 2020, p. 2)

O *Chief Information Officer (CIO)* deverá ter uma preocupação ambiental dentro das organizações e a virtualização é uma técnica chave para reduzir o número de máquinas

físicas, economizando recursos e energia. Esta preocupação ambiental é definida como *Green IT,* sendo uma recomendação da União Europeia (UE).

O *Green IT* engloba as boas práticas de TIC, nomeadamente a redução do consumo de energia e a pegada de carbono, incluindo a gestão do lixo eletrónico, preservando o meio ambiente (Landum et al., 2020). Os autores Landum et al. (2020) consideram que a sustentabilidade ambiental assenta em três objetivos: prevenção da poluição, gestão de produtos e tecnologias limpas. Em que as mesmas devem ser aplicadas em três níveis: individual, organizacional e social.

Os sistemas de microserviços facilitam o uso da virtualização e da *cloud computing,* indo de encontro ao respeito pelo *Green IT.*

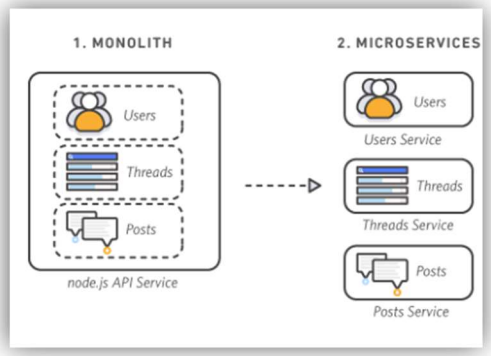
Sistemas monolíticos e sistemas de microserviços representam duas abordagens distintas para a arquitetura de *software*, com características, vantagens e desvantagens distintas.

A arquitetura monolítica já não consegue fazer face às necessidades de escalabilidade, tendo em consideração que a eficiência e a otimização dos recursos humanos e tecnológicos são cruciais. Assim sendo, a arquitetura de microserviços torna-se uma solução, pois é constituída por serviços que operam independentes. Propõe-se a decomposição vertical das aplicações operando em subconjuntos.

Ilustrado na Figura 17 arquitetura monolítica e de microserviços. Na arquitetura monolítica as aplicações fazem parte de um bloco conjunto, em que sempre que se faça uma atualização numa das aplicações, as outras poderão sofrer interrupções.

Na arquitetura de microserviços está decomposto verticalmente, mas sempre que exista a necessidade de realizar uma atualização ou sempre que essa aplicação pare, não interfere com as restantes aplicações.

Figura 17- Divisão monolítico em microserviços



Fonte: “AWS microserviços” (AWS, 2024)

Através da sua decomposição, cada componente pode ser operado e desenvolvido de forma independente, sendo o código de cada componente reutilizável, permitindo aos programadores continuar a criar recursos sem necessitar de reescrever código (AWS, 2024).

Uma organização que administra os seus dados em ambientes de nuvem pode aplicar os *benchmarkings* para otimizar a sua gestão financeira, identificando os microserviços que consomem mais recursos.

A contratação de serviços de *cloud*, a compreensão e a implementação de microserviços, bem como o uso de ferramentas de *benchmarking* como *Bench,* são fundamentais para garantir que os serviços contratados vão de acordo com as necessidades de negócio de uma forma eficaz e eficiente, juntamente com a capacidade de avaliar o desempenho, otimizar custos e gerir o relacionamento com os provedores de nuvem de uma forma proativa.

Os acordos com os provedores de serviço podem ser através de uma política de *Service Level Agreement (SLA)*. *SLA* é um contrato baseado no desempenho, focando-se nos resultados pretendidos definindo o nível de serviço esperado, a duração do contrato e as penalidades ou recompensas financeiras pelo incumprimento do contrato.

1.4.4 Segurança e Privacidade

Num estudo elaborado pela IBM, (2023) entre março de 2022 e março de 2023, num universo de 553 organizações, em 16 países, em 17 setores de atividade distintos, um custo médio de uma violação de dados em 2023 foi de USD 4,45 milhões (4 milhões de euros), um aumento de 2,3% em relação a 2022, conforme tabela 10.

***Tabela 10*- Custo Total de uma Violação de Dados (em milhões de USD)**

Ano	Custo (milhões de USD)
2017	3.62
2018	3,86
2019	3,92
2020	3,86
2021	4,24
2022	4,35
2023	4,45

Fonte: Adaptado de "*Cost of a data breach report"* (IBM, 2023, p. 10)

A tabela 10 relata uma evolução nos custos desde 2017 até 2023, reforçando a importância nos cuidados a ter em termos de segurança, nomeadamente na elaboração de políticas de segurança, *Zero Trust (ZT),* encriptação de dados, monitorização e análise e inclusive auditoria.

A tabela 11, descreve a política de investimentos por parte das organizações, de salientar que através dos dados disponibilizados pela IBM, (2023), 50% das organizações investiu no Planeamento e Testes de Resposta a Incidentes e 46% na formação dos colaboradores.

Tabela 11- Diversidade de áreas onde as organizações estão a investir para melhorar a segurança na *cloud*

Tipo de Investimento	Percentagem de Organizações	Descrição
Planeamento e Testes de Resposta a Incidentes	50	Preparar e testar a capacidade de uma organização de responder a incidentes de segurança.
Formação dos Colaboradores	46	Melhora a conscientização e a capacidade dos funcionários de identificar e responder a ameaças de segurança.
Tecnologias de Deteção e Resposta a Ameaças	38	Ferramentas avançadas para detetar e responder a ameaças, protegendo ambientes na nuvem.
Serviços de Segurança	31	Soluções terceirizadas para monitoramento e gestão contínua da segurança.
Ferramentas de Proteção de Dados	25	Garantir a segurança dos dados armazenados e processados na nuvem.
Seguros de Proteção	18%	Investimentos em seguros de proteção após uma violação.

Fonte: Adaptado de “Cost of a Data Breach Report 2023” (IBM, 2023)

Após uma violação de dados, 51% das organizações planeiam aumentar os investimentos em segurança, o que se pode traduzir numa ausência de preocupação na proteção dos dados, anterior à violação dos mesmos ou ausência de literacia na segurança.

De salientar que 16% das violações de dados começaram com *phishing*, causando um custo médio de 4,76 milhões de dólares e 15% foram devido a roubo de credenciais (justificando os 46% na formação dos colaboradores), tendo um tempo médio para identificar e conter uma violação de dados de 277 dias. A tabela 12, resume, com os pontos considerados mais importantes para o trabalho em questão, o relatório da cibersegurança (2023), ameaças ao ciberespaço de interesse nacional, em 2022/2023.

