ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M

MESTRADO
ENGENHARIA INFORMÁTICA

A arquitetura TI e o seu papel na configuração e manutenção do ambiente IT: um caso prático

José Alves
João Paulo Magalhães

04/2018

José Alves; João Paulo Magalhães. A arquitetura TI e o seu papel na configuração e manutenção do ambiente IT: um caso prático

04/2018

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M

MESTRADO
ENGENHARIA INFORMÁTICA

A arquitetura TI e o seu papel na configuração e manutenção do ambiente IT: um caso prático
José Alves
João Paulo Magalhães

Agradecimentos

A realização desta dissertação só foi possível devido à contribuição e compreensão de várias pessoas que fazem parte da minha vida. Quero assim agradecer a todos os que de alguma forma permitiram a conclusão desta etapa.

Agradeço do fundo do coração e dedico este trabalho à minha esposa Maria do Carmo, à minha filhota Diana e ao meu filhote Tiago, por todo o apoio e paciência durante todo o percurso académico e que me foram "perdoando" as minhas longas horas de ausência.

Agradeço de forma muito especial ao Professor Doutor João Paulo Magalhães, que na primeira aula me surpreendeu ao fazer questão de me apresentar aos colegas, tendo em conta que eu era um elemento novo na ESTG. Agradeço também o facto de ter aceite ser meu orientador o qual me transmitiu entusiasmo, confiança e incentivo, permitindo o alcance dos objetivos propostos. Muito obrigado por ser assim.

Agradeço a todos os professores que me transmitiram conhecimento e me permitiram alcançar novas perspetivas e formas de encarar desafios e oportunidades.

Aos meus colegas de curso, quero também expressar o meu agradecimento pelo companheirismo, apoio e amizade.

Agradeço também ao Miguel Freitas pelo voto de confiança que permitiu o desenvolvimento prático deste projeto em ambiente organizacional.

Não poderia deixar de referir o meu agradecimento a todos os elementos da empresa onde exerço a minha atividade laboral, por toda a flexibilidade e compreensão demonstrada, o que me permitiu conciliar os deveres académicos com os deveres laborais.

Resumo

Os negócios das organizações vão crescendo, o papel das tecnologias de informação para suportar esses negócios também. Em muitos casos a evolução das TI vai-se fazendo de forma *ad-hoc* condicionando o crescimento do negócio ou criando desperdício tecnológico. A arquitetura de TI e a existência de um perfil de arquiteto de TI contribui para um melhor alinhamento entre as TI e o negócio.

Partindo de um desafio real, neste trabalho constatamos esta realidade. As equipas de gestão reconhecem a necessidade de evoluir, mas não se sentem capazes de decidir sobre a infraestrutura mais adequada às suas necessidades atuais e futuras, nem dispõem de perfis de arquitetos de TI para o efeito. Neste âmbito, este trabalho incide sobre uma estratégia e criação de um conjunto de referências e etapas para renovação tecnológica das organizações considerando as suas reais necessidades de TI. A criação de um manual de referência, permitirá a sensibilização da estrutura de gestão para o problema. O manual de referência contempla os procedimentos para fazer uma análise da situação de TI atual, alinhar essa análise com o negócio e a definição de planos de otimização e evolução tecnológica. Neste trabalho é apresentado a sua aplicação a um caso real.

Palavras-Chave: Arquitetura de TI; *Design*; Metodologia; Frameworks; Virtualização.

Abstract

The business of enterprises are growing, the role of information technology to support these businesses as well. In many cases, the IT evolution it´s taking place by ad-hoc, conditioning the growth of the business or creating technological waste. An IT architecture and the existence of an IT architect profile contribute to a better alignment between IT and business.

Starting from a real challenge, in this work we verify this reality. Management teams recognize the need for evolution, but do not feel able to decide on a more appropriate infrastructure such as their current and future needs, nor do they have IT architects profiles for that purpose. In this process, the work focuses on a strategy and creation of a set of references and steps for technological renovation on organizations considering their real IT needs. The creation of a reference manual, a perception of the management structure for the problem. The reference manual includes procedures to make an analysis of the current IT situation, align this analysis with the business and a definition of optimization plans and technological evolution. In this work, we present the application of this to a real case.

Keywords: IT Architecture; Design; Methodology; Frameworks; Virtualization.

Índice

Lista de Figuras

Lista de Quadros

Lista de Abreviaturas

BC – Business Continuity

BCDR – Business Continuity and Disaster Recovery

CAPEX – Capital Expenditure

CBT – Change Block Tracking

CEO – Chief Executive Officer

CIO – Chief Information Officer

CISO – Chief Information Security Officer

CNA – Converged NetWork Adapter

CTO – Chief Technology Officer

DAS – Direct-Attached Storage

DLP – Data Loss Prevention

DMZ – Demilitarized Zone

DR – Disaster Recovery

FC – Fibre Channel

HBA – Host Bus Adapter

I/O – Input/Output

IOPS – Operações de Input/Output por segundo

IP – Internet Protocol

IPS – Intrusion Prevention System

(i)SCSI – (Internet) Small Computer System Interface

LAN – Local Area Network

LUN – Logical Unit Number

MAC – Media Access Control

M2M – Machine to Machine

NAS – Network Attached Storage

NIC – Network Interface Card

OLTP – OnLine Transaction Processing

OPEX – Operational Expenditure

P2V – Physical-to-Virtual

V2V – Virtual-to-Virtual

PaaS – Platform-as-a-Service

RAID – Redundant Array Independent Disks

ROI – Return On Investment

RPO – Recover Point Objective

RTO – Recover Time Objective

SAN – Storage Area NetWork

SAS – Serial Attached SCSI

SATA – Serial Advanced Technology Attachment

SO – Sistema Operativo

TCO – Total Cost of Ownership

TCP – Transmission Control Protocol

TI – Tecnologias de Informação

ToE – TCP/IP Offload Engine

UTM – Unified Threat Management

VLAN – Virtual Local Area NetWork

VPN – Virtual Private Network

WAN – Wide Area NetWork

WLAN – Wireless Local Area Network

1. Introdução

Agilidade organizacional é nos dias de hoje uma palavra de ordem. Porém, e de acordo com um relatório da IDC realizado em 2016 [1], cerca de um terço das organizações portuguesas de grande e média dimensão estão em risco de desaparecer por falta de maturidade digital. O atual panorama económico, no qual as organizações enfrentam um mercado global, levanta novos desafios. Estas organizações vêem-se obrigadas a tomar posições mais definidas de forma a fazer alterações e melhorias ágeis nos seus métodos, desde a gestão organizacional até à gestão da produção e a reavaliar a sua estratégia e a sua missão, de modo a manter ou aumentar o seu nível de competitividade no mercado. Atualmente, todas as organizações utilizam as Tecnologias de Informação (TI) como ferramenta de suporte ao seu negócio. Esta maior utilização traduz-se numa dependência em muitos dos casos crítica para os negócios, na medida em que situações de indisponibilidade dos sistemas ou perdas de performance levam a prejuízos financeiros, operacionais e de reputação da marca graves. Com o crescimento do negócio aumentam os níveis de exigência das plataformas e recursos de TI, impondo uma elevada dinâmica tecnológica de forma a responder às emergentes necessidades das organizações. Face à constante evolução, quer dos negócios quer das tecnologias, surge aqui uma necessidade recorrente de análise, otimização e expansão de sistemas e plataformas de TI assentes em princípios de tolerância a falhas (FT), providas de mecanismos de alta disponibilidade (HA), modularidade e escalabilidade e em linha com a agilidade organizacional e consequentemente com a continuidade do negócio (BC) em cenários de desastre.

O impacto das TI nos modelos de negócio, economia e em praticamente todas as áreas é claramente visível, pois abriu a possibilidade da criação de sistemas ubíquos capazes de responder, otimizar e de certa forma solucionar questões e necessidades dinâmicas e emergentes que surgem numa sociedade de informação cada vez mais voraz e exigente. De acordo com o apresentado por James Kerr no seu livro [7], as organizações terão de ter a capacidade de responder rapidamente às mudanças no mercado e agilizar as operações para que as alterações do fluxo de trabalho possam ser feitas *on-the-fly*. No entanto, para minorar, evitar ou até mesmo garantir que não existem erros de dimensionamento dos recursos e suporte de TI, é imperativo arquitetar soluções capazes de otimizar e integrar os recursos, garantir elevado *uptime* e acesso à informação de modo rápido e seguro.

Para suportar, otimizar e gerir estas infraestruturas de forma segura e eficiente torna-se necessário arquitetar e consolidar numa única solução o conhecimento de várias áreas de TI. Esta conciliação obriga a um estudo e otimização permanente das tecnologias disponíveis, análise de mercado e ao conhecimento dos recursos internos e externos, alinhando as questões da segurança com base na

avaliação e mitigação de risco. Desta forma será possível o desenvolvimento de uma arquitetura de TI dimensionada e personalizada tendo em conta a realidade da uma determinada organização. O alinhamento estratégico com uma política de continuidade permite, na medida do possível, evitar o desperdício de recursos e obsolescência permitindo em simultâneo a integração dos sistemas legados e garantido o acesso à informação seguindo a politica dos "3 as" (*anytime, anywhere, any workload*) [26]. O mesmo será dizer que a evolução da arquitetura de TI requer uma visão global e holística, alinhada com a realidade atual e com as expetativas futuras das organizações permitindo elevar os níveis de serviço (SLA) dos novos sistemas que por sua vez irão compor e suportar o funcionamento do negócio. Estas tarefas extravasam as funções de um CIO ou CEO. Elas são inerentes a um perfil de arquiteto de TI que articulado com o CIO, CEO, CISO, CTO analisa, desenha e planeia a transformação digital adequada ao negócio e suas perspetivas.

1.1 Desafios

O crescimento das organizações e do seu negócio causa um consequente crescimento e dependência das tecnologias de informação e comunicação, nomeadamente o número de aplicações informáticas, quantidade de dados armazenados, aumento e diversidade de equipamentos e necessidades de conetividade e mobilidade. Transversalmente a todos estes fatores está subjacente o fator risco e segurança. Esta dinâmica gera um conjunto de desafios que requerem uma visão holística e a adoção de soluções escaláveis, modulares e flexíveis permitindo uma mais rápida adaptação a novas realidades. As exigências das organizações ainda que por vezes momentâneas e esporádicas, terão de ser satisfeitas de forma proactiva pois, caso contrário, poderão de alguma forma penalizar ou atrasar a estratégia do negócio.

Alguns autores [4], referem que nas organizações tradicionais que ainda não tenham sido aplicados os princípios de modernização na arquitetura de TI, poderão existir diversos constrangimentos. Por exemplo demasiadas plataformas (software ou hardware), demasiadas ilhas ou silos de informação e ou falta de controlo de utilizadores com privilégios máximos (administradores/root users). Organizações que tenham estes cenários têm um maior esforço para a realização do trabalho, devido à redundância da informação e à falta de integração dos sistemas existentes. Têm ainda maior dificuldade de manutenção e consequentemente custos mais elevados num ambiente propicio a falhas.

Atualmente é muito frequente encontrar organizações que possuem infraestruturas físicas dedicadas para cada aplicação/serviço, nomeadamente servidores. Por outro lado, devido ao custo dos servidores físicos, muitas organizações optam por concentrar num único servidor físico todas as aplicações e serviços.

Apesar da existência de produtos que supostamente reduzem os tempos de paragem associados à falha, normalmente estes possuem vários constrangimentos, nomeadamente a complexidade de implementação, a limitação no suporte para diferentes sistemas operativos (SO) e ainda os custos de licenciamento associados que tendem a ser significativos. Tal implica que no caso de avaria física de um servidor, haverá quebras de disponibilidade dos recursos associados e o consequente impacto no negócio. Em casos extremos, a reposição do bom funcionamento do sistema estará condicionada fisicamente quanto à disponibilidade de um novo servidor, reposição de sistema operativo e aplicações e restauro do último *backup* disponível. O tempo associado a este processo de reposição dos sistemas poderá demorar entre dias a semanas, comprometendo a organização numa perspetiva de custos e imagem perante os seus clientes e parceiros. Outra problemática comum tem a ver com a manutenção de infraestrutura, que terá de ser cuidadosamente planeada nomeadamente no que diz respeito aos tempos de paragem associados, por falta de alternativa de mobilidade de processamento aplicacional, ou seja, pela inexistência de serviço durante o período de intervenção. As intervenções deverão ser realizadas de forma calculada e prevista numa determinada janela temporal, evitando na medida do possível o impacto no período laboral. Tais intervenções devem ainda contemplar planos de contingência cuidados que permita a reposição normal do serviço no caso de derrapagens ou problemas durante a intervenção.

Com o crescimento exponencial de dados nas organizações [12], a utilização de tecnologias tradicionais de armazenamento *Direct-Attached Storage* (DAS) torna praticamente insustentável o crescimento e gestão da informação devido a limitações físicas dos servidores, nomeadamente, o número de discos físicos suportados. Outro problema a ter em conta é o aumento da carga de Input/Output (I/O) resultante do aumento do número de acessos aos recursos informáticos sendo que deverá haver uma separação do tráfego IP. Manter todo o tráfego misturado não é recomendado por fabricantes [14] devido a eventuais problemas de desempenho como por exemplo as aplicações *OnLine Transaction Processing* (OLTP) que são sensíveis à latência, prejudicando a funcionalidade e usabilidade das mesmas.

Um estudo da SUSE reportado em [12] alerta que em 2017 estima-se que 85% dos dados das organizações serão dados não estruturados (dados do tipo *flat files* ou armazenados em bases de dados "NoSQL"). O crescimento do volume de dados não estruturados é ilustrado na Figura 1. Estes dados irão representar um custo total de propriedade (TCO) elevado caso o armazenamento seja suportado pelos tradicionais *arrays* de discos.

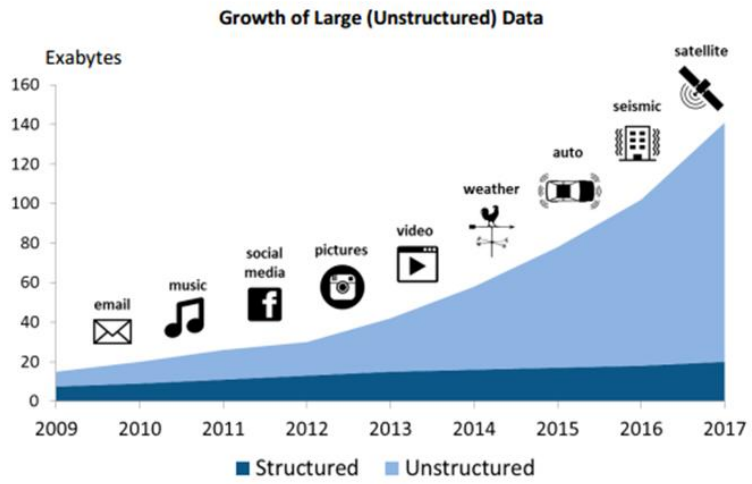

Figura 1 - Crescimento de "Large Unstructured Data" [12]

Este estudo recomenda ainda que para suportar o volume e velocidade de geração de dados dever-se-á adotar tecnologias de armazenamento do tipo *software-defined*. Esta abordagem possibilita a criação de áreas de armazenamento que possibilitam o aproveitamento mais eficaz e eficiente do armazenamento facultado pelos servidores. Simultaneamente, há uma abstração de tecnologias proprietárias sendo possível aglomerar *hardware* de diferentes fabricantes com discos de diferentes tamanhos e tecnologias. Esta junção é possível devido a métodos de armazenamento avançados que permitem a criação de LUNs (Logical Units) e volumes virtuais com base em suportes físicos distintos e de velocidades diferentes otimizando a performance com recurso a tecnologias de análise de I/O como por exemplo o *auto-tiering*, isto é, a movimentação dos dados entre tecnologias de discos e em funções de critérios de utilização (e.g. os dados mais acedidos permanecem em disco do tipo SSD e os menos acedidos em discos SATA). A adoção destes softwares em conjunto com os suportes físicos (servidores, discos, NAS e SAN entre outros), poderá ser uma solução eficiente para a crescente problemática do armazenamento.

Ainda e no que diz respeito a planos de contingência e ação que englobam ambientes de *Disaster Recovery* (DR), as organizações terão de cumprir determinados requisitos para garantir a continuidade do negócio em caso de falha dos seus recursos de TI. Um exemplo disso é a lei norte-americana que obriga a que as empresas cotadas em bolsa tenham um plano de ação para garantir a continuidade do negócio em cenários de desastre. Os *backups* são também uma importante componente a ter em conta na solução de uma arquitetura de TI. O processo de *backup* dos dados gera elevadas cargas de trabalho a nível de I/O, nomeadamente elevadas taxas de leitura de dados e consequente escrita nos sistemas de *backup*. São despoletados grandes níveis de transferências de dados, consumindo um elevado *troughput* na rede de dados (LAN ou eventualmente WAN caso os repositórios de backup se encontrem em sites remotos). Torna-se assim importante agendar a realização dos *backups* em períodos de menor atividade.

Com o crescimento da informação, o volume de dados a salvaguardar é ainda mais acentuado, levando por vezes à extensão da janela temporal de *backup* podendo influenciar períodos de produção. O desempenho dos servidores é afetado, pois os recursos vão estar ocupados pelos trabalhos de *backup* quando deveriam estar disponíveis para os utilizadores.

De forma a facilitar a relação entre desenvolvimento de software e operações de TI surgiu uma prática denominada de DevOps. DevOps é um acrónimo de *Development and Operations* e dá nome a uma cultura de trabalho (filosofia) em TI que promove uma estreita colaboração entre os profissionais destas duas áreas, para conseguir uma entrega de valor ao negócio muito mais rápida e constante, baseada nos princípios de *Continuous Delivery* e *Continuous Integration* [2]. O papel e funções de um arquiteto de TI está assim incluído nesta filosofia. A arquitetura de TI engloba não só o desenvolvimento de software e operações de TI, mas de uma forma global tudo o que está relacionado com as TI. Os desafios e operações inerentes a arquiteturas de TI inserem-se prática DevOPs. O arquiteto de TI abrange todas as considerações, desde a recolha de dados e desenho de modelos conceptuais, lógicos, físicos até à validação, monitorização e continuidade da solução desenvolvida. Um arquiteto de TI é assim um profissional que inserido na filosofia DevOps arquiteta, desenha e valida soluções com base na perspetiva global (*big picture view*), considerando não só o presente, mas também a sua continuidade.

1.2 Motivação

Tendo como *background* a realidade de várias organizações que tenho tido a oportunidade de visitar no decorrer da minha atividade profissional, tenho vindo a constatar que grande parte das organizações possui, de acordo com a definição em [4], modelos tradicionais de arquitetura de TI. São infraestruturas que foram crescendo de forma *ad-hoc* e com várias lacunas. Por outro lado, denota-se ainda um grande receio e apreensão por parte de responsáveis informáticos na adoção de princípios modernos de arquitetura de TI. Por exemplo o recurso à virtualização, autenticação centralizada (SSO) ou redes de armazenamento de dados (SAN), entre outros, são ainda considerados algo confuso e de difícil implementação. Este receio deve-se sobretudo ao desconhecimento técnico e dificuldades de compreensão e assimilação dos conceitos e níveis de abstração. Estes conceitos e tecnologias são inerentes aos princípios de modernização das tecnologias de TI sendo consideradas por alguns responsáveis de TI algo como disruptivo em relação aos sistemas tradicionais.

No terreno surgem com muita frequência questões do género, “Mas afinal onde estão os dados?” ou “Se eu quiser aceder a diretamente ao servidor, não posso ligar um monitor e trabalhar?”. Assim como afirmações do tipo “os servidores físicos são muito mais rápidos” ou “...eu gosto de saber onde estou a mexer…”. Outra situação que se verifica no terreno é o sobredimensionamento dos recursos. Por falta

de conhecimento e receio, os administradores de TI tendem a comprar tecnologias com mais recursos computacionais de que aqueles que realmente necessita. Tendo com conta que atualmente os equipamentos informáticos possuem um elevado poder computacional, o fabricante VMware (atualmente líder em tecnologias de virtualização), demonstrou num estudo publicado em [11] que a maior parte das organizações não utilizam eficientemente o poder computacional dos seus recursos físicos. De acordo com o estudo, o aproveitamento varia apenas entre 5 a 10% da sua real capacidade. É assim dito que o potencial retorno derivado da aquisição de um novo servidor é na maior parte das vezes reduzido face ao investimento realizado, devido à ineficácia no aproveitamento da sua potencialidade computacional.

Em suma, é notória a resistência à mudança e evolução tecnológica e tal tem como principal causa a sensação de perda de controlo sobre os recursos físicos e o facto dos conceitos de virtualização, escalabilidade e elasticidade ser algo "pouco palpável" e complexo. Assim, considerando a necessidade de adequar as infraestruturas tecnológicas aos desafios dos tempos modernos e à flexibilidade que os negócios exigem e, por outro lado, a resistência ou dificuldade sentida por muitos administradores tecnológicos, há uma clara necessidade de desmitificar, reestruturar e redesenhar soluções assentes em princípios modernos de TI. Simultaneamente é uma oportunidade de exploração e otimização de novas e emergentes tecnologias, possibilitando um uso mais eficiente das TI, minorando os custos associados à manutenção e crescimento da mesma. A criação de um manual de referência, a desenvolver neste trabalho e subjacente a uma metodologia, para renovação tecnológica das organizações considerando as suas reais necessidades de TI pretende ser um passo nesse sentido.

Tal manual de referência é importante na medida em que permitirá por um lado, de uma forma clara e simplificada, o acesso a informações e documentação técnica relevante e facilmente percetível. Ajudará também a esclarecer, eliminar ou minorar os receios inerentes à mudança e evolução das arquiteturas de TI. Simultaneamente potencia a antevisão, a evidenciação e a sensibilização para as necessidades e problemas consequentes da falta de visão holística e negligência no desenho e implementação de soluções de arquiteturas de TI. Estes problemas que vão surgindo e se revelam ao longo do tempo causam por vezes a paragem dos sistemas e perdas de informação sendo que poderão ter um impacto nefasto no bom funcionamento das organizações. Ao mitigar estas situações está-se inevitavelmente a evitar perdas operacionais, financeiras e de reputação. O manual a desenvolver deverá funcionar como um plano de análise e ação assente em boas práticas de TI, permitindo arquitetar uma solução robusta eficiente e adaptável, seguindo um método faseado tendo como objeto de estudo a realidade de uma determinada empresa. De forma sistemática o plano deverá responder a quatro questões principais:

- Qual o estado atual do ambiente de TI?
- Qual a estratégia e objetivos/expetativas futuras em termos de negócio e TI?

- Que trabalho é necessário para estabelecer o ambiente de TI desejado (*GAP analysis*)?
- Após o desenvolvimento e a implementação questionar: foram as necessidades identificadas nos pontos anteriores colmatadas?

Para além do estudo preliminar, tal plano abrange tecnicamente três áreas basilares, nomeadamente, conetividade, servidores e armazenamento. Cada uma destas áreas será analisada tendo sempre presente os conceitos de segurança e risco. Após a definição de um manual de referência pretende-se avaliar o mesmo através da sua aplicação em contexto real de trabalho que maximize várias das vertentes apresentadas na Tabela 1. Por fim, pretende-se que a solução desenvolvida assim como a documentação produzida possa ser adaptável a diferentes organizações independentemente da área de negócio.

Aumentar a eficácia temporal associado ás tarefas de manutenção
Criar e parametrizar mecanismos de proatividade para a gestão e monitorização de equipamentos e recursos (e.g. *triggers* para envio de alertas)
Maximizar o aproveitamento das capacidades computacionais e de armazenamento dos equipamentos
Diminuir o número de equipamentos e espaço físico (consolidação)
Aumentar a eficiência energética e promover o *green-computing*
Diminuir a complexidade das plataformas de TI
Garantir mecanismos de redundância e alta disponibilidade
Flexibilizar e alocar recursos de forma dinâmica (evitar ociosidade de recursos)
Desenvolver documentação
Controlar e reduzir custos

Tabela 1 – Pontos a atingir no âmbito do manual de referência a criar

A componente prática do trabalho consistirá assim na análise em contexto real de trabalho e englobará o desenhar, documentar, implementar e validar uma solução de arquitetura de TI, ajustada à realidade de uma organização que será alvo de estudo. Espera-se que os trabalhos e a documentação realizada ao longo deste projeto possa ser adotada como exemplo e metodologia, para quem pretender seguir uma estratégia de modernização e competitividade alavancada pelas tecnologias de informação.

Outro fator motivacional é o facto de este trabalho ser multidisciplinar e albergar várias áreas de conhecimento e tecnologias consolidando-as, permitindo criar soluções que possam servir de orientação a vários grupos de profissionais, tais como arquitetos de TI, administradores de sistemas, gestores de projeto e consultores de TI entre outros.

1.3 Estrutura da dissertação

Este relatório encontra-se dividido em cinco capítulos. No capítulo 2 é apresentado o estado da arte relacionado com a temática da administração e arquitetura de sistemas e infraestruturas tecnológicas, fazendo-se um paralelo entre as abordagens tradicionais e as atuais. No terceiro capítulo é apresentada a metodologia subjacente à criação do manual de referência de arquitetura IT e o resultado da aplicação dessa mesma metodologia. No capítulo 4 é apresentado um caso de estudo real, que serviu igualmente de motivação ao trabalho. Finalmente no quinto capítulo é feita a conclusão do trabalho e indicados aspetos de trabalho futuro.

2 Estado da Arte

Neste capítulo, apresentamos os modelos e componentes relevantes de inovação na área de IT com focus em infraestruturas dinâmicas, escalável e robustas. Subjacente à descrição, faz-se o enquadramento das tecnologias nomeadamente da componente de virtualização, redes locais e de dados, armazenamento partilhado, backups e segurança.

Num cenário de crescimento organizacional e tecnológico constante é crucial manter o controlo dos ativos de uma arquitetura de TI. De acordo com [5], tal controlo é fundamental para reduzir os próprios custos provenientes das rápidas variações tecnológicas. Segundo o apresentado em [4], as organizações que seguiram uma estratégia de modernização terão tudo integrado tais como serviços centralizados de diretório e autenticação, soluções de *"messaging"*, planos de *backup e disaster recovery*, armazenamento de dados, soluções de segurança entre outros. De acordo com a literatura [4] da área os critérios de sucesso de uma arquitetura de TI, englobam:

- A redução de custos de suporte e operacionais;
- A definição de técnicas assentes em standards;
- A redução do risco (segurança da informação, indisponibilidade do serviço);
- A otimização da continuidade operacional;
- A redução de redundância indesejável, mantendo a tolerância ás falhas;
- A facilitação dos processos de negócio;
- A definição de um "*clear upgrade path*" para tecnologias futuras.

Em [5], o autor afirma que o valor das TI deverá ser demonstrado através de comparações entre os custos e a qualidade dos serviços de TI tendo como resultado o "valor pelo dinheiro". Isto é, deverá ser aferido o custo da indisponibilidade e a adoção e medidas que sejam *cost-effective*, ou seja o valor a aplicar para reduzir o risco não seja superior ao custo da própria indisponibilidade. Para tal quantificação deve-se ter em consideração que qualquer paragem dos sistemas poderá traduzir-se em elevados custos produtivos, descontentamento dos utilizadores e consequentemente custos financeiros. Além da indisponibilidade, é importante considerar a performance. De acordo com o apresentado em [8] o acesso rápido a informação é um fator estratégico que pode influenciar a continuidade e sucesso de uma organização nos dias de hoje. Tal é também reportado por vários autores [7] referindo números como: *"43% of businesses that experience disasters never re-open and 29% close within 2 years."* (McGladrey and Pullen)"; *"40% of all companies that experience a major disaster will go out of business if they cannot gain access to their data within 24 hours."* (Gartner)"; "*Businesses can no longer expect that their*

customers will be willing to wait for them. Rather, consumers and trading partners alike are ready and able to move on if their needs are not met expeditiously."

Por muito que se deseje um SLA (Service Level Agreement) de 100% tal não é viável [3]. Os sistemas falham e os custos associados à disponibilidade são também maiores à medida que nos aproximamos do 100%. Em [5] o autor conclui que um SLA de 99,99% (quatro noves) de capacidade e disponibilidade é dezasseis vezes mais caro do que 99,9% (três noves). A par do correto dimensionamento do SLA objetivo, e partindo do principio que existem e terão de continuar a existir sistemas legados, é cada vez mais estratégico para as organizações ter uma visão atual das TI e projetarem-se nessa mesma realidade para evoluir. Pois, evoluindo tecnologicamente as organizações ficarão melhor preparadas para enfrentar a própria evolução do negócio.

Para um arquiteto de TI a análise da realidade da organização e a definição de uma estratégia de evolução requer uma visão integrada e global e de acordo com o apresentado em [12] e [14] qualquer alteração das TI deverá ser cuidadosamente planeada. A ausência do planeamento e desenho de uma solução integrada de TI irá limitar a curto prazo a sua usabilidade, tendo como consequência constrangimentos no desempenho do próprio negócio. Porém a tarefa de planeamento não é fácil. Segundo [4], existe uma infinidade de conflitos difíceis de antever até ao momento em que é necessário evoluir e reajustar a arquitetura de TI. Alguns exemplos são as incompatibilidades de comunicação entre protocolos que suportam novos equipamentos ou que estão presentes em novos sistemas operativos, assim como a falta de suporte por parte dos parceiros tecnológicos que causa a obsolescência dos sistemas e tecnologias obrigando a adotar novas estratégias de TI, entre outros.

2.1 Modelos de negócio, frameworks e boas práticas de TI

A informação é um recurso fundamental para todas as organizações e a tecnologia desempenha um papel significativo desde o momento que a informação é criada até o momento em que ela é destruída. A tecnologia da informação está cada vez mais avançada, tornando-se pervasiva nas organizações e nos ambientes sociais, públicos e corporativos [35]. A Internet criou uma nova plataforma tecnológica universal sobre a qual são constituídos novos produtos, serviços, estratégias e modelos de negócio.

