



Licenciatura em Sistemas e Tecnologias de Informação

Microsoft Exchange Online como solução de correio electrónico empresarial e profissional

Projecto Final de Licenciatura

Elaborado por Mário Filipe Elias de Almeida

Aluno nº 20111527

Orientador: Professor Sérgio Rodrigues Nunes

Barcarena

Junho 2014

O autor é o único responsável pelas ideias expressas neste relatório
Não foi utilizado o novo acordo ortográfico na criação do mesmo.

Agradecimentos

Agradeço a toda a minha família, com especial dedicatória para a minha esposa Sandra e filha Beatriz por todo o apoio e suporte nestes 3 longos anos de esforço e dedicação.

Agradeço igualmente a todos os colegas e amigos que me ajudaram e partilharam este caminho comigo.

Resumo

Microsoft Exchange Online como solução de correio electrónico empresarial e profissional

Este trabalho visa o estudo da tecnologia Microsoft Exchange Online como solução de correio electrónico para as organizações e empresas, com o intuito de agregar informação de âmbito predominantemente técnico, sendo revisto o estado da arte em relação à computação em nuvem, com destaque para a mudança de paradigma que estamos a viver, as características essenciais, os tipos de serviço, os modelos de implementação, e segurança. Foi igualmente revista a visão da Microsoft sobre o sistema operativo da computação em nuvem, bem como a plataforma de serviços Microsoft Office 365, que inclui entre outros serviços o Exchange Online, Lync Online e Sharepoint Online. Será também dado a conhecer o estudo de caso realizado na Universidade Atlântica sobre a migração do serviço de correio electrónico para o Office 365 e identificado o estado da infra-estrutura de Exchange da UATLA antes e após a migração. Serão igualmente apresentadas várias propostas de possíveis melhorias que poderão ser realizadas na Universidade Atlântica em relação à oferta Microsoft na plataforma Office 365.

Palavras-chave: Exchange, Online, Office 365, computação em nuvem, Windows Azure, Microsoft, híbrido, migração, implementação, gestão, configuração.

Abstract

Microsoft Exchange Online as a solution for corporate and professional email

This work aims to study the Microsoft Exchange Online technology as an e-mail solution for organizations and companies, in order to aggregate information from a predominantly technical level, being revised the state of art regarding cloud computing, highlighting the change of paradigm we are living, the essential characteristics, types of service, deployment models, and security. It has been also revised the Microsoft vision of the cloud computing operating system, as well as the Microsoft Office 365 service platform, which includes among other services Exchange Online, Lync Online and SharePoint Online. In this work it will also be presented the case study held at Universidade Atlântica regarding the e-mail service migration to Office 365 and identified the Exchange infrastructure state of UATLA before and after migration. Several proposals will also be presented for possible improvements that could be implemented in Universidade Atlântica regarding the Microsoft offer on Office 365 platform.

Keywords: Exchange, Online, Office 365, cloud computing, Windows Azure, Microsoft, hybrid, migration, implementation, management, configuration

Índice

1. Introdução.....	1
1.1. Motivação	1
1.2. Objectivos	2
1.3. Metodologia	2
2. Conceitos Básicos e Trabalhos relacionados	2
2.1. Computação em nuvem (<i>Cloud Computing</i>)	2
2.2. Segurança	7
2.3. Sistema Operativo da Computação em Nuvem	10
2.4. Office 365	17
3. Exchange Online	22
3.1. Tipos de Migrações.....	23
3.2. Implementação de Office 365	27
3.3. Ambiente híbrido	28
3.4. Gestão e administração	35
3.5. Segurança e <i>Compliance</i>	36
4. Estudo de Caso.....	38
4.1. Perfil da Universidade.....	38
4.2. Situação.....	38
4.3. Solução.....	45
4.4. Melhorias	57
5. Considerações Finais.....	66
5.1. Limitações.....	67
5.2. Trabalho Futuro	67

Bibliografia 68

Índice de figuras

Figura 1 – Modelo visual da definição de Computação em nuvem do NIST	7
Figura 2 – Questões de segurança na nuvem. Retirado de (Singh & Pandey, 2013).....	10
Figura 3 - Visão Cloud OS da Microsoft – Retirado de Windows Azure for Windows Server	12
Figura 4 – Esquema de funcionamento do Windows Azure. Retirado de Microsoft Azure Poster	15
Figura 5 – Portal de cliente Windows Azure – retirado de (Microsoft, 2013).....	16
Figura 6 – Esquema do Hybrid Configuration Engine. Retirado de (Microsoft, 2014)..	29
Figura 7 – Diagrama de rede simplificado da UATLA antes da migração	39
Figura 8 – Exchange Server 2010 Roles. Fonte Microsoft	40
Figura 9 – Interações do Exchange 2010 Mailbox Server. Fonte Microsoft.....	41
Figura 10 – Arquitectura da role de Unified Messaging. Fonte Microsoft	43
Figura 11 – Cenário de implementação de AD FS. Fonte Microsoft.....	50
Figura 12 – Arquitectura Exchange Server 2013. Retirado de (Smith, 2013)	54
Figura 13 – Interação entre as roles CAS e MAILBOX – Retirado de Microsoft, 2013	56
Figura 14 - Diagrama de rede simplificado da UATLA após a migração	56