Tabela 12- Relatório da cibersegurança 2022/2023

Resultado do relatório	Ameaça	Contributo para mitigação da ameaça
Maior risco de aumento dos usos da *Internet* e serviços digitais.	*Ransomware, Phishing*, comprometimento de contas	**Negativo**
Insuficiência na adoção de Políticas de Segurança da Informação.	Todas as ameaças enunciadas em cima	**Negativo**
Maior conhecimento do tema cibersegurança.	Todas as ameaças enunciadas em cima	**Positivo**
Aplicação de algumas medidas nas organizações (Atualização do *software*, palavras-passe seguras)	Comprometimento de contas, *Ransomware, Phishing*	**Positivo**

Fonte: Adaptado de “Cibersegurança em Portugal” (Cibersegurança, 2023)

Da tabela 12, destaca-se a insuficiência na adoção de Políticas de Segurança da Informação, documento crucial para o bom funcionamento de todas as organizações, onde estão descritas as normas para o uso dos dispositivos eletrónicos com recurso à *Internet,* indo de encontro a um outro ponto, também ele negativo, maior risco de aumento dos usos da *Internet* e serviços digitais. Considerando que ambos os pontos estão interligados.

A 19 de julho de 2024, a *Crowdstrike,* com o *Crowdstrike Falcon* que integra todos os aspetos da segurança na nuvem- *CWP, CSPM, CIEM, CDR* e *ASPM,* lançou uma atualização de configuração para os sistemas *Windows*. A atualização da configuração resultou numa falha do sistema *cloud* da *Microsoft* (Crowdstrike, 2024).

No documento da cibersegurança (2023) que elaborou um estudo sobre cibersegurança em Portugal, relativo a 2022, descrevem que Portugal tem mais empresas com Políticas de Segurança das TIC do que a média da União Europeia, mas menos de metade dispõe documentação deste tipo.

O documento em questão, bem como o respeito e as boas práticas, permitem mitigar os riscos, salvaguardando os dados e as informações cruciais para qualquer organização. Nele é descrito algumas práticas, tais como:

- Normas de utilização de contas e palavras-passe;
- Normas de confidencialidade e privacidade das informações;
- Normas de utilização de *hardware, software* informático;
- Normas de cópias de segurança das informações;
- Normas de autorização de acesso aos servidores/ *cloud;*
- Normas de gestão da violação da proteção de dados.

As normas a aplicar pelas organizações são estipuladas pelas próprias e pode divergir de organização para organização, sendo apenas mais uma metodologia para a segurança da informação, ajustadas a outras medidas enunciadas anteriormente.

Um ponto importante que todas as organizações devem ter em consideração é a metodologia de *Zero Trust.*

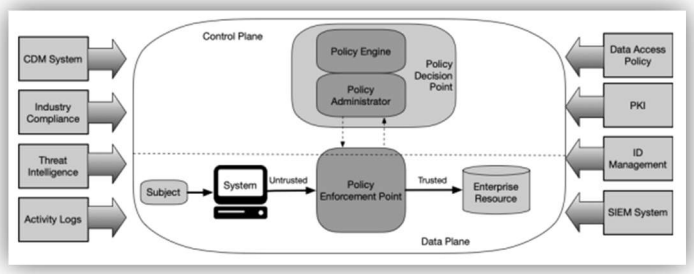
Zero Trust é um conjunto evolutivo de paradigmas de cibersegurança que desloca as defesas dos perímetros estáticos e baseados na rede para se concentrar nos utilizadores, bens e recursos. Realçam que não concede confiança implícita a ativos ou contas dos utilizadores, requerendo autorização e autenticação explícitas de cada instância de acesso ou comunicação de recursos.

A Figura 18 descreve os componentes de arquitetura de segurança *Zero Trust,* dividida em dois planos principais: o Plano de Control (*Control Plane)* e Plano de Dados (*Data Plane).*

Na vertente de Plano de Control, pode-se encontrar a *Policy Engine, Policy Administrator* e *Policy Decision Point.*

A outra vertente, Plano de Dados, está apresentado o *Subject, System, Policy Enforcement Point* e *Enterprise Resource.*

Figura 18- Arquitetura de segurança *Zero Trust*



Fonte: *"Zero Trust Networks"* (NIST, 2024).

A arquitetura *Zero Trust* ilustrada na Figura 18 enfatiza a necessidade de considerar todos os sistemas como não confiáveis até que se prove o contrário. O processo de verificação envolve múltiplos componentes que trabalham em conjunto para garantir que apenas os acessos legítimos sejam permitidos.

Além disso, a integração com sistemas externos permite uma abordagem abrangente e contínua de segurança, garantindo que as políticas estejam sempre atualizadas e que as atividades sejam monitorizadas em tempo real.

A prática de manter o *software* atualizado e usar as corretas credenciais é fundamental para reduzir os riscos. Tendo em consideração que não existe um sistema infalível, mas sim práticas adequadas para mitigar a quebra de segurança.

A segurança da informação bem como a sua privacidade deve ser mantida, para que a mesma seja considerada um recurso valioso, tem de respeitar a integridade, confidencialidade, disponibilidade e acessibilidade.

O artigo elaborado pelos autores Kitsios et al. (2023) aborda como a norma ISO/IEC 27001:2013 deve ser aplicada para melhorar a segurança da informação e gerar valor a partir dos dados. Trata-se de uma norma internacional, que especifica os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI), focando-se em implementar, estabelecer, manter e melhorar continuamente um SGSI.

Ao implementar a ISO 27001, as organizações beneficiam a nível reputacional perante os clientes, pois estes tendem a confiar em organizações certificadas.

Além da ISO/IEC 27001:2013 enunciada por Kitsios et al. (2023), os autores Putra & Soewito, (2023) reconhecem a norma ISO/IEC 27005:2018 e o NIST SP 800-30, em que a ISO 27005:2018 é uma norma que fornece diretrizes para a gestão de riscos de segurança da informação e a NIST SP 800-30 uma avaliação dos riscos, um complemento dessa mesma norma.

Para além das ISO já mencionadas, existe também a ISO/IEC 27002:2013, sendo um código de boas práticas da segurança da informação, ISO/IEC 27002:2022 a respeito dos controlos segurança da informação, cibersegurança e proteção da privacidade e a ISO 31000:2018, em que fornece diretrizes sobre a gestão dos riscos enfrentados pelas organizações, bem como a ISO/IEC 27005:2018 gestão dos riscos de segurança da informação.

1.5 Enquadramento Legal

A Constituição da República Portuguesa, no artigo 35º, ponto 1 descreve, “todos os cidadãos têm o direito de acesso aos dados informatizados que lhe digam respeito…”, no ponto 3 “a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do seu titular,…” e no ponto 4 “ é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.” (Portuguesa, 2005).

A Lei nº 109/2009, de 15 de Setembro, aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

No artigo 3º descreve Falsidade Informática como: “ quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades, juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias” (Assembleia República, 2015).

A lei nº 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança do ciberespaço em Portugal, transpondo a Diretiva (União Europeia) 2016/1148 do Parlamento Europeu e do Conselho.

Representando uma evolução na legislação de cibersegurança em Portugal, indo de acordo com as diretrizes europeias, com alguma abrangência e detalhe com o intuito de estabelecer uma estrutura sólida e eficaz no que toca à proteção do ciberespaço.

O Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) considera o seguinte no ponto 1: "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental.

O artigo 8º, nº 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16º, nº1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito" (UE, 2016).