O negócio de grande escala de organizações como a UBER ou a Amazon está diretamente relacionado e dependente das tecnologias de informação. A indisponibilidade de serviços (ainda que momentâneo) suportados pelas TI, neste tipo de modelo de negócio tem um impacto significativo podendo gerar prejuízos avultados ou a falência do negócio. Atualmente os modelos de negócio tradicionais estão cada vez mais dependentes das TI, em rota de convergência com o grau de dependência de negócios que

surgiram das TI. A eventual adaptação de metodologias, frameworks e boas práticas auxiliam as organizações a evoluir os seus modelos de negócios.

A arquitetura empresarial (EA) e a sua gestão são temas que recebem interesse contínuo de investigadores, profissionais de TI, organismos de padronização (standards) e fabricantes. Neste âmbito segundo [13], existem várias metodologias, frameworks e boas práticas que contemplam as várias áreas de gestão e infraestrutura de TI. De entre múltiplas opções, algumas das mais conhecidas e aceites são por exemplo a COBIT [6], ITIL [20], TOGAF [18] ou Zachman Framework [19].

A Zachman Framework é uma estrutura lógica (matriz) que permite perspetivas múltiplas e a categorização de artefactos. A estrutura consiste numa matriz de 6 colunas por 6 linhas. As colunas correspondem a perguntas (What/Who/Where/When/Why/How) a ser aplicadas à organização. As colunas referem-se aos diferentes aspetos relevantes de que é necessário ter conhecimento e retratam a organização. As linhas da matriz referem-se aos diferentes pontos de vista e níveis de detalhe relativos à informação que descreve a organização. O conteúdo das células, geradas pela interseção das linhas com colunas, é relativo a informação especifica que combina o aspeto e o ponto de vista correspondentes.

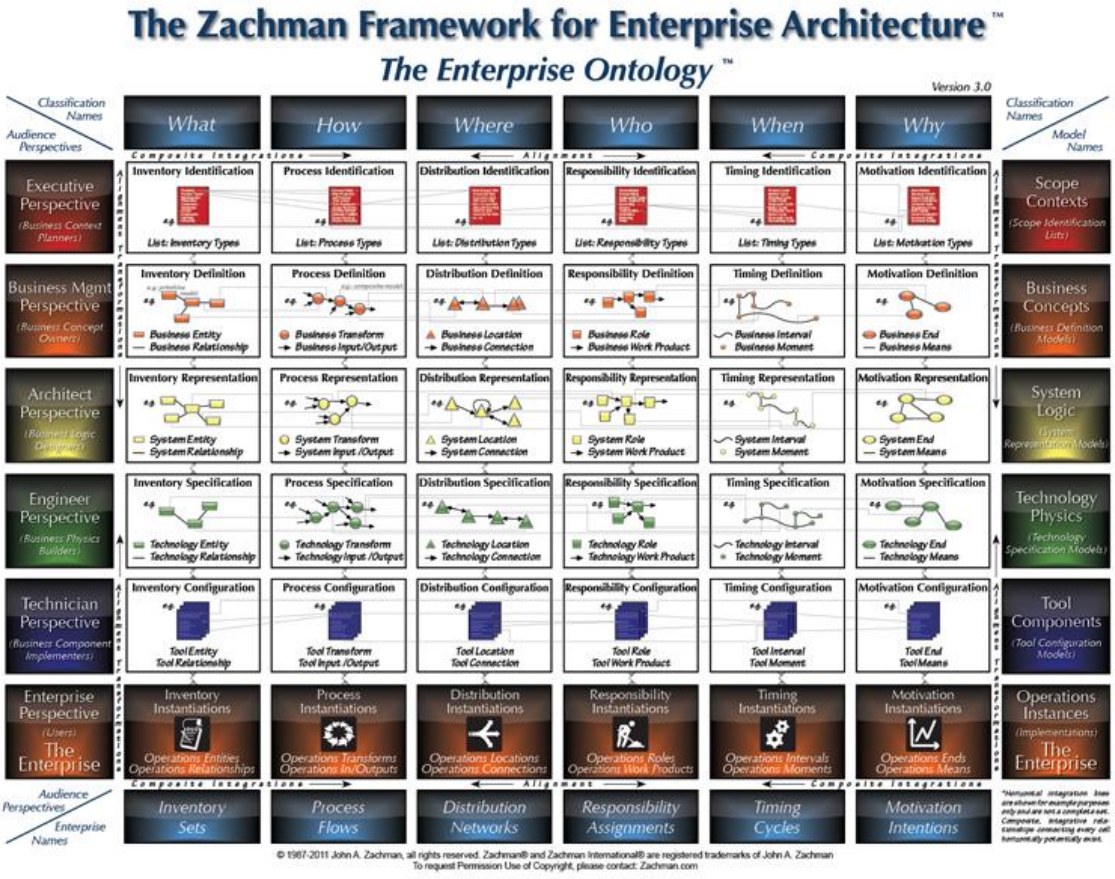

Figura 2 - Zachman Framework [19]

Uma das críticas mais frequentes da Zachman Framework, é o facto de estar focada nos sistemas de informação, criando uma ideia de que estes são os únicos recursos utilizados pelas organizações que suportam os processos de negócio. De um ponto de vista metódico a Zachman Framework não faz descrições detalhadas (e.g. não são descritas atividades de gestão ou tarefas), ou seja, proporciona a estruturação da informação, mas não um método para a sua construção [9]. Neste sentido e para suprir essa necessidade, muitos profissionais TI recorrem também a outras frameworks, como por exemplo a TOGAF. A framework TOGAF é desenvolvida e mantida pelo *The Open Group*, entidade sem fins lucrativos mantida por empresas de TI, tais como IBM, SAP, Oracle e HPE. O TOGAF fornece metodologias e ferramentas de suporte para organizar e gerir a tecnologia, garantindo que os projetos atinjam os objetivos das organizações através de processos sistemáticos e repetitivos.

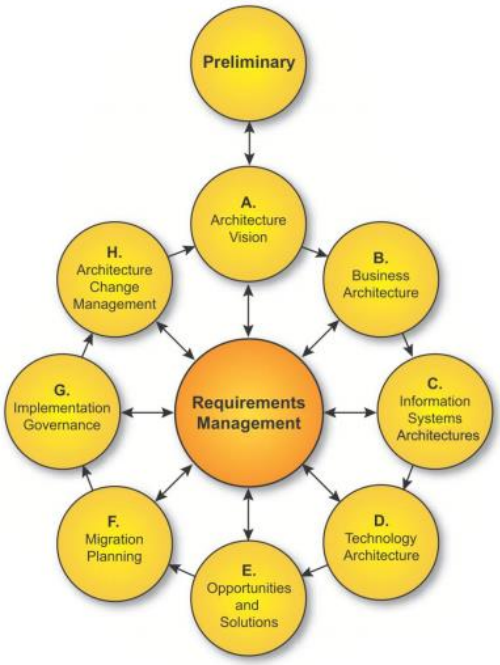

Figura 3 - O método de desenvolvimento de arquitetura de TOGAF [13]

No *core* da estrutura TOGAF está o método de desenvolvimento de arquitetura (ADM). O ADM descreve a metodologia para desenvolver e gerir o ciclo de vida de uma arquitetura através de fases contínuas/cíclicas e iterativas. Consiste em oito fases interconectadas de desenvolvimento complementadas por uma fase preliminar e gestão centralizada de requisitos. O TOGAF propõe a estruturação da arquitetura em diferentes domínios que representam subconjuntos da arquitetura global, nomeadamente [19]:

- ***business Architecture****:* relacionada com aspetos estratégicos, governamentais, organizacionais e processos;

- ***data Architecture**:* descreve a estrutura de bens ativos e recursos de gestão de uma organização.
- ***application Architecture**:* considera os sistemas aplicacionais, as suas iterações e relações com os processos de negócio.
- ***technology Architecture**:* descreve os requisitos de software e hardware necessários para suportar o desenvolvimento do negócio e serviços de dados e aplicacionais

O *core content metamodel* (Figura 4) refere os elementos que devem ser considerados para o desenvolvimento de uma arquitetura empresarial.

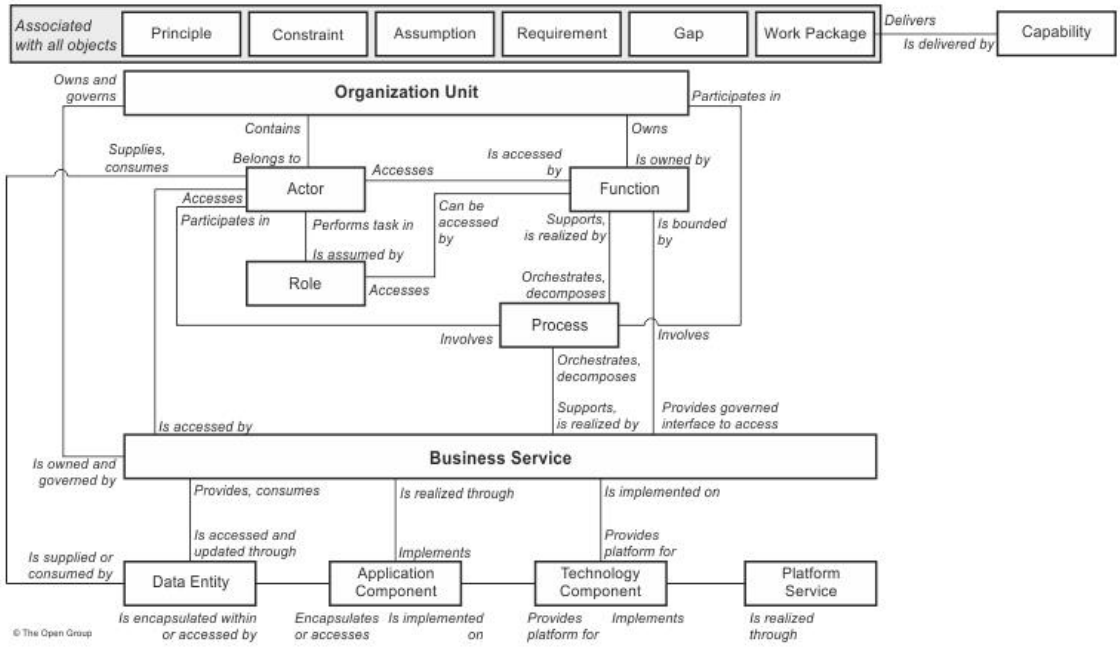

Figura 4 - The core content metamodel of TOGAF [13]

Um dos problemas da abordagem baseada na framework TOGAF é o facto de estar focada apenas na arquitetura associada à gestão de projetos e não na solução global com vista à sua continuidade. A framework TOGAF praticamente finaliza no nível da fase de implementação, com exceção dos mecanismos de gestão que são aplicados nesta fase. Esta abordagem implica que apesar de recolha de informações (fase preliminar), estas não são atualizadas ao longo da continuidade da solução desenvolvida [19]. Outro ponto a assinalar é o facto da framework TOGAF ser bastante abrangente permitindo ser aplicada a qualquer tipo de iniciativa de arquitetura empresarial. No entanto como referido em [17], estima-se que a sua aplicação total abrange apenas 5% das vezes em que é aplicada.

A ITIL é um conjunto de publicações e boas práticas, que fornecem orientação para o desenvolvimento,

entrega e gestão dos serviços de TI (*ITSM – IT service management*). A ITIL procura alinhar os serviços de TI com as necessidades do negócio e apoia os seus principais processos. Providencia a organizações e indivíduos orientações sobre como usar as TI como uma ferramenta para facilitar as alterações transformação e crescimento dos negócios [24]. O ITIL V3 (forma mais recente) consiste numa série de 5 volumes. Cada volume cobre uma fase do ciclo de ITSM diferente. A Figura 5 identifica cada uma destas fases.

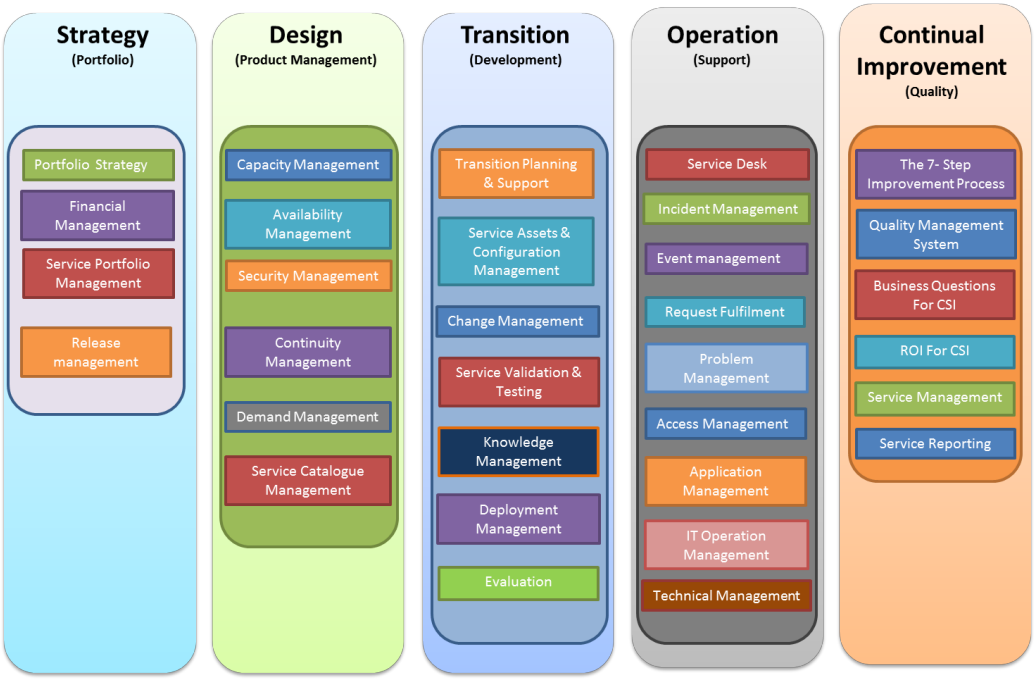

Figura 5 - Fases do ITIL V3 [25]

Cada uma destas fases define um conjunto de orientações procurando completar o ciclo referente aos diversos serviços, nomeadamente:

- **Estratégia de Serviço (*Strategy*):** fase onde se define a direção estratégica dos serviços de TI, quem são os seus clientes e quais os serviços que serão disponibilizados.
- **Desenho de Serviço (*Design*):** fase que inclui a avaliação dos processos de gestão do negócio (nível serviço, disponibilidade, capacidade, etc.) para desenhar e desenvolver novos serviços ou melhorar serviços já oferecidos.
- **Transição de Serviço (*Transition*)**: fase que cobre a transição do desenvolvimento para as operações, incluindo testes e controlo de qualidade.
- **Operação de Serviço (*Operation*):** fase onde são coordenadas e executadas as atividades e processos necessários para entregar os serviços aos clientes e utilizadores, gerindo os níveis de serviços acordados.
- **Melhoria Contínua de serviço (*Continual Improvement*)**: fase que procura manter os níveis de qualidade, sendo o seu propósito alinhar e realinhar continuamente os serviços de TI de

acordo com as necessidades do cliente, identificando e implementando melhorias aos serviços de TI que suportam os processos de negócio.

No entanto, o âmbito e conceitos do ITIL são muito abrangentes, o que por um lado pode ser visto como uma mais valia, por outro lado o seu uso "excessivo" pode levar a custos consideráveis. A abordagem apresentada pelo ITIL não garante que os requisito mínimos dos processos sejam efetivamente implementados, uma vez que o ITIL é descritivo. Neste aspeto a ISO 20000 atua complementado o ITIL, pois determina aquilo que é mandatório realizar.

Criado pelo "IT Governance Institute and the Information Systems Audit and Control Association (ISACA)", a framework COBIT tem como objetivo ajudar as organizações na criação, monitorização e manutenção de práticas de gestão e administração de TI. Atualmente, na versão 5, é usado para garantir qualidade, controlo e confiabilidade de sistemas de informação nas organizações. Em [35] é referido que o COBIT permite que as TI sejam geridas de forma holística através de uma perspetiva global, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI. O COBIT 5 baseia-se em cinco princípios básicos (Figura 6) para administração e gestão de TI da organização.

Figura 6 - Princípios do COBIT [35]

O objetivo principal é o alinhamento entre os objetivos do negócio e os objetivos da TI, fazendo com que a TI atenda às necessidades de negócio (requisitos de negócios) da maneira mais eficiente possível. O COBIT 5 foi desenvolvido considerando uma série de outros padrões e modelos de referência [35], conforme Figura 7.

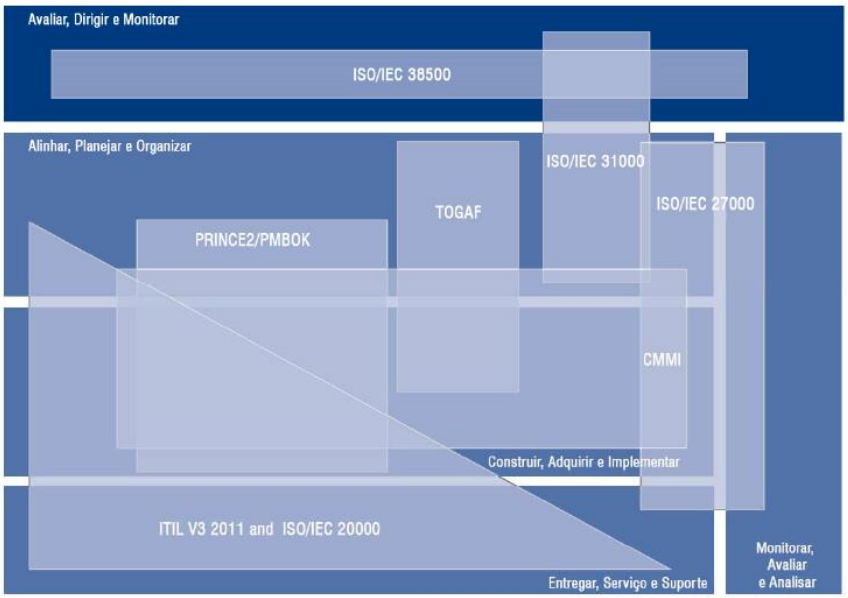

Figura 7 - Cobertura da outros Padrões e Modelos pelo Cobit 5 [35]

Apesar do COBIT ser uma framework bastante influente e abrangente, alguns investigadores [36] referem que uma das maiores desvantagens é que exige uma grande quantidade de conhecimento para entender a framework, antes que ela possa ser corretamente aplicada.

A adoção de frameworks e práticas recomendadas, ajustadas ao modelo de negócio poderá traduzir-se em benefícios para as organizações, no entanto é necessário entender qual o(s) problema(s) a ser revolvido e qual a framework capaz de o(s) resolver. Se por um lado a adoção de uma única framework poderá não ser suficiente, por outro lado a adoção da várias frameworks poderá tornar-se algo complexo. Torna-se assim crítico saber optar, combinar e adaptar o uso de diferentes frameworks no âmbito de um projeto.

2.2 Arquitetura de TI – Opções para um Data Center

De acordo com [26] existem quatro categorias nas quais um arquiteto de TI pode projetar a criação/evolução de um centro de dados. Estas categorias são: tradicional; convergente (*converged*); hiperconvergente (*hyperconverged*); e composta (*composable*). Tal como é ilustrado na Figura 8, estas categorias estão relacionadas com a otimização das operações de gestão e a flexibilidade aplicacional que trazem.

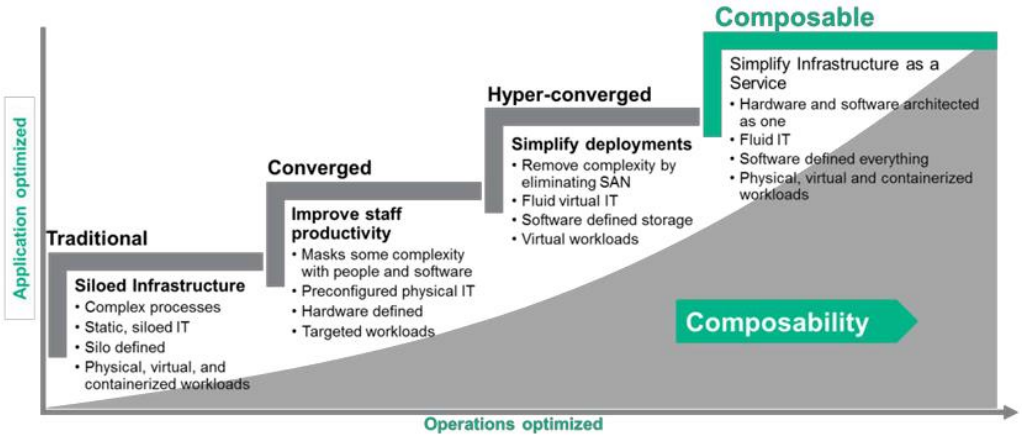

Figura 8 - Evolução das categorias de infraestrutura de TI [35]

A arquitetura do tipo tradicional foi a primeira a aparecer e é sobre a qual ainda muitas organizações operam. Estas soluções de infraestrutura são anteriores ao aparecimento da virtualização, baseando-se em servidores físicos. Este tipo de arquitetura é mais "rígida" (um ambiente estático com falta de flexibilidade e escalabilidade) em termos de manutenção e evolução criando constrangimentos à medida que o negócio das organizações evolui e exige mais das TI [4]. Nestas infraestruturas coabitam diferentes tipos de hardware e software, que podem requerer diferentes conhecimentos (*skills*) acabando por elevar o custo e complexidade de manutenção da mesma.

As arquiteturas do tipo convergente assemelham-se à abordagem tradicional. Os principais objetivos são diminuir ou até mesmo resolver os problemas de compatibilidade entre servidores, sistemas de armazenamento e dispositivos de rede, reduzindo custos de cablagem, arrefecimento, energia e espaço. Neste ambiente, a solução adquirida é validada (testada) e pré-configurada pelo fabricante, garantido que tudo irá funcionar conforme planeado e esperado. Alguns dos benefícios desta abordagem em [26] englobam: a melhoria da produtividade da equipa de TI, pois não há perdas de tempo com a preocupação com a assemblagem e compatibilidade entre os equipamentos, maximizando a sua usabilidade em vez de simplesmente conseguir colocá-los a trabalhar em conjunto; a possibilidade de concentrar a gestão da infraestrutura através de ferramentas de administração que poderão gerir todo o ambiente de uma forma mais eficaz; a maior simplicidade com a aquisição de equipamentos, tendo em conta que todos os equipamentos são comprados de uma só vez como uma solução já validada. Neste tipo o hardware continua a ser idêntico ao da abordagem tradicional havendo apenas a garantia de convergência do fabricante. Mantêm-se os constrangimentos de falta de flexibilidade necessário para responder à evolução das necessidades do negócio.

A híper-convergência a nível de infraestruturas surge com base no "repensar" de todos os serviços inerentes a um *datacenter*, tendo como foco a máquina virtual ou a carga de trabalho (*workload*). Todos

os elementos da infraestrutura hyperconvergente assentam na virtualização para a construção básica do *datacenter* [31]. Este tipo de abordagem permite a abstração física de recursos do tipo servidores, rede e armazenamento diminuindo a complexidade e as barreiras associadas à arquitetura convergente. A infraestrutura hyperconvergente utiliza o conceito de *Software-Defined Storage* (SDS) [26] para suportar, gerir e coordenar o armazenamento local em cada nó criando um completo ambiente de armazenamento distribuído e escalonado sem necessidade de uma SAN monolítica. Entre as vantagens na adoção deste tipo de arquitetura, temos: a facilidade de gestão na medida em que não é necessário gerir recursos dedicados de armazenamento. Toda a gestão é realizada diretamente no *hypervisor* ou com base em ferramentas integradas facultadas pelo fabricante do software utilizado na infraestrutura; uma maior simplicidade de escalonamento de recursos computacionais; um melhor controlo de custos na medida em que se poderá adicionar capacidade ao longo do tempo. Um estudo da Gartner [32] afirma que em 2019, aproximadamente 30% da capacidade global de armazenamento instalada em centros informáticos será suportada por arquiteturas baseadas em sistemas de armazenamentos definido por software (SDS) ou sistemas integrados hiperconvergentes (HCIS). Sendo que 20% das aplicações criticas irão ser transferidas para HCIS em 2020. Uma das desvantagens deste tipo de infraestrutura é a impossibilidade de integrar servidores físicos com servidores virtuais numa única plataforma, obrigando a manter no mínimo as duas plataformas.

A quarta opção refere-se à infraestrutura composta (*composable infrastructu*re). Esta é uma categoria emergente de infraestrutura de *datacenter* que procura (des)agrupar recursos de computação, armazenamento e recursos de rede em *pools* de recursos partilhados que podem estar disponíveis para alocação mediante as necessidades [33].

As organizações atualmente suportam dois modelos muito diferentes a nível aplicacional. O primeiro é o modelo tradicional e o segundo é o modelo economia de ideias (*Idea Economy*) [34]. O modelo tradicional opera num ambiente convencional e estacionário que se concentra na minimização do risco através de metodologias padrão e fornecedores convencionais, normalmente para correr aplicações de suporte aos processos do negócio como por exemplo ERP, OLTP ou base de dados relacionais. O modelo *Idea Economy* foca aplicações e serviços móveis, *big data* e aplicações na *cloud* para os quais aspetos como a elasticidade são mais significativos. O ambiente *composable* permite às organizações suportar ambos os modelos através de conceitos e tecnologias inovadoras. O objetivo primário é responder às mais exigentes necessidades das organizações, agrupando ou desagrupando *pools* de recursos dinamicamente de acordo com três elementos de design [35]: *Fluid Resource Pools; Software-Defined Intelligence; Unified API*. Uma visão integrada dos três elementos subjacentes a esta arquitetura é apresentada na Figura 9.

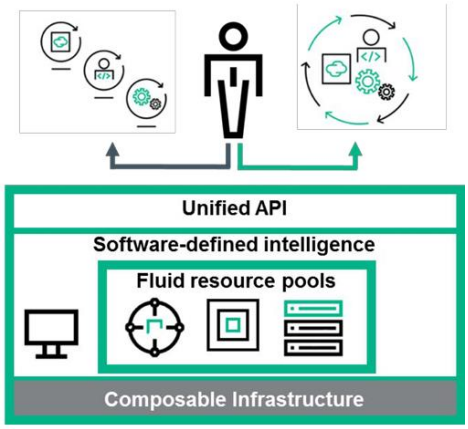

Figura 9 - Componentes principais da arquitetura de composable Infrastructure [35]

Para concluir esta secção, poder-se-á afirmar que a evolução das infraestruturas de TI segue a tendência evolutiva do negócio e requer cada vez mais um alinhamento contínuo e dinâmico reduzindo custos de infraestrutura, operacionais e maximizando o alinhamento dos recursos computacionais ao funcionamento do próprio negócio.

2.3 Arquitetura de TI – Tecnologias

Para desenhar soluções de arquiteturas de TI eficientes relativas é necessário selecionar e consolidar várias tecnologias. No âmbito de uma arquitetura moderna essas tecnologias devem possibilitar elevados níveis de escalabilidade, flexibilidade, performance e segurança. Estes conceitos são inerentes a uma estratégia de crescimento, assentes numa visão holística suportada por boas práticas de TI. Uma infraestrutura IT agrega várias tecnologias. Nesta secção serão apenas abordadas as mais relevantes para o projeto.

2.3.1 Virtualização

A virtualização é uma forma de abstração das aplicações e componentes subjacentes, do *hardware* e recursos físicos que as suportam apresentando uma visualização lógica ou virtual desses recursos [21]. Os recursos poderão ser por exemplo servidores, dispositivos de armazenamento, dispositivos de rede entre outros. Os objetivos da virtualização são aumentar aos níveis de performance, escalabilidade, confiabilidade, disponibilidade, agilidade, segurança, monitorização e gestão.

A virtualização, segundo [21] pode de um modo genérico ser dividida em sete camadas que refletem as diferentes formas de virtualização que atualmente existem:

- **Access virtualization:** permite o acesso de cliente remotos a aplicações a partir de diferentes

dispositivos. Um exemplo de um produto que trabalha nesta camada é o XenDesktop da Citrix [29];

- **Application virtualization:** permite que aplicações desenvolvidas para uma determinada versão de um S.O. seja executada num outro ambiente. Alguns exemplos de produtos que se enquadram nesta camada são o XenApp da Citrix [29] e o VMware ThinApp [33].
- **Processing virtualization**: permite que um único sistema suporte cargas de processamento como se fossem vários sistemas, ou permite que o processamento seja distribuído por vários sistemas como se estes fossem um único sistema. Alguns exemplos de produtos são o Citrix XenServer [37] ou Microsoft Hyper-V [38].
- **Network virtualization:** permite criar, provisionar e gerir redes através de software utilizando a rede física de uma forma simplista para apenas encaminhar os pacotes de dados. É neste tipo que se enquadra o *Software-Defined Networking* (SDN). Produtos como o VMware NSX [45] ou Juniper CONTRAIL [46], são alguns dos produtos que permitem a virtualização de redes.
- **Storage virtualization:** permite a abstração dos dispositivos de armazenamento (SAN, NAS, DAS), podendo agrupar ou particionar diferentes recursos, de diferentes fabricantes, tecnologias (iSCSI, NFS, FC, SATA, SSD, SAS). A capacidade de armazenamento de diferentes dispositivos é gerida como *pools* partilhadas rentabilizando melhor o espaço de armazenamento. A nível de performance é possível a aplicação de técnicas de *auto-tiering* permitindo a alocação dinâmica do processamento de dados críticos a dispositivos que permitem um maior número de IOPs (Operações de Input/Output por segundo). É neste âmbito que se enquadra o *Software-Defined Storage* (SDS). O VMware vSAN [49] ou DataCore SANsymphony [58] são exemplos de tecnologias para *Storage Virtualization*.
- **Security for virtual environments:** A camada de segurança para ambientes virtuais tem como finalidade monitorizar e proteger todas as outras camadas de virtualização, garantindo que os recursos são acedidos apenas por acessos autorizados. Alguns dos maiores *players* nesta área são os fabricantes de soluções de segurança como a Sophos, a TrendMicro ou a Kaspersky.
- **Management for virtual environment:** A camada "management for virtual environment" é uma tecnologia baseada em software que de forma simplificada permite a monitorização e gestão de ambientes virtuais Vários fabricantes como por exemplo a VEEAM, VMware ou Microsoft, oferecem software para gestão e segurança de ambientes virtuais.