Índice de tabelas

Tabela 1 - Necessidades dos prestadores de serviços e empresas. Retirado de (Microsoft, 2013)	14
Tabela 2 - Comparação de tipos de migração. Baseado em Microsoft, 2014.....	24
Tabela 3 – Requisitos dos certificados para um ambiente híbrido de Exchange. Baseado em (Microsoft, 2014)	33
Tabela 4 – Quadro de comparação de prioridades versus esforço, na implementação das melhorias do estudo de caso.	57

Lista de abreviaturas e siglas

AD - Active Directory

ADFS - Active Directory Federation Services

ADLDS - Active Directory Lightweight Directory Services

CAS - Client Access Server

DAG - Database Availability Group

DirSync - Microsoft Online Services Directory Synchronization

DLP - Data Loss Prevention

DMZ - Demilitarized Zone

DNS - Domain Name System

DoS – Denial of Service

EAC - Exchange Admin Center

EMC - Exchange Management Console

EMS - Exchange Management Shell

EOP - Exchange Online Protection

FQDN - Fully Qualified Domain Name

GAL - Global Address List

GB - Gigabyte

HCE - Hybrid Configuration Engine

HCW - Hybrid Configuration Wizard

HTTP - Hypertext Transfer Protocol

IM - Instant Messaging

IMAP - Internet Message Access Protocol

IP - Internet Protocol

IRM - Information Rights Management

ISP - Internet Service Provider

LDAP - Lightweight Directory Access Protocol

MAPI - Messaging Application Programming Interface

MBX - Mailbox

MX - Mail exchanger

NIST - National Institute of Standards and Technology

NSPI - Name Service Provider Interface

OAB - Offline Address Book

OAuth - Open Authorization

OWA - Outlook Web App

PBX - Private Branch eXchange

POP3 - Post Office Protocol version 3

RMS - Rights Management Services

RPC - Remote Procedure Call

RTP - Realtime Transport Protocol

S/MIME - Secure/Multipurpose Internet Mail Extension

SAN - Subject Alternative Name

SIP - Session Initiation Protocol

SMTP - Simple Mail Transfer Protocol

SP - Service Pack

SPF - Sender Policy Framework

SSL - Secure Sockets Layer

SSO - Single Sign-On

TB - Terabyte

TCP - Transmission Control Protocol

TIC - Tecnologias de Informação e Comunicação

TLS - Transport Layer Security

TPD - Trusted Publishing Domain

TXT - Text

UM - Unified Messaging

UPN - User principal name

URL - Uniform Resource Locator

VOIP - Voice over IP

1. Introdução

Tal como acontece com todas as mudanças tecnológicas, a era da nuvem apresenta oportunidades para quem está disposto a abraçar o novo modelo, oferecendo a capacidade de resolver problemas, aumentar a eficiência, competir de forma mais eficaz, e descobrir novas oportunidades de negócios (Microsoft, 2013).

Na conferência “Cloud Computing: futurologia ou inevitabilidade?” (APDC, 2013) Paolo Campoli referiu que olha para as soluções na nuvem como "um *enabler* em todas as áreas" porque está na base de uma transformação dos modelos de negócio. O desafio é saber qual o modelo certo para mudar a adopção da computação em nuvem e ultrapassar muitas barreiras mentais que ainda persistem. Alerta para o facto de este ser um negócio que, para ser competitivo, tem que ser de larga escala. Perante a multiplicidade de ofertas e a dificuldade de as distinguir, é preciso criar-se um ecossistema consistente e este é um processo de transição que, quer do lado da oferta, quer da procura, ainda está apenas no início.

Um dos principais objectivos da computação da nuvem passa por reduzir os custos, mas há também preocupações de flexibilização e de ganhos de eficiência, de redução do tempo de desenvolvimento de aplicações e de ligação mais estreita ao cliente ou ao fornecedor.

A própria Microsoft que disponibiliza uma ampla oferta de computação em nuvem, está a migrar os seus serviços. O Director Geral da Microsoft Portugal, João Couto, garante que "a tecnologia e as soluções estão disponíveis e já muito desenvolvidas", e adianta que o tema da segurança tem atrasado a adopção, um tema que tem que ser explicado porque esta é uma questão ultrapassada a seu ver.

O intuito deste trabalho é o de agregar várias informações de âmbito predominantemente técnico, e pretende dar a conhecer as várias formas de integração com sistemas existentes nas empresas, possíveis factores e barreiras de adopção identificados, e utilização dos serviços Microsoft na nuvem.

1.1. Motivação

A motivação principal deste trabalho prendeu-se com a necessidade de conhecer com maior detalhe esta tecnologia, dado que o período de escolha do tema para o trabalho final de curso, coincidiu com uma mudança a nível profissional. Esta mudança permitiu-me trabalhar directamente com as tecnologias disponibilizadas no Office 365 com especial atenção para o Exchange Online.

Achei igualmente muito interessante conhecer o processo de migração da Universidade Atlântica para o Exchange Online, e poder propor eventuais melhorias na utilização de

todas as tecnologias que compõem a oferta do Microsoft Office 365 e que possam aumentar e melhorar a experiência de utilização dos vários serviços disponibilizados.