O Regulamento Geral de Proteção de Dados (RGPD) entrou em vigor no dia 25 de maio de 2018 e a sua adequação à lei portuguesa é realizada pela lei nº 58/2019, de 8 de agosto.

A lei nº 58/2019, de 8 de agosto, apesar de assegurar a execução, na ordem jurídica nacional do Regulamento (EU) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, conforme o artigo 2º, nº 3, a mesma não se aplica aos ficheiros de dados pessoais constituídos e mantidos sob a responsabilidade do Sistema de Informações da República Portuguesa, que se rege por disposições específicas, nos termos da lei (Diário República, 2019).

O RGPD é um conjunto de normas/ regras, para serem aplicadas dentro da União Europeia, abrangendo empresas e cidadãos, assim como empresas que não fazem parte da União Europeia, mas têm transações com empresas ou cidadãos residentes na União Europeia.

A autoridade responsável em Portugal para o cumprimento do RGPD é a Comissão Nacional de Proteção de Dados (CNPD), sendo uma entidade administrativa independente.

O RGPD, secção 4, artigo 37º, designa um encarregado da proteção de dados, do inglês *Data Protection Officer* (DPO), no artigo 38º a sua posição e o artigo 39º as suas funções.

A CNPD aconselha as organizações, de forma atempada, à designação de um DPO, com o intuito de apoiar a transição das mesmas na aplicação do regulamento, dando especial atenção à sua posição dentro da organização, o seu reporte direto ao mais alto nível assim como às suas funções que lhe serão atribuídas, cujo desempenho requer determinadas condições.

Na realização das suas funções, o DPO, deve ter em consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento (artigo 39º).

As organizações têm a obrigação de conservar os dados apenas durante o período e para os fins estritamente necessários (limitação da conservação), devendo o seu prazo ser limitado e comunicado ao titular no ato da sua recolha.

Deve ser mantida a integridade e confidencialidade dos dados a serem tratados, garantindo a sua segurança e proteção contra o tratamento não-autorizado ou ilícito, salvaguardando a sua perda, destruição ou dano acidental, tendo medidas técnicas ou organizativas adequadas (integridade e confidencialidade).

Volume de dados recolhidos, tratamento dos mesmos ou a sua natureza, são fatores relacionados com as medidas técnicas ou organizativas.

O DPO deve salvaguardar e comunicar junto da CNPD qualquer violação dos direitos dos titulares, sendo eles considerados dados sensíveis (responsabilidade).

São considerados dados sensíveis:

- Dados pessoais que revelem a origem racial ou étnica;
- Opiniões políticas;
- Convicções religiosas ou filosóficas;
- Filiação sindical;
- Dados genéticos ou biométricos para identificar uma pessoa;
- Dados relativos à saúde;
- Dados relativos à vida sexual ou orientação sexual (artigo 9º RGPD).

Os seus titulares têm direito à solicitação da eliminação, bem como à sua visualização, sempre que considerarem pertinentes, sendo o seu pedido concedido de imediato e sem quaisquer custos associados (tratamento transparente).

O DPO ao salvaguardar a privacidade, a integridade e a confidencialidade dos titulares dos dados, limita os riscos que a CMB incorre, no sentido do risco operacional, nomeadamente no caso das TIC não estarem adaptadas tendo em consideração às maiores exigências.

O Tribunal de Justiça da União Europeia, em outubro de 2015, numa decisão conhecida como *Schrems I*, determinou que o acordo entre a União Europeia e os Estados Unidos, no que conferia autorização para a partilha de dados de clientes e organizações, foi considerado nulo (União Europeia, 2015), pois não garantia a salvaguarda da segurança da informação dos cidadãos europeus.

A União Europeia e os Estados Unidos, após a decisão do tribunal europeu, negociaram um novo acordo, *The Privacy Shield,* considerado nulo em julho de 2020, ficando conhecido como *Schrems II* (Parliament, 2020)*,* sendo utilizado o mesmo argumento, a não garantia da segurança da informação.

Segundo o documento do tribunal europeu (Parliament, 2020) os programas de vigilância dos Estados Unidos, *PRISM* e *UPSTREAM*, não estariam de acordo com os direitos e com a privacidade dos cidadãos da União Europeia.

Nos dias de hoje, existe a Decisão de execução (UE) 2021/914 da Comissão de 4 de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (Comissão Europeia, 2021).

No espaço europeu a diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) nº 910/2014 e a Diretiva (EU) 2018/1972, e que revoga a Diretiva (UE) 2016/1148 (Diretiva NIS 2) (Europeia, 2022)

Esta diretiva aborda medidas para assegurar um nível elevado e comum de cibersegurança na União Europeia (UE), substituindo a anterior Diretiva NIS, Diretiva (UE) 2016/1148.

2 Objetivos e Metodologia

O presente trabalho pretende analisar os Sistemas de Informação (SI) e as Tecnologias de Informação e Comunicação (TIC) no município da Câmara Municipal do Barreiro, com o objetivo de analisar as práticas instituídas e propor otimizações.

Pretende-se estudar o uso da *cloud computing,* os seus benefícios, a escolha de fornecedor, bem como os entraves para a autarquia.

Entender se a autarquia usa uma arquitetura monolítica ou uma arquitetura de microserviços, bem como, e se, no caso de usar um sistema de microserviços, qual o tipo de virtualização.

A razão para a realização deste trabalho estará relacionada com as imposições legais e as restrições orçamentárias. A CMB, como qualquer outra organização, precisa de se adaptar às mudanças tecnológicas para permanecer eficiente e responder às necessidades dos seus munícipes.

Por fim, as restrições orçamentárias podem limitar as capacidades da Câmara Municipal para implementar mudanças significativas nos seus sistemas de TIC/SI com a necessidade de um estudo aprofundado.

A metodologia subjacente ao trabalho será uma abordagem qualitativa e como estratégia de abordagem incidirá na recolha de dados de forma indutiva, procurando identificar padrões e significados, através de uma forma não estruturada, utilizando técnicas como a entrevista e a análise de documentos (Fortin, 2009).

A metodologia quantitativa também será usada, pois liga-se ao paradigma positivista, ou seja, a realidade é única, pois os factos existem independentemente do investigador (Fortin, 2009). A vertente da metodologia quantitativa, tendo em consideração ao paradigma positivista (realidade é única), emprega-se à vertente dos Sistemas de Informação (SI) e às Tecnologias de Informação e Comunicação (TIC), sendo a metodologia qualitativa, naturalista, ao modo como as mesmas SI e TIC são usadas.

Utilizando métodos qualitativos, irá ser aprofundado neste contexto, capturando a complexidade e a riqueza das interações e relações dentro dele. Proporcionando uma compreensão mais completa do trabalho em questão.

O método qualitativo é particularmente valioso para explorar as perspetivas, experiências e perceções dos indivíduos envolvidos no trabalho.

Enfatizado por Fortin, Côté e Fillion (2009), que destacam a importância da recolha de dados que revelem as visões subjetivas dos participantes. Irá ser necessário entender como as pessoas interpretam e vivenciam um determinado contexto crucial para o trabalho, e a pesquisa qualitativa é uma maneira eficaz de fazer isso.