Os elevados custos energéticos e a diminuição da pegada ecológica na área de TI (*green-computing*), são também dois fatores que contribuem para a adoção da virtualização como modelo de consolidação de recursos de forma eficiente. Este modelo quando comparado com as soluções tradicionais, permite reduzir o número de equipamentos físicos, facilitando a gestão e manutenção tendo como consequência direta a eficiência e rentabilização da infraestrutura. A virtualização é pelas várias razões uma revolução

tecnológica que veio para ficar. Ela é assumidamente utilizada pelas organizações sendo a sua adoção maioritariamente feita de três formas distintas: Virtualização de servidores; Virtualização de aplicações; Virtualização de desktops.

No âmbito da virtualização de servidores existem três tipos de virtualização [22], nomeadamente:

- **Virtualização de sistemas operativos (*containers*)**: servidor a correr um único kernel e através deste é feito o controlo dos sistemas operativos dos servidores virtuais. Um exemplo claro deste modelo é o Docker ou Solaris Containers.
- **Emulação de hardware**: virtualização baseada em emulação de hardware que permite que um servidor físico (*host*) em conjunto com uma camada de software denominada *hypervisor* possa suportar vários servidores virtuais designados de *virtual machines* (VM).
- **Paravirtualização:** semelhante à virtualização total, mas não tenta emular o hardware. Um hypervisor baseado em paravirtualização coordena o acesso direto à camada física de alguns recursos do hardware do servidor obtendo maiores níveis de performance uma vez que evita a camada subjacente à emulação do hardware. A Figura 10 ilustra um exemplo de paravirtualização da arquitetura Citrix Xen.

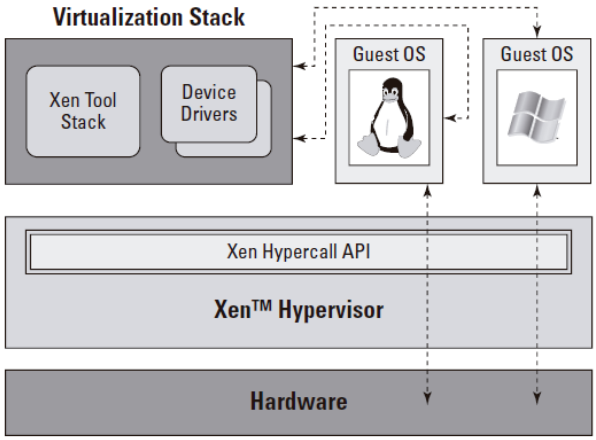

Figura 10 - Arquitetura de paravirtualização - Citrix Xen [29]

Os sistemas de virtualização facilitam a criações de clusters, que podem ser de dois tipos: alta disponibilidade (HA) ou tolerância à falha (FT). Para um maior nível de alta disponibilidade e eliminar o downtime em *workloads* críticos, poderá recorrer-se a um cluster FT. Neste tipo de cluster é mantida uma cópia redundante da VM, a correr num host (do mesmo cluster) diferente. Para tirar partido das funcionalidades, e de acordo com [28], é importante acautelar o correto desenho da rede física, a redundância da conetividade, o armazenamento partilhado assim como outros recursos inerentes à solução arquitetada. As VMs poderão ser instaladas de raiz, geradas via modelos (*templates*), importadas (OVA, OVF) ou convertidas [10] (p2v, v2v).

Apesar de todas as vantagens e benefícios da virtualização existem novas considerações a ter em conta quanto à arquitetura de sistemas. O facto de se consolidar servidores num único servidor físico levanta outras necessidades, como por exemplo maiores exigências a nível de hardware dos *hosts* físicos para garantir os devidos recursos. O correto dimensionamento de recursos tais como memória física, capacidade de processamento, armazenamento e conetividade entre a rede virtual e a rede física, são críticos para o sucesso da solução.

2.3.2 Conetividade

A conetividade reúne diferentes formas de comunicação permitindo maior agilidade entre processos que de outro modo seriam morosos ou inexequíveis. O crescimento da conetividade surge não só nas comuns e tradicionais ligações físicas, mas cada vez mais está presente nas soluções de mobilidade (Wi-Fi, M2M, IoT), voz e interligação de sites remotos.
Com toda esta dinâmica e diversidade de tecnologias e fabricantes há uma preocupação acrescida com a estabilidade, fiabilidade e performance das comunicações alinhadas com as boas práticas de segurança.

Nesta secção abordam-se métodos e tecnologias de conetividade de suporte as necessidades de uma arquitetura de TI.

2.3.3 A conetividade na virtualização

A virtualização acrescenta uma nova dinâmica à conetividade devido à abstração dos recursos físicos e às tecnologias que incorpora. Eliminar ou evitar pontos únicos de falha, garantir redundâncias, elevar a fiabilidade, alta disponibilidade, performance e segurança a nível de acessos e protocolos são exemplos desses fatores. A correta implementação a nível de conetividade, assente em boas práticas, potencia a otimização da capacidade e aproveitamento computacional dos equipamentos. O recurso à segmentação, isolamento de redes, VLANs, listas de controlo de acessos (ACLs), utilização de protocolos como por exemplo o *rapid spanning-tree* (RSTP), LACP ou utilização de *jumbo frames* são alguns dos aspetos a considerar no desenho e implementação de uma solução moderna de uma arquitetura de TI [45].

À semelhança dos recursos físicos, os recursos virtuais necessitam de parametrizações otimizadas, para um aproveitamento deveras eficiente dos recursos. A conetividade a nível de Ethernet entre os recursos virtuais e físicos são suportados por *uplinks* entre switches virtuais (vSwitches) e switches físicos. As redes virtuais suportam na generalidade as mesmas funcionalidades das redes físicas, mas existem diferenças técnicas nas operações e terminologias que devem ser tidas em conta [4].

Os métodos e procedimentos de configuração variam consoante os fabricantes, no entanto os conceitos e objetivos são comuns. Utilizando como exemplo um fabricante líder, nomeadamente a VMware, existem 2 tipos de switches virtuais, nomeadamente o standard switch (vSS) e o distributed switch (vDS ou dvswitch) [27]. O standard switch permite a conetividade entre *hosts* e máquinas virtuais. Os adaptadores de rede físicos (NIC) dos *hosts*, são consideradas uplink ports no switch virtual sendo a conetividade entre a rede virtual e a rede física suportada por estas. Os switches virtuais são criados individualmente em cada *host* e pertencem unicamente ao *host*. Na Figura 11 é ilustrada a interligação das máquinas através de standard switches.

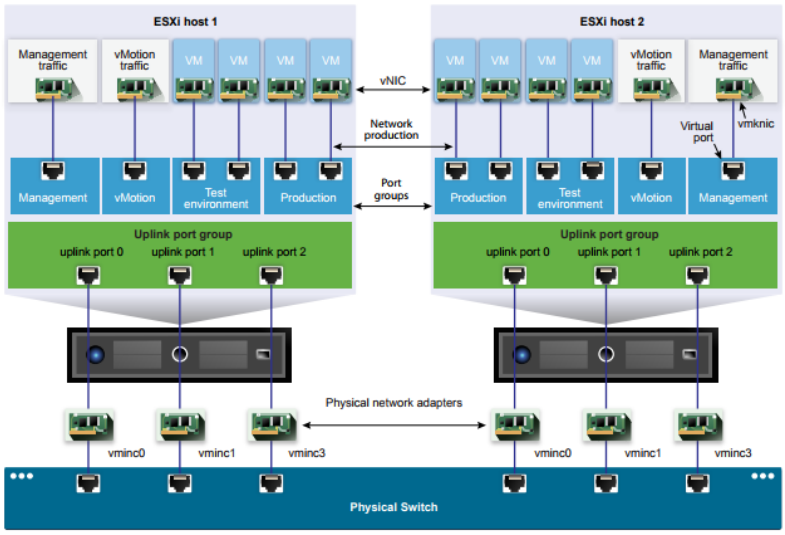

Figura 11 - Arquitetura do vSphere Standard Switch [27]

Os distributed switches (vDS ou dvswitch) são similares aos standards vSwitches, mas têm mais funcionalidades e permitem ultrapassar barreiras físicas e lógicas. A Figura 12 faz um paralelismo entre as duas soluções, tendo em consideração a tecnologia usada pela VMware.

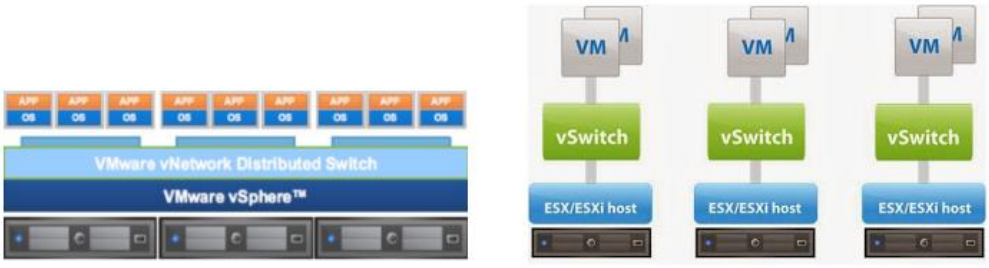

Figura 12 - virtual Distributed Switches vs virtual Standard Switches

Cada VM, à semelhança de uma máquina física, pode ter um ou vários adaptadores de rede (vNIC) com o respetivo IP e *Media Access Control* (MAC) e pertencer a várias VLANs ou vários vSwitches. As

velocidades de comunicação entre a rede virtual e a rede física podem ser diferentes da velocidade de comunicação entre as máquinas virtuais ligada a um mesmo switch virtual. Na rede virtual todo os processos de transferência de dados ocorrem na RAM, eliminando colisões e outros problemas associados ás redes físicas. Conforme em [23] a utilização de adaptadores de rede paravirtuais permitem maior eficiência com menor custo de CPU.

2.3.3.1 Redes de área local e públicas

As redes locais desempenham um papel ativo e de extrema importância numa arquitetura de TI, pois são responsáveis por todo o fluxo de tráfego de "ponta-a-ponta". A esmagadora maioria de redes locais assenta na arquitetura Ethernet, não só pela facilidade de instalação e manutenção, mas também porque tem uma excelente relação custo/desempenho. Um bom design de uma rede local garante a resiliência e acesso ininterrupto aos recursos disponibilizados pela arquitetura de TI. A introdução de plataformas e tecnologias de virtualização, acrescenta novas considerações e maiores exigências a nível de redes locais.

Para garantir a maior largura de banda possível e *uptime* de serviços, devem ser consideradas as configurações que permitam a otimização máxima dos recursos facultados pelos equipamentos. A agregação de portas tem especial interesse em ambientes de virtualização. Tendo em conta que um único servidor físico poderá suportar vários servidores virtuais e centenas de aplicações e que toda a carga de I/O flui pelas interfaces de rede, é necessário evitar "*bootlenecks*" por escassez de largura de banda e garantir a alta disponibilidade, aproveitando todas as interfaces existentes através da sua agregação. A nível de virtualização existem várias politicas de *nic teaming* [42] que poderão ser aplicadas e adaptadas de acordo com os requisitos de vários fabricantes e equipamentos.

Com o aumento de servidores, sistemas e plataformas de virtualização há cada vez mais a necessidade de segmentar o tráfego da rede, assim como isolar zonas, de forma a manter o desempenho e segurança. De acordo com a VMware [43] existem três abordagens recomendadas para atingir este objetivo. A primeira abordagem é através da segmentação por zonas físicas. Uma ilustração desta abordagem é apresentada na Figura 13. A segmentação é alcançada através de dispositivos físicos e não requer alteração da rede local física nem a criação de VLANs. Os *hypervisors* (hosts) são colocados fisicamente em segmentos diferentes o que requer um maior número de *hosts*. A única diferença para uma infraestrutura puramente física é o facto de os servidores estarem virtualizados. Tem como vantagens a simplicidade de configuração. Por outro lado, limita a consolidação e otimização dos recursos que a virtualização pode proporcionar.

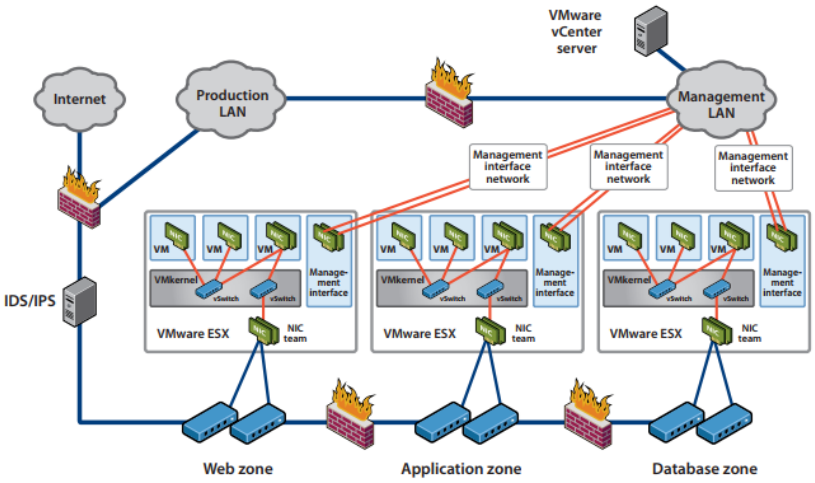

Figura 13 - Segmentação física [43]

A segunda abordagem refere-se à segmentação virtual, através da criação de segmentos com recurso aos switchs virtuais existentes no mesmo *hypervisor*. Utilizando este método é possível ter servidores virtuais com diferentes níveis de segurança dentro do mesmo *hypervisor*. Apesar de estarem incluídos dispositivos físicos de segurança nesta configuração, esta abordagem consolida os servidores virtuais no mesmo host, diminuindo substancialmente o número de servidores físicos (hosts) necessários. A segmentação da rede ocorre tanto no domínio da rede virtual como no domínio da rede física. A Figura 14 ilustra a abordagem de segmentação virtual.

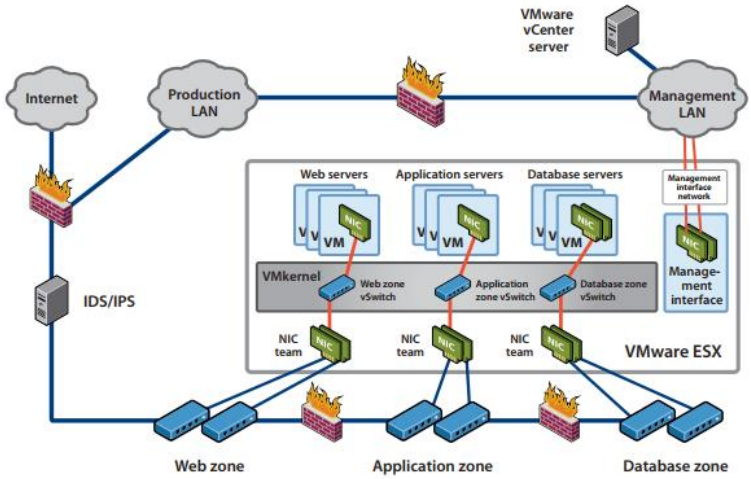

Figura 14 - Segmentação virtual parcial [43]

Por último, a terceira abordagem permite maximizar a consolidação de servidores e dispositivos de segurança de rede através da virtualização, permitindo a segmentação e isolamento de servidores virtuais e redes através da gestão de dispositivos de segurança virtuais (*appliances*). É uma abordagem

totalmente flexível e escalável, no entanto devido à sua complexidade aumenta o risco de más configurações e exige um maior cuidado no seu planeamento e execução. Como vantagens, permite a utilização total dos recursos substituindo dispositivos físicos de segurança por virtuais, menor custo com a aquisição e manutenção de equipamentos e a possibilidade de gestão de toda a rede a partir de um único computador. A Figura 15 ilustra este tipo de segmentação.

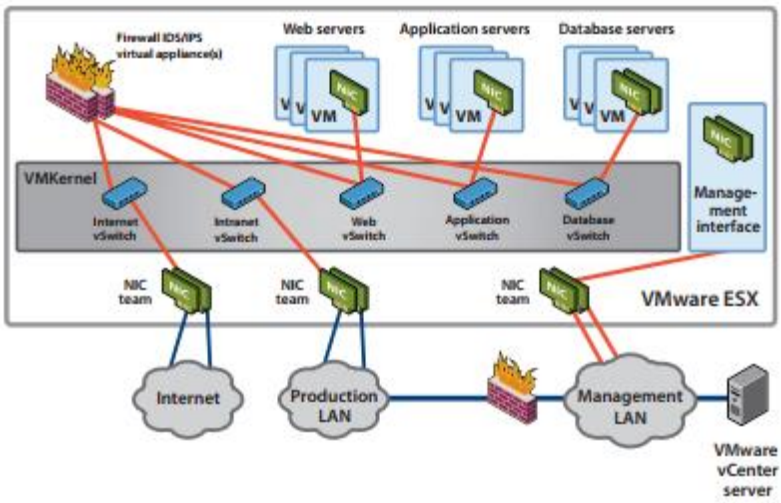

Figura 15 - Segmentação Virtual Total

Recentemente um relatório da IDC [44] demonstra que o mercado mundial de SDN (Software Defined Network), que compreende infraestrutura de rede física, software de virtualização e controlo, aplicativos SDN (incluindo serviços de rede e segurança) e serviços profissionais, terá uma taxa de crescimento anual composta de 53,9% de 2014 a 2020 e valerá aproximadamente US $12,5 mil milhões em 2020. Apesar de ser um conceito relativamente recente e em rápida evolução, é percetível grandes benefícios que esta nova abordagem proporciona relativamente às redes tradicionais. As redes virtuais são independentes do hardware de rede IP subjacente. Assim, a rede física é apenas utilizada como uma *pool* de capacidade de transporte que pode ser consumido e reutilizado conforme as necessidades [45]. Esta abstração é ilustrada na Figura 16.

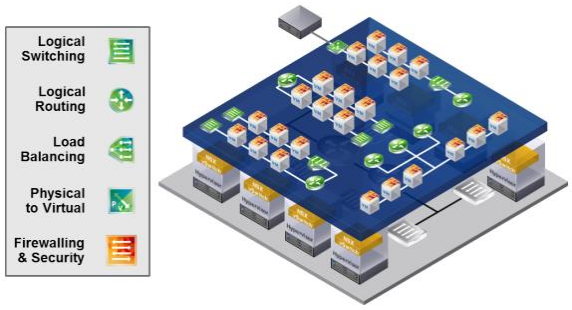

Figura 16 - Camada de abstração de virtualização de rede e infraestrutura subjacente [45]

As redes sem fios locais (*Wireless Local Área Networks*), atualmente são uma componente de arquitetura de TI à qual é atribuída cada vez mais relevância. As exigências e necessidades sobres as *WLANs* são cada vez maiores, devido à rápida proliferação de novos dispositivos e aplicações que dependem deste tipo de rede. As redes sem fios permitem estender o acesso dos recursos suportados pelas redes físicas e virtuais, possibilitando conetividade de forma ubíqua para dados, voz, equipamentos e acesso à Internet.

Conforme em [47], a gestão centralizada e unificada de redes *wireless* permite incrementar a segurança, facilitar a configuração, manutenção, e monitorização de múltiplos dispositivos. Estas controladoras podem ser físicas ou por software, permitindo a centralização da configuração e controlo de *APs*. A realização de *sites survey wireless*, permitem a colocação estratégica dos APs.

A segurança dos acessos a uma *WLAN* é um risco que terá de ser devidamente acautelado, pois devido à abrangência do sinal *wireless,* não é possível limitar de forma efetiva o acesso a partir do meio físico. Por não existir controlo físico, deverão existir mecanismos de proteção da rede sem fios. O IEEE 802.11 refere-se ao conjunto de standards que definem a transmissão e cifra de dados para as WLANs [48]. Os mecanismos mais comuns e simples de implementar foram desenvolvidos com base no padrão 802.11i, pela "Wi-Fi Alliance" [51], sendo conhecidos como WEP, WPA e WPA2. Em *enterprise WLANs,* sempre que possível, recomenda-se a configuração de mecanismos de encriptação WPA2 com AES-CCMP e autenticação 802.1x. A utilização de WEP e WPA não é recomendada devido a vulnerabilidades conhecidas. O design da rede WLAN deverá considerar as tendências e futuras necessidades das organizações, devendo seguir os seguintes conceitos-chave [47]:

- A rede deverá ser escalável e flexível ao longo do tempo para atender ás demandas da organização.
- Os pontos de acesso sem fio (APs) deverão suportar as tecnologias mais recentes como por exemplo o 802.11ac que excede 1 Gbps. A rede física deverá suportar estas e outras velocidades sem necessidade de alteração dos cabos.
- A adoção de equipamentos PoE é recomendada, pois simplifica o controlo energético, evitando custos com passagem de cabos de corrente elétrica. Um único cabo de rede permite a transferência de dados e energia.
- Sempre que possível devem ser adotados os devidos mecanismos de segurança no acesso à rede, para evitar o acesso indevido

Na perspetiva de um arquiteto de TI, a componente Internet deverá ser englobada no design da solução e representa uma preocupação constante em termos de monitorização e segurança. Para além da

necessidade de garantir a estabilidade e performance da Internet, a segurança e controlo de acesso para e da Internet, são fatores que requerem o devido planeamento e consideração. A arquitetura *SAFE* da CISCO [52], é uma abordagem holística na forma em como os locais seguros da rede (*Secure PINs*) modelam a infraestrutura física e os domínios de segurança (*Secure Domain*) representam os aspetos operacionais da rede. Esta arquitetura utiliza têS tipos de fluxo de negócio para simplificar a segurança necessária para as funções empresariais:

- **Fluxos internos**: referem-se às atividades que os colaboradores executam na rede da empresa.
- **Fluxos de terceiros**: são os convidados, vendedores, fornecedores, ou parceiros que acedem à rede da empresa.
- **Fluxos de clientes**: podem ser uma variedade de serviços tais como portais web e informações de clientes.

A arquitetura SAFE estabelece um mapeamento entre a capacidade de segurança e a ameaça presente numa superfície de ataque. A superfície de ataque é definida pelo fluxo de negócio, as pessoas e tecnologia existente. Atualmente, as organizações têm necessidade de conexão permanente com a internet ou redes externas. Os gateways por vezes designados de *routers*, *firewalls* ou *UTMs* [53] são colocados na periferia da rede interna e permitem no mínimo o roteamento do tráfego entra as zonas *LAN* e *WAN*. Atualmente os *gateways* mais evoluídos permitem filtrar todo o tráfego entre 2 ou mais pontos oferecendo proteção contra-ataques, filtros anti-malware e *reporting*, aliados à simplicidade de configuração e monitorização.

2.3.3.2 Redes de armazenamento de dados

A informação é um bem a proteger devendo estar segura e disponível, alinhada com os diferentes requisitos inerentes ás organizações. O volume e velocidade de dados que é criada pelos negócios de hoje, está a fazer com que o armazenamento se torne num investimento estratégico, independentemente do tamanho ou área de negócio das organizações. As organizações têm necessidades de gerir cada vez mais de forma eficiente o armazenamento e a expansão dos volumes de dados, garantir a sua disponibilidade e níveis de acesso. Esta demanda está a impulsionar o movimento do armazenamento para a rede.

As redes de armazenamentos de dados (SANs) surgem assim como uma abordagem flexível, escalável e segura, na gestão e armazenamento de informação. A *Storage Networking Industry Association* (SNIA) [55] define a rede de área de armazenamento (SAN) como uma rede especializada de alta velocidade, que fornece acesso ao armazenamento baseado na escrita e leitura de blocos (*block-level*), através da rede. As SANs também podem abranger várias localizações (*sites*). Uma SAN permite

transferências de dados diretas e de alta velocidade entre servidores e dispositivos de armazenamento, fazendo isto de três formas distintas [54]:

- **Servidor para armazenamento**: este método é o modelo tradicional de interação com dispositivos de armazenamento. A vantagem é que o mesmo dispositivo de armazenamento pode ser acedido em série ou simultaneamente por vários servidores.
- **Servidor para servidor**: uma SAN pode ser usada para comunicações de alta velocidade e alto volume entre servidores.
- **Armazenamento para armazenamento**: capacidade de transferência ou migração de dados direta entre dispositivos. Permite que os dados sejam transferidos sem a intervenção do servidor, libertando os recursos do servidor para outras atividades.

O recurso a uma SAN oferece vários benefícios, sendo que a troca de servidores (de forma isolada) não implica necessariamente a troca dos dispositivos de armazenamento, o que faz das SANs um investimento com maior durabilidade. Conforme em [54], as SANs permitem:

- **Maior disponibilidade aplicacional**: o armazenamento é independente das aplicações e acessível através de vários caminhos de dados (*multipath*), para melhor confiabilidade, disponibilidade e facilidade de manutenção.
- **Maior desempenho das aplicações**: o processamento do armazenamento é externo aos servidores, sendo transferido para uma rede separada, libertando recursos dos servidores (*CPU*, *RAM*) para o processamento das aplicações.
- **Gestão e armazenamento centralizado e consolidado**: simplifica a gestão, aumenta o nível de escalabilidade, flexibilidade e disponibilidade.
- **Transferência de dados e *vaulting* para sites remotos**: possibilidade de efetuar cópias remotas para proteção contra desastres e ataques maliciosos.
- **Segurança**: snapshots, replicação de dados, encriptação.

Atualmente existe um conjunto de componentes e tecnologias, exaustivamente testadas, com base no protocolo SCSI que suportam toda a infraestrutura da SAN. As tecnologias mais utilizadas para SANs conforme [54] são: Fibre Channel (FC); Internet Small Computer System Interface (iSCSI); Fibre Channel over Ethernet (FCoE); Fibre Channel over IP (FCIP); Fibre Channel CONnection (FICON).

Existem dois tipos de abordagem, globalmente aceites, para arquitetar uma SAN, nomeadamente uma abordagem assente num design com recurso ao iSCSI e outra abordagem com recurso à tecnologia Fibre Channel (FC). Devido ao menor *overhead* do FC, comparativamente com o iSCSI, a adoção da FC é a mais utilizada em ambientes sensíveis à latência e com elevados *workloads*. Em termos de comparação, o fabricante DataCore Software [58] afirma que em testes realizados, um HBA FC de 8GB tem até 30%

mais performance que uma NIC iSCSI de 10GB.

Um bom design de uma rede de armazenamento de dados (SAN) passa pela avaliação de diversas considerações tais como [57]:

- **Layout físico**: os locais de edifícios, servidores e sistemas de armazenamento determinam as ligações SAN necessárias.
- **Disponibilidade de dados**: uma SAN resiliente minimiza a vulnerabilidade no *fabric* ou a falhas no dispositivo e maximiza o desempenho.
- **Conetividade**: determinar o número de portas suficientes para ligar servidores, sistemas de armazenamento e componentes do *fabric*.
- **Capacidade de armazenamento**: alinhar os requisitos de capacidade de armazenamento total e determinar o tipo e o número de sistemas de armazenamento necessários para os requisitos atuais e futuros.
- **Plataformas heterogéneas e sistemas operativos**: A SAN deverá ser personalizada para plataformas e sistemas operacionais específicos. Em ambientes heterogêneos, a interoperabilidade dos componentes depende das capacidades e limitações de cada plataforma.
- **Escalabilidade e migração**: o design deverá possibilitar a expansão de forma incremental ao longo do tempo, pois as necessidades de armazenamento e conectividade tendencialmente aumentam.
- **Cópias de segurança e restauro**: garantir a conectividade e largura de banda adequada para maximizar o desempenho do backup baseado em SAN.
- **Tolerância ao desastre**: considerar eventuais requisitos de replicação de dados remotos para garantir a proteção contra falhas do site e recuperação de dados críticos
- **Localização de dados, desempenho e *workloads*:** fornecer um nível adequado de desempenho com base nas cargas de trabalho das aplicações.
- **Gestão**: simplificar a gestão a partir de uma consola centralizada
- **Segurança**: configuração sistemas de alarmística proactivos para garantir a segurança dos dados em toda a SAN e evitar problemas tais como de falta da capacidade e tentativas de acessos indevido entre outros.

Estas considerações permitem o alinhamento e integração de tecnologias de armazenamento de dados, nomeadamente tipo e capacidade de discos, niveis de RAID e *perfomance*, com a reais necessidades da organização para a qual é desenvolvida solução.

2.3.4 Armazenamento de dados

Os sistemas de armazenamento podem suportar várias tecnologias, para consolidar toda a informação numa estrutura eficaz, capaz de proteger os dados, ser escalável, flexível e simplificar a gestão.

Os discos físicos são o local onde toda a informação está armazenada, independentemente da sua localização ou sistema ("*chassi*") de armazenamento. As tecnologias subjacentes à construção dos discos determinam a sua durabilidade, performance, compatibilidade e custo. Os discos rígidos podem ser do tipo mecânicos (HDD) ou baseados em memória flash (SSD), possuindo interfaces do tipo *serial attached SCSI* (SAS), *Serial Advanced Technology Attachment* (SATA) [54] ou o PCIe/PCIe NVMe. Na prática, há uma distinção globalmente aceite que simplifica a identificação dos tipos de discos, não fazendo a distinção entre a interface e o tipo (mecânico ou flash). Assim, convencionou-se que existem 3 tipos de discos [60], nomeadamente:

- **SATA ou NL-SAS**: rotação entre os 5.4 krpm e as 10 krpm, até 90 iops
- **SAS:** velocidade de rotação 7.2 krpm (90 iops), 10 krpm (150 iops), 15 krpm (180 iops)
- **SSD:** discos de alta performance, com tecnologia flash, que poderão permitir mais de 3500 iops

A seleção do tipo de discos está relacionada com as necessidades de desempenho, sendo este o fator com maior impacto no custo, conforme Tabela 2.