1.2. Objectivos

O objectivo principal deste trabalho é o de dar a conhecer a tecnologia de Exchange Online, a um nível técnico, realizar uma revisão de literatura para demonstrar como pode ser uma solução viável de correio electrónico empresarial, qualquer que seja a dimensão da organização a que se destina.

Para isso irei identificar as principais características das tecnologias envolvidas, avaliar a arquitectura tecnológica, avaliar as possíveis barreiras e factores de adopção, realizar um estudo de caso sobre a implementação desta tecnologia na Universidade Atlântica e propor possíveis melhorias de utilização dos serviços utilizados, bem como a adopção/implementação de outros serviços de computação na nuvem.

1.3. Metodologia

Este trabalho irá utilizar como base a revisão da literatura para poder de acordo com os objectivos de investigação, identificar as características das tecnologias envolvidas, avaliar a arquitectura tecnológica e as barreiras e factores de adopção do Microsoft Office 365, com foco na tecnologia Exchange Online. Irei utilizar dados agregados (*secondary data*) e realizar um estudo de caso. Para recolher estes dados pretendo utilizar a metodologia Interpretativista. Dado que a realidade é demasiado abrangente e complexa, e o ambiente de mudança das organizações é uma certeza, optei por seguir uma abordagem qualitativa, que orienta-se por uma perspectiva mais interpretativa e construtivista.

2. Conceitos Básicos e Trabalhos relacionados

Neste capítulo será feita uma revisão bibliográfica da Computação em Nuvem, dando a conhecer as suas características e modelos, a mudança de paradigma o sistema operativo da nuvem, incluindo a visão da Microsoft, o Windows Azure, e os vários componentes da tecnologia Office 365.

2.1. Computação em nuvem (*Cloud Computing*)

De acordo com o NIST - *National Institute of Standards and Technology* a definição de computação em nuvem é descrita como “um modelo que permite acesso conveniente e ubíquo realizado a pedido, a um conjunto partilhado de recursos de computação

configuráveis, (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e instalados com mínimo esforço de gestão ou interacção com o fornecedor desses serviços” (Mell & Grance, 2009)

Segundo outros autores, entre eles Ian Foster, a computação em nuvem é um paradigma de computação distribuída em grande escala, impulsionada pela economia de escala, em que um grupo virtualizado e dinamicamente escalável, conseguiu o poder de computação, onde o armazenamento, plataformas e serviços são entregues a pedido para clientes externos através da internet. (Foster, et al., 2008)

A computação em nuvem assenta em características, como a capacidade de computação gerada de forma dinâmica e economicamente eficiente, aliada à capacidade do consumidor final (seja ele um indivíduo ou uma organização) retirar o maior proveito possível desse poder de computação, sem ter que gerir a complexidade subjacente a essa tecnologia. (Silva, 2012)

De acordo com Rajkumar Buyya e outros, a computação está a ser transformada num modelo que consiste em serviços que são entregues de um modo semelhante aos serviços públicos tradicionais, tais como água, electricidade, gás e telefone. (Buyya, et al., 2009)

Como referido pela Microsoft, a nuvem é uma maneira amigável de descrever serviços informáticos baseados na *Web* alojados fora da sua organização. Quando utiliza serviços baseados na nuvem, a sua infra-estrutura de TI reside fora da sua propriedade (fora do local) e é mantida por terceiros (alojada) em vez de residir num servidor situado na sua casa ou empresa (no local). Por exemplo, com o Office 365, o armazenamento de informações, informática e o *software* localizam-se e são geridos remotamente em servidores que pertencem à Microsoft. Muitos dos serviços que utiliza diariamente pertencem à nuvem, tudo desde o correio electrónico baseado na *Web* ao acesso a contas bancárias via dispositivos móveis e ao armazenamento de fotografias *online*. Devido ao facto de a infra-estrutura estar localizada *online*, pode aceder à mesma a partir de qualquer local com um PC, *tablet*, *smartphone* ou outro dispositivo com ligação à Internet.

Cloud Computing é um novo termo para um sonho de longa data da computação como um utilitário, que surgiu recentemente como uma realidade comercial. É provável que a computação em nuvem tenha o mesmo impacto sobre o *software* que as fundições tiveram na indústria de hardware. Refere-se a aplicações entregues como serviços através da Internet, do *hardware* e sistemas de *software* nos *datacenters* que fornecem esses serviços (Armbrust, et al., 2009).