Quivy & Campenhoudt (2005) apontam que a pesquisa qualitativa permite uma abordagem flexível e adaptável à recolha de dados. Para este trabalho, os detalhes poderão emergir de maneira imprevisível, será preciso estar aberto a ajustar as perguntas e as abordagens à medida que a pesquisa for avançando. Os métodos qualitativos oferecem esta flexibilidade, permitindo explorar a fundo as questões em evolução.

Um trabalho frequentemente envolve uma análise aprofundada de um único caso ou um pequeno número de casos. Os métodos qualitativos permitem uma análise detalhada e minuciosa dos dados recolhidos, tornando possível identificar padrões, tendências e *insights* profundos que podem ser perdidos em abordagens quantitativas. Creswell (2009) destaca que a pesquisa qualitativa é ideal para revelar a complexidade inerente a muitos trabalhos.

A pesquisa qualitativa também pode ser usada para a construção de uma teoria, como sugerido por Creswell (2009). Ao explorar profundamente um trabalho e capturar informações detalhadas, poderá desenvolver-se teorias e *frameworks* que expliquem o fenómeno trabalhado. Será especialmente relevante quando se procurar compreender as dinâmicas internas e as relações dentro do caso específico.

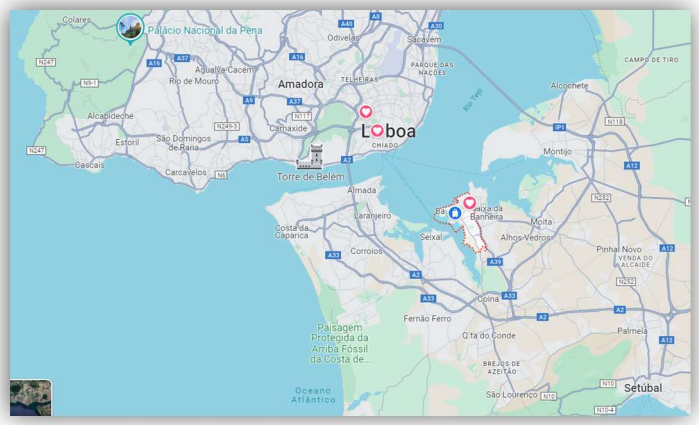
Em resumo, a escolha do método qualitativo para o trabalho é justificada pela ênfase na compreensão do contexto, na exploração das perspetivas dos participantes, na flexibilidade para se adaptar às necessidades da pesquisa, na análise aprofundada e na capacidade de construir uma melhoria. Estas razões são sustentadas pelas contribuições dos autores Creswell, Fortin, Côté, Fillion, Quivy e Campenhout nas suas obras sobre pesquisa qualitativa e métodos de investigação.

3 Caracterização da organização

O Município do Barreiro, situado nos Paços do Concelho, Rua Miguel Bombarda 58, 2830-355 Barreiro, é um dos 308 municípios do território português, sendo que existem 278 municípios no Continente, 19 na Região Autónoma dos Açores e 11 na Região Autónoma da Madeira (Autárquico, 2024).

A Figura 19, representa a área do município do Barreiro, a tracejado vermelho.

Figura 19- Área do Município do Barreiro



Fonte: *Google Maps* (Google, 2024).

Conforme a Figura 19, o município do Barreiro faz parte integrante da área metropolitana de Lisboa, encontra-se na margem sul do rio Tejo, sendo constituído por três uniões de freguesia e uma freguesia, a saber:

- União das freguesias do Alto do Seixalinho, Santo André e Verderena;
- União das freguesias de Barreiro e Lavradio;
- União das freguesias de Palhais e Coina;
- Junta de freguesia de Santo André da Charneca (CMB, 2023).

No artigo 236º, Categorias de autarquias locais e divisão administrativa, da Constituição da República, no ponto 1, refere que: “No continente as autarquias locais são as freguesias, os municípios e as regiões administrativas” e no ponto 2 refere: “As regiões autónomas dos Açores e da Madeira compreendem freguesias e municípios” (Portuguesa, 2005).

O planeamento, a gestão e o investimento são competências da Câmara Municipal do Barreiro, nomeadamente nos seguintes setores:

- Ordenamento do Território e Urbanismo;
- Promoção e Desenvolvimento;
- Cooperação Externa;
- Ação Social;
- Habitação;
- Transportes e Comunicações;
- Equipamento Rural e Urbano;
- Energia;
- Ambiente e Saneamento Básico;
- Saúde;
- Educação;
- Desporto;
- Defesa do Consumidor;
- Proteção Civil;
- Cultura e Património (CMB, 2023)

O seu atual presidente é Frederico Costa Rosa (CMB, 2023).

3.1 Recursos humanos

A tabela 13, mapa de pessoal da Câmara Municipal do Barreiro, descreve o número de colaboradores, bem como as carreiras, cargos e categorias.

Descreve o número de postos de trabalho do mapa de pessoal bem como o número de postos de trabalho ocupados.

Discrimina se é a tempo indeterminado ou a tempo resolutivo.

De referir que a contratação de uma ou mais vagas requer concurso público, não podendo existir contratação direta, como acontece no setor privado.

Tabela 13- Mapa de Pessoal

Cargo/ Carreira/ Categoria	Nº de postos de trabalho do Mapa de Pessoal		Nº de postos de trabalho ocupados	
	Tempo indeterminado	Tempo resolutivo	Tempo indeterminado	Tempo resolutivo
Diretor de Departamento	2	0	2	0
Chefe de Divisão	16	0	16	0
Dirigente Intermédio de 3º Grau	2	0	2	0
Coordenador Municipal de Proteção Civil	1	0	1	0
Técnico Superior	169	9	127	7
Coordenador Técnico	15	0	10	0
Assistente Técnico	155	0	136	0
Encarregado Geral	1	0	0	0
Encarregado Operacional	32	0	31	0
Assistente Operacional	443	49	392	49
Docente	1	0	1	0
Especialista de Informática	4	0	3	0
Técnico de Informática	6	0	4	0
Fiscal Municipal	11	0	9	0
Mestre de Tráfego Fluvial	2	0	2	0
Marinheiro de Tráfego Fluvial	6	0	0	0
Chefe de Armazém	1	0	1	0
Fiscal de Higiene Municipal	3	0	3	0
Total	870	58	740	56

Fonte: Adaptado do site da Câmara Municipal do Barreiro (CMB, 2023)

Após análise da tabela 13 e tendo em consideração às colunas de Nº de Postos de Trabalho do Mapa de Pessoal e Nº de postos de trabalho Ocupados, existe uma discrepância de 130 colaboradores a tempo indeterminado e 2 a termo resolutivo.

A contratação a um cargo público deve ter em conta a legislação aplicável, nomeadamente pelas disposições constantes da Lei Geral do Trabalho em Funções Públicas, aprovada em

anexo à lei nº 35/2014, de 20 de junho, na atual redação, e pela Portaria nº 233/2022, de 9 de setembro.