Flash - Pros	Flash - Cons
Low cost per IOPS	High cost per Gigabyte
Performance is primary driver	Expensive initial procurement
High performance	
Low power needs	
SAS - Pros	**SAS - Cons**
Low cost per Gigabyte	High cost per IOPS
Capacity is primary driver	Used alone, poor performance
Long history of Reliability	High power needs
SATA - Pros	**SATA - Cons**
Lowest cost per Gigabyte	High cost per IOPS
Capacity is primary driver	Used alone, poor performance
	High power needs
	ATA Commands, half duplex

Tabela 2 -Comparativo do tipo de discos [59]

Um sistema de armazenamento empresarial, além de possibilitar (caso considerado) a redundância de componentes físicos permite a criação de RAIDs de discos. O nível do RAID e o tipo de discos sobre o qual é aplicado define o nível de tolerância à falha e o desempenho. A *cache* presente nas controladoras de discos permitem acelerar o I/O, através de algoritmos de escrita e leitura, como por exemplo o *write-back cache, write-through caching e read-ahead caching* [56]. A escolha do tipo de RAID poderá ser

realizada através da recolha e análise de dados sobre as aplicações e workloads, ou em alternativa, com base na documentação dos fabricantes relativo a práticas recomendadas para determinados cenários.

Para melhorar a eficiência e reduzir custos, os sistemas de armazenamento podem suportar *storage tiering*. Por exemplo, é possível de forma automatizada (*automated tiering*) usar discos mais caros e de elevada performance para armazenar dados críticos e de acesso frequente (*hot data*), e utilizar discos mais baratos e mais lentos para arquivo dos dados como pouco acesso (*cold data*) [54]. Tipicamente existem três camadas (*tiers*) que são categorizadas com base no desempenho e custo por gigabyte [61]: *Performance*: discos SSD; *Standard*: discos SAS; *Archive*: discos NL-SAS / SATA.

O recurso ao *thin provisioning* permite a aquisição de discos apenas quando efetivamente necessário [61] o que poderá permitir poupanças de custos operacionais (OPEX) devido a menor exigências energéticas, e evitar o investimento (CAPEX) antecipado em armazenamento.

2.3.5 Backups e DR

Os dados das organizações são considerados um ativo de elevado valor. A perda de dados pode limitar drasticamente a produtividade dos trabalhadores e em casos extremos pode ameaçar a própria existência de uma organização, prejudicando irremediavelmente a reputação de uma empresa, tornando-a incapaz de servir os clientes [63]. Para evitar tais cenários, os sistemas de backup e recuperação devem assegurar uma proteção contínua de dados, acompanhando as mudanças e novos requisitos da organização. Desenvolver e implementar um plano compreensivo e eficiente de cópias de segurança e recuperação de dados, permite que uma organização se proteja da perda de dados e de *downtimes* dispendiosos que resultam de falhas de hardware ou software, falha de energia, desastre natural, intrusão ou erro humano. Em arquiteturas de backup, é importante entender as várias funções de *backup*. Podemos definir "*backup*" como simplesmente uma ferramenta ou método para executar duas funções principais [64]:

- ***Business Continuity* (BC):** para fornecer uma cópia local de dados a ser utilizada em caso de falha de aplicações, componentes da infraestrutura ou corrupção de dados. Para a continuidade do negócio, é fundamental que o tempo de *downtime* seja o menor possível.
- ***Disaster Recovery* (DR):** para fornecer uma cópia de dados que pode ser mantida fora do *site* e que pode ser restaurada a partir de um outro local.

Uma solução otimizada suportará não só a continuidade do negócio (BC) mas também a recuperação em caso de desastres (DR), este tipo de solução designa-se de plano de "BCDR" [64]. A continuidade do negócio (BC) refere-se ao conjunto de atividades realizadas diariamente para manter a qualidade do serviço, consistência e garantir que as funções críticas do negócio estarão disponíveis para clientes,

fornecedores e outras entidades. A recuperação em caso de desastre (DR) são os processos, políticas e procedimentos relacionados com a preparação para a recuperação, que são vitais para uma organização após um desastre natural ou provocado pelo homem. Enquanto a continuidade do negócio envolve o planeamento para manter todos os aspetos do negócio em funcionamento em meios propícios a eventos disruptivos, a recuperação de desastres concentra-se nos sistemas de TI ou tecnologia que suportam as funções empresariais [64].

As SANs podem facilitar soluções de BCDR devido à maior flexibilidade permitida na ligação de dispositivos de armazenamento a servidores. Na Figura 17 pode-se observar um exemplo de uma arquitetura que envolve uma solução básica de DR.

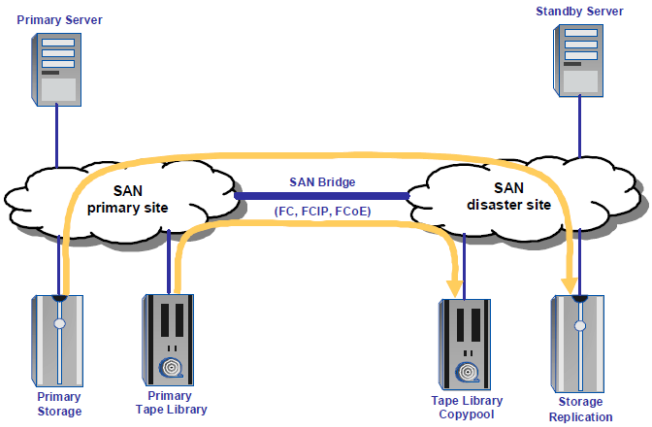

Figura 17 - DR para um site remoto

É importante referir que uma abordagem do tipo "*one-size-fits-all*", não é viável. As estratégias de backup e recovery devem estar estrategicamente alinhadas com os requisitos do negócio, para balancear disponibilidade e custos. Uma boa estratégia de *backup* e recuperação de dados deve definir a proteção adequada de dados críticos e a proteção de dados de baixa prioridade, como por exemplo e-mails, que ainda devem ser retidos para cumprimentos legais ou objetivos competitivos [63]. Esta distinção permite às organizações ajustar e definir com mais precisão os objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO). O RTO é uma métrica utilizada para quantificar o tempo que uma organização pode manter a continuidade do seu negócio sem aceder aos dados em falta, ou o tempo mínimo de reposição de um sistema ou aplicação em caso de falha. Esta métrica exige a classificação do nível de criticidade ou valor para o negócio dos dados ou aplicações. O RPO [64] refere-se ao tempo máximo aceitável para a perda de dados, ou seja, se se considerar um único backup diário, então considera-se que se poderá perder até 24h de dados. Para satisfazer as necessidades de RTO e RPO do negócio devem ser considerados os níveis apropriados de granularidade pelos processos de backup [65]. A granularidade refere-se à possibilidade de recuperação desde o nível de um ficheiro até ao nível de

recuperação total (*bare-metal*).

A proteção contínua de dados (CDP) [58] oferece uma granularidade de um segundo em reversões (*roolbacks*) e fornece o melhor RPO e RTO de qualquer solução de proteção de dados. Uma solução otimizada irá considerar o mínimo de RTO e RPO (se possível 0), tendo em conta as necessidades particulares de cada organização.

A janela temporal associadas *backups*, está condicionada por vários fatores tais como desempenho de equipamentos e software, tamanho e classificação dos dados, métodos de periodicidade dos *backups*. Conforme [64] existem três métodos tradicionais de *backup*:

- **Completo**: maior janela temporal para *backup*, maior necessidade de armazenamento;
- **Incremental**: reduz o tempo de *backup*, mas aumenta o tempo de recuperação por considerar todos os incrementos;
- **Diferencial**: aumenta o tempo de *backup*, mas reduz o tempo de recuperação por considerar apenas o último backup diferencial.

A abordagem para um plano de *backups* pode ser *on-premise*, *cloud* ou hibrida. A abordagem do tipo *on-premise* é a mais utilizada, permitindo um maior controlo e diminuição o RPO e RTO. É comum a utilização de repositórios de *backup* baseados em discos ou unidades de fita (*tapes*). A abordagem em *cloud*, implica a utilização de mecanismos de segurança (e.g., encriptação, VPN) e apresenta uma maior latência resultante de menores larguras de banda. Na abordagem hibrida, são consideradas as outras duas abordagens em que se tenta obter o melhor de ambas, mantendo os níveis de RTO e RPO e simultaneamente os benefícios proporcionados pela *cloud*.[65].

A deduplicação e a compressão são tecnologias utilizadas para diminuir o tamanho dos dados. Em ambientes virtuais normalmente existem VMs que apesar de executarem tarefas distintas têm estruturas idênticas. Nestes ambientes, as poupanças de espaço de armazenamento e a transferência de dados conseguidas com a deduplicação são muito elevadas. Os softwares de backup podem integrar com as APIs do hypervisor e desta forma obter a lista de blocos alterados desde o último backup*, com* base na funcionalidade de *change block tracking* (CBT) [66]. Este método de *backup* conjugado com o método de *snapshot*, permitem a realização de *backups* com pouco ou sem impacto no funcionamento das máquinas virtuais.

A fim de alinhar adequadamente o custo do backup com o valor dos dados, as organizações devem assegurar que informações menos importantes sejam relegadas para menores custos, suportados por dispositivos de menor desempenho. O *Backup Lifecycle Management* (BLM) é uma abordagem

abrangente desenvolvida pela “Asigra” [63] que classifica os dados de backup em dois tipos diferentes: ***Young Backup* Data** (dados fundamentais que uma organização precisa para se manter operacional); ***Old Backup Data*** (dados que não são mais necessárias para o normal funcionamento do negócio).

À medida que a informação passa de "*young*" para "*old*", pode ser movida dentro de um sistema de backup em camadas, onde os dados críticos são copiados e mantidos em sistemas de backup de alto desempenho. Por sua vez os dados antigos e de menor valor são relegados para sistemas de backup de baixo custo. A Figura 18 ilustra uma perspetiva global sobre os vários níveis (*tiers*) de backup e a deslocação dos dados para níveis inferiores ao longo do tempo.

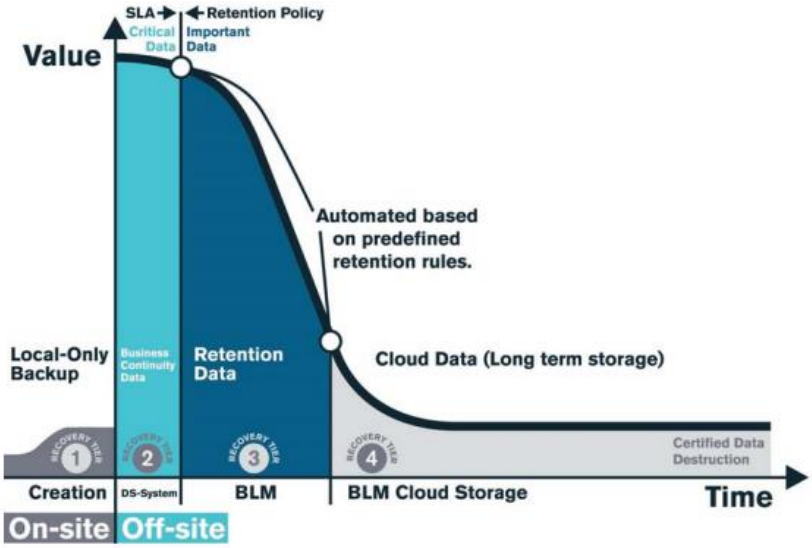

Figura 18 - Backup Lifecycle Management [63]

3 Manual de referência IT Architect - Metodologia

A área de IT está envolta em contantes mudanças. Não só surgem novas tecnologias capazes de concentrar em menor espaço físico capacidades computacionais maiores, como também surgem novos paradigmas de computação que visam acomodar-se à forma como as organizações realizam as suas atividades (e.g. cloud-computing, virtualização, SDN, virtual containers). Ás organizações restam duas alternativas, ou adotam o cenário de constante evolução tecnológica concebendo e alinhando os recursos computacionais para evoluírem neste contexto, ou manter os sistemas tradicionais em funcionamento, o que poderá a médio/longo prazo fazer com que fiquem obsoletos e deixem de responder de forma efetiva a novos requisitos. É certo que a primeira abordagem é a mais indicada, mas tal implica deter conhecimento e pessoas capazes de endereçar a questão da renovação tecnológica em linha com o negócio. Este conhecimento enquadra-se na área de arquitetura de TI que propõe desde logo uma abordagem faseada para a resolução dos vários problemas associados à renovação tecnológica. Os fundamentos teóricos da área sugerem que um projeto deste género poderá ter três abordagens diferentes, nomeadamente:

a) **Renovação**, mantendo a arquitetura de TI existente com a continuidade das tecnologias já implementadas;
b) **Projeto de raiz**, tendo como base de planeamento de toda uma nova arquitetura de TI;
c) **Projeto de evolução**, aproveitando e otimizando tecnologias existentes complementando com novas tecnologias e equipamentos de TI.

Ao longo deste trabalho iremos debruçarmo-nos sobretudo sobre a última abordagem, na qual se enquadra a componente de análise para recolher dados que permitam o correto dimensionamento de uma solução que compreenda a realidade da organização, a definição das necessidades e a respetiva margem de crescimento. A solução a definir, seguindo uma metodologia assente em boas práticas, terá como base um conjunto de tecnologias atuais, devidamente testadas/validadas. Tratando-se da especificação de uma metodologia, não serão discutidas tecnologias em especifico, mas é de salientar que nesta fase é importante conhecer o que existe no mercado e avaliar, por exemplo através de provas de conceito (POC) as mais valias das mesmas para a organização.

3.1 Fases para desenvolvimento de um design de arquitetura

Para o sucesso do desenvolvimento do design de uma arquitetura de TI é necessário segmentar o desenvolvimento em 4 etapas sequenciais e interdependentes. Na Figura 19 são ilustradas as etapas consideradas necessárias para o desenho de uma solução de TI. As etapas são especificadas em [16] e corresponde a um ciclo iterativo através do qual se desenha, implementa, revê e valida a solução.

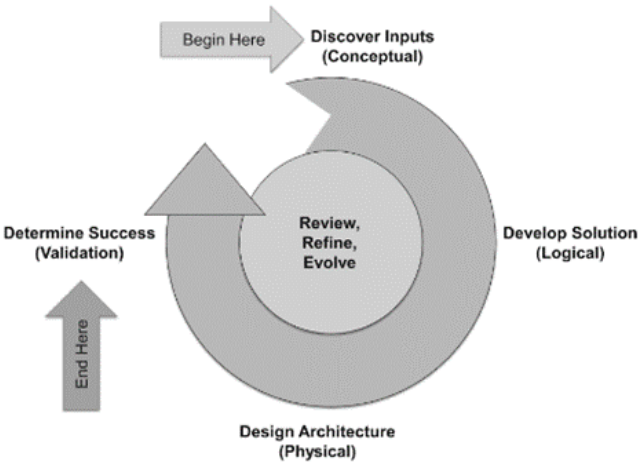

Figura 19 - Etapas para desenhar uma solução de arquitetura de TI [16]

As quatro grandes etapas especificadas para desenhar uma solução, são respetivamente:

1. Na primeira fase, ***Discover Inputs*** é considerado o modelo conceptual. Consiste em identificar requisitos, constrangimentos, riscos e pressupostos. Estes elementos são utilizados para justificar as decisões efetuadas e os modelos escolhidos;
2. A segunda fase, ***Develop Solution*** refere-se ao desenvolvimento da solução e consiste em desenvolver a arquitetura lógica demonstrando o desenho de alto nível sem entrar na especificação das tecnologias utlizadas. Durante esta fase, é criada a solução lógica que permanecerá para além da arquitetura física e demonstrará a relação entre os "*inputs*" e o "*design*";
3. A terceira fase é designada por ***Design the Architecture and Operations*** e define a arquitetura física e os detalhes operacionais da infraestrutura. Nesta fase, são especificados os detalhes da implementação das tecnologias selecionadas e configurações. É também o momento em que os guias de operações conduzem as atividades para garantir o sucesso das operações e da gestão. Nesta fase deverá ser implementada a solução definida;
4. Por último na quarta fase, ***Determine Success***, será efetuado a validação da solução. Esta fase final garante que todos os requisitos foram cumpridos e que os constrangimentos e riscos foram validados garantindo o sucesso do projeto através da validação de componentes críticos e procedimentos.

No entanto, dependendo do grau de complexidade do projeto poderão surgir situações em que se poderá agrupar ou evitar fases. Transversalmente existem atividades designadas por *Review/Refine/Evolve* que, apesar de não ser considerado uma fase, são comuns a todas as outras fases. A análise (*review*) neste contexto não significa revisão, mas sim verificar se a infraestrutura continua a responder às necessidades do negócio. Caso contrário, a solução poderá ser aperfeiçoada/expandida (*refined* /*evolved*) para

suportar novas necessidades. O processo de verificar/otimizar/evoluir pode ocorrer a qualquer ponto do projeto, uma vez que as organizações não são estáticas e podem surgir necessidades após o desenho da solução que obriguem efetuar alterações à solução inicialmente desenhada.

Considerando as fases acima apresentadas, a abordagem proposta para a realização deste projeto consistirá em:

1. Na fase inicial analisar a organização a nível de requisitos estratégicos e de negócio assim como necessidades atuais e urgentes de resolução através de auditorias internas à arquitetura existente (*Discover Inputs*).
2. De seguida, será obtida informação sobre a estratégia e expetativas de crescimento do negócio e realizada a análise da infraestrutura de TI (*Discover Inputs*).
3. Com base nas informações obtidas proceder-se-á ao desenvolvimento e desenho de uma solução de arquitetura de TI ajustada à realidade atual e expetativas futuras da organização (*Develop Solution) e (Design the Architecture and Operations)*.
4. Através de uma visão holística serão analisados vários fatores como a integração, consolidação e segurança de todas as áreas e componentes tecnológicas inerentes à solução arquitetada. Simultaneamente serão realizadas avaliações aos componentes, sistemas e segurança antevendo constrangimentos, necessidades e outros fatores considerados pertinentes, tendo sempre presente a mitigação de risco (*Develop Solution) e (Design the Architecture and Operations)*.
5. Por último, será realizada a implementação prática e respetiva validação em contexto real (*Determine Success)*.

3.2 Desenvolvimento da arquitetura de TI

Os arquitetos de TI têm um papel fundamental na metodologia utilizada na arquitetura de TI organizacional. Os trabalhos desenvolvidos compreendem não só os trabalhos de infraestruturas de grande ou pequena dimensão, mas também todos os aspetos necessários para a solução completa. Se o desenho da solução não for passível de implementação e utilização, então o arquiteto falhou. Os arquitetos deverão ter domínio das considerações a nível de projeto e a nível operacional incluído as considerações basilares inerentes à arquitetura de TI a desenvolver [16]. Tais considerações deverão abranger as seguintes áreas:

- Compreender diferentes estratégias de arquitetura e elaboração;
- Identificar e compreender os requisitos de negócio;
- Validar pressupostos e presunções;
- Identificar constrangimentos e riscos;
- Traduzir requisitos de negócio em requisitos técnicos;

- Tomar e justificar decisões;
- Compreender o impacto das escolhas relativas à solução projetada;
- Compreender como determinar o melhor caminho para uma solução de qualidade.

Na apresentação de um projeto dever-se-á ter em conta as considerações de todos os participantes da reunião. Os participantes poderão ser os *stakeholders* do projeto, colaboradores ou uma comissão de certificação do projeto. Os participantes avaliam a apresentação, e decidem se a solução efetivamente responde a todos os requisitos, constrangimentos e mitigação dos riscos identificados. Há também uma avaliação de como o arquiteto responde ás questões e como justifica as opções e decisões que tomou. A justificação das decisões deverá estar explicita em toda a documentação realizada, incluído a documentação técnica, de negócio e funcional. De acordo com [16] existem três regras importantes a seguir quando se desenvolve um projeto, nomeadamente:

- Utilizar os requisitos de negócio para orientação e suporte das decisões de criação e implementação da arquitetura de TI;
- Assegurar que a solução é adequada para as aplicações criticas assim como outras aplicações que apesar de não criticas são importantes para a continuidade do negócio;
- Assegurar que a solução permita suporte para um ambiente gerenciado e inclua diretrizes operacionais.

Para desenvolver e implementar uma arquitetura de TI, previamente deverão ser desenvolvidas e finalizadas três fases relativas ao design [16]. Em primeiro lugar, é necessário criar o modelo conceptual, uma abstração dos requisitos do negócio e das suas relações. Em segundo lugar desenvolver o design lógico (*logical design*). Tal consiste no desenvolvimento do *layout* de alto nível da arquitetura que irá suportar o modelo conceptual e inclui componentes físicos e lógicos sem referenciar fabricantes, produtos versões ou configurações. Desta forma assegura-se que o design é escalável e resiliente evitando alterações ao longo do tempo a não ser em caso de alteração dos requisitos de negócio. O *logical design* persiste para além do design físico (*physical design*). O desenvolvimento do *physical design* está diretamente relacionado com o *logical design*, sendo um derivado deste. É desenvolvido um *layout* contendo todos os componentes, identificando os fabricantes, produtos, versões e configurações, assim como a sua conetividade. O *physical design* poderá sofrer alterações ao longo do tempo à medida que novas tecnologias são introduzidas e tecnologias mais antigas são substituídas.

Para suportar o desenvolvimento de cada uma desta fases do design da arquitetura de TI, é necessário realizar tarefas de avaliação e levantamento de requisitos baseados nas necessidades de negócio, funcionalidades e tecnologias que são utilizadas para suportar o negócio. Um exemplo de um método utilizado durante a tarefa de levantamento de requisitos é o *virtualization assessment*. Através deste

método são analisados os sistemas candidatos para ser virtualizados, sendo identificados e definidos os recursos necessários para os sistemas. Esta avaliação poderá ser realizada em sistemas físicos ou sistemas virtuais existentes, permitindo a recolha de informações para dimensionar os componentes constituintes do *physical design*. Uma avaliação da virtualização para servidores por si só não permite identificar necessidades a nível aplicacional [16]. Para determinar se as aplicações a correr nos servidores físicos analisados poderão correr numa infraestrutura virtualizada, poderá ser necessário recorrer-se à avaliação das aplicações como uma extensão da avaliação da virtualização de forma a percecionar dependências, funcionalidades e necessidades de interoperabilidade. A avaliação de segurança na virtualização de servidores irá ajudar a identificar eventuais problemas e constrangimentos relativos à segurança da infraestrutura virtual e a estabelecer e otimizar medidas e controlos, para mitigação de qualquer risco identificado.

Outra ferramenta utilizada durante a fase de levantamento de requisitos é o *health check* [16]. Esta ferramenta permite uma análise de base a um determinado ambiente e compara a infraestrutura existente com a aplicação de boas práticas. Estas boas práticas são baseadas na tecnologia e experiência no terreno englobando clientes, fabricantes e consultores. Apesar de normalmente a utilização de boas práticas ser aplicável à maioria dos cenários, poderão existir casos específicos em que a sua aplicação não será possível ou recomendada. A teoria da contingência pode ser aplicada em relação ao uso de boas práticas, pois existem situações internas e externas que podem conduzir à aplicação de uma prática recomendada específica para uma determinada solução, que não se enquadre nas boas práticas padronizadas. A maior parte dos *health checks* são baseados em comparativos com arquiteturas de referência base [16]. As arquiteturas de referência base proporcionam detalhes de como uma determinada tecnologia pode ser implementada. Em alguns casos a arquitetura de referência é fornecida pelo fabricante, podendo ser alterada e adaptada para se adequar aos requisitos de negócio. Em outros casos a arquitetura de referência é criada para suprir as necessidades de uma determinada área de negócio, atuando em paralelo como uma linha base para desenvolvimentos futuros e como *checkpoint* durante o ciclo de desenvolvimento de uma infraestrutura de TI.

Tal como referido anteriormente existem, transversalmente às quatro fases do desenvolvimento de uma solução de arquitetura de TI, as atividades "Review/Refine/Evolve". Estas atividades definem e avaliam as operações realizadas ao longo do projeto e durante a vida útil da infraestrutura. Desta forma é possível ajustar os projetos ás novas necessidades, consequentes das alterações dos requisitos de negócio que afetam o desenho inicial da infraestrutura. Estas atividades fluem durante a fase de descoberta de *inputs* para desenvolver o modelo conceptual, da fase de desenvolvimento da solução ou modelo lógico da arquitetura, da fase de desenvolvimento e criação do modelo físico da arquitetura e da fase final que consiste na validação da solução incluindo testes aos requisitos do projeto. Apesar de uma forma

simplista o desenvolvimento ser divido em quatro fases, na realidade a maior parte das infraestruturas de TI têm um ciclo de vida dinâmico. Uma solução implementada hoje muito provavelmente sofrerá várias alterações de forma a ser adaptada aos novos requisitos que irão surgir. Assim, e de acordo com [16], cada projeto é considerado completo na medida em que responde às necessidades, mas continuamente evolutivo e adaptativo para responder aos desafios criados por novas necessidades relativas às dinâmicas inerentes ao negócio.

3.2.1 Arquitetura Conceptual – (Perspetiva do Proprietário)

A arquitetura conceptual é utilizada para demonstrar de uma forma abstrata os componentes necessários de um sistema, relativamente ao conjunto de requisitos previamente identificados [16]. Apesar de não existirem detalhes específicos, são incluídas as relações e componentes que irão influenciar o modelo lógico. O objetivo da arquitetura conceptual é elevar a solução para que a abordagem escolhida seja entendível a pessoal não técnico. Os requisitos e ambientes são traduzidos de forma abstrata em ideias e as suas relações [16]. As ideias e relações referem-se aos objetivos e expetativas da organização e ás suas relações com as necessidades e requisitos (abstratos) inerentes à sua obtenção. Esta arquitetura é formalizada através de diagramas e textos que transmitem de forma abstrata uma representação inicial e não técnica do modelo a desenvolver. Engloba decisões que irão influenciar a composição do design subjacente, incluindo pontos chave da arquitetura.

Um exemplo (básico) de arquitetura conceptual para uma organização com a necessidade de uma infraestrutura para um centro de dados, que lhe permita correr o seu negócio resultará em algo como:

- O responsável da organização pretende uma infraestrutura que suporte todas as aplicações necessárias à continuidade e evolução do negócio;
- O responsável da organização pretende suporte para virtualização de servidores e postos de trabalho através de uma solução hibrida em *cloud* para reduzir o TCO, aumentar o ROI e suportar a agilidade do negócio;
- A infraestrutura requer recursos específicos para suportar as cargas de trabalho das aplicações, tais como capacidade de processamento, conetividade e armazenamento;
- A infraestrutura deverá suportar mecanismos de segurança;
- A infraestrutura deverá permitir mecanismos de recuperação tais como cópias de segurança/restauro e alta disponibilidade.

Na arquitetura conceptual existe apenas informação genérica, mas não detalhes específicos. A arquitetura lógica englobará os componentes genéricos e as especificações tais como a utilização de tecnologias de virtualização. A arquitetura física irá incluir componentes específicos e especificações

tais como por exemplo tecnologias e configurações. A Figura 20 ilustra a relação entre o modelo conceptual, lógico e físico.

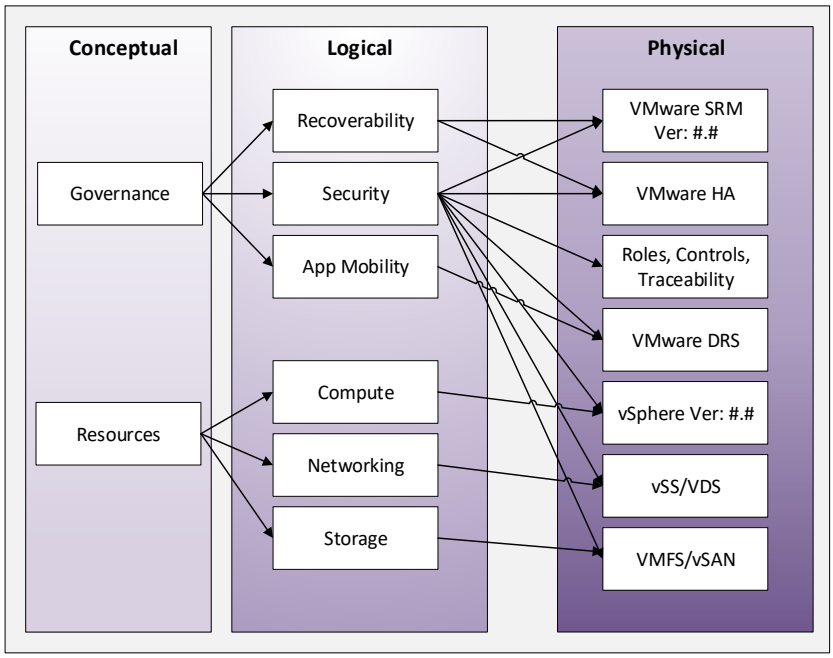

Figura 20 - Relação entre o modelo conceptual, lógico e físico [16]

3.2.2 Arquitetura Lógica – (Perspetiva do Arquiteto)

A arquitetura lógica tem como base o modelo conceptual, permitindo uma visão mais detalhada dos componentes e relações, que serão necessários para atingir as funcionalidades e os objetivos definidos. A Figura 21 é um exemplo de uma arquitetura lógica para um componente pertencente a essa mesma arquitetura (um nó computacional no caso). Os vários blocos constituintes da arquitetura lógica são unidos através de relações interligando os requisitos de negócio identificados na arquitetura conceptual e os componentes de infraestrutura que os suportam.