Este termo denota a infra-estrutura como uma nuvem, a partir do qual empresas e utilizadores podem aceder a aplicações em qualquer lugar, e desta forma o mundo da

computação está em rápida transformação no desenvolvimento de *software* para consumo como um serviço. (Buyya, et al., 2009)

A computação em nuvem irrompeu no cenário da computação de alto desempenho nos últimos anos, e estabeleceu-se como uma alternativa viável para *clusters* de sistemas customizados, dado existirem muitos clientes que não tem recursos (tempo e/ou dinheiro) para construir, configurar e manter os seus próprios clusters. A capacidade de pagarem por serviços e recursos apenas derivado da sua utilização e necessidade, e da facilidade de expansão, implementação, e remoção desses recursos é muito atractivo. (Hill, et al., 2010)

2.1.1. Mudança de Paradigma

Segundo Arlindo Marcon Jr, Marcos Laureano, Altair Santin e Carlos Maziero, baseados em outros autores, referem que há quase 50 anos foi criado o sistema de partilha de tempo (*time-sharing*). Este sistema fornecia acesso a poder computacional para utilizadores que não possuíam o seu próprio *mainframe*, que utilizavam sistemas do tipo *hub-and-spoke*. No começo dos anos 1980 com a chegada dos computadores pessoais, programas e dados não dependiam mais de um centro computacional para serem executados. Cada indivíduo passou a controlar seu próprio ambiente de trabalho, podendo customizá-lo de acordo com suas necessidades. O modelo cliente-servidor, introduzido na mesma época, oferecia um serviço que podia ser invocado através da rede para atender uma necessidade do cliente. (Marcon, et al., s.d.)

No começo dos anos 90, Ian Foster e Carl Kesselman apresentaram o conceito de “Grid”, fazendo uma analogia com o fornecimento de electricidade. O termo *Grid Computing* apareceu para descrever as tecnologias que iriam permitir aos consumidores usufruir da computação distribuída e assim endereçar o problema do processamento de problemas complexos, numa escala distribuída (Foster, et al., 2008)

Baseado em John Erikson e outros autores, as tarefas computacionais podem ser migradas dos computadores e servidores corporativos para a nuvem computacional. Um número crescente de pequenas e médias empresas procuram melhorar a sua eficiência operacional e aplicações de negócio ao utilizar este acesso, que anteriormente estava apenas disponível a grandes empresas (Erickson, et al., 2009)

À medida que cada vez mais prestadores de serviço e tecnologias entrem no mercado, os programadores são confrontados com o problema cada vez mais difícil de comparar as várias ofertas e decidir qual o fornecedor para colocar uma aplicação em produção. Um passo essencial no processo de avaliação das várias ofertas de computação em nuvem será o determinar o desempenho dos serviços oferecidos e coincidi-los com os requisitos da aplicação. (Hill, et al., 2010)

2.1.2. Características essenciais

Self-service a pedido (On-demand self-service)

De acordo com as suas necessidades, um utilizador pode providenciar de forma unilateral e automática, recursos de computação tais como tempo de servidor ou armazenamento em rede, sem necessidade de interacção humana com cada fornecedor de serviços.

Acesso por banda larga (*Broad network access*)

Os recursos estão disponíveis na rede e podem ser acedidos através de mecanismos padrão que promovam a sua utilização por diferentes plataformas (por exemplo, telemóveis, *tablets*, computadores portáteis e estações de trabalho).

Conjunto de recursos (*Resource pooling*)

Os recursos computacionais do fornecedor do serviço são reunidos para servir vários utilizadores usando um modelo de múltiplos utilizadores, com diferentes recursos físicos e virtuais atribuídos dinamicamente de acordo com os pedidos destes últimos. Há um sentido de independência de localização em que geralmente o cliente não tem nenhum controlo ou conhecimento sobre o local exacto dos recursos fornecidos, mas pode ser capaz de especificar o local num nível mais elevado de abstracção (por exemplo, país, estado ou centro de dados). Armazenamento, processamento, memória e largura de banda de rede são exemplos destes recursos.

Elasticidade rápida (*Rapid elasticity*)

Os recursos podem ser configurados elasticamente e disponibilizados, em alguns casos automaticamente, muito rapidamente para fora e de uma forma que procura um aperfeiçoamento activo. Do ponto de vista do consumidor, parece que os recursos disponíveis são muitas vezes ilimitados e passíveis de serem utilizados e apropriados em qualquer quantidade e a qualquer momento.

Serviço medido (*Measured service*)

Os sistemas de *Cloud Computing* controlam e optimizam automaticamente a utilização dos recursos, aproveitando uma capacidade de medição num nível de abstracção apropriado para o tipo de serviço (por exemplo, armazenamento, processamento, largura de banda e contas de utilizador activas). O uso dos recursos pode ser monitorizado e controlado, fornecendo transparência quer para o provedor quer para o consumidor final do serviço utilizado. Baseado em (Silva, 2012) e (Bhargava & Samant, 2013)

2.1.3. Tipos de Serviço

Software como serviço (*Software as a Service - SaaS*)

É disponibilizada ao utilizador, a capacidade de usar as aplicações do fornecedor do serviço, assentes numa infra-estrutura na nuvem. As aplicações podem ser acedidas através

de vários dispositivos, tais como um navegador ou através de um programa. O utilizador não gere nem controla a infra-estrutura subjacente da nuvem, incluindo a rede, os servidores, sistemas operativos, armazenamento de dados ou até mesmo definições do aplicativo, com a possível exceção de definições de configuração do aplicativo, específicas do utilizador

Plataforma como serviço (*Platform as a Service - PaaS*)

O recurso fornecido ao consumidor é o de este implementar para a infra-estrutura da *cloud*, aplicativos criados por si usando linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo fornecedor do serviço. O utilizador não gere nem controla a infra-estrutura subjacente da nuvem, incluindo a rede, os servidores, sistemas operativos, armazenamento de dados, mas tem controlo sobre os aplicativos desenvolvidos e sobre as definições de configuração para o ambiente de alojamento de aplicativos.