A Divisão de Informática e Transição Digital da Câmara Municipal do Barreiro conta com sete colaboradores: três especialistas de informática e quatro técnicos de informática, tendo como chefe de divisão o doutor Manuel Landum.

3.2 Caracterização dos SI/ TIC

Neste ponto será enunciado a caracterização dos SI/TIC da Câmara Municipal do Barreiro.

Será abordado a virtualização e servidores, *datacenters* e *cloud,* segurança, bem como as necessidades e desafios tecnológicos. Entender as motivações para a migração para a *cloud,* a sua estratégia e compreender as melhorias operacionais.

3.2.1 Virtualização e Servidores

A comunicação entre os vários edifícios da câmara é realizada através de *Multiprotocol Label Switching* (MPLS) e de *Virtual Private Network (VPN)* do operador. Acedidos virtualmente, existem cerca de 7 servidores físicos e cerca de 100 servidores virtuais. Sendo maioritariamente em *Capex.*

MPLS é uma rede com um conjunto finito de *routers* e interfaces que define como os pacotes devem ser encaminhados, em caminhos curtos (identificando links virtuais), substituindo os endereços de rede longos (Duijn et al., 2022).

O autor Winter (2011) descreve MPLS como uma tecnologia de comutação de rótulos que encaminha pacotes de dados através de redes utilizando rótulos em vez de *Internet Protocol* (IP) tradicionais. No mesmo documento, o autor refere que existem três operações principais associadas aos rótulos de MPLS, a saber:

- *Label Swapping:* Substitui o rótulo atual por outro novo;
- *Label Pushnig:* Adiciona um novo rótulo no topo de rótulos;
- *Label Popping:* Remove o rótulo do topo da pilha.

O MPLS foi projetado para ser compatível com diversas tecnologias para redes óticas, demonstrando desta forma versatilidade e capacidade de evolução (Winter, 2011).

O processo de virtualização implementado pela autarquia do Barreiro, proporcionou a troca de cerca de 400 computadores físicos, por *thin clientes.* Esta implementação permite uma poupança de 65 mil euros anuais em energia elétrica. Este projeto proporciona simultaneamente um bom alinhamento com o Green *IT,* reduzindo desta forma as emissões de CO2 para a atmosfera, entre outras vantagens.

Está também alinhado com o regulamento da EU que estabelece uma estrutura de medidas para fortalecer o ecossistema de fabrico de produtos de tecnologia net-zero da Europa, também conhecido como *Net-Zero Industry Act`(NZIA)* (Council, 2024).

A Câmara Municipal do Barreiro adquiriu em sistema de *aaS* um *Security Operation Center (SOC)* de modo a proteger a sua infraestrutura, monitorizando em tempo real milhares de *log`s* e tem ainda implementado *Security Information and Event Management (SIEM)* utilizando inteligência artificial.

Os autores Vitorino et al. (2023) consideram que é importante que as organizações tenham em atenção à forma como realizam a Deteção de Intrusão de Rede (NID[1]), sendo a Inteligência Artificial um recurso extremamente valioso, pois reconhecem padrões e anomalias nos fluxos de tráfego de rede até à classificação de ciberataques complexos.

O uso pela autarquia do *SIEM* é muito importante, pois conforme descrito pelos autores Rikhtechi et al. (2021), o *SIEM* armazena e monitoriza eventos no *software* e o acesso não autorizado aos registos, provocando ameaças à segurança, como a fuga de informações e a violação da confidencialidade.

Ao ser detetado o acesso não autorizado a um servidor, o mesmo é automaticamente bloqueado, protegendo as informações nele contidas pela autarquia. Cada aplicação tem um ou mais administradores e em alguns casos só é permitido a leitura dos documentos, não podendo fazer alterações.

A monitorização dos servidores por parte da autarquia através do SOC e do SIEM, vai de acordo com a política de *Zero Trust.*

3.2.2 Datacenters / *Cloud Computing*

No relatório Intelligence (2024), em que o mesmo se foca na análise das causas, custos e consequências das falhas que ocorrem em *datacenters,* tendo identificado como principais a

[1] No inglês Network Intrusion Detection.

energia e a rede como as causas mais comuns de falhas graves, refletindo a importância de manter os sistemas robustos.

A Câmara Municipal do Barreiro tem *datacenters* próprios à técnica de virtualização, com *backups* encriptados utilizando *IaaS*, situados em Lisboa e que replica para o Porto, favorecendo a redundância e a latência. Mantendo toda a informação diária nos servidores localizados na câmara.

Ao manter *backups* em *datacenters* com 314 Km de distância um do outro, mantem as infraestruturas independentes de energia e refrigeração, estando toda a informação pertinente da câmara protegida no caso de uma região sofra uma interrupção causada pela perda de energia ou desastres naturais. De salientar que as regiões são selecionadas usando critérios de avaliação de risco.

A elaboração de um contrato para a utilização da *cloud computing* por parte da câmara tem de se reger por regras, a contratação deste tipo de serviço é diferente do setor privado, em que estes podem contratualizar os serviços com os operadores que considerarem pertinentes.

No caso do setor público podem contratar diretamente os serviços até um valor de 20 mil euros. De 20 mil euros até aos 75 mil tem de existir uma consulta com um mínimo de 3 empresas, acima dos 75 mil terá de ser realizado um concurso público.

A Câmara Municipal do Barreiro utiliza *cloud* nos serviços de Desporto e Associativismo e Educação, Gestão Escolar e *Call Center*, com utilização de *PaaS* do operador ou fornecedor. Sendo celebrado um contrato com o operador ou fornecedor com enquadramento com o RGPD. Dos produtos ou aplicações que estão na *cloud* do operador ou fornecedor, não se reconhecem quaisquer constrangimentos.

A 19 de julho de 2024, devido ao problema pela *Crowdstrike,* o *Call Center* da câmara sofreu perturbações e como reconhecido, uma perturbação alheia à câmara.

Os dados recolhidos pelo operador, através dos departamentos de Desporto e Associativismo e Educação e Gestão Escolar são considerados sensíveis. A confidencialidade, a disponibilidade e a integridade devem ser respeitadas ao abrigo do RGPD, reconhecido pela Câmara Municipal do Barreiro, respeitando desta forma os colaboradores, fornecedores e pelos cidadãos do município do Barreiro.

3.2.3 Segurança

As credenciais de acesso por parte dos colaboradores são compostas por um mínimo de 9 dígitos, com exceção da administração e do departamento de TIC em que as mesmas são compostas por um mínimo de 13 dígitos, sendo regra geral a alteração efetuada em curtos

períodos e cumprindo uma série de regras implementadas e aprovadas pela autarquia, aumentando deste modo os requisitos de segurança.

Outra medida implementada é a autenticação de dois fatores (2FA), é uma segurança adicional para a gestão de identidade, requerendo duas formas de autenticação (Security, 2024). O roubo ou comprometimento de credenciais foi identificado como o vetor de ataque inicial em 15% das violações de dados analisadas, sendo a segunda forma mais comum de ataque (IBM, 2023).