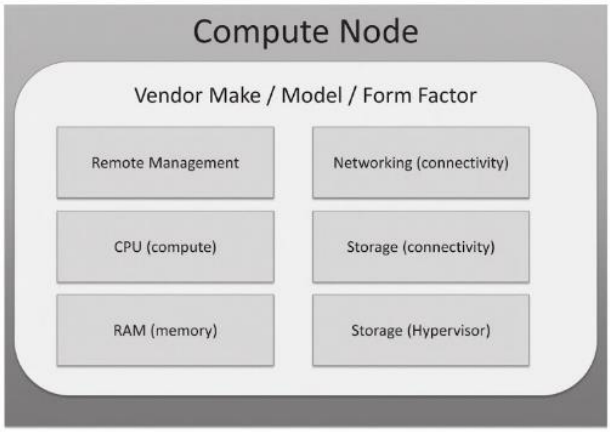

Figura 21 - Exemplo de um componente de arquitetura lógica [16]

Através de um exemplo como o ilustrado na Figura 21 é possível apresentar, de uma forma inicial, os componentes que compõem o bloco servidor. Diagramas posteriores podem conter informação sobre clusters de servidores como um bloco único, sem incluir detalhes específicos de cada bloco de servidor. Desta forma, é possível criar uma arquitetura de referência de componentes, que podem ser alterados conforme as mudanças de requisitos ou constrangimentos, sem alterar toda a arquitetura lógica. Este exemplo é apenas uma demonstração de como apresentar este tipo de informação, pois cada projeto terá componente lógicos diferentes adaptados à arquitetura pretendida. Por exemplo, no *design* de infraestrutura com arquitetura de referência VMware vSphere, existem outros itens específicos a examinar, tais como o VMware vCenter, Storage Arrays ou segmentação da rede assim como componentes externos (e.g.: soluções de *backup*).

Em [16] são apresentados itens adicionais organizados por objetivos que podem ser incluídos, dependendo da solução a desenvolver. De entre esses itens destacam-se:

- Objetivos de negócio
    - Consolidação de servidores
    - Continuidade do negócio
- Objetivos do ciclo de vida (lifecycle)
    - Arquitetar
    - Implementar
    - Atualizar
    - Monitorizar
    - Recuperar
    - Retirar (de produção)
- Continuidade de negócio e conformidade
    - Proteção de dados

    - Alta disponibilidade
    - Recuperação em caso de desastre
    - Conformidade
- Localização dos *data center*
    - Interno (na empresa)
    - Extranet empresarial
    - Provedor de serviço
    - Escritório remoto ou filial
- Atividades
    - Aprovisionamento
    - Consumo
    - Resolução de problemas

Os itens deverão ser considerados conforme as necessidades do design arquitetado.

3.2.3 Arquitetura Física – (Perspetiva do Fabricante)

A arquitetura física refere-se a produtos, protocolos e representação de dados. De acordo com [39] e [16] a arquitetura física proporciona a visão detalhada das especificações dos componentes e interfaces. Nela devem ser especificados fabricantes, modelos e versões dos componentes (por exemplo "conexão de 1Gbps Ethernet, através de adaptadores de rede Intel (I350-T4), com cabo CAT-6 UTP, ligado a um switch Cisco 6513").

Quando se seleciona *hardware* especifico, deve-se considerar a solução como um todo, incluído os requisitos de negócio e os constrangimentos inerentes ao projeto. A criação de um design físico, de acordo com [16], não se limita só a satisfazer os requisitos do projeto. Deve também considerar-se a nível operacional, todos os aspetos referentes ás atividades de manutenção e continuidade do mesmo. Na medida de possível deverá incluir a eliminação de pontos únicos de falha e as considerações de como manter todos os itens incluídos no design. A validação das decisões tomadas, padrões de design, características operacionais e funcionalidades técnicas é um passo fundamental no processo de design físico.

3.2.4 Metodologia de Avaliação

Para desenhar uma boa solução é necessário e importante obter informações sobre o estado passado, presente e expetativas futuras [16]. O estado futuro está diretamente relacionado com o planeamento da

capacidade, ou seja, garantir que a solução desenvolvida e implementada no presente seja suportada à medida que o ambiente se altera. Ao formular um projeto é necessário obter o máximo de informação relevante através de questões, análises e avaliações tecnológicas. Com base nestas informações é necessário definir prioridades e alinhar com o design a desenvolver e que as irá suportar. A metodologia de avaliação engloba os seguintes itens:

- **A análise e avaliação do estado atual**: traduz-se na revisão da infraestrutura existente através da análise de *hardware* e *software* [16]. A infraestrutura existente poderá ser física, virtual ou baseada em *cloud*. O *hardware* físico, sistema operativo e *footprint* das aplicações são tidos em consideração para o *design*. A análise será composta por diversas informações e comentários sobre a infraestrutura na sua totalidade. A avaliação da infraestrutura deverá incidir sobre a conetividade, sistemas de armazenamento, componentes e possibilidades de evolução ou continuidade da infraestrutura existente. A perceção e compreensão de fatores, tais como, problemas, constrangimentos, capacidade atual, performance e requisitos permite uma comparação entre o design atual e design futuro com os recursos a considerar (GAP Analysis).
- ***Data Points***: A recolha de pontos de análise deverá ser realizada de forma continua num determinado espaço temporal. Uma análise típica poderá ficar completa normalmente em 30 dias de recolha de estatísticas de utilização de recursos. A experiência reportada no estado da arte [16] indica que são necessários entre 30 a 90 dias de *data points* sobre a utilização de recursos e atividades, para desenvolver um design bem-sucedido. Esta informação é utilizada para determinar os requisitos em termos de recursos para as máquinas físicas ou virtuais que irão suportar o processamento e armazenamento do trabalho realizado. Se possível deverão ser identificadas as dependências físicas externas tais como chaves de proteção do software e licenciamento (chaves HASP) e dispositivos de I/O.
- **Recomendações**: são consequentes da análise e são agrupadas em classes: "melhor escolha" e "alternativa". Se a "melhor escolha" não puder ser a opção, então a "alternativa" deverá ser adequada aos requisitos especificados e ao orçamento disponível. Os projetos são limitados pelos orçamentos permitidos ou negociados, sendo que esta consideração deverá ser tomada em conta para evitar trabalhos e constrangimentos no desenvolvimento da arquitetura. As recomendações deverão ter sempre em linha de conta os requisitos de negócio, constrangimentos, boas práticas e a experiência.
- **Avaliação financeira**: a disponibilidade de verbas financeiras é um fator condicionante em qualquer projeto. Em termos financeiros, as propostas subjacentes a um design bem-sucedido deverão estar alinhadas com os orçamentos disponíveis (*budget*) de forma a determinar o que se irá enquadrar dentro dos seus limites. Em alguns casos o *budget* poderá pré-determinar a iniciativa, e a solução terá de se limitar ao orçamento disponível. Em outros casos o orçamento poderá ser flexível dependendo dos potenciais benefícios, tais como redução de custos e

perspetivas futuras. Uma das responsabilidades de um arquiteto de sistemas de TI, é ajudar a organização a identificar e quantificar os benefícios esperados assim como qualquer redução de custos projetada. Isto irá permitir a justificação dos fundos necessários para suportar um projeto bem-sucedido e simultaneamente ajudar a organização a adotar uma perspetiva global do projeto [16]. Independentemente da origem dos fundos ou estratégia da organização a nível financeiro, é muito importante perceber o impacto financeiro que uma decisão poderá provocar no projeto.

3.2.5 Caraterísticas do design

As características do design representam os fatores a ter em consideração para desenvolver uma infraestrutura de TI. Um bom design permite alcançar os requisitos, com tecnologias adequadas e processos operacionais devidamente documentados, dentro do orçamento e do tempo estimado. Os requisitos, constrangimentos e presunções são mapeados em um ou mais dos seguintes fatores [16]:

- **Disponibilidade do serviço:** característica que define o tempo de atividade suportado pelos componentes tendo em conta o *workload*. O design deverá permitir altas taxas de disponibilidade dos componentes considerados críticos para a organização. A alta disponibilidade de recursos é assim uma caraterística relevante na solução arquitetada;
- **Capacidade de gestão:** efeito na facilidade de gestão do ambiente e manutenção das operações de rotina.
- **Desempenho:** efeito na performance das aplicações, sistemas operativos e componentes.
- **Recuperação:** efeito sobre a capacidade de recuperação da infraestrutura, cargas de trabalho e dados em caso de falhas inesperadas que afetem a disponibilidade do ambiente.
- **Segurança:** efeito na infraestrutura e *workloads*, incluindo componentes e sistemas para cumprir os requisitos de segurança do projeto. O design deverá fornecer controlo generalizado dos dados, confidencialidade, integridade, acessibilidade e gestão de risco, incluindo a capacidade de demonstrar ou alcançar o cumprimento com a regulamentação.

3.2.6 Considerações para o design

A criação de um design envolve a consideração de vários aspetos. Durante a fase de análise e descoberta junto da organização, esses aspetos referem-se a:

- **Requisitos**: os requisitos podem ser diretos ou indiretos e são inerentes à organização. Um requisito direto poderá estar relacionado com um nível de serviço (SLA). Um requisito indireto pode derivar da regulamentação como por exemplo requisitos de conformidades ou politicas de segurança.

- **Constrangimentos**: os constrangimentos são considerações normalmente difíceis de alterar. Um exemplo poderá ser falta de *budget* para o projeto ou uma escolha pré-determinada do fabricante por parte do cliente.
- **Riscos**: os riscos estão relacionados com o negócio ou com a infraestrutura de apoio ao negócio. Podem ser técnicos ou não técnicos. O risco técnico com por exemplo uma falha de um dispositivo, poderá ser endereçado através de redundância ou tolerância à falha. Um risco não técnico como por exemplo um tremor de terra poderá causar danos num determinado local, mas poderá não ser critico caso exista redundância do datacenter num outro local. É importante identificar os riscos presentes em qualquer design, avaliar o impacto e potenciais estratégias de mitigação, de forma a eliminar ou minorar o dano do risco identificado.
- **Presunções**: as presunções são considerações que devem ser validadas. Um exemplo de uma presunção poderá ser o facto de se assumir que organização possui pessoal devidamente treinado e com conhecimentos para gerir a solução que foi desenhada e implementada. Caso as presunções não sejam validadas o resultado final poderá ser a falha do projeto.

3.2.7 Metodologia para o manual de referência IT Architect

Considerando o apresentado ao longo deste capítulo, vamos nesta secção apresentar de forma sintética e esquematizada a metodologia adotada para o Manual de referência IT Architect. Com base no estudo das frameworks e metodologias já referidas, na Figura 22 é esquematizado o modelo da metodologia desenvolvida e proposta que cobre todo o ciclo de vida de um projeto de arquitetura de TI. Começa na fase da descoberta e finaliza com a monitorização da solução e atualização (contínua) da documentação.

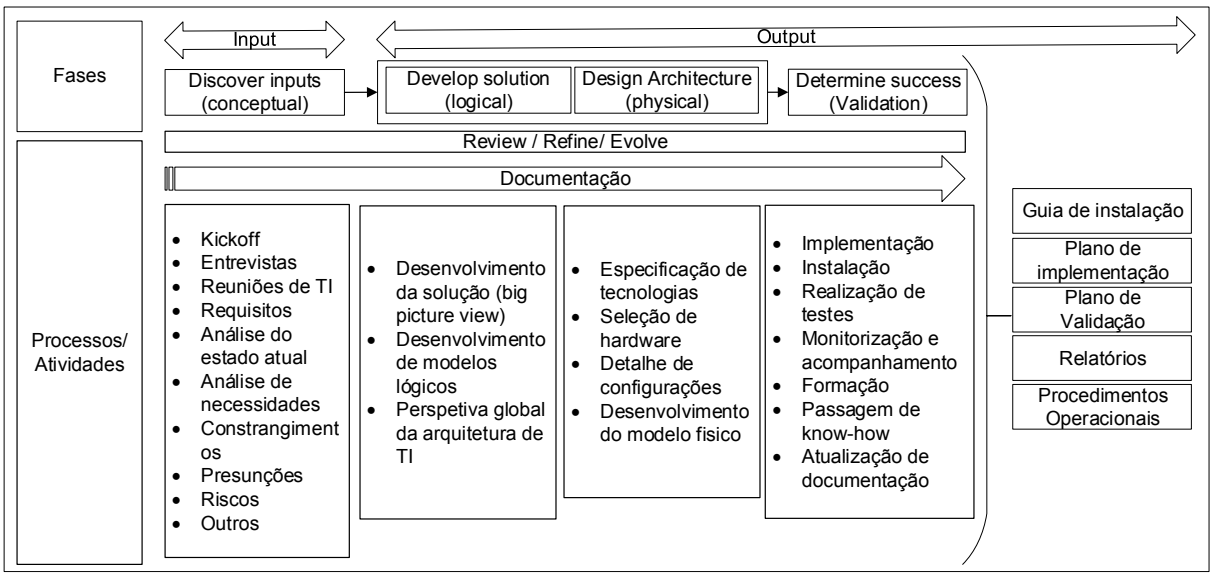

Figura 22 - Esquema da Metodologia proposta

Cada uma das fases é composta por processos e atividades a desenvolver. Os processos e atividades permitem o avanço do projeto até à sua conclusão. Transversalmente a todas as fases há a necessidade continua de verificar se está tudo em conformidade, com os objetivos estabelecidos ou requisitos que entretanto sofreram alterações, realizando ajustes caso necessário. O projeto termina com a passagem de *know-how* e documentação atualizada de todo o projeto.

A documentação é um aspeto por vezes negligenciado e desvalorizado, no entanto tem um papel fundamental durante todas as fases do projeto e permanecerá para além do mesmo. A documentação contribui para a correta continuidade e evolução do projeto e poderá servir de base a novos projetos. O conjunto de documentos realizados deverá abranger todo o projeto, sendo da responsabilidade do arquiteto determinar como serão criados os documentos e a forma de apresentação destes na solução. O guia de instalação fornece os detalhes da instalação e configuração da solução, adequada à organização. O plano de implementação fornece os detalhes das estimativas temporais do projeto e formação. Inclui funções, alocação de responsabilidades, cronogramas e orientações. O plano de validação considera o design de forma global e fornece os testes que deverão ser efetuados de forma a assegurar o sucesso da solução. Poderá incluir testes unitários (ULT), testes a nível do sistema (SLT), testes a nível de integração (ILT), testes de performance/stress, assim como outros testes considerados apropriados à validação da solução. Os procedimentos operacionais fornecem as atividades regulares necessárias para a equipa de suporte de TI. Inclui as atividades recorrentes e agendadas. Também deverá incluir atividades menos frequentes que estão documentadas para suportar a estabilidade e sustentabilidade.

O desenvolvimento de um projeto de arquitetura de TI inclui vários componentes que serão criados. O design da arquitetura, guia de instalação, plano de implementação, plano de validação e procedimentos operacionais são o mínimo de componentes a incluir no projeto. O design da arquitetura inclui o design funcional e técnico. O design funcional inclui requisitos, constrangimentos, pressupostos, riscos e uma lista de itens *out-of-scope* [16]. O design técnico inclui o design conceptual, design lógico, design físico, assim como as considerações, diagramas e tabelas que suportam a solução. As justificações e implicações das considerações do design são relevantes para inclusão na documentação para o proprietário, arquiteto e implementador da solução. Com base na figura 5 de [16], procedeu-se à criação da tabela 3, onde se identificam as diferentes fases, ações e itens a considerar.

Fase	**Ação**	**Itens**	**Observações**
Input	Reunião de Kick-off	• conhecimento das entidades envolvidas (responsáveis, stakeholders e equipa associada ao projeto) • componentes iniciais do modelo	Esta reunião é de extrema importância, pois além de marcar o arranque, define as orientações iniciais do projeto.

		conceptual	
Input	Entrevistas Reuniões de TI	• definição de conceitos chave • validação de presunções • resolução de conflitos • requisitos e constrangimentos.	Permite obter uma visão geral e ou detalhada das dificuldades e expetativas da organização.
Input	Análise do estado da atual	• o ambiente existente • infraestruturas • tecnologias • atividades de TI • workloads • requisitos e constrangimentos • riscos • dependências técnicas • dependências operacionais	Uma análise do estado atual é tipicamente realizada para constatação da realidade da organização assente nos vários itens.
Input	Planeamento de capacidade	• análise de capacidade • escalabilidade • recursos	Permite determinar as atuais capacidades e a sua escalabilidade para suportar o design que será criado. Diversos fabricantes têm ferramentas que poderão ajudar na análise de capacidade. A VMware, por exemplo, disponibiliza uma ferramenta denominada de "Capacity Planner". O resultado desta análise ajuda na determinação de padrões e tecnologias que irão suportar o projeto. Uma revisão da documentação existente (caso possível), será uma mais valia para entender o ambiente, processos de negócio e aplicações suportadas pela infraestrutura existente. [16]
Input	Revisão da documentação existente	• perceção do ambiente • perceção dos processos de negócio • aplicações existentes	Caso exista, a documentação existente facilita o entendimento e o que justifica a realidade da organização em termos de TI
Input	Avaliação de prontidão operacional	• capacidade de respostas • níveis de eficiência	O grau de prontidão (tecnologia e operações), permite desenvolver documentação e identificar necessidades de

			formação necessário à solução a desenvolver
Input	Análise de segurança e regulamentações	• especificações de compatibilidade • controlo e gestão	Fatores como politicas internas e externas condicionam a gestão e controlo dos recursos de TI. É necessário garantir a conformidade a todos os níveis.
Lógica	Desenvolvimento da solução (*big picture view*)	• perspetiva global da arquitetura de TI • Componentes • relações	A criação de um modelo lógico permite de abstrair e subentender as necessidades da organização em alto nível.
Física	Desenvolvimento do design físico	• especificação de tecnologias • Seleção de hardware • Detalhe de configurações • Desenvolvimento do modelo físico	A criação de um modelo físico permite detalhar tecnologias, configurações e decisões técnicas.
Validação	Implementação	• testes tolerância a falhas • testes funcionais • testes de desempenho • monitorização • formação • Passagem de *Know How* • atualização de documentação • fecho do projeto	Implementar a solução permite validar a solução desenhada. A correta implementação é critica para o sucesso da solução, e das tecnologias incorporadas

Tabela 3 - Resumo de ações e considerações por fase

As decisões ao nível do design irão suportar os requisitos do projeto direta ou indiretamente. Quando uma determinada tecnologia é necessária para atingir um objetivo do design, é importante justificar esta decisão. Por cada decisão há um impacto pretendido, vantagens e desvantagens e podem afetar outras áreas positiva ou negativamente. Em cada uma destas decisões, as desvantagens poderão ser identificadas como riscos potenciais. As áreas de maior risco deverão ser resumidas no inicio ou no final do design. Os riscos menores poderão ser introduzidos na área de apresentação das decisões do design. A gestão de risco de acordo com a ISO 31000 [40] é utilizada para definir um conjunto de ações estratégicas, como identificação, administração, condução e prevenção de riscos ligados a uma determinada atividade. No caso das atividades ligadas às tecnologias de informação, a gestão de risco é baseada na análise, design e operações. Inclui identificação de riscos, avaliação de probabilidades e priorização. Assim, a gestão de riscos é focada na diminuição do impacto através da monitorização e controlo. O seu sucesso significa identificar, perceber e mitigar os riscos. Em termos de infraestrutura de TI, são avaliados pontos únicos de falha, falhas a nível de sistemas e a nível de localização física. A mitigação poderá incluir redundância de hardware, software e instalações físicas.

Independentemente da metodologia aplicada, o arquiteto de TI é responsável pelo sucesso da solução. Cada arquitetura de TI é única e o objetivo é responder aos requisitos da organização para a qual foi desenvolvida. A metodologia aqui referenciada abrange todos os aspetos considerados necessários ao correto planeamento e implementação de uma solução, tendo em linha de conta a evolução e adaptação a novos ambientes.

4 Manual de referência IT Architect - Caso de estudo

Neste capítulo apresentamos o resultado da adoção dos princípios de arquitetura IT a um caso real. Trata-se de uma empresa com um elevado nível de crescimento e com necessidades dinâmicas na área de TI. É uma empresa que não dispôs de um perfil técnico para o aconselhamento/planeamento da evolução de TI, tornando-se assim um bom caso para aplicar as fases detalhadas no capítulo anterior.

4.1 Enquadramento

A organização alvo deste estudo desenvolve a sua área de negócio no ramo da construção civil e energias renováveis, tendo já uma forte presença no mercado (Portugal, Angola, Chile e Polónia). Possui aproximadamente 400 trabalhadores diretos e geograficamente distribuídos. Nesta empresa e devido a um inúmero conjunto de fatores, existe uma grande incerteza sobre a qualidade e capacidade evolutiva da sua infraestrutura de TI. A quase inexistência de documentação, faz com que qualquer problema possa causar graves constrangimentos na continuidade de negócio e levar a eventuais perdas de informação. As queixas por *downtime* estão tendencialmente a aumentar e apesar de existir consciência de alguns riscos, estes não estão devidamente identificados nem existe qualquer tipo de plano de mitigação. Outra grande preocupação é a segurança da informação. Devido à dimensão quer em número de utilizadores quer em localizações geográficas há grandes receios de perdas de dados e de eventuais acessos externos não autorizados.

4.2 Desenvolvimento da Arquitetura

Tal como apresentado no capítulo anterior, o desenvolvimento da arquitetura de TI implica a criação do design conceptual, lógico e físico com base em *inputs* relativos ao levantamento da situação atual e criação de modelos. Estes modelos proporcionam as orientações (*guidelines*) durante todo o ciclo de vida da arquitetura de TI e definem o tipo de abordagem em cada uma das situações a resolver. Ao longo das próximas subseções percorremos cada uma das fases subjacentes ao desenvolvimento da arquitetura de TI.

4.2.1 Avaliação do estado atual (*Discover Inputs*)

Para determinar o estado da arquitetura de TI, no *kick-off* do projeto foram realizadas reuniões presenciais com elementos chave da organização (TI e administrativos). O objetivo destas reuniões foi definir em linguagem de alto nível os requisitos, bem como identificar constrangimentos e pressupostos.

Com base nesta informação foram definidas orientações e tomadas decisões que permitiram a definição dos requisitos de alto nível, conforme os seguintes:

- A solução terá de permitir a consolidação, personalização, integração e armazenamento de todo o conjunto de interações resultantes dos movimentos transacionais e das necessidades aplicacionais dos utilizadores;
- A solução deverá reaproveitar na medida do possível os equipamentos existentes, através da sua reconfiguração ou *upgrade* conforme necessário;
- A solução deverá incluir tecnologias de virtualização, tornando-a mais flexível e escalável, reduzindo o TCO, aumentar o ROI e suportar a agilidade do negócio;
- A segurança do sistema é considerada critica, especialmente na acessibilidade e controlo de acessos (físicos ou remotos), assim como na conetividade *site-to-site*;
- Devido à tendência de crescimento acentuado de dados, devem ser consideradas as necessidades de armazenamento, margem de crescimento e facilidade de expansão;
- A solução deverá suportar o upgrade do ERP SAP (Windows/Sybase) para a versão SAP HANA (Windows/HANA e Linux/HANA), conforme requisitos a especificar pelo fabricante e parceiros, considerando a tendencial evolução do crescimento das bases de dados e adição futura de desenvolvimentos ou novos módulos;
- O acesso à infraestrutura deverá possuir mecanismos de segurança (físicos e lógicos);
- Deverá existir um plano proactivo de segurança de dados, e mecanismos que permitam a continuidade do negócio e recuperação de dados.

4.2.2 Análise da infraestrutura atual

Nesta fase procedeu-se à análise da infraestrutura de TI existente. Tal foi feito através da realização de auditorias e análises aos vários componentes da infraestrutura: conetividade, servidores, armazenamento, segurança e mecanismos de *BCDR*. Na Figura 23 é ilustrada a arquitetura lógica atual.

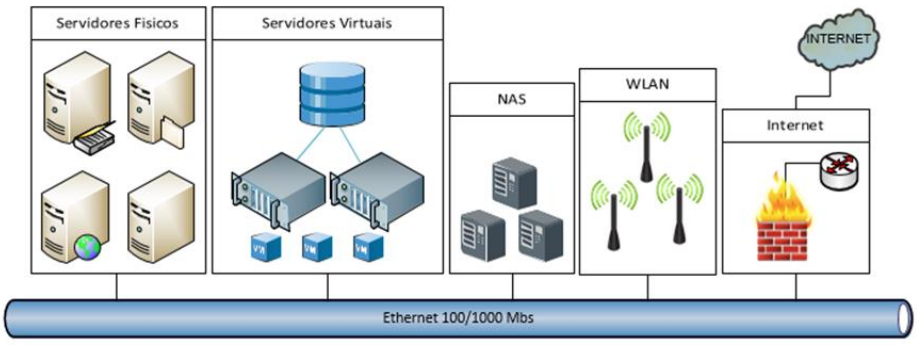

Figura 23 - Arquitetura da infraestrutura do caso de estudo

4.2.2.1 Conetividade - estado atual

A infraestrutura física de cablagem e equipamentos de *networking* constitui um ponto crítico no bom e estável funcionamento de um sistema informático, sendo por isso extremamente importante a sua correta configuração e otimização.

A nível de conetividade constatou-se que a LAN era composta por três bastidores de rede com *uplinks* através de cabo de fibra ótica multimodo, criando uma rede em topologia estrela. O bastidor 1 de rede tem um total de 42U e está instalado fisicamente na sala do *data center.* É composto por 1 switch PoE ZYXEL GS2210-24HP dedicado a telefones IP PoE, 1 switch CISCO DSG-300 28P como switch "*core*", 1 switch D-Link DGS 1510-52. Existe também 1 UTM CYBEROAM CR35ia que permite o acesso à internet através da conexão da porta WAN com um router CISCO 2921 do operador Vodafone. O serviço de internet é fornecido por fibra ótica e existe uma pool de 16 IPs públicos fixos (14 uteis). O bastidor 2 com 42U, contém 1 switch ZYXEL GS2210-24HP dedicado aos telefones IP PoE, 2 switches CISCO DSG-300 28P sendo que 1 deles tem uma porta *uplink* para o switch "*core*" no bastidor principal, 1 switch D-Link DGS1024D. Todos os switchs do bastidor 1 e bastidor 2 suportam Layer 2 ou superior e em termos de velocidade suportam 1Gb por porta. O bastidor 3 de 8U tem 1 switch CISCO SF302-08P 10/100 com uma porta em *uplink* para o bastidor principal.

A rede *wireless* é composta por três *Access Points* (APs) Cisco AIRONET 1040 e um AP Cisco AIRONET 1600, que estão configurados em modo *standalone*. Foram identificados mais de 40 clientes Wireless num só AP. Na fase de levantamento de constrangimentos havia sido referida a fraca cobertura da rede *wireless* com indicação de zonas em que o sinal era muito fraco ou inexistente.

Na infraestrutura de conetividade existente, foram identificados vários constrangimentos e possíveis riscos provenientes de alguma negligência nas configurações e desenho físico da infraestrutura. Entre os constrangimentos e riscos, destaca-se:

- O bastidor 1 e 2 contêm switchs de três marcas diferentes, nomeadamente CISCO, ZYXEL e D-LINK, estando já muito próximo da sua capacidade máxima;
- Cada switch é configurado e gerido de forma diferente, o que obriga a um conhecimento técnico diferenciado por cada equipamento e atenção redobrada para evitar conflitos e más configurações;
- Uma única rede é utilizada para gestão e produção, não existindo isolamento do tráfego, o que em termos de segurança poderá causar uma falha permitindo o acesso indevido a componentes críticos da infraestrutura;

- Foram identificadas a existência de três VLANs, nomeadamente a VLAN ID 1 (*default*), VLAN ID 10 e VLAN ID 100 (telefones voip). A VLAN ID 10 não está a ser utilizada e não é transversal aos switchs e não há conhecimento por parte dos elementos internos de TI da sua potencial usabilidade;
- Quase todos os switches têm todas as portas em modo *trunk* com o *tag* de todas as VLANs. Por questões de segurança e performance, recomenda-se especificar as devidas portas por VLAN, bloqueando acessos indevidos e fluxo de pacotes desnecessários;
- Não existe documentação sobre os *uplinks*. É necessária uma análise detalhada sobre todos os switchs de forma a documentar e determinar quais os protocolos, portas e configurações ativas;
- Não existe redundância de *uplinks* nem balanceamento de tráfego entre os switchs;
- Não existe uma rede wireless unificada, o que dificulta o controlo dos clientes wireless e as operações de resolução de problemas;
- Existe apenas uma rede *wireless* para todos e quaisquer dispositivos, sendo que esta rede permite acesso direto à LAN. Este cenário poderá permitir que entidades externas à organização consigam com muita facilidade aceder a recursos privados sem autorização;
- Através da realização de *site survey* constatou-se que existem zonas em que o sinal é fraco ou inexistente e zonas em que um único AP está a servir mais de 40 clientes em simultâneo, denotando-se quebras e latência elevada;
- A rede *wireless* está protegida por password com cifra WEP. Esta cifra possui vulnerabilidades conhecidas e não é recomendável por colocar em causa a segurança do acesso à rede wireless;
- A UTM CYBEROAM CR35ia está tecnologicamente obsoleta e proporciona apenas um *troughput* UDP de 750 Mbps e TCP de 500 Mbps. Este baixo *troughput* provoca uma maior e visível latência na conetividade com a internet;
- Constatou-se ainda que existe um mapeamento explicito de portas entre a UTM e o *gateway* de internet, a fazer *port forwarding* da *pool* de 14 endereços públicos para endereços privados da *subnet* 10.0.0.0/24 na interface WAN da UTM. Por sua vez existe uma tabela de NAT com *port forwarding* (virtual host) para a *subnet* interna 192.168.0.0/22. Tendo em conta que o gateway de internet é gerido pelo operador (ISP), este cenário cria uma dependência do operador que gere o router e que tem de configurar o *port forwarding* inicial, obrigando a uma segunda configuração de *port forwarding* na UTM. Constatou-se que por vezes as tabelas de NAT ficam de alguma forma não conformes, obrigando a reiniciar o router do operador e a UTM.

4.2.2.2 Servidores – estado atual

Atualmente a organização tem cinco servidores físicos *standalone* e dois servidores físicos que integram uma plataforma de virtualização. As características dos servidores constam na Tabela 4.