Infra-estrutura como serviço (*Infrastructure as a Service - IaaS*)

O recurso fornecido ao consumidor é o de fornecer o processamento, armazenamento, redes e outros recursos fundamentais de computação onde o consumidor é capaz de desenvolver, implementar e executar *software*, tal como sistemas operativos e aplicações. O utilizador não gere nem controla a infra-estrutura subjacente da nuvem, mas tem controlo sobre sistemas operativos, armazenamento e aplicações instaladas (e possivelmente também poderá ter controlo, embora limitado, de alguns componentes de rede seleccionados, tais como *firewalls*). (Silva, 2012)

2.1.4. Modelos de Implementação

Nuvem Privada (*Private cloud*)

A infra-estrutura da nuvem é configurada para uso exclusivo de uma única organização que compreende múltiplos utilizadores (por exemplo, unidades de negócio). Pode ser de propriedade, gerida e operada pela própria organização, por uma entidade terceira, ou por uma combinação destas duas modalidades. Poderá existir dentro ou fora das instalações da organização.

Nuvem de Comunidade (*Community cloud*)

A infra-estrutura da nuvem é configurada para uso exclusivo de um conjunto específico de utilizadores, que pertencem a empresas ou organizações que têm interesses comuns (por exemplo, requisitos de segurança, política de privacidade e aspectos de conformidade). Pode ser de propriedade, gerida e operada por uma ou mais das organizações da comunidade, por uma entidade terceira, ou por alguma combinação destas modalidades. Poderá existir dentro ou fora das instalações da organização.

Nuvem Publica (*Public cloud*)

A infra-estrutura da nuvem é configurada para utilização aberta ao público em geral. Pode ser de propriedade, gerida e operada por uma empresa, instituição de ensino ou organização governamental, ou por alguma combinação destas modalidades. Existe nas instalações do fornecedor da *cloud*.

Nuvem Híbrida (*Hybrid cloud*)

A infra-estrutura da nuvem é uma composição de duas ou mais infra-estruturas de nuvem distintas (de comunidade, privada ou pública) que se mantêm entidades únicas, mas que estão ligadas por uma tecnologia padronizada ou proprietária que permite a portabilidade dos dados e das aplicações. (Silva, 2012)

A figura 1 demonstra visualmente o modelo de definição de computação em nuvem do NIST, que inclui as características essenciais, os tipos de serviço e os modelos de implementação referidos anteriormente.

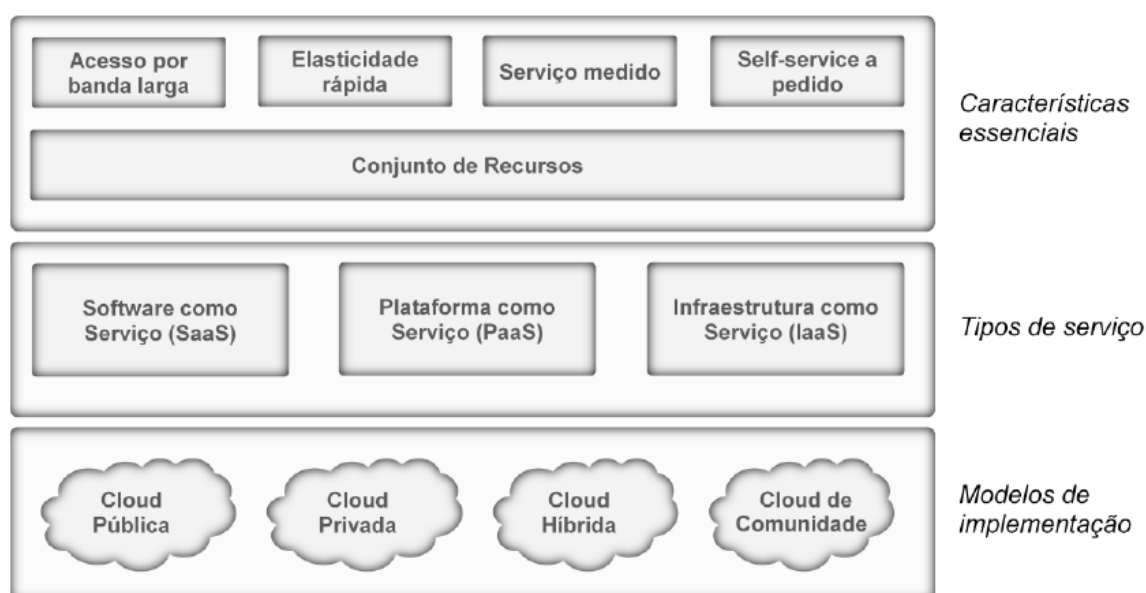


Figura 1 – Modelo visual da definição de Computação em nuvem do NIST

2.2. Segurança

Segundo Rita de Castro e Verónica de Sousa, o paradigma da Computação em Nuvem embora esteja fundamentado na utilização de ferramentas fortemente difundidas nas Tecnologias da Informação e Comunicação, tem como principal característica a transformação dos modos tradicionais de como as empresas utilizam e adquirem os recursos de TIC. Na adopção do modelo de Computação em Nuvem os processos de negócios e procedimentos precisam levar em conta a segurança e privacidade das informações que ficarão na nuvem. Num ambiente computacional tradicional, é comum

observarmos que os requisitos de segurança são ignorados em detrimento dos requisitos funcionais dos sistemas. Tal facto ocasiona o desenvolvimento de sistemas e ambientes extremamente vulneráveis aos ataques externos (Castro & Sousa, s.d.)