Segundo a Microsoft (2024) os benefícios de dupla autenticação são enormes, pois os colaboradores não necessitam de transferir um gerador de *tokens,* sendo apenas necessário um dispositivo móvel. No caso da autarquia, não é permitido a utilização de dispositivos móveis pessoais, apenas os da câmara.

Com o intuito de salvaguardar a segurança dos dados e proteger o uso das credenciais por parte de colaboradores, os computadores entram em inatividade, sempre que os utilizadores deixam de estar a utilizar os mesmos e inadvertidamente não os bloqueiam, como regra de higiene de segurança. É uma medida fortemente trabalhada e constantemente reforçada pela divisão de informática, ou seja, solicita-se a todos os colaboradores da câmara que sempre que exista a necessidade de abandonar o seu posto de trabalho que suspendam os computadores.

Desta forma, para além de proteger os interesses da autarquia a nível de segurança de roubo de dados, acesso a aplicações, instalação de *software* malicioso ou mesmo a utilização de uma *pendrive* contendo vírus, pois todo o sistema fica vulnerável, os colaboradores protegem-se de um ato malicioso por parte de um colega de trabalho mal-intencionado ou mesmo de quem tenha acesso à zona em questão.

Tendo em atenção às credenciais dos colaboradores, a autarquia elaborou uma política de segurança em que os departamentos devem participar e em especial aos recursos humanos, a saída de todos os colaboradores, no prazo máximo de 3 dias, a fim da divisão de informática eliminar as autorizações dadas aos mesmos, sendo enviado a toda a cadeia hierárquica. Desta forma, elimina-se a hipótese de no caso de uma saída menos amigável, a possibilidade de transmissão dos dados de acesso.

As políticas de segurança da autarquia são aprovadas pela câmara a fim, sendo depois publicadas em atas, transformando-se em documento interno a ser seguido em todos os edifícios da câmara, independentemente do departamento.

O tema da segurança e cibersegurança está alinhado com a ISO/ IEC 27001:2013 segurança da informação, ISO/IEC 27005:2018 diretrizes para a gestão dos riscos de segurança da

informação, ISO/ IEC 27002: 2013 código de boas práticas da segurança da informação, decreto regulamentar 41/2018que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais, assim como com o DL 65/2021 e a NIS 2.

A NIS2 define os requisitos de segurança cibernética na União Europeia, sendo de carácter obrigatória, prevendo-se a sua transposição até 17 de outubro de 2024 (Siemens, 2024).

3.3 Necessidades e Desafios Tecnológicos

O autor De Lauretis (2019), descreve microserviços como uma técnica para o desenvolvimento de aplicações de *software*, permitindo estruturar uma aplicação baseada em serviços como uma coleção de pequenos serviços de *software*. Salientando ainda que a arquitetura pode ser vista como um novo paradigma para a programação de aplicações através da composição de pequenos serviços, em que cada um pode executar os seus próprios processos, comunicando através de mecanismos leves.

A autarquia do Barreiro, considerou ser pertinente ter uma arquitetura em microserviços, desta forma poderá mais facilmente adotar e atualizar as suas diversas aplicações individualmente, conforme as suas necessidades, sem prejudicar o funcionamento das restantes.

Adotando desta forma a virtualização com hipervisor tipo 1, *Bare Metal* da *Microsoft Hiper-V.*

O hipervisor tipo 1, gere diretamente os recursos de *hardware,* controlando as máquinas virtuais que são executadas.

É de realçar que a fibra ótica da autarquia tem uma velocidade de 1*Gigabit* a nível interno dos edifícios e nos *links* entre os mesmos é de 10 *Gigabits*.

3.4 Motivações para Adoção da *Cloud*

A autarquia considerou pertinente a migração para a nuvem com o intuito da redução do *Capex*, evitando desta forma altos investimentos iniciais em *hardware* e *software,* aquando da migração dos departamentos enunciados anteriormente (ponto 3.2.2), substituindo-os por *Opex*.

A migração para a nuvem, evitou que a autarquia tivesse de investir em mais recursos humanos, pois o *know how* da manutenção e segurança estaria do lado do fornecedor.

A autarquia pretendia com a migração para a *cloud* redução de custos, aumento da escalabilidade, melhoria da segurança e inovação tecnológica.

3.4.1 Estratégia de Migração

A autarquia elaborou uma estratégia em que foram considerados todos os fatores de risco de segurança e de operacionalidade, nomeadamente:

- Avaliação dos recursos e capacidades das aplicações, criando uma lista das aplicações, dos colaboradores que irão trabalhar nas mesmas e a sua frequência;
- Determinou-se as aplicações qualificadas e especificado os requisitos de segurança e conformidade;
- Identificação dos recursos de cargas de trabalho a migrar, entre outros.

A arquitetura de microserviços teve um impacto bastante positivo na elaboração da estratégia por parte da Divisão de Informática e Transição Digital.

3.4.2 Planeamento e Etapas

Após a escolha do fornecedor e da estratégia de migração, a autarquia confiou a migração por parte do fornecedor. Toda a migração foi realizada durante a noite aquando da paragem dos serviços, estando completamente operacional no dia seguinte pela manhã. Não se conhecendo quaisquer complicações.

3.4.3 Escolha de Serviços

Conforme descrito no ponto 3.2.2, a escolha de serviços e de fornecedor ou operador decorre de forma distinta do setor privado. Sendo necessário consulta pública e sempre tendo em consideração os valores em causa.

A operação de migração para a *cloud* ocorreu no ano de 2019.

3.4.4 Desafios Durante a Implementação

Foi realizada uma análise detalhada das aplicações antes da migração para identificação de incompatibilidades, desta forma a sincronização de dados entre sistemas e a *cloud* não foi complexa nem levantou questões de latência, tendo em consideração ao estudo prévio.

3.4.5 Melhorias Operacionais

Os *sites* da autarquia estão atualmente na *cloud,* proporcionando maior escalabilidade, segurança e disponibilidade. De modo a distribuir o tráfego nos seus 20 servidores, tendo em consideração o seu volume, é usado Load *Balancer.*

Load Balancer permite em caso de um servidor ter muito tráfego, redirecionar ou equilibrar o tráfego para um outro servidor com dados replicados, direcionando e controlando o tráfego da *Internet* entre os respetivos servidores das aplicações e os munícipes (Amazon, 2023).

A autarquia para manter os seus níveis de segurança elevados e com a preocupação com os dados dos seus munícipes, elabora *pentests* anuais a todo o seu domínio, verificando qual o seu grau de vulnerabilidade de segurança, comunicando com o fornecedor os resultados obtidos sempre que se justifique.

Na procura da melhoria operacional, a autarquia utiliza inteligência artificial, perspetivando a utilização de *machine learning* num futuro.

Conclusões e Perspetivas de Trabalho Futuro

A elaboração do presente trabalho, permitiu uma compreensão sobre a *cloud computing,* nomeadamente os seus desafios, características e benefícios, bem como às questões propostas.

A autarquia em estudo, optou pelo uso de *datacenters* próprios em duas regiões, Lisboa que replica para o Porto, em conjunto com a *cloud* pública a nível de armazenamento dos seus dados em regime de *backups* e dos sites da autarquia, usando *Load Balancer*.