Modelo	RAM (GB)	Cpu (GHz)	Cores	Nics	HDD (DAS)
HP DL380 G6	10	2.13	4	2	4*300 GB SAS RAID5 2*600 GB SAS *STANDALONE*
HP DL 380G5	8	3.00	2	2	4*250 GB SAS RAID5
Linha branca	4	2.20	2	1	1*500 Gb SATA
Linha branca	4	2.20	2	1	2*500 GB SATA
SUPERMICRO X10SL7-L	8	3.10	6	2	1*250 SSD 6*2TB SATA
SUPERMICRO X9DRH-7TF/7F/iTF/iF	128	2.60	6	4	2*300 SAS
SUPERMICRO X9DRH-7TF/7F/iTF/iF	128	2.60	6	4	2*300 SAS

Tabela 4 - Lista de servidores físicos existentes

O controlador de domínio, serviços essenciais da LAN (DNS, DHCP, AD) e o servidor de correio eletrónico Microsoft Exchange 2010, são suportados pelo servidor físico HP DL380G6 através da suite Microsoft Windows SBS 2008. O servidor físico HP DL 380G5 tem a função de servidor de acesso remoto através do serviço de "Terminal Services" da Microsoft. Os restantes dois servidores linha branca têm a função de servidor de ficheiros e servidor de terminais. O servidor SUPERMICRO X10SL7-L apesar de conter dados antigos de cópias de segurança, aparentemente não está a ser utilizado. A plataforma de virtualização é composta por dois servidores físicos SUPERMICRO X9DRH-7TF/7F/iTF/iF que assumem o papel de *hosts* tendo instalado ao hypervisor VMware vSphere ESXi 5. As máquinas virtuais estão alojadas na SAN da marca dotHill que está ligada diretamente (inexistência de switches) aos hosts por *patch cords* de fibra ótica através de interfaces iSCSI a 10Gb. Existe um bastidor de 42U onde estão colocados todos os servidores de *rack*.

A análise do estado atual da infraestrutura de servidores existente, revelou vários problemas que elevam riscos de perda de dados, nomeadamente:

- O serviço de DHCP não está a atualizar dinamicamente o DNS, o que poderá causar um maior tempo na resolução de nomes na LAN, aumentado o número de pacotes de *broadcast* e latências na rede;
- O DHCP tem três âmbitos, nomeadamente para a subnet 192.168.0.0/22, subnet 10.1.1.0/24 e subnet 10.100.100.0/24. Apenas o âmbito na subnet 192.168.0.0/22 está a ser utilizado;
- Existe um único servidor a desempenhar as funções de controlador de domínio, serviço de DNS e DHCP. Uma eventual falha deste servidor irá comprometer o bom funcionamento de todos os outros recursos de TI;
- A plataforma de virtualização existente apresenta erros graves na sua configuração. Apesar de cada *host* possuir uma HBA com duas interfaces e a SAN possuir duas controladoras, não há redundância de caminhos (*multipath*);

- Constatou-se uma tentativa de configuração de um cluster, sendo que este não está a funcionar e com erros visíveis. A rede virtual das máquinas virtuais está diferente em cada um dos *hosts* e errada pois não está a tirar proveito das *nics* dos *hosts*. No *host* dois quando se liga a 2º placa de rede o sistema entra em *LOOP* e a rede fica em baixo (sinal evidente de má configuração);
- A atribuição do processamento das máquinas virtuais aos *hosts* não está corretamente distribuída, sendo que um host está com excesso de carga e o outro está praticamente livre;
- Verificou-se a atribuição de uma interface iSCSI (supostamente dedicada à conetividade com a SAN) ao switch virtual que tem a port group que está associada ás máquinas virtuais para acesso à LAN. Esta configuração causa conflitos no tráfego entre as máquinas virtuais e a LAN e no tráfego entre a SAN e os *hosts*;
- A interface de gestão (IPMI) do host 1 está com *link* (camada 1 do modelo OSI) alternado entre ativo e desativo, o que poderá indicar anomalia física, erro de *firmware* ou conflito de IP;
- A consola de gestão do VMware apresenta alertas e erros críticos que refletem o estado conflituoso e não otimizado das configurações existentes;
- A SAN é o equipamento de importância extrema, no entanto tem as credenciais de gestão que vêm por defeito, permitindo a qualquer utilizador entrar na gestão da SAN e potencialmente causar sérios danos como, por exemplo, eliminar o volume lógico e com isso todas as máquinas virtuais existentes;
- Os servidores virtuais estão em "workgroup", ou seja, separados da infraestrutura cliente-servidor suportada pelos servidores físicos. Recomenda-se a adoção consistente de uma arquitetura cliente-servidor, por questões de segurança, controlo de partilhas e acessos, prevenção de conflitos entre domínios, protocolos e métodos de autenticação;
- Não existem mecanismos de controlo de *updates*, *firmwares* e *patches.*

4.2.2.3 Armazenamento - estado atual

O armazenamento de dados está distribuído por vários dispositivos existentes na infraestrutura de TI tais como servidores, SAN e NAS. A distribuição dos dados observada foi compilada na Tabela 5.

Modelo	**Quantidade de discos**	**Capacidade aprox útil bruta (Gb)**
HP DL380 G6	4*300 GB SAS RAID5 2*600 GB SAS *STANDALONE*	2100
HP DL 380G5	4*250 GB SAS RAID5	750
Servidor linha branca	1*500 GB SATA	500
Servidor linha branca	2*500 GB SATA (RAID1)	500
SAN dotHill AssuredSAN 3821	11*900 10k SAS (10 em RAID50 + 1 Spare)	7200
SUPERMICRO X10SL7-L	1*120 GB SSD 6*2TB GB SATA (RAID5+0)	8312

QNAP TS209	2*500 GB SATA (RAID1)	500
QNAP TS212	2*500 TB SATA (RAID1)	500
QNAP TS420	4*1 TB SATA (RAID5)	3072
Total global		**26626**

Tabela 5 -Capacidade de Armazenamento de dados por dispositivo

É de referir que os aproximadamente 26TB referidos na Tabela 5 contemplam toda a capacidade sem considerar o tipo de armazenamento. O dimensionamento do armazenamento deve ser separado em necessidades de armazenamento ativo (e margem de crescimento) e necessidades de armazenamento para cópias de segurança, réplicas e ou arquivo tendo em conta os períodos de retenção. Tal não era tido em conta aquando do levamento da situação atual. Relativamente ao armazenamento de dados foram identificados os seguintes constrangimentos:

- O controlador de domínio apresenta falta de espaço na partição do sistema operativo (C:\ com apenas 12% livre) e na partição de dados (D:\ com apenas 4%) o que além de causar problemas de performance está na iminência de ficar sem espaço levando à indisponibilidade dos seus recursos e funções, afetando toda a infraestrutura;
- O servidor HP DL380 G6 tem dois discos de 600 GB em modo standalone. A base de dados do Exchange 2010 ocupa 360GB e reside num único disco, ou seja, além da menor performance por falta de *striping* não há redundância o que em caso de avaria além do *downtime* do serviço de email, poderá originar perda total ou parcial da base de dados. A única forma de recuperar a informação é através dos backups caso estes existam e estejam operacionais;
- Na SAN dotHILL existe apenas um volume lógico (LUN), impossibilitando o balanceamento de I/O entre as controladoras da SAN. A ligação iSCSI a 10Gb entre a SAN e os HOSTS não está otimizada, não faz balanceamento e redundância. A configuração da transferência do tamanho máximo dos pacotes (MTU) está no valor de defeito (1500) quando poderia estar otimizado para os 9000 (jumbo frames), otimizando assim o desempenho;
- Constatou-se ainda a existência de dispositivos de armazenamento do tipo NAS que além de armazenarem os *backups*, estão simultaneamente a servir ficheiros. Esta informação não está a ser salvaguardada sendo que em caso de avaria do NAS a informação poderá ser perdida.

4.2.2.4 Mecanismos de BCDR – estado atual

Constatou-se que os *backups* estão a ser realizados de forma ad-hoc, ou seja, não há um plano de ação definido com os procedimentos operacionais para salvaguardar e recuperar dados. Os *backups* não estão documentados nem testados e existe uma grande incerteza na forma como estes estão a ser feitos. Alguns *backups* são realizados via agendamento de *scripts* ou *softwares* que não oferecem garantias da integridade do *backup*, nem funcionalidades de compressão ou deduplicação. Grande parte dos dados

ativos não são sequer salvaguardados, fazendo com que em caso de corrupção (e.g., *ransomware*, falhas de corrente abruptas) ou falha do dispositivo de armazenamento a informação seja impossível de recuperar por via de um restauro. Não há um controlo efetivo dos *backups* dos servidores virtuais. O *backup* está a ser realizado por um software em modo *trial* que já expirou. Não existem mecanismos de alarmística sobre o estado dos componentes físicos, virtuais ou backups realizados.

O que se verifica na situação atual é muito grave, pois em caso de desastre não há qualquer garantia da continuidade de negócio, expetativas de cumprimento de RTO, RPO e recuperação da informação.

4.2.3 Conclusões sobre o levantamento da situação atual e propostas de atuação

O objetivo do levantamento da fase inicial foi identificar requisitos, inconformidades, problemas e necessidades, de forma a permitir arquitetar uma solução global e integrada que permita responder às necessidades atuais e futuras da organização, assente numa visão holística e alinhada de forma estratégica e sustentável com o negócio.

Constatou-se que apesar da organização possuir uma infraestrutura informática com alguma dimensão, já não consegue responder aos requisitos atuais, assim como, a perspetivas de crescimento futuro. Estando neste momento a enfrentar vários problemas relativos a constrangimentos causadas pela presente e estagnada arquitetura de TI. No decorrer desta fase inicial, foram identificados problemas críticos de urgente resolução causados por erros crassos e decisões de certa forma negligentes (por exemplo a ausência de um plano bem definido de *backups* e *disaster recovery*).

Para além do desenvolvimento de uma nova solução de TI, devem ser tomadas decisões e realizadas operações imediatas para a resolução dos problemas críticos. No cenário atual a avaria de um simples componente de hardware ou problemas causados sobre os dados (e.g. um ataque de *ransomware*) levará à indisponibilidade dos serviços e muito provavelmente à perda permanente de informação, penalizando a produtividade dos utilizadores e a imagem da empresa.

O recurso a tecnologias de virtualização é fundamental para se atingir uma consolidação dos sistemas físicos e aplicações. Tal permitirá maiores níveis de flexibilidade, escalabilidade e segurança. A sua adoção também facilita a criação de mecanismos de alta disponibilidade com um custo reduzido e permitirá um maior retorno do investimento realizado nos equipamentos de TI através de um melhor aproveitamento da capacidade computacional dos equipamentos.

A adoção de tecnologias modernas de armazenamento permite a otimização de I/O, acomodar e gerir e

escalar terabytes de dados, sendo fundamentais para colmatar as necessidades consequentes da tendência do crescimento do volume de informação. Estas tecnologias possibilitam *snapshots*, replicação de dados e integração em planos de disaster recovery (DR). Desta forma, é possível diminuir a janela temporal e uma maior eficiência na reposição de dados e recuperação dos sistemas. Algumas tecnologias de armazenamento de dados, como por exemplo as *Storage Area Networks* (SAN) ou *Network Attached Storage* (NAS) proporcionam alta disponibilidade sobre o armazenamento e conetividade para com os servidores. A consolidação de armazenamento e servidores faz também com que seja necessário otimizar as Local Area Networks (LAN) por forma a suportarem o tráfego endereçado pelos servidores e dispositivos de armazenamento (e.g. segmentação). De igual forma, a solução relativa ao plano *backups* terá de ter em conta a janela temporal para a sua execução por forma a garantir que os recursos estão disponíveis para os utilizadores, e ser escalável acompanhando o crescimento dos dados. A segurança transversal a todos estes pontos traduz-se em técnicas específicas de cada área que permitem restringir acessos e proteger o ambiente.

Em linha com as fases de arquitetura de TI, o desenvolvimento do projeto com vista à evolução da infraestrutura passa por uma série de considerações de análise, desenho e implementação de acordo com quatro fases distintas [16]: design lógico, design físico, implementação e por fim detalhes e validação. Estas fases são descritas ao longo das próximas subsecções.

4.2.4 Design Lógico

A identificação dos requisitos, constrangimentos, riscos e pressupostos, foram compilados e resultaram numa listagem de um conjunto significativo de problemas a vários níveis. A solução a desenvolver visa colmatar esses problemas e otimizar algumas tecnologias presentes na arquitetura atual. Contempla a implementação de novas tecnologias, elevando o nível de escalabilidade, flexibilidade e potencial integração futura com tecnologias emergentes. Assim, e aplicando princípios modernos de arquiteturas de TI, tendo em conta a realidade e expetativas da organização, após análise de tecnologias e contactos com parceiros tecnológicos, desenvolveu-se um modelo lógico da arquitetura de TI, que servirá de base ao desenvolvimento e implementação de toda a arquitetura. O modelo lógico desenvolvido é ilustrado na Figura 24.

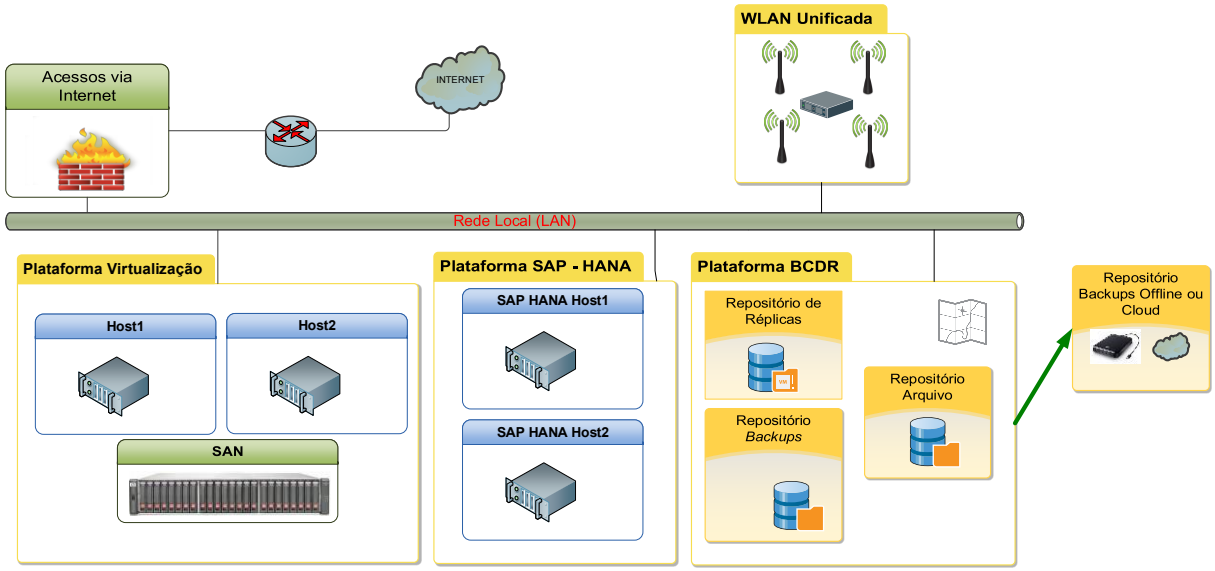

Figura 24 - Modelo Lógico da Arquitetura de TI

Conforme modelo apresentado na Figura 24, a arquitetura de TI englobará três componentes basilares assentes numa rede Ethernet, nomeadamente: Plataforma de Virtualização, Plataforma ERP SAP HANA, Plataforma de BCDR.

A plataforma de virtualização de alta disponibilidade (HA) contempla um cluster com dois nós e armazenamento partilhado (SAN). Servirá para consolidar todos os servidores físicos e todo o armazenamento de dados, permitindo centralizar e simplificar as tarefas inerentes à criação, manutenção, gestão e monitorização de servidores e dados. A consolidação de servidores, será realizada através da conversão dos servidores físicos em virtuais (p2v) e da migração dos servidores virtuais existentes (v2v), para a nova plataforma. Os dados críticos que se encontram distribuídos por vários dispositivos de armazenamento serão migrados para a SAN e geridos por servidores virtuais.

A plataforma ERP SAP HANA, será composta por um cluster com dois nós que se complementam em termos de funções e simultaneamente efetuam réplicas entre eles, permitindo que em caso de falha de um dos nós o outro nó consiga manter os serviços do nó em falha.

A plataforma de BCDR permitirá a continuidade de negócio, RTO, RPO e recuperação de dados com vários níveis de granularidade (ficheiros, discos virtuais, servidores ou todo o centro de dados). É composta por repositórios de *backup*, estrutura de replicação e repositórios de arquivo para dados não ativos ou em fim de vida útil. Esta plataforma, apesar de estar ligada à rede local, ficará fisicamente distante do centro informático (CI), prevenindo a paragem do sistema em caso de desastre físico no CI. Serão ainda realizadas cópias para dispositivos *offline* ou armazenamento baseado em nuvem, elevando

o nível de salvaguarda de dados.

Tendo em conta a crescente necessidade de conetividade wireless, será contemplada uma WLAN unificada, com gestão e monitorização centralizada. A rede WLAN suportará várias redes *wireless* (SSIDs) complementadas com VLANs, de forma a isolar e separar o tráfego de dispositivos *wi-fi* e aumentar o nível de segurança.

O controlo de acessos via internet será realizado através de uma UTM | Firewall de nova geração (NGFW) que para além das funcionalidades típicas de firewall, engloba filtros anti-malware e de conteúdo, IPS, DLP, proteção de email, aplicacional e servidor de VPN entre outras tecnologias de segurança.

A rede local será do tipo Ethernet e deverá ser ajustada para suportar todas as necessidades de conetividade com os diversos equipamentos da rede.

De forma a salvaguardar riscos elétricos todos os equipamentos de TI ficarão ligados a unidades de alimentação ininterruptas (UPS) do tipo *online*. As UPS além de manter os equipamentos ligados (por um determinado período de tempo) em caso de falhas de corrente elétrica, permitem uma proteção proativa sobre a variação e anomalias de energia.

Serão implementados sistemas proativos de alarmística que irão abranger componentes físicos, aplicações, tentativas de acesso indevido e monitorização de recursos. A proteção do acesso físico ao centro de dados e equipamento de TI é de extrema importância. Neste âmbito serão adotados mecanismos e politicas internas da organização, que visam o condicionamento do acesso apenas a pessoal devidamente autorizado.

4.2.5 Design Físico

Tendo como base o modelo lógico, procedeu-se ao design da arquitetura física. Para tal, foram determinadas e selecionadas tecnologias, equipamentos, tipo de ligações, configurações e operações a realizar. É de referir que os problemas encontrados a nível da tecnologia de virtualização na presente infraestrutura, não tinham origem na tecnologia, mas sim na má configuração da mesma e no *hardware* de suporte. Tendo em conta vários fatores, tais como garantias de evolução e continuidade, ROI, CAPEX e OPEX, optou-se pelo VMware como tecnologia de virtualização para suportar uma nova plataforma de alta disponibilidade. Os componentes da plataforma existentes podem ser reaproveitados para a plataforma de *disaster recovery,* que irá conter replicas das VMs críticas para a continuidade do negócio.

Após análise dos requisitos de processamento, armazenamento e conetividade, foram selecionados três possíveis fabricantes para aquisição de equipamentos, nomeadamente a HPE, DELL e Fujitsu-Siemens. Considerados os custos (iniciais e de manutenção), *SLAs* e garantias entre outros, optou-se por selecionar a HPE como fornecedor dos equipamentos para conetividade, servidores, sistemas de energia (*PDUs* e *UPSs*) e bastidor para o centro de dados. Assente numa arquitetura de convergência, a plataforma SAP HANA será suportada por uma solução HPE *TDI* (*Tailored Data Integration*) [67] certificada. Esta solução do tipo *vendor-based* é certificada pelos fabricantes (HPE e SAP), assegurando um elevado nível de compatibilidade e desempenho, reduzindo significativamente riscos e constrangimentos quando comparada com uma solução *ad-hoc*. Como requisito do SAP HANA e também assente numa visão de continuidade e evolução, a conetividade Ethernet deverá suportar 10Gb. Com este cenário foi possível desenvolver o modelo físico da arquitetura de TI a implementar. O design físico é ilustrado na Figura 25 e tal como se verifica pela figura, o modelo físico segue o modelo lógico concretizando as tecnologias a adotar com referência a marcas, modelos e versões dos fornecedores.

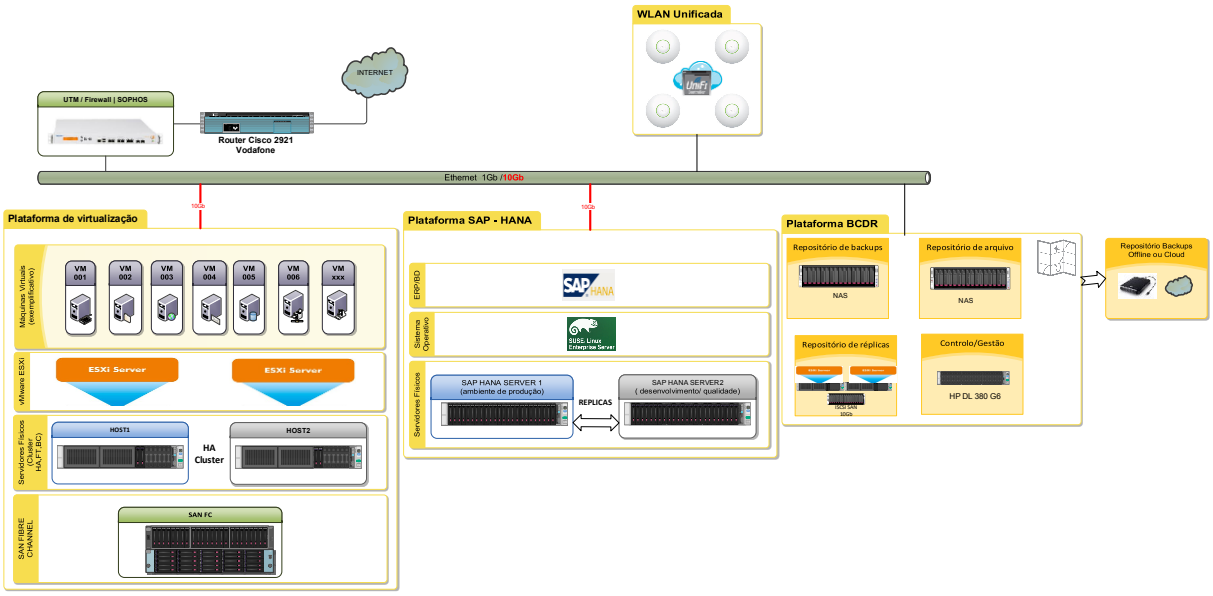

Figura 25 – Esquema da Arquitetura de TI

4.2.5.1 Redes Locais – design físico

A rede local (LAN) *Ethernet* irá evoluir de forma a suportar velocidades de 10Gb através de três novos *switchs* de *Layer* 3 HPE Aruba 2920-48G ligados em *stack*. Todos os *switchs* serão reconfigurados de forma a otimizar o desempenho e segurança. Estes switchs serão a base (*core*) de toda a conetividade Ethernet e serão colocados no bastidor 1 (centro de dados). A nível da LAN foi desenvolvido o seguinte modelo físico ilustrado na Figura 26.

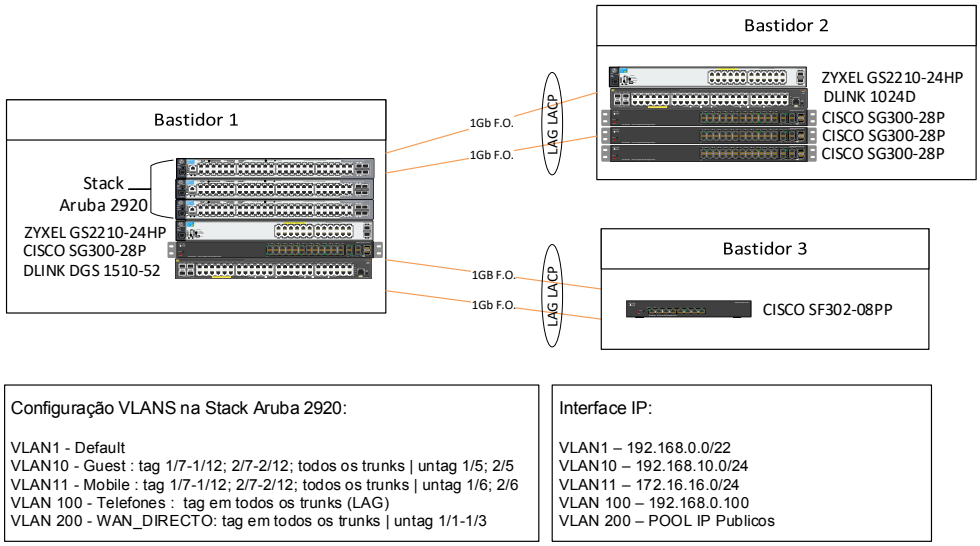

Figura 26 - Conetividade entre bastidores da LAN

Conforme Figura 26, a partidor do bastidor 1 são estabelecidos *uplinks redundantes,* através da criação de 1 *LAG* LACP via fibra ótica para cada um dos bastidores. A velocidade dos *uplinks* mantêm-se a 1Gb por questões de reaproveitamento de equipamentos e não ser um requisito obrigatório. Para além da VLAN *default*, serão criadas VLANs de forma a isolar redes, otimizar desempenho e incrementar a segurança. Devido à necessidade de manter o máximo número de portas Ethernet disponíveis em cada bastidor, o *switch* CISCO SG300 28P passará do bastidor 1 para o bastidor 2. O resumo dos equipamentos e capacidade da LAN pode ser observado na Tabela 6.

Descrição	**Qtd**	**Qtd portas 1Gb**	**Qtd portas 10Gb**	**Qtd portas SFP**
Aruba 2920-48G	3	3x48	3x4	3x4
ZYXEL GS2210-24HP	2	2x24	0	2x4
CISCO SG300 28P	3	3x26	0	3x2
DLINK DGS 1510-52	1	48	0	4
DLINK 1024D	1	24	0	0
CISCO SF302-08PP	1	8	0	2
TOTAL	**11**	**350**	**12**	**32**

Tabela 6 - Resumo de equipamentos e capacidade da LAN

Relativamente à rede WLAN, foram delimitadas as zonas a abranger. Para dimensionar o número de APs procedeu-se a um *site survey* em cada zona. O *site survey* foi feito através da ferramenta inSSIDer [62]. Considerou-se a qualidade de sinal, o tipo de uso e a estimativa do número máximo de dispositivos clientes de forma escalar o número de APs por localização. A Tabela 7 apresenta o resumo das necessidades relativas ao numero de APs por zona.

Zona	**Qtd APs**	**máximo de clientes (aprox)**
Administração	1	20
Escritório	1	10

Dpt. Engenharia	2	25
Salas de reuniões	2	30
Salas de formação	2	40

Tabela 7 - Resumo de numero de APs por zona

Com base nos resultados e em conjunto com a organização procedeu-se a uma análise de custo/beneficio. Em resultado, concluiu-se que a aquisição de uma nova solução de WLAN unificada seria mais vantajosa do que realizar um upgrade ao existente. A nova solução, além de possuir uma interface mais simples a nível de configuração e monitorização, permite maior desempenho através de tecnologias mais eficientes como por exemplo o suporte para norma 802.11ac. Foi também definido a criação de várias redes *wireless* para separar e controlar o tráfego dos acessos internos, externos, *smartphones* ou equivalentes. Atendendo à relação custo/qualidade, flexibilidade e escalabilidade foi selecionada uma solução empresarial unificada *Wi-Fi* da Ubiquiti [15]. Esta solução permite, através de uma única consola, realizar todas as configurações e controlos necessários da rede *wireless*, suportando a criação de *hot-spots* e redes do tipo *guest* com *captive-portal*, assim como, a possibilidade de isolamento dos clientes wireless, entre outros. A controladora *wireless* será instalada num servidor e gerida através de interface gráfico via browser. Todos os APs são alimentados eletricamente via PoE e ligam-se a LAN a 1Gbps.

No que diz respeito ao endereçamento IP, devido ao impacto e constrangimentos que poderiam surgir, optou-se por manter a configuração atual na subnet 192.168.0.0/22, o que representa 1024 endereços IPv4 (entre 192.168.0.0 e 192.168.3.255). As VLANs terão endereçamento IP facultado pelo *gateway,* conforme necessário na fase de implementação

4.2.5.2 Plataformas – design físico

Tendo em conta todos os fatores determinados na fase de análise, foram dimensionados os recursos necessários para os componentes da plataforma de virtualização, plataforma SAP HANA e plataforma BCDR. A Tabela 8 resume os componentes dos clusters presente em cada uma das plataformas

Modelo do servidor	**CPU**	**RAM**	**# Nics**	**Versão vSphere**	**Nome Cluster**	**# hosts no cluster**	**Tecnologia de acesso ao armazenamento**
HP ProLiant DL380 Gen9	Intel Xeon E5-2640v3@2.6GHz	256GB	4 x 1Gb 2 x 10Gb	6	HACluster	2	Fibre Channel 8GB
HP DL380p Gen9	Intel Xeon E5-2640v3@2.6GHz	512GB	8*1Gb 2*10Gb	N/A	SAPCluster	2	DAS
SUPERMICRO X9DRH	Intel Xeon E5-2630 v2 @2.60GHz	128	2*1Gb	6	DRCluster	2	iSCSI 10Gb

Tabela 8 - Hardware utilizado nos clusters

A plataforma de virtualização é composta por um cluster (HACluster) com dois servidores HPE Proliant GEN9 e armazenamento partilhado através de uma SAN FC. A conetividade entre os servidores físicos e a SAN é *Fibre Channel* (FC) a 8 Gbps. A escolha do FC deve-se ao menor *overhead* que esta tecnologia tem face ao iSCSI ou SAS. Tendo em conta que a SAN tem duas controladoras com quatro portas FC cada e que fisicamente apenas existem dois hosts em que cada host terá um HBA com duas portas FC, os hosts serão ligados diretamente (*direct-attach*) à SAN em FC configurado em modo *point-to-point*. Esta decisão elimina a necessidade de dois switches FC, mantendo a redundância e balanceamento, permitindo ainda a adição futura de até mais dois hosts. A Figura 27 ilustra a ligação de dois servidores do mesmo modo que o aqui descrito.