Segundo Shuchita Bhargava e Rahul M. Samant, existem uma série de questões de segurança compostas por um conjunto de redes, base de dados, sistemas operativos, virtualização, gestão de transacções de memória.

Questões de Infra-estrutura: A infra-estrutura é um paradigma de segurança enfrentado pelos prestadores de serviço. Na nuvem os dados serão distribuídos por vários servidores independentemente de onde os dados irão ser armazenados no final. O sistema de virtualização adoptado pode trazer benefícios a *hackers* e *crackers* para eventuais roubos de dados. As estatísticas mostram que um terço das quebras de seguranças, devem-se a perda e/ou roubo de portáteis ou outros dispositivos, expondo acidentalmente os dados na internet.

Pelo contrário, os problemas que os clientes enfrentam na nuvem são devidos à lentidão e degradação das conexões, e por esse motivo os clientes não conseguem realizar o *login* ou manter a conexão com o correio electrónico *online*, finalizar transacções ou pagamentos, levando desta forma a que mantenham a dependência na infra-estrutura tradicional. A nuvem necessita de alta qualidade e largura de banda em conexões de alta velocidade para um funcionamento e utilização eficiente. A qualidade de serviço pode ser julgada no número de vezes que a ligação é desconectada, o tempo de resposta, a extensão de atrasos no processamento de dados, e perda de dados.

Segurança de Aplicações cliente: Aplicações e dados na nuvem estão vulneráveis a muitos ataques. O prestador do serviço e o cliente devem ter um acordo para prevenir possíveis questões de segurança.

O prestador do serviço deve gerir a infra-estrutura e disponibilidade das aplicações, mas não deve ter acesso aos dados sem a permissão explícita do cliente. Os dados podem ser acedidos por autoridades legais ou colaboradores internos, mas neste caso o cliente deverá ser sempre informado previamente.

Privacidade, Armazenamento de dados e Transferência de dados: Protecção de dados e privacidade são frequentemente apresentados como sendo riscos chave de informação pessoal. A irresponsabilidade e negligência dos colaboradores pode causar muitas vulnerabilidades e quebras de segurança. A cibercriminalidade também esta a aumentar. Mover os dados para a nuvem pode ser perigoso se o fornecedor é fraco ou descuidado em termos de segurança. Muitas preocupações também surgem pelas organizações devido aos dados sensíveis que podem correr riscos num ambiente multi-tenant.

Um ambiente multi-tenant consiste no princípio de uma ou mais instâncias de *software* serem executadas num servidor, servindo múltiplos clientes ou organizações.

Existem outras preocupações em relação á privacidade dos dados, tal como a divulgação accidental ou deliberada. Os administradores de sistemas são depositários de uma enorme quantidade de dados. Estes dados podem ser deliberadamente ou acidentalmente divulgados, com consequências indesejáveis.

O problema da privacidade dos dados é amplamente conhecida, e a computação em nuvem vem amplia-la. (Ryan, s.d.)

“Cloud is purchased at lower price and provides faster deployment of applications. 52% cloud application target business application. By 2013, 80% companies will spend 7 to 30% of their IT budget in cloud.” (Bhargava & Samant, 2013)

Segundo a Gartner Inc., empresa de consultoria e pesquisa sobre tecnologias de informação, as seguintes questões de segurança são as mais prementes para os utilizadores que utilizam a tecnologia na nuvem:

- Acesso do utilizador
- Conformidade regulamentar
- Localização dos dados
- Segregação dos dados
- Verificação de recuperação de desastres (*Disaster recovery*)
- Recuperação de desastres (*Disaster recovery*)
- Viabilidade a longo prazo

As questões jurídicas e regulamentares são bastante importantes na computação em nuvem. Um dos mais importantes assuntos jurídicos é a questão da jurisdição. Os bits e os bytes que são armazenados na nuvem residem fisicamente num servidor algures. (Bhargava & Samant, 2013)

As soluções de computação em nuvem têm tido um impacto substancial sobre a maneira em que os negócios são conduzidos, embora a segurança dos dados na nuvem tem sido uma preocupação constante, segundo Vaishali Singh e S. K. Pandey. Quem tem de tomar decisões conscientes, necessita de informação, e a nuvem facilita o acesso e utilização dessas informações. A segurança da informação é de máxima importância tanto para os clientes como para os prestadores de serviço.