Com o regime de *backups* da *cloud computing*, a CMB paga pela capacidade de armazenamento, podendo controlar os seus custos.

Comprovando-se a confiança depositada a nível da segurança, bem como na redução de custos em colaboradores especializados, optando pela arquitetura de virtualização em microserviços, com hipervisor tipo 1, *Bare Metal* da *Microsoft Hiper-V*, indo de encontro ao *Green IT*.

A CMB tem uma política de *Zero Trust*, tendo implementado autenticação de dois fatores, um SOC para monitorizar em tempo real milhares de *Log`s* e um SIEM. Estando alinhada com o regulamento da EU conhecido como *Net-Zero Industry Act`.*

Por questões de confidencialidade inerentes à atividade da organização em estudo, não foi possível apresentar determinado nível de detalhe.

Como perspetivas de trabalho futuro sugere-se a cooperação entre autarquias na utilização de *cloud* comunitária, dada a dificuldade na contratação de um fornecedor de serviço. A transversalidade da problemática em estudo tem impactos em todas as câmaras municipais podendo constituir valor acrescentado a utilização de *cloud* comunitária, partilhando os custos da infraestrutura e potenciando a colaboração entre os diversos municípios.

Uma outra vertente considerada uma mais-valia subjacente à partilha poderá ser a salvaguarda dos dados, tanto de ataques com origem criminosa ou de catástrofe natural por

forças da natureza, criando no mínimo três regiões para *backups,* nomeadamente em Lisboa, Porto e Algarve, tendo sempre em consideração a salvaguarda da baixa latência.

Referências

Abdulle, A., Ali, A., & Abdullah, R. (2022). Cost-benefit analysis of public cloud versus in-house computing. *International journal of engineering trends and technology*. https://doi.org/https://doi.org/10.14445/22315381/IJETT-V70I6P231

Aldahwan, N., & Ramzan, M. (2022). Hindawi- Scientific Programming. *Descriptive literature review and classification of community cloud computing research*. https://doi.org/https://doi.org/10.1155/2022/8194140

Amazon, A. (2023). *What is Load Balancing?* Amazon AWS: https://aws.amazon.com/what-is/load-balancing/

Assembleia República. (2015). *Lei nº 109/2009, de 15 de Setembro*. Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693

Autárquico, P. (2024). *Portal Autárquico*. Portal Autárquico: https://portalautarquico.dgal.gov.pt/pt-PT/administracao-local/entidades-autarquicas/municipios/

AWS. (2024). *Manual do usuário Amazon Virtual Private Cloud.* AWS: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/vpc-ug.pdf#vpc-network-acls

AWS. (2024). *Microserviços*. AWS: https://aws.amazon.com/pt/microservices/

AWS. (2024). *O que é a latência de rede?* Amazon AWS: https://aws.amazon.com/pt/what-is/latency/

Barreiro, C. (2023). *Mapa de pessoal*. Câmara Municipal Barreiro: https://www.cm-barreiro.pt/municipio/recursos-humanos/mapa-de-pessoal/

Barreiro, C. (2023). *Presidente*. Câmara municipal Barreiro: https://www.cm-barreiro.pt/municipio/camara-municipal-do-barreiro/presidente/

Bartock, M., Dodson, D., Souppaya, M., Carroll, D., Masten, R., Scinta, G., Massis, P., Prafullchandra, H., Malnar, J., Singh, H., Ghandi, R., Storey, L., Yeluri, R., Shea, T.,

Dalton, M., Weber, R., Scarfone, K., Dukes, A., Haskins, J., Phoenix, C., & Swarts, B. (2022). NIST special publication 1800-19. *Trusted Cloud: security practice guide for VMware hybrid cloud infrastructure as a service (IaaS) environments*. https://doi.org/https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-19.pdf

Bello, S., Oyedele, L., Akinade, O., Bilal, M., Delgado, J., Akanbi, L., Ajayi, A., & Owolabi, H. (2021). Automation in construction. *Cloud computing in construction industry: Use cases, benefits and challenges*. https://doi.org/https://doi.org/10.1016/j.autcon.2020.103441

Cibersegurança, O. d. (2023). *Cibersegurança em Portugal.* https://www.cncs.gov.pt/docs/rel-sociedade2023-observ-cncs-dig.pdf

CISCO. (2016). *MPLS FAQ for beginners*. CISCO: https://www.cisco.com/c/pt_br/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html

CMB. (2015). *As armas municipais do Barreiro.* Barreiro- Memória e Futuro: http://memoriaefuturo.cm-barreiro.pt/arq/fich/Hera__769_Idica_Municipal.pdf

CMB. (2023). *Município*. Barreiro Câmara Municipal: https://www.cm-barreiro.pt/municipio/

Comissão Europeia. (2021). *Decisão de execução (UE) 2021/914 da Comissão de 4 de junho de 2021.* Jornal oficial da União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021D0914

Council, E. (2024). *Net-zero industry act: council and parliament strike a deal to boost EU`S green industry*. European Council: https://www.consilium.europa.eu/en/press/press-releases/2024/02/06/net-zero-industry-act-council-and-parliament-strike-a-deal-to-boost-eu-s-green-industry/

Creswell, J. (2009). *Research design: qualitative, quantitative, and mixed approaches.* https://doi.org/978-1-4129-6557-6

Crowdstrike. (2024). *Remediation and guidance hub: falcon content update for windows hosts*. Crowdstrike: https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

Crowdstrike. (2024). *Technical details: Falcon content update for windows hosts*. Crowdstrike blog: https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/

De Lauretis, L. (2019). From monolithic architecture to microservices architecture. *2019 IEEE International symposium on software reliability engineering workshops (ISSREW).* https://doi.org/10.1109/ISSREW.2019.00050

Diário República. (2019). *Lei nº 58/2019, de 8 de agosto.* Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Dubey, K., Shams, M., Sharma, S., Alarifi, A., Amoon, M., & Nasr, A. (2019). IEEE Xplore. *A Management System for Servicing Multi-Organizations on Community Cloud Model in Secure Cloud Environment*. https://doi.org/10.1109/ACCESS.2019.2950110

Duijn, I., Jensen, P., Jensen, J., Beck, T., Madsen, J., Schmid, S., Srba, J., & Thorgersen, M. (2022). IEEE/ACM Transactions on Networking. *Automata- Theoretic Approach to Verification of MPLS Networks Under link Failures*. https://doi.org/https://doi.org/10.1109/TNET.2021.3126572

Europeia, U. (2022). *Directive (EU) 2022/2555 of the european parliament and the council of 14 december 2022*. Official journal of the european union: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

Fortin, M.-F. (2009). *Fundamentos e etapas do processo de investigação.* https://doi.org/9789898075185

Gartner. (2024). https://www.gartner.com/en/information-technology/glossary/community-cloud

Google. (2024). *Google Maps*. Google: https://www.google.pt/maps/@38.5730072,-9.1673309,10.5z?hl=pt-PT&entry=ttu

IBM. (2023). *Cost of data breach report.* https://www.ibm.com/downloads/cas/E3G5JMBP