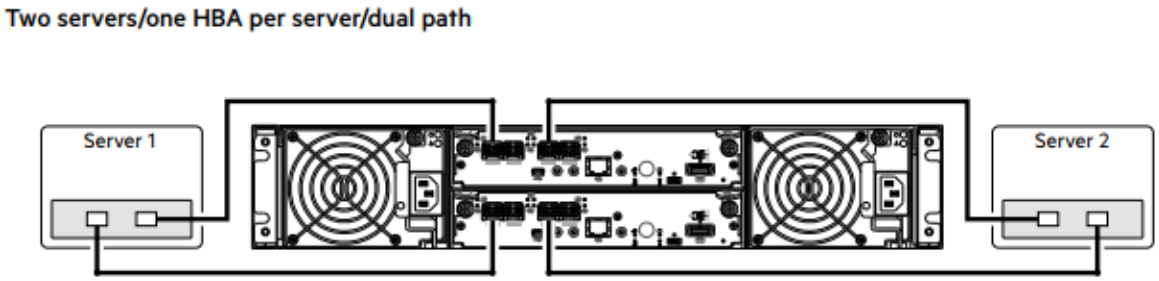

Figura 27 - Ligação de Hosts: direct attach [56]

Cada host terá duas fontes de alimentação de 500W e dois discos SAS de 300GB, onde será instalado o hypervisor VMware vSphere ESXi 6 Essentials Plus [30]. A conetividade Ethernet será facultada através de duas interfaces de rede a 10 Gbps cada. Cada host terá pelo menos uma interface de rede a 1Gbps dedicada para a migração (VMotion) de máquinas virtuais e duas interfaces para a rede de gestão.

Ao nível do armazenamento para a plataforma de virtualização, considerou-se necessária uma capacidade total útil para dados ativos de aproximadamente 27 TB. Esta capacidade será fornecida por uma SAN HPE MSA 2040 em conjunto com uma *enclosure* HPE D2700, com 38 discos de 900GB 6G SAS 10K SFF. Tendo em conta as necessidades de performance e armazenamento, os 38 discos serão distribuídos por níveis de RAID conforme a Tabela 9.

	# discos	# penalização RAID	armazenamento útil (GB)
Global Spares	2	2	0
RAID1+0	8	4	3600
RAID6	28	2	23400
Total	38	n/a	27000

Tabela 9 - Distribuição lógica da capacidade de armazenamento.

O grupo de discos em RAID1+0 suportará as máquinas virtuais e dados que necessitem de maior performance e o RAID6 suportará o restante.

A plataforma SAP HANA será composta por um cluster (SAPCluster) com dois hosts. Conforme solução *TDI*, o sistema operativo SUSE Linux Enterprise Server servirá de base ás aplicações e bases de dados do SAP HANA. Cada *host* terá um RAID50 com 16 discos de 600GB 6G SAS 10K SFF e 2 *Global Spares*. A conetividade Ethernet será facultada através de duas interfaces de rede 10 Gbps cada. A replicação será realizada através de quatro interfaces de rede a 1Gbps. A Tabela 10 ilustra o cluster da plataforma SAP Hana com a indicação do respetivo *hardware*.

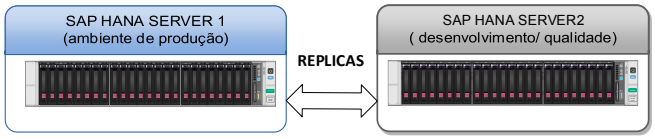	Servidor HP DL380 Gen9P • S.O: Suse Linux Enterprise Server • 2 CPU Intel XEON E5-2640v3@2.6Ghz / 8 Cores • 256 GB de RAM • HP Smart Array P440ar/2GB • 18 HDD 900 GB SAS 12G 10K • 4 Nics 1 Gb • 2 Nics10 Gb • 2 Power Supply 500W

Tabela 10 - Caraterísticas dos hosts da Plataforma SAP HANA

A plataforma de BCDR é composta por vários componentes. O componente que irá suportar a replicação das VMs é um cluster (DRCluster) VMware vSphere 6, constituído por dois hosts e uma SAN (reaproveitados). A tecnologia de armazenamento é iSCSI. A SAN terá 10 discos de 900 GB SAS em RAID50 e um *global spare*. A conetividade Ethernet será facultada através de duas interfaces de rede a 1 Gbps cada. O servidor físico HP DL380 G6 será reaproveitado para controlo de backups e gestão da infraestrutura. O servidor SUPERMICRO X10SL7-L será reaproveitado e utilizado como NAS através da instalação da distribuição Linux FreeNAS, criando um RAID5 com 6 discos de 2TB SATA, permitindo uma capacidade útil de aproximadamente 10TB. Este NAS será o repositório primário de *backups* diários para dados críticos. Os backups serão realizados através do software Veeam Backup&Replication. Para repositório de dados de arquivo (*cold data*) existirá um NAS da QNAP com quatro discos de 4 TB em RAID5 (12 TB). Adicionalmente serão realizadas cópias periódicas para dispositivos externos ou *cloud* de forma a possibilitar a retenção de cópias de segurança em modo *offline*.

4.2.5.3 Servidores – design físico

Os servidores físicos e virtuais existentes serão consolidados na plataforma de virtualização VMware vSphere 6. Conforme requisitos previamente definidos, serão criados servidores virtuais novos para suportar as necessidades novas e futuras da organização. O resumo das máquinas virtuais a criar é apresentado na Tabela 11.

Nome	Função	Sistema operativo	vRAM (GB)	# vCPU	armaz. (GB)	Tipo Armazenamento
vCenter Server Appliance 6	Gestão vSphere	Linux based	8	2	116	RAID 6+0
SRVDC1	DC	Windows 2012 R2 Std 64 Bits	8	2	120	RAID 6+0
SRVDC2	DC, WSUS	Windows 2012 R2 Std 64 Bits	8	2	120	RAID 6+0
SRVFS1	FS	Windows 2012 R2 Std 64 Bits	12	4	240	RAID 6+0
SRVDB1	DB	Windows 2012 R2 Std 64 Bits	12	8	160	RAID 1+0
SRVTS1	RDP TS	Windows 2012 R2 Std 64 Bits	12	8	160	RAID 1+0
SRVTS2	RDP TS	Windows 2012 R2 Std 64 Bits	12	8	160	RAID 6+0
SRVAPP	APP	Windows 2012 R2 Std 64 Bits	12	4	180	RAID 6+0
Servidores físicos virtualizados e servidores virtuais migrados						
vSBS	DC, EMAIL, FS	Windows 2008	12	4	1710	RAID 6+0
vKonica	Print Server	Windows 2012 64Bits	8	4	100	RAID 6+0
vPontoCSS	Relógio de ponto. APP	Windows 2012 R2 Std 64 Bits	8	2	250	RAID 6+0
vSAP_ADS	SAP	Windows 2012 64Bits	12	4	160	RAID 6+0
vSAP_CS	SAP	Windows 2012 64Bits	8	4	120	RAID 6+0
vSAP_DEV	SAP	Windows 2012 64Bits	32	16	300	RAID 1+0
vSAP_PRD	SAP	Windows 2012 64Bits	32	16	300	RAID 1+0
vIPBRICK	Gestão documental	Linux IPBRICK	8	4	100	RAID 6+0
vTS1	RDP TS	Windows 2012 64Bits	4	4	180	RAID 6+0
vTS2	RDP TS	Windows 2012 64Bits	4	4	210	RAID 6+0

Tabela 11 - Resumo das VMs na plataforma de virtualização

Todo o tráfego entre VLANs terá como *gateway* a UTM. A UTM terá uma interface configurada para cada VLAN e permitirá controlar os acessos e atribuir o endereçamento IP. Tendo em conta que será mantida a *subnet mask* de 22 bits, a nível da LAN (VLAN 1) o endereçamento IP será distribuído de acordo como indicado na Tabela 12.

Endereçamento IP	VLAN ID	Descrição
192.168.0.x	VLAN 1	Endereços reservados para gestão de equipamentos e impressoras
192.168.1.x	VLAN 1	Endereços reservados para servidores
192.168.2.x e 192.168.3.x	VLAN 1	Endereços reservados para clientes DHCP na LAN
10.0.0.0/24	VLAN 10	Endereços para a rede de Guests
172.16.16.0/24	VLAN 11	Endereços para a rede Mobile
192.168.100.0/24	VLAN 100	Endereços para a rede de telefones VoIP

POOL IPs Públicos	VLAN 200	Endereços públicos para usos da UTM e VM IPBRICK

Tabela 12 - Atribuição de endereçamento de IP

4.2.5.4 Monitorização, controlo e métodos de acesso – design físico

A gestão de utilizadores e controlo de acessos será suportado através do Microsoft Active Directory. Os controladores de domínio SRVDC1 e SRVDC2 irão suportar a Active Directory e consequentemente todas as funções de gestão e segurança inerentes ao serviço de diretório.

O controlo de acesso à Internet será realizado através de uma UTM de última geração do fabricante SOPHOS. A UTM foi recomendada pelo fabricante considerando a fasquia de 80 utilizadores a fazer uso simultâneo da Internet (*web surfing*, *email*, *downloads*), com todos os módulos de proteção ativos. A segurança e controlo de acesso à Internet será realizado com as credenciais de autenticação no domínio interno aquando do *logon*. Será implementado um sistema *single sign on* (SSO). O sistema de autenticação da UTM através integração LDAP com o Active Directory simplifica e assegura não só o acesso da rede interna a recursos externos, mas também o acesso externo via Internet a recursos internos. Qualquer acesso externo via internet será sempre realizado com recurso a VPN utilizando protocolos seguros (IPSEC, SSL).

Os sistemas de alarmística serão configurados nos diversos componentes da infraestrutura, a nível físico ou lógico. As notificações serão enviadas via email. A nível dos componentes da plataforma de virtualização os mecanismos de alarmística serão configurados da seguinte forma:

- **Servidores HPE Proliant**: configuração de envios de notificações proativa sobre eventos de alerta ou críticos referentes ao hardware através das interfaces de gestão IPMI (ILO);
- **SAN HPE MSA2040**: configuração de envio de notificações de forma proativa e envio de *logs* de forma periódica sobre eventos com nível critico ou alerta;
- **vSphere vCenter Server**: configuração de envio de notificações sobre o estado do *cluster* e dos *hosts*. Deverá incluir qualquer evento que potencie uma falha, como por exemplo anomalias de *hardware*, limites dos volumes das *storages*, quebras de conetividade, tentativas de acesso indevido, reinicio atípico de VMs.

Adicionalmente, na plataforma de virtualização, será utilizado a ferramenta Veeam ONE [50] para monitorização em tempo real, *reporting*, previsão e planeamento de capacidade de recursos e sistema de alarmística detalhado. O Veeam ONE permitirá também a monitorização e envio de notificações sobre os *backups* das VMs.

Ao nível dos componentes da plataforma SAP HANA os mecanismos de alarmística serão configurados tantos nos servidores HPE Proliant (alertas referentes a hardware através das interfaces de gestão IPMI) como na camada aplicacional através do envio de notificações sobre o estado do sistema, replicação de dados e conetividade entre outros.

Ao nível dos componentes da plataforma de BCDR os mecanismos de alarmística serão configurados da seguinte forma:

- **Servidores Nexus**: configuração de envios de notificações proativa sobre eventos de alerta ou críticos referentes ao hardware através das interfaces de gestão IPMI;
- **SAN dotHILL**: configuração de envio de notificações de forma proativa e envio de *logs* de forma periódica sobre eventos com nível critico ou alerta;
- **vSphere vCenter**: configuração de envio de notificações sobre o estado do *cluster* e dos *hosts*. Deverá incluir qualquer evento que potencie uma falha, como por exemplo anomalias de hardware, limites dos volumes das *storages*, quebras de conetividade, tentativas de acesso indevido;
- **NAS**: envio de alertas sobre o estado dos componentes, quebras de conetividade e alcance dos limites (*thresholds*) mínimos relativos ao espaço disponível;
- **Veeam Backup@Replication**: envio diário dos relatórios de backups e replicação.

A controladora wireless UNIFI despoletará alertas conforme definição de *triggers* referente a eventos de falhas, anomalias de APs ou conetividade, tentativas de acesso indevido ou clientes com elevados consumos de largura de banda.

A UTM SOPHOS XG210 que irá substituir a firewall Cyberoam CR35ia enviará notificações sobre *updates* de *firmware*, *reboots*, *logons* de acesso à interface de gestão. Serão também enviados relatórios de segurança diários ou semanais que incluem informação de *web surfing*, ataques e riscos, indicadores estatísticos relativos aos vários módulos de proteção, assim como controlo dos acessos VPN.

4.2.6 Implementação

As fases de *design* lógico e *design* físico permitiram a análise da realidade da organização e o desenvolvimento da arquitetura. Após reunião para apresentação da proposta e respetiva aceitação da nova arquitetura de TI, procedeu-se a implementação da solução desenhada. A implementação permite rever, reajustar (caso necessário) e validar a solução garantindo o sucesso da mesma, assente no alinhamento estratégico e sustentável com o negócio.

O inicio da implementação começa com uma reunião com a equipa do departamento de TI, onde numa visão de alto nível são definidas as prioridades, tarefas e operações, estimativas temporais e atribuição de funções aos elementos de TI. Esta reunião permite a criação do plano de ação, onde se resume o trabalho necessário (o que é preciso fazer), para atingir os objetivos propostos com o máximo de eficiência, minorando eventuais *downtimes*. Todas as fases da implementação são projetadas de forma a minimizar o impacto no negócio da organização. A implementação do projeto segue cinco fases globais, nomeadamente: *Staging;* Instalação; Configuração; Validação (testes); Documentação.

A fase de *staging*, permite verificar e otimizar os equipamentos, evitando constrangimentos que poderão colocar em causa os tempos estimados para a instalação e configuração. Nesta fase serão desenvolvidas as atividades de assemblagem de componentes, de carregamento das últimas versões de software e *firmware*, de verificação da operacionalidade de todos os componentes ativos da solução e de identificação e etiquetagem dos equipamentos.

A fase de instalação contempla a distribuição dos equipamentos por cada local de instalação, a fixação e instalação de equipamentos em bastidor, a interligação física dos equipamentos, os testes de conectividade e a instalação de software (*hypervisors*, sistemas operativos, serviços, aplicações).

A fase de configuração consiste na parametrização de cada um dos equipamentos de acordo com as especificações descritas no *design* físico. São atribuídas tarefas aos elementos da equipa de TI, de forma a permitir o correto fluxo dos trabalhos. Entre várias configurações temos:

- **Switches**: Endereçamento IP, Gestão remota, Perfis de Acesso, Configuração das VLANs, Configurações de Trunks, Configuração de alertas e notificações.
- **Wireless**: Endereçamento IP, Gestão remota, Configuração das VLAN's, Configuração de SSIDs, Configurações de segurança, Configuração de notificações.
- **UTM/Firewall**: Endereçamento IP, Configuração de regras de firewall, Configuração de filtros (conteúdo, aplicacional), Configuração dos diversos módulos de proteção, Configuração de VPNs (*site-to-site, remote client*), Configuração perfis de acesso à internet, Configuração de acessos de gestão, Configuração de notificações.
- •**Servidores**: Endereçamento IP, Configurações de hardware, Configurações de conetividade, Configurações de software e aplicações, Migração de dados, Migração de serviços e aplicações, Configuração de notificações
- **Dispositivos de armazenamento**: Endereçamento IP, Configuração de hardware, Configurações de conetividade, Configuração de notificações.

Na fase de validação são executados testes de aceitação e funcionais de modo a avaliar o e comparar o

grau de sucesso da solução de acordo com os requisitos e expetativas. Os testes abrangem testes de tolerância a falhas de hardware, os testes de tolerância a falhas aplicacionais, testes de *performance* e testes inerentes ao plano de BCDR.

A documentação tem como objetivo principal proceder ao registo de toda a informação útil referente aos equipamentos, ligações e configurações para que a qualquer momento a informação esteja disponível para quem dela necessitar. A existência deste tipo de documentação é de grande importância para o trabalho de manutenção e operação da infraestrutura.

As tarefas a realizar foram discutidas com a equipa da empresa e o resultado obtido compilado num mapa de Gantt, tal como ilustrado na Figura 28. A sequência de atividades resultou da definição de prioridades e tarefas a realizar por cada componente basilar, tendo sempre presente a perspetiva global e o possível impacto na organização. Por cada componente foi determinada a ordem de tarefas a efetuar e as estimativas temporais.

FOLHA DE TAREFAS

	WBS	Task Name	Duração	Início	Conclusão	Predecessoras
1	**1**	**[redacted] | Networking (LAN)**	**5 dias**	**Seg 05/06/**	**Sex 09/06/17**	
2	**1.1**	**Fase 1 - Execução**	**3 dias**	**Seg 05/06/**	**Qua 07/06/17**	
3	1.1.1	Stagging dos equipamentos novos (switchs aruba 2920)	0,5 dias	Seg 05/06/	Seg 05/06/17	
4	1.1.2	Stagging de equipamentos existentes	1 dia	Seg 05/06/	Seg 05/06/17	
5	1.1.3	Cumprimento de requisitos apresentados no design fisico	1 dia	Ter 06/06/	Ter 06/06/17	
6	1.1.4	Instalação física de equipamento e configuração base	0,5 dias	Qua 07/06,	Qua 07/06/17	
7	1.1.5	Criação da stack com os 3 switchs aruba 2920	20 mins	Qua 07/06,	Qua 07/06/17	
8	1.1.6	Criação das VLANS e atribuição de portas	45 mins	Qua 07/06,	Qua 07/06/17	7
9	1.1.7	Configuração dos Trunks	30 mins	Qua 07/06,	Qua 07/06/17	8
10	1.1.8	Configuração de LAGS LACP	1 hr	Seg 12/06/	Seg 12/06/17	9
11	1.1.9	Reconfiguração de todos os switchs de acordo com as novas especificações	1 dia	Seg 12/06/	Ter 13/06/17	10
12	1.1.10	Ativação dos Links (LAGs) entre os Switchs	2 hrs	Ter 13/06/	Ter 13/06/17	11
13	1.1.11	Testes de conetividade	0,25 dias	Qua 07/06,	Qua 07/06/17	12
14	1.1.12	Alteração do tráfego para o novo hardware	0,5 dias	Qui 08/06/	Qui 08/06/17	13
15	**1.2**	**Fase 2 - Monitorização & Controlo**	**1 dia**	**Qui 08/06/**	**Qui 08/06/17**	**14**
16	1.2.1	Monitorização de trafego	1 dia	Qui 08/06/	Qui 08/06/17	
17	1.2.2	Análise de logs	1 dia	Qui 08/06/	Qui 08/06/17	
18	**1.3**	**Fase 3 - Encerramento**	**1 dia**	**Sex 09/06/**	**Sex 09/06/17**	**15**
19	1.3.1	Atualização de documentação técnica	1 dia	Sex 09/06/	Sex 09/06/17	

Figura 28 - Lista de tarefas para implementação de equipamentos da LAN

Conforme a Figura 28, após a execução, é necessário garantir que tudo está a funcionar corretamente através de mecanismos de monitorização e controlo. A documentação é transversal a todas as fases e será atualizada sempre que necessário, com especial atenção no encerramento do projeto. No presente caso de estudo foram realizadas listas de tarefas para a implementação de: Networking (LAN, WLAN); Plataforma de virtualização; Plataforma SAP HANA; Plataforma BCDR; Firewall e respetivos módulos de proteção.

A janela temporal relativa à implementação total do projeto foi estimada em aproximadamente 1,5

meses, considerando o número e *know-how* dos elementos da equipa de TI. Foi também considerado um tempo efetivo de trabalho de 40 horas semanais.

Em termos de prioridades foi definido que logo após a reestruturação da LAN e WLAN, seria prioritária a implementação da plataforma de virtualização e parte parcial da plataforma de BCDR. A prioridade atribuída à plataforma de virtualização prende-se com os riscos identificados nos servidores físicos e dispositivos de armazenamento existentes, pois como já referido não ofereciam garantias de continuidades e redundância. A plataforma de virtualização possibilitará a consolidação de servidores físicos e a instalação de servidores novos (VMs) conforme os requisitos, libertando equipamentos existentes para reconfiguração e reaproveitamento como equipamentos ativos da arquitetura de TI. Para garantir a salvaguarda de informação e continuidade do negócio, é também prioritário a implementação de um plano inicial de backups composto por software e armazenamento. De seguida procedeu-se à implementação técnica da infraestrutura da plataforma SAP HANA, preparando a plataforma para a migração e *upgrade* do SAP.

Tendo em conta os equipamentos reaproveitados, procedeu-se à finalização da implementação do cluster de replicação e repositórios de dados e arquivos pertencentes à plataforma de BCDR. Os trabalhos relativos à substituição da firewall foram definidos como menos prioritários.

4.2.7 Detalhes e Validação

Ao longo de toda a implementação, foi necessário tomar decisões, desenvolver e realizar configurações e testes relativos a diversas tecnologias. Muitas decisões e opções têm como base as recomendações dos fabricantes e boas práticas. No entanto, é importante referir, exemplificar e justificar as decisões e opções tomadas que permitam ultrapassar as dificuldades e atingir os objetivos propostos.

A nível de *networking*, de forma a otimizar conetividade da rede física (LAN) foram configurados três switchs novos em stack e criados os LAGs entre os switchs dos três bastidores. O recurso ao *stacking* de *switches* simplifica a gestão, aumenta o *uptime* e a resiliência da rede evitando os tradicionais uplinks. Tendo em conta a existência de switches de vários fabricantes e as necessidades de criação de uplinks, optou-se por criar agregações de duas portas (LAGs) por cada *uplink* através de LACP. Cada *uplink* foi testado através da simulação de falha física de cada uma das portas e validado estado do LACP. A Figura 29 ilustra o estado dos *uplinks* e estado das LAGs.

Figura 29 - Uplinks e LAGs LACP

A nível de VLANs, optou-se pela configuração *port-based* devido à menor complexidade, e ao facto deste tipo de configuração permitir atingir os requisitos estabelecidos. O suporte para *jumbo frames* com MTU de 9000 foram ativadas apenas na DEFAULT_VLAN, onde residem equipamentos também otimizados com o tamanho máximo das frames. Para evitar a possibilidade de *loops na rede ativou-se o Rapid Spanning-Tree Protocol (RSTP)*.

Ao nível da implementação da plataforma de virtualização após a instalação dos *hypervisors*, foram criados quatro *switchs* virtuais, separando o trafego das *VMs*, *vMotion, Management* e a VM IPBRICK. Esta separação permite o isolamento, segurança e otimização de desempenho do tráfego da LAN. O estado dos *switchs* virtuais é ilustrado na Figura 30.

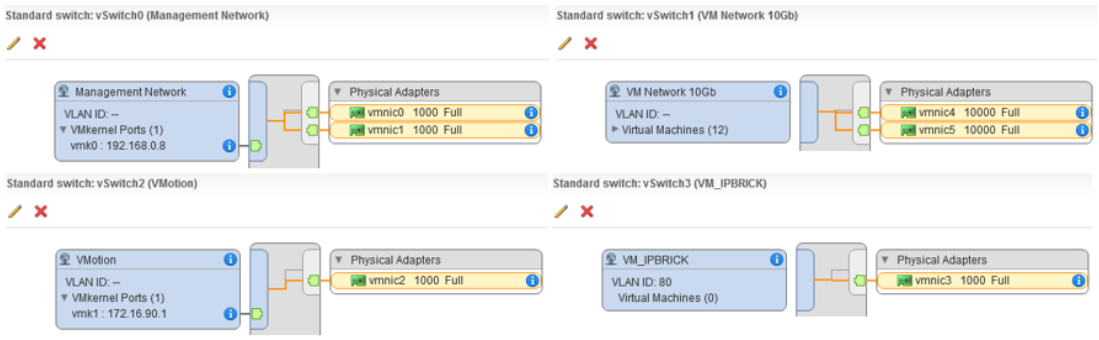

Figura 30 - Swicthes Virtuais

No esquema da Figura 31 pode-se observar as ligações entre a SAN e o cluster de alta disponibilidade da plataforma de virtualização. No esquema, são referenciadas com detalhe configurações relativas a endereçamento IP e VLANs.

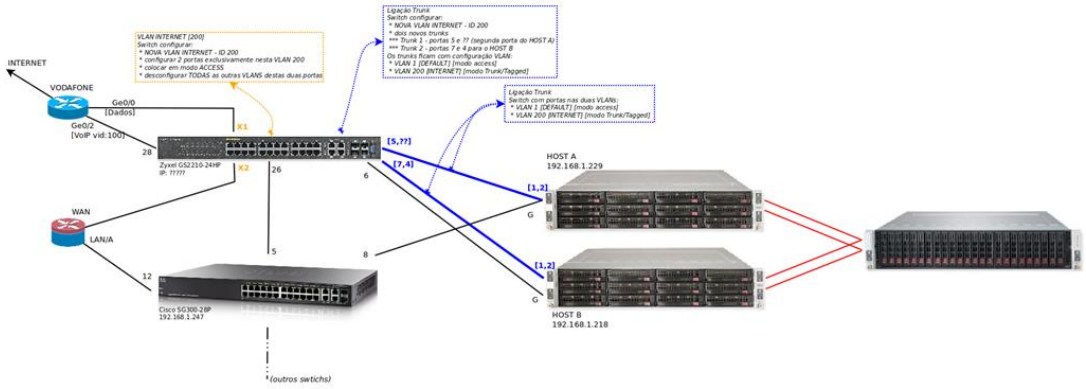

Figura 31 - Detalhe de configurações de conetividade entre a LAN e Cluster HA

Na SAN MSA2040 FC, tendo em conta o balanceamento do I/O pelas duas controladoras de armazenamento, assim como a relação performance/custo, foram criados dois volumes virtuais. O volume 1 foi assignado à controladora A e é suportado por um RAID 1+0. O volume 2 foi assignado à controladora B e assenta sobre dois RAID 6 criando um RAID 6+0. A razão de se ter criado dois RAID 6 deve-se ao facto de que na SAN MSA2040 FC cada grupo de discos pode ter no máximo 16 discos, assim, optou-se por criar dois grupos de discos com 14 discos cada em RAID 6. Perspetivando futuras necessidades de escalamento e otimização de performance com recursos a auto-tiering com discos SSDs, procedeu-se à criação de volumes virtuais em vez de volumes lineares. Seguindo as recomendações de boas práticas VMware, nos hosts foram criados dois volumes de armazenamento em VMFS5 que refletem o tamanho e nível de armazenamento proporcionado pela SAN.

Ao nível do cluster HA VMware configuraram-se as proteções contra falha de HOST, falha de conetividade de storage ou falha de VM. Apesar da possibilidade, não se considerou relevante parametrizar a proteção de falhas a nível aplicacional (*watchdog para aplicações e S.O.*), tendo em conta os ambientes existentes. Feitas as configurações, foram realizadas simulações de falha física de cada um dos hosts, de falha de conetividade entre os *hosts* e a SAN (alternadamente) e falha esporádica de uma VM, de forma a validar as configurações do cluster e a determinar os tempos de *recovery*.

Em caso de falha de conetividade de uma porta FC entre um host e a SAN, logo que era detetada pelo *heartbeat* (com intervalos de 1 segundo), o tráfego era automaticamente direcionado para a porta FC que estava a *on-line*, comprovando o bom funcionamento da redundância. Este tipo de falha não causava *downtime.*

Em caso de falha física de 1 host (p*ower off*), apenas passado aproximadamente entre 15 a 20 segundos, as VMs afetadas eram automaticamente reiniciadas no host em funcionamento. A razão para este intervalo de tempo deve-se à arquitetura de *host monitoring* no cluster da VMware HA, tendo como

objetivo evitar falsos positivos.

Em caso de falha esporádica de uma VM (e.g. *bluescreen*), a VM demorava cerca de 60 segundos a ser reiniciada (reset). Esta janela temporal estava de acordo com a sensibilidade configurada (Medium) a nível e monitorização de VMs. No entanto no intervalo de 1 hora apenas poderia ser reiniciada de forma anómala 3 vezes, conforme definição por defeito presente no cluster VMware HA.

As expectativas de desempenho consequentes da migração do SAP em Windows/Sybase para Windows/HANA e Linux/HANA deixavam dúvidas à equipa da empresa. Assim e em conjunto com o parceiro SAP, foram realizados testes de performance e comparativos entre as plataformas Windows/HANA e Linux/HANA. Foram testadas as seguintes transações: ME2L, MM60, MB52, S_ALR_87012332 e S_ALR_8701361. Mediu-se os tempos de resposta entres as duas instalações. Os resultados obtidos são apresentados na Tabela 13.