O criar protecção na nuvem, refere-se aos princípios de segurança aplicados para proteger os dados armazenados, aplicações em uso e a infra-estrutura associada com a tecnologia de nuvem. (Singh & Pandey, 2013). Como referido pelos autores, na Figura 2 podemos verificar as várias questões relacionadas com a segurança dos serviços na nuvem,

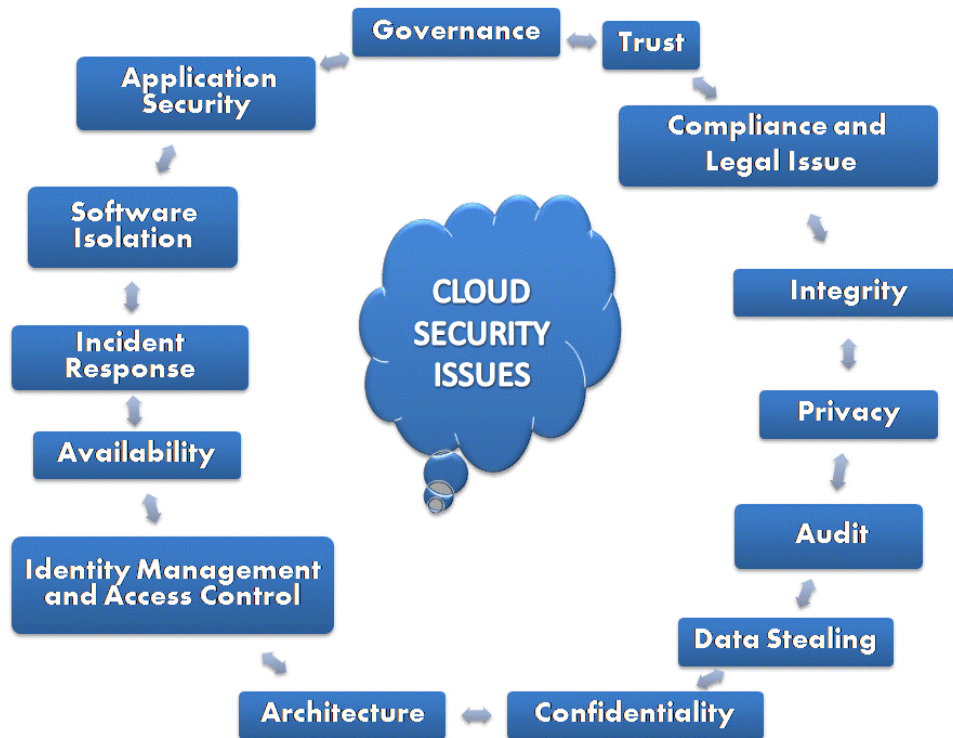


Figura 2 – Questões de segurança na nuvem. Retirado de (Singh & Pandey, 2013)

2.3. Sistema Operativo da Computação em Nuvem

Segundo a Microsoft, o advento da computação em nuvem está reescrevendo muitas das regras e pressupostos há muito estabelecidos para as tecnologias de informação (TI) empresariais.

As quatro paredes do *datacenter* corporativo já não restringem as aplicações e a carga de trabalho, dado que os administradores de sistemas e programadores procuram nos prestadores de serviços e nuvem de computação pública (*Public Cloud*) uma maneira mais eficiente e ágil para entregar valor ao negócio.

Tal como acontece com todas as mudanças tecnológicas, a era da nuvem apresenta oportunidades para quem está disposto a abraçar o novo modelo, oferecendo a capacidade de resolver problemas, aumentar a eficiência, competir de forma mais eficaz, e descobrir novas oportunidades de negócios

As empresas estão a aprender com a expansão e generalização da adoção orgânica de serviços de nuvem privada, e com a possibilidade de escolha em termos de agilidade e preços com base na utilização. Como resultado os departamentos de TI das empresas procuram cada vez mais um modelo interno de prestador de serviços como um meio de obter retorno e ter visibilidade.

Para os prestadores de serviços, há uma enorme oportunidade de albergar as cargas de trabalho corporativas que agora estão libertas do *datacenter* corporativo. Os prestadores de serviços que consigam superar as preocupações das empresas, relativamente ao desconhecimento da plataforma tecnológica e mobilidade, terão maiores hipóteses de ganhar a confiança das empresas.

Ao longo dos últimos anos, temos visto um aumento maciço no uso de redes e aplicações sociais. A maioria das empresas hoje incorpora a sua presença social no *Facebook* ou no *Twitter* e/ou a sua própria aplicação móvel.

Este aumento das redes sociais e aplicações móveis tem levado a uma explosão de dados em massa. As organizações agora têm mais informações do que nunca para utilizar. Por exemplo, muitas organizações tendem a obter feedback instantâneo sobre os seus produtos e serviços a partir das redes sociais e a opinião sobre a concorrência. Para competirem eficazmente no mercado, as organizações necessitam de recolher, armazenar e processar esses dados (*Big Data*)

A transformação de dispositivos móveis, como o telemóvel e o *tablet* em ferramentas de produtividade, têm desafiado os departamentos de TI. Os colaboradores pretendem utilizar estes dispositivos como ferramenta de trabalho, porque estão familiarizados com os mesmos devido ao uso diário. Os departamentos de TI necessitam de abraçar a consumerização das Tecnologias de Informação e oferecer aos colaboradores, opções de trabalho mais flexíveis. Além destes factos, todo o processo de computação está a alterar-se. Os modelos de computação em nuvem substituíram as abordagens tradicionais em que aplicações específicas ficam assentes em servidores específicos. Nesta nova abordagem as organizações de TI podem implementar aplicações como serviços elásticos de *self-service*.

Com estas mudanças surgiram inovações em tecnologia que ajudam a viabilizar e suportar estes cenários de computação. Chips *multi-core* mais poderosos aumentam a densidade da memória, enquanto levam a que os custos baixem. Os custos relacionados com as tecnologias de armazenamento, como as *Solid State Drive (SSD)*, também estão a baixar, proporcionando uma grande oportunidade para o *datacenter* tirar proveito do *hardware* padrão da indústria, enquanto proporciona capacidade de nível empresarial. Depois existe a rede, onde interconexões rápidas entre armazenamento e nós de computação estão a alavancar quantidades impressionantes de inovação. (Microsoft, 2013)

2.3.1. A visão da Microsoft

A visão do Cloud OS da Microsoft (demonstrada na Figura 3) visa oferecer aos clientes uma plataforma consistente para infra-estrutura, aplicações e dados. Esta plataforma única

estende-se pelos *datacenters* dos clientes, provedores de alojamento de serviços e a nuvem pública da Microsoft.



Figura 3 - Visão Cloud OS da Microsoft – Retirado de Windows Azure for Windows Server

Esta visão permite que os clientes tenham uma estratégia unificada e uma plataforma consistente que pode alcançar o seguinte:

Transformar o *datacenter*: A unidade tradicional de computação está a mover-se do servidor único para o nível de *datacenter*. Os clientes necessitam de uma infra-estrutura que forneça um salto geracional em agilidade, elasticidade e escalabilidade num conjunto de recursos partilhados e que ofereça mais automação e self-service.

Desbloquear a compreensão sobre quaisquer dados: Com o aumento exponencial do volume de dados, os clientes necessitam de uma plataforma que lhes forneça uma visão completa dos dados de forma a poderem competir mais eficazmente. Necessitam igualmente de aceder a grandes volumes de dados, especialmente dados não estruturados, para realizarem novas perguntas e descobrir novas fontes de dados, que podem ser combinados com os dados existentes, de forma a poder fornecer conhecimento.

Capacitar as pessoas centradas nas TI: A proliferação e a variedade de novos dispositivos, significa que as empresas precisam de abraçar a vertente de utilizar dispositivos pessoais e capacitar as pessoas centradas nas tecnologias de informação. Os utilizadores actuais esperam ser produtivos, independentemente do que escolherem ou do dispositivo que escolherem. Os departamentos de TI necessitam de ser capazes de gerir facilmente esses dispositivos e entregar as aplicações de modo seguro num ambiente móvel alargado.

Habilitar aplicações modernas: As aplicações actuais necessitam de interagir com outras aplicações criadas em várias plataformas e linguagens de programação. Estas aplicações irão ter a necessidade de serem utilizadas no local (*on-premises*), remotamente (*off-premises*) e serem disponibilizadas em múltiplos dispositivos.

Esta visão permite executar em massa serviços *online* e soluções locais a partir das mesmas ferramentas de monitorização que já estão instaladas (caso utilizem tecnologia Microsoft) e que são familiares aos clientes, o que permite elevar a consistência dos ambientes.

Esta consistência abrange muitas facetas, incluindo o seguinte:

- Desenvolvimento de aplicações de modo flexível, que inclui plataformas Microsoft e de código aberto
- Providenciar uma abordagem de gestão, consistente e unificada através destes *datacenters*
- Oferecer uma plataforma de dados abrangente
- Distribuir uma identidade comum e uma abordagem de segurança
- Fornecer virtualização integrada

Segundo palavras exactas da Microsoft “Este recursos consistentes, juntamente com a nossa experiência em primeira, ao ter em execução mais de 200 serviços de nuvem para mais de 1 bilião de clientes e mais de 20 milhões de empresas em todo o mundo, faz com que o *Cloud OS* seja uma proposta única” (Microsoft, 2013)

2.3.2. Prestadores de Serviço e Empresas

Na era da computação em nuvem, as aplicações corporativas e a carga de trabalho das Tecnologias de Informação foram movidas para além das restrições físicas do *datacenter* corporativo. Em sentido crescente, cada vez mais empresas procuram mover a carga de trabalho de desenvolvimento, teste e produção para nuvens públicas como meio de alcançar flexibilidade e agilidade, e reduzir custos.

Estas organizações estão dispostas a negociar despesas de capital investido em *hardware* por despesas operacionais, com prestadores de serviço ou subscrições de nuvem pública, em que pagam apenas o que utilizam.

Como resultado desta prática, os prestadores destes serviços viram uma grande oportunidade de crescimento, mas para aproveitar esta oportunidade precisam de reposicionar a sua plataforma tecnológica e negócio para atrair as empresas. Um dos factores mais importantes para este reposicionamento é a habilidade de ter uma tecnologia familiar, em que as empresas possam confiar e integrar com os *datacenters* locais.

O serviço IaaS - Infra-estrutura como serviço é o mais atraente para