Intelligence, U. (2024). *Annual outage analysis 2024.* https://uptimeinstitute.com/uptime_assets/2564c126499732e5fb721dd333bc7daade3c4f6dff9875b2763a3051578518bf-GA-2024-03-annual-outage-analysis-2024.pdf

Islam, R., Patamsetti, V., Gadhi, A., Gondu, R., Bandaru, C., Kesani, S., & Abiona, O. (2023). Scientific research Publishing. *The future of cloud computing benefits and challenges*. https://doi.org/https://doi.org/10.4236/ijcns.2023.164004

Kaspersky. (2024). *O que é endereço IP e como proteger o seu?* Kaspersky: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability*. https://doi.org/https://doi.org/10.3390/su15075828

Landum, M., Reis, L., & Moura, M. (2020). 15 th Iberian conference on information systems and technologues (CISTI). *Boas práticas de TIC em alinhamento com o Green IT*. https://doi.org/10.23919/CISTI49556.2020.9141166

Mell, P., & Grance, T. (2011). National Institute of Standards and Techonology. *The NIST definition of cloud computing*. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Microsoft. (2024). *Azure*. O que é uma VM (Máquina Virtual): https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-a-virtual-machine

Microsoft. (2024). *Microsoft*. Rede de cloud híbrida: https://learn.microsoft.com/pt-pt/training/modules/intro-to-azure-hybrid-services/3-hybrid-cloud-networking

Miyachi, C. (2018). *Column: focus on community.* What is cloud? It is time to update the NIST definition?: https://ieeexplore.ieee.org/ielx7/6509491/8383643/08383652.pdf

Muhic, M., Bengtsson, L., & Holmstrom, J. (2023). Barries to continuance use of cloud computing: Evidence from two case studies. *Information & Mangement*. https://doi.org/https://doi.org/10.1016/j.im.2023.103792

NIST. (2024). *NIST*. Community Cloud: https://csrc.nist.gov/glossary/term/community_cloud

NIST. (2024). *Zero Trust Networks*. NIST: https://www.nist.gov/programs-projects/zero-trust-networks

Pallathadka, H., Sajja, G., Phasinam, K., Ritonga, M., Naved, M., Bansal, R., & Choquecota, J. (2022). An investigation of various appliactions and related challenges in cloud computing. *Materials Today: proceeding*. https://doi.org/https://doi.org/10.1016/j.matpr.2021.11.383

Pallathadka, H., Sekhar Sajja, G., Phasinam, K., Ritonga, M., Naved, M., Bansal, R., & Quiñonez-Choquecota, J. (2022). An investigation of various applications and related challenges in cloud computing. *Materials Today: Proceedings*. https://doi.org/https://doi.org/10.1016/j.matpr.2021.11.383

Parliament, E. (2020). *The CJEU judgment in the Schrems II case.* European Parlament: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

Portuguesa, C. d. (2005). *Constituição da República Portuguesa*. Página oficial da Assembleia da República: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

Putra, A., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International of Advanced Computer Science and Applications*. https://doi.org/10.14569/IJACSA.2023.0140468

Quivy, R., & Campenhoudt, L. (2005). *Manual de investigação em ciências sociais.* https://doi.org/233090/2005

Raeber, R. (2009). *CISCO vmware.* VBlock Architecture Accelerating Deployment of the Private Cloud: https://www.cisco.com/c/dam/global/en_dz/assets/expoegypt2010/assets/docs/vblock_architecture_rene_raeber.pdf

República, A. d. (2005). *Constituição da República Portuguesa*. Assembleia da República: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

Rikhtechi, L., Rafe, V., & Rezakhani, A. (2021). Journal of information systems and telecommunication. *Secured access control in security information and event management systems*. https://doi.org/https://doi.org/10.52547/jist.9.33.67

Security, M. (2024). *O que é a autenticação de dois fatores*. Microsoft security: https://www.microsoft.com/pt-pt/security/business/security-101/what-is-two-factor-authentication-2fa

Shilpashree, S., Patil, R., & C., P. (2018). Cloud computing an overview. *International Journal of Engineering & Technology*, 1. https://doi.org/10.14419/ijet.v7i4.10904

Siemens. (2024). *Segurança cibernética: conformidade com NIS2*. Siemens: https://www.siemens-advanta.com/capabilities/offers/nis2-compliance?gclid=CjwKCAjwoJa2BhBPEiwA0l0ImJDkvwBu8FJN0g6Guw4D9P3O4JHFyRkqhg6_RSzq4V2LfryZrFFYxRoCeYwQAvD_BwE&acz=1&gad_source=1

Tavbulatov, Z., Zhigalov, S., & Patrusova, A. (2020). Types of cloud deployment. *Journal of Physics: Conference Series*. https://doi.org/10.1088/1742-6596/1582/1/012085

Technologies, D. (2024). *Dell Tecnologies*. Dell OpenManage Systems Management Overview Guide Version 8.0: https://www.dell.com/support/manuals/pt-pt/dell-opnmang-sw-

v8.2/smog_6.0-v3/dell-active-system-manager?guid=guid-ac50107a-b033-44cc-a9c8-84b1abfd1090&lang=en-us

Uddin, M., Ahmad, S., & Afzal, M. (2021). Disposable Virtual and Challenges to Digital Forensics Investigation. *International Journal of Advanced Computer Science and Applications*. https://doi.org/10.14569/IJACSA.2021.0120299

UE. (2016). *Regulamento (UE) 2016/679 do parlamento Europeu e do Conselho de 27 de abril de 2016.* Jornal Oficial da União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

União Europeia. (2015). *Court of Justice of the European Union.* Press and Information: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

Vitorino, J., Praça, I., & Maia, E. (2023). Computers & Security. *SoK: Realistic adversarial attacks for intelligent network intrusion detection*. https://doi.org/https://doi.org/10.1016/j.cose.2023.103433

Vmware. (2024). *What is a bare metal hipervisor*. Vmware: https://www.vmware.com/topics/glossary/content/bare-metal-hypervisor.html

Winter, R. (2011). IETF Standards Update. *The coming of age of MPLS*. https://doi.org/https://dx.doi.org/10.1109/MCOM.2011.5741150

Wright, G., & Gillis, A. (2021). *Side-chanel attack*. TechTarget: https://www.techtarget.com/searchsecurity/definition/side-channel-attack

Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., Parchure, A., & Luzcando, E. (2022). IEEE Transactions on smart grid. *Practical adoption of cloud computing in power systems- drivers, challenges, guidance, and real-world use cases*. https://doi.org/10.1109/TSG.2022.3148978

Zhang, X., Zheng, X., & Wang, Z. (2020). High-density multi-tenant bare-metal cloud. *ASPLOS`20: Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems.* https://doi.org/https://doi.org/10.1145/3373376.3378507

Zhou, J., Wang, T., Cong, P., Lu, P., Wei, T., & Chen, M. (2019). Journal of Systems Architecture. *Cost and makespan-aware workflow scheduling in hybrid clouds*. https://doi.org/https://doi.org/10.1016/j.sysarc.2019.08.004