Transação	Tempo em sistema DEV Windows/HANA		Data	Tempo em sistema TST Linux/HANA		Data	Conclusão
	%ABAP	% DB		% ABAP	% DB		
ME2L – variante MIG	26.255 ms		24.07.2017	26.213 ms		26.07.2017	Não existe ganho de performance significativa pois o tempo de processamento ABAP é elevado, superior a 30%, bem como a transação faz várias *database calls*.
	39,9%	58,9%		52,1%	47,7%		
MM60	14.276 ms		24.07.2017	16.977		26.07.2017	O tempo de processamento é essencialmente ABAP, não é expectável qualquer alteração de performance significativa.
	89,4%	10,6%		86,6%	13,3%		
MB52	21.430 ms		24.07.2017	21.201 ms		26.07.2017	O tempo de processamento é essencialmente ABAP, não é expectável qualquer alteração de performance significativa.
	75,9%	24%		81,2%	18,7%		
S_ALR_87012332	346.065 ms		24.07.2017	340.245ms		26.07.2017	Não existe ganho de performance significativa pois o tempo de processamento ABAP é elevado, superior a 30%, bem como a transação faz várias *database calls*.
	50,8%	49,2%		59,4%	40,6%		
S_ALR_87013611	5.601 ms						O tempo de processamento é essencialmente ABAP, não é expectável qualquer alteração de performance significativa.
	77,9%	21,9%					

Tabela 13 - Testes de performance SAP HANA

Quanto ao plano de *backups* e *disaster recovery* este é suportado pelos componentes da plataforma de BCDR. Através do reaproveitamento dos equipamentos existentes procedeu-se à criação do cluster que irá suportar as réplicas das VMs consideradas criticas para a continuidade do negócio. Foram reconfigurados dois servidores físicos (hosts) e uma SAN iSCSI. A Figura 32 ilustra a configuração da plataforma de virtualização para *disaster recovery.*

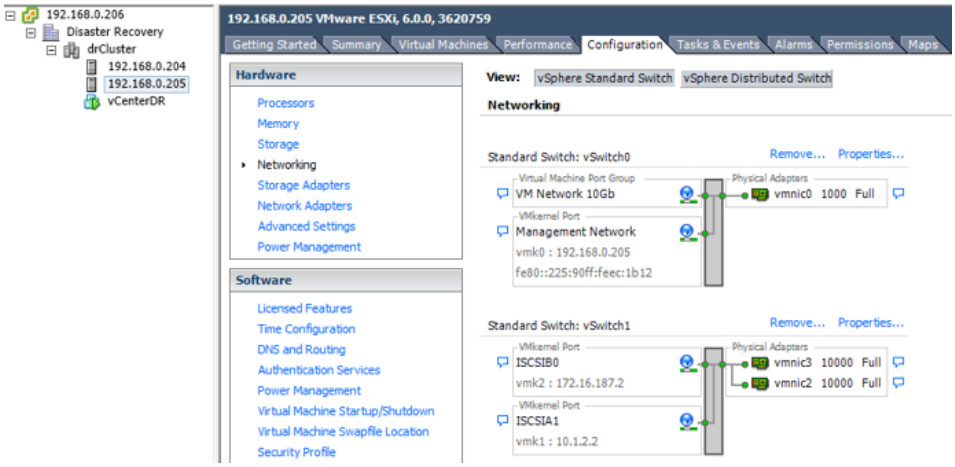

Figura 32 - Cluster de Disaster Recovery

Um fator a ter em consideração é o facto da plataforma de DR não possuir as mesmas capacidades em termos de recursos físicos, da plataforma de virtualização ativa. No entanto, a configuração da conetividade para as VMs é idêntica. O *network label* do *port group* é obrigatoriamente igual para não causar disrupção no caso de ser necessário arrancar com uma VM replicada. O armazenamento da SAN iSCSI é suportado com um RAID 5+0 com 10 discos e um *global spare*, tendo em conta a redundância e performance. Devido à SAN iSCSI não suportar funcionalidades avançadas (auto-tiering, volumes virtuais), foi criado um volume *Linear* com a capacidade de aproximadamente 7 TB. Os trabalhos de replicação de VMs foram especificados em períodos de quatro horas para VMs criticas com bases de dados e de 24h para as restantes VMs consideradas para replicação.

Para salvaguardar as VMs e dados foram criados repositórios de armazenamento com recursos a tecnologia do tipo NAS. Foram definidos planos de backups com cópias diárias, semanais e mensais e respetivas retenções. Todos os trabalhos de backup e replicações são geridos através da consola centralizada do software VEEAM Backup@Replication, o que simplifica a gestão e monitorização. São enviados relatórios via email por cada trabalho de backup, replicação ou restauro de dados. Conforme plano de BCDR, foi criada uma *backup jobs* aqui apresentada na Tabela 14.

***Backups* Diários – VEEAM Backup@Replication v9**					
Job	**Servidores**	**Repositório**	**Tipo**	**Retenção**	**Frequência**
Cópia Diária SAPs	vSAP_ADS vSAP_CS vSAP_DEV vSAP_PRD SAP_TST	NASBCK01	*Full*: Sábados ás 04:00 *Incremental*: Seg a Sex ás 22:30	07	24h
Cópia Diária PontoCSS_KONICA_IPBRICK	vKonica vVMIPBRICK Vpontocss	NASBCK01	*Full*: Sábados ás 04:00 *Incremental*: Seg a Sex ás 22:30	5	24

Cópia Diária SRVAPP, SRVTS1, SRVDB1 SRVDC1.	SRVFS1 SRVDC2	NASBCK01	*Full*: Sábados ás 04:00 *Incremental*: Seg a Sex ás 22:30	7	24
***Backups* Semanais – VEEAM Backup@Replication v9**					
Cópia Semanal SAPs	vSAP_ADS vSAP_CS vSAP_DEV vSAP_PRD SAP_TST	NASBCK02	*Full*: 1º domingo de cada mês ás 04:00 *Incremental*: restantes domingos ás 04:00	4	24h
Cópia Semanal PontoCSS_KONICA_IPBRICK	vKonica vVMIPBRICK Vpontocss	NASBCK02	*Full*: 1º domingo de cada mês ás 10:00 *Incremental*: restantes domingos ás 10:00	4	24
Cópia Semanal SRVAPP, SRVTS1, SRVDB1 SRVDC1.	SRVFS1 SRVDC2	NASBCK02	*Full*: 1º domingo de cada mês ás13:00 *Incremental*: restantes domingos ás 13:00	4	24
***Backups* Mensais – VEEAM Backup@Replication v9**					
Copia Mensal SAPs	vSAP_ADS vSAP_CS vSAP_DEV vSAP_PRD SAP_TST	NASBCK03	*Full*: último domingo de cada mês ás13:00 *Incremental*: restantes domingos ás 13:00	12	
Cópia Mensal Outros	vKonica vVMIPBRICK Vpontocss SRVFS1 SRVDC2	NASBCK03	*Após o job "Copia Mensal SAPs"*	12	

Tabela 14 - Backup jobs

Todos os *backup jobs* salvaguardam as VMs de forma completa (full) com recurso a snapshots, CBT e *application-aware processing*. Desta forma, é preservada a integridade e permitida a recuperação de dados com diferentes níveis de granularidade. É possível recuperar desde apenas 1 ficheiro ou 1 objeto da AD a um disco virtual ou toda a VM de forma integral. A janela temporal dos *backup jobs* dependem do tamanho dos dados a salvaguardar, do tipo de backup (*full* ou *incremental*), da taxa de deduplicação e da performance dos recursos físicos. Tendo em conta estes fatores, os servidores foram agrupados por função e por sistema operativo. Para determinar os tempos associados aos *backups*, foram analisados e comparados os *logs* ao longo de duas semanas. Para validar o resultado, constatou-se que durante as duas semanas, o *overhead* causado pelos *backup jobs* não tiveram relevância no normal funcionamento dos serviços, mesmo quando realizados na hora de trabalho. Nesta fase não foi considerado o arquivo para dados em fim de vida útil.

Como parte integrante de plano de BCDR foi ativado o serviço de cópias de sombra nos servidores Microsoft Windows Server. Esta funcionalidade evita o recurso aos *backups* em caso de eliminação ou

overwrite acidental de ficheiros, permitindo ao utilizador selecionar uma versão anterior do ficheiro ou pasta que pretende recuperar. As cópias de sombra são realizadas diariamente às 07:00 e às 12:00. Adicionalmente, são realizadas cópias para dispositivos *offline*, (discos USB externos), ficando em análise a possibilidade futura de *backups* para a *cloud*.

A substituição da *firewall* permitiu essencialmente a resolução de três problemas: Latências no uso da internet, Falta de controlo e monitorização, Falta de filtros de malware e intrusão na segurança de perímetro.

Para resolver o problema de existirem duas tabelas de NAT, originado por um duplo mapeamento de IPs e portas entre a pool de IPs públicos fixos no router e a gama interna 10.0.0.x/24 utilizada na interface WAN da UTM, alterou-se a atribuição da pool de IPs públicos para modo bridge na interface interna do router Cisco 2921 na VLAN 200. A porta WAN da UTM foi também configurada na VLAN 200. Desta forma é possível especificar diretamente nas regras de NAT da UTM o IP público e porta pretendida sem necessidade de contactar o suporte do ISP.

Com base na integração do sistema de autenticação da UTM com a AD presente nos *domain controllers,* configurou-se o *single sign on* (sso). Assim, qualquer utilizador que aceda à Internet ou aceda remotamente via VPN terá de se autenticar com as credenciais de *logon* no domínio da organização. A grande vantagem é o facto de se evitar redundância de credenciais em locais distintos para acesso aos recursos de TI e simplificar a sua gestão. Procedeu-se também à criação de regras do tipo *business application rule*, para proteger e controlar acesso a servidores e serviço, assim como regras do tipo *user/network rule,* para controlo de tráfego de utilizadores e redes. Um excerto das regras criadas na firewall é ilustrado na Figura 33.

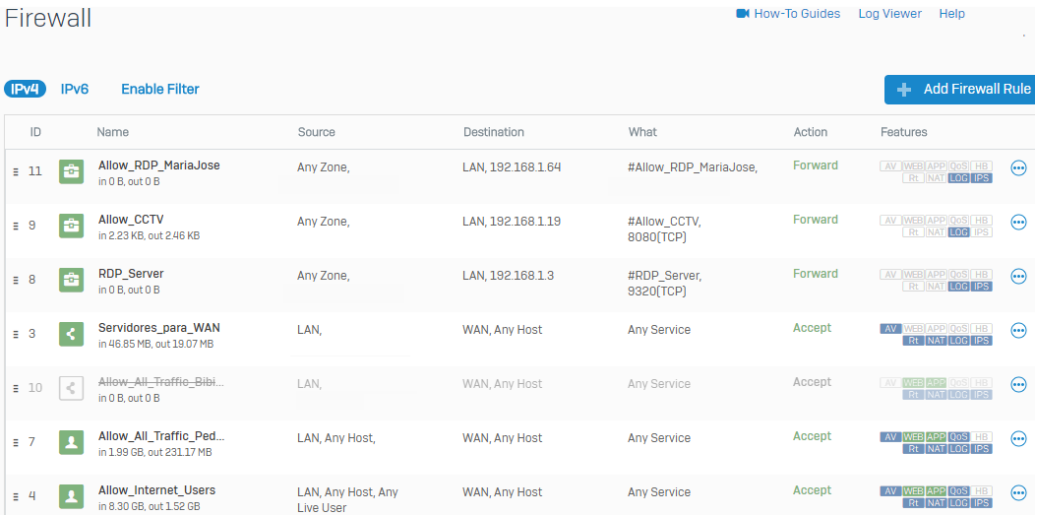

Figura 33 - Regras de Firewall

A monitorização da firewall é realizada através do módulo de *reporting*. Neste módulo, é possível obter uma visão global ou detalhada do uso da Internet e recursos subjacentes através da aplicação de filtros. Os filtros podem ser aplicados em função de um período temporal e da análise de segurança pretendida. A Figura 34 ilustra a *interface* de monitorização da UTM.

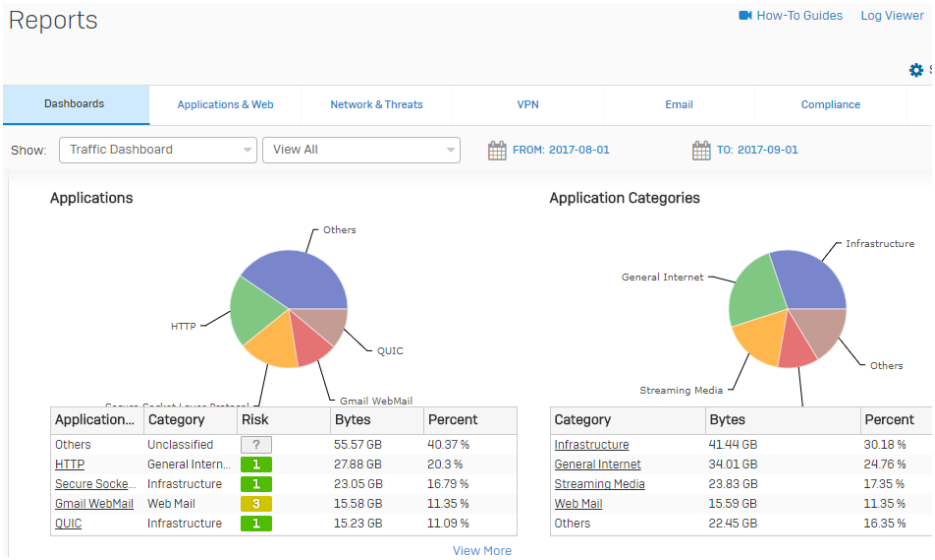

Figura 34 - Reporting da UTM

5 Conclusões

Ainda que para muitas das organizações a tecnologia não seja o seu negócio *core*, é através dela que se suporta cada vez mais o funcionamento dos negócios. Neste âmbito é importante a criação de mecanismos que auxiliem as organizações a analisar e decidir de forma clara direções futuras no que diz respeito à evolução da TI, alinhadas com as suas expetativas e negócio.

Cabe ao arquiteto de TI avaliar os requisitos do sistema de forma a configurar e manter o ambiente IT em funcionamento, contribuindo para a boa *performance* do negócio. Ser arquiteto de TI implica ter um bom *background* técnico e de gestão, permitindo uma constante atualização face à evolução tecnológica e a capacidade de gerir um projeto de manutenção da infraestrutura alinhado com o negócio e orçamento disponível.

Infelizmente nem todas as organizações dispõe de uma pessoa com o perfil de arquiteto de IT que avalie no seu dia-a-dia o estado atual e faça uma análise entre esse mesmo estado e um estado ideal, no qual a eficiência da organização seria maximizado. Por forma a reduzir esta deficiência de pessoal especializado e compreendo a real necessidade de manter as infraestruturas IT alinhadas com o negócio, uma das possibilidades passa pela definição de modelos que balizem a adoção de boas práticas.

Foi partindo desta necessidade, colocada numa fase inicial por uma empresa, que se desenvolveu o projeto aqui apresentado. Entendeu-se desde logo que a necessidade e dificuldade da empresa será comum a muitas mais. Estabeleceu-se assim objetivo principal desta dissertação a pretensão de que qualquer organização que pretenda ou que tenha necessidade de analisar/reestruturar/otimizar/evoluir a sua arquitetura de TI, consiga com base neste trabalho identificar-se e efetuar uma abordagem correta, nomeadamente ser capaz de responder as questões como:

- Qual o estado atual do ambiente de TI?
- Qual a estratégia e objetivos/expetativas futuras em termos de negócio e TI?
- Que trabalho é necessário para estabelecer o ambiente de TI desejado (*GAP analysis*)?

E ainda, com base às respostas obtidas, proceder a um desenho lógico e físico de uma nova solução e à sua implementação prática não esquecendo a análise final sobre o real suprimento das necessidades identificadas inicialmente.
Sendo um trabalho complexo entendeu-se desde logo uma divisão estruturada permitindo um melhor cumprir as etapas. Trata-se de uma metodologia de arquitetura IT faseada e direcionada ao contexto vivenciado pela organização, sem, no entanto, romper com o que está estabelecido na literatura da área.

Feita uma divisão metódica de abordagem à arquitetura de IT com base em boas práticas procedeu-se a uma validação prática da mesma. Trata-se de uma empresa da área da construção civil que não dispõe de um perfil de arquiteto de sistemas, mas que percebeu que os seus sistemas estavam a limitar o próprio funcionamento e expansão do negócio e que por isso decidiram atuar no sentido de perceber o seu estado atual e o que fazer para evoluir no sentido do crescimento e bom funcionamento do próprio negócio. No caso de estudo, recorrendo à adoção de princípios modernos de arquitetura de TI nomeadamente tecnologias de virtualização, foi possível avaliar a situação atual, fazer o desenho lógico e físico da uma solução IT alinhada com o negócio e fazer uma parte considerável da sua implementação.

Em resultado foram consolidados 18 servidores virtuais em 4 servidores físicos, criados ambientes com tolerância à falha e alta disponibilidade e com possibilidade de criar mais servidores virtuais sem custos de *hardware*. Comparativamente a uma infraestrutura tradicional, reduziu a necessidade de espaço físico ocupado na ordem dos 77%, reduzindo também os custos energéticos, os custos de manutenção e operacionais. Na perspetiva financeira esta solução permite um ROI mais curto através da redução do CAPEX e o OPEX.

As otimizações das configurações e evolução ao nível da conetividade traduziram-se em maior aproveitamento dos recursos da LAN. Constatou-se que a taxa de transferência entre servidores virtuais ultrapassa os limites da interface física e que a taxa de transferência entre servidores virtuais e o meio físico atingiu 112 MB/s na rede a 1 Gbps (máximo 125 MB/s), variando entre os 85 e os 102 MB/s. Ao nível da mobilidade e conetividade wireless constatou-se que o balanceamento de clientes pelos APs levou a uma redução significativa da latência e que as quebras de rede foram praticamente eliminadas. Além disso, a centralização e monitorização em tempo real permitiu um controlo efetivo do número de dispositivos ligados em cada AP e SSID e a verificação da qualidade da ligação de cada um destes.

O plano de backup e *disaster recovery* adotado com recurso a *backups* frequentes e replicação periódica das máquinas virtuais, permitiu proteger o ambiente IT de acordo com o RTO e RPO convencionados. O recurso a tecnologias de deduplicação, *snapshots* e CBT permitiram diminuir o espaço de armazenamento, reduzir as janelas temporais e o eventual impacto associado à execução dos trabalhos de salvaguarda de dados.

A nível de segurança a UTM implementada permitiu a visibilidade e controlo necessário no uso de recursos via Internet, além de elevar o nível de segurança através de filtros anti-malware e de mecanismos de proteção de ataques e intrusão. O recurso a SSO simplificou a autenticação dos utilizadores e gestão de credenciais, mantendo os elevados padrões de segurança facultados pelo Active

Directory.

Um dos aspetos relevantes foi o facto da diminuição das queixas dos utilizadores consequentes dos problemas observados antes da implementação da solução desenvolvida, o que libertou a equipa de TI ao nível de procedimentos operacionais de caráter curativos, permitindo tempo para o desenvolvimento de outras atividades.

É também de destacar que aplicando uma metodologia, as fases são melhor coordenadas ficando todos os envolvidos a par do que é feito e mais conscientes da importância das ações que se tomam.

O sucesso da realização do trabalho foi reconhecido pela empresa e para além do projeto desenvolvido, houve ainda possibilidade de aplicar este estudo e metodologia em dois outros projetos de arquitetura de TI. Um projeto foi desenvolvido para uma empresa de águas e saneamentos e outro para uma empresa têxtil. Apesar de existirem pontos comuns, estes dois projetos vieram comprovar que devido a um complexo conjunto de fatores de diversas origens (estratégias, negócio, cultura organizacional, fatores demográficos, expetativas) cada organização é única e não existem soluções iguais. No entanto a metodologia e abordagem foi idêntica em ambos os projetos.

Este trabalho é importante na medida em que ajudará a sensibilizar, antever e evidenciar os problemas consequentes da falta/má gestão das infraestruturas de TI. Estes problemas que vão surgindo e se revelam ao longo do tempo causam por vezes a paragem dos sistemas e perdas de informação sendo que poderão ter um impacto nefasto no bom funcionamento das organizações. Estas situações, por vezes negligentes, poderão refletir-se em custos que poderiam facilmente ser evitados caso existisse maior consciência sobre o estado atual e a existência em simultâneo de um plano de atuação abrangente e coerente com metodologias de análise e boas práticas na implementação da arquitetura de TI.

Relativamente a trabalhos futuros, o desenvolvimento do referencial de boas práticas de arquitetura IT poderá ser complementado por:

- Otimização de processos de realização de documentação;
- Especificação de serviços centralizados de monitorização, alertas e notificações que permita controlar não só os equipamentos principais (servidores e armazenamento) mas todos os equipamentos da infraestrutura;
- Especificação de sistemas de backup de dados e replicação de VMs para sistemas em *cloud* ou *sites* remotos via WAN.
- Desenvolver os processos relativos á manutenção e continuidade da solução desenvolvida.

Referências Bibliográficas

[1] IDC, “Directions 2016, DIGITAL TRANSFORMATION AT SCALE, INNOVATION IN A CHANGE WORLD”. IDC, 2016..

[2] ”DevOps: Uma nova profissão que veio para ficar”, Pplware, 11-Abr-2017. .

[3] Ferreira, Daniel, IT Service Management como Implementar. Estratégia Interna ou Outsourcing? Escrytos|ed. Autor, 2013.

[4] K. K. Hausman e S. L. Cook, IT architecture for dummies. Hoboken, NJ: Wiley Pub, 2011.

[5] R. Hunter e G. Westerman, O Verdadeiro Valor De Ti: Como transformar Ti de um centro de custo em um centro de valor e competitividade. M.Books, 2010.

[6] “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT”. [on-line]. Disponível em: http://www.isaca.org/cobit/pages/default.aspx. [Acedido: 17-Abr-2017].

[7] J. M. Kerr, The best practices enterprise: a guide to achieving sustainable world-class performance. Ft. Lauderdale, FL: J. Ross Pub, 2006.

[8] A. Vico Mañas, Gestão de tecnologia e inovação. São Paulo: Érica, 2001.

[9] S. Buckl e C. M. Schweda, “On the State-of-the-Art in Enterprise Architecture Management Literature”. 2011.

[10] “What is physical to virtual (P2V) ? - Definition from WhatIs.com”, SearchServerVirtualization. [on-line]. Disponível em: http://searchservervirtualization.techtarget.com/definition/physical-to-virtual. [Acedido: 17-Abr-2017].

[11] “Reducing Server total cost of ownership with VMWare Virtualization Software, Withe Paper”. VMware, 2006.

[12] F. Berry, “5 Year TCO Case Study”. IT Brand Pulse, 2016.

[13] R. Weisman, “An Overview of TOGAF Version 9.1”. The Open Group, 2011.

[14] “EMC Unified Storage Fundamentals for Performance and Availability, Applied Best-Practices”. EMC Corporation, 2011.

[15] “UniFi Enterprise Wi-Fi System Datasheet”. Ubiquiti, 2016.

[16] J. Y. A. VCDX-001, M. G. VCDX-023, e C. M. VCDX-079, IT Architect Series: Foundation in the Art of Infrastructure Design: A Practical Guide for IT Architects. 2017.

[17] “TOGAF Strength and Weaknesses”. [on-line]. Disponível em: https://www.eacomposer.com/knowledge-base/togaf-strength-weakness.aspx. [Acedido: 04-Mai-2017].

[18] “TOGAF, an Open Group standard | The Open Group”. [on-line]. Disponível em: http://www.opengroup.org/subjectareas/enterprise/togaf. [Acedido: 04-Mai-2017].

[19] J. A. Zachman, “The Concise Definition of The Zachman Framework by: John A. Zachman”, Zachman International | Enterprise Architecture. [on-line]. Disponível em: https://www.zachman.com/about-the-zachman-framework. [Acedido: 04-Mai-2017].

[20] “ITIL | IT Service Management | ITSM | AXELOS”. [on-line]. Disponível em: https://www.axelos.com/best-practice-solutions/itil. [Acedido: 04-Mai-2017].

[21] D. Kusnetzky, Virtualization: a manager’s guide, First edition. Beijing ; Sebastopol: O’Reilly, 2011.

[22] B. Golden, Virtualization For Dummies®, 3rd HP Special Edition. Wiley Publishing, Inc., 2011.

[23] C. Kumar, “Achieving a Million I/O Operations per Second from a Single VMware vSphere 5.0 Host, White Paper”. VMware, 2011.

[24] “What is ITIL Best Practice? | ITIL | AXELOS”. [on-line]. Disponível em: https://www.axelos.com/best-practice-solutions/itil/what-is-itil. [Acedido: 04-Mai-2017].

[25] “COBIT vs ITIL vs TOGAF: Which Is Better For Cybersecurity?” [on-line]. Disponível em: https://www.upguard.com/articles/cobit-vs.-itil-vs.-itsm-which-is-better-for-cybersecurity-and-digital-resilience. [Acedido: 04-Mai-2017].

[26] S. D. Lowe, Composable Infrastructure For Dummies®, HPE Special Edition. John Wiley & Sons, Inc., 2016.

[27] “vSphere Networking, White Paper”. VMware, Inc., 2017.

[28] “VMware vSphere® vMotion® Architecture, Performance and Best Practices in VMware vSphere, White Paper”. VMware, Inc., 2011.

[29] “XenApp e XenDesktop - Aplicativos e desktops virtuais”, Citrix.com. [on-line]. Disponível em: https://www.citrix.com/products/xenapp-xendesktop/. [Acedido: 16-Mai-2017].

[30] “vSphere - Essentials Kit & Essentials Plus Kit Datasheet “. VMware, Inc., 2015

[31] S. D. Lowe, Hyperconverged Infrastructure For Dummies®, SimpliVity Special Edition. John Wiley & Sons, Inc., 2014.

[32] “Gartner Reprint”. [on-line]. Disponível em: https://www.gartner.com/doc/reprints?id=1-3E3UTVI&ct=160804&st=sb. [Acedido: 06-Mai-2017].

[33] “Virtual Applications | Virtual Apps | ThinApp | VMware”. [on-line]. Disponível em: https://www.vmware.com/products/thinapp.html. [Acedido: 16-Mai-2017].

[34] “HPE Composable Infrastructure Bridging traditional IT with the Idea Economy”. Hewlett Packard Enterprise Development LP, 2015.

[35] “Modelo Corporativo para Governança e Gestão de TI da organização”. ISACA, 2012.

[36] M. Simonsson, P. Johnson, and H. Wijkström, “Model based IT governance maturity assessments

with COBIT". The 15th European Conference on Information Systems, vol. 34, 2007.

[37] "XenServer – Virtualização e consolidação de servidor – Citrix", Citrix.com. [on-line]. Disponível em: https://www.citrix.com/products/xenserver/. [Acedido: 16-Mai-2017].

[38] "Descrição geral do Hyper-V". [online]. Disponível em: https://msdn.microsoft.com/pt-pt/library/hh831531(v=ws.11).aspx. [Acedido: 16-Mai-2017].

[39] W. Weinmeyer, "An Introduction to Fundamental Architecture Concepts", 2017.

[40] "ISO 31000 Risk management". [on-line]. Disponível em: https://www.iso.org/iso-31000-risk-management.html. [Acedido: 10-Mai-2017].

[41] "STP may cause temporary loss of network connectivity when a failover or failback event occurs (1003804)". [on-line]. Disponível em: https://kb.vmware.com/s/article/1003804. [Acedido: 10-Mai-2017].

[42] "NIC teaming in ESXi and ESX (1004088)". [on-line]. Disponível em: https://kb.vmware.com/s/article/1004088. [Acedido: 12-Jun-2017].

[43] "Network Segmentation in Virtualized Environments". VMware, Inc., 2009.

[44] "The Impact of SDN on Portfolio Development: Network Consulting and Integration Services". IDC, 2017.

[45] "VMware NSX Reference Design Guide". VMware, Inc., 2015.

[46] "Contrail Networking – Juniper Networks". [on-line]. Disponível em: https://www.juniper.net/us/en/products-services/sdn/contrail/contrail-networking/. [Acedido: 25-Nov-2017].

[47] "Campus LAN and WirelessLAN Design Guide". Cisco Systems, 2016.

[48] "IEEE 802.11, The Working Group Setting the Standards for Wireless LANs". [on-line]. Disponível em: http://www.ieee802.org/11/. [Acedido: 12-Jun-2017].

[49] "VMware vSAN powers industry-leading Hyper-Converged Infrastructure solutions with a vSphere-native, high-performance architecture.", VMWare. [on-line]. Disponível em: https://www.vmware.com/products/vsan.html. [Acedido: 12-Jun-2017].

[50] "Veeam ONE para VMware e Hyper-V", Veeam Software. [on-line]. Disponível em: https://www.veeam.com/br/virtualization-management-one-solution.html. [Acedido: 13-Jun-2017].

[51] "Wi-Fi Alliance". [on-line]. Disponível em: https://www.wi-fi.org/. [Acedido: 13-Jun-2017].

[52] "SAFE Architecture Guide, Places in the Network: Secure Internet Edge". Cisco Systems, 2016.

[53] "NGFW or UTM: How to Choose", 21-Dez-2016. [on-line]. Disponível em: https://www.watchguard.com/wgrd-resource-center/help-me-choose. [Acedido: 18-Jun-2017].

[54] J. Tate, P. Beck, H. H. Ibarra, S. Kumaravel, e L. Miklas, "Introduction to Storage Area Networks". IBM, 2016.

[55] "What Is a Storage Area Network? | SNIA". [on-line]. Disponível em: https://www.snia.org/education/storage_networking_primer/san/what_san. [Acedido: 20-Jun-2017].

[56] “MSA 2040 User Guide”. Hewlett Packard Enterprise, 2015.

[57] “HPE SAN Design Reference Guide”. Hewlett Packard Enterprise, 2017.

[58] “DataCore | Software-defined Storage & Data Infrastructure Software”. [online]. Disponível em: https://www.datacore.com/. [Acedido: 28-Jun-2017].

[59] G. Maraias, “DataCore™ Certified Solutions Architect Course”. DataCore, 2016.

[60] “EMC VNX2 Unified Best Practices for Performance”. EMC Corporation, 2016.

[61] “MSA 1040/2040 Best practices”. Hewlett Packard Enterprise, 2014.

[62] “inSSIDer Office - WiFi Troubleshooting and Optimization from MetaGeek”. [on-line]. Disponível em: https://www.metageek.com/products/inssider/. [Acedido: 11-Jul-2017

[63] “A Modern Guide to Optimizing Data Backup and Recovery”. Structured, 2014.

[64] F. Moore, “Implementing a Modern Backup Architecture”. Horison, Inc., 2014.

[65] “Backup and Recovery Approaches Using AWS”. Amazon, 2016.

[66] “Veeam Backup & Replication,User Guide for VMware vSphere”. Veeam, 2017.

[67] “HPE Systems, Solutions & Services for SAP HANA | HPE™ Portugal”. [on-line]. Disponível em: https://www.hpe.com/pt/en/solutions/sap-hana.html. [Acedido: 11-Nov-2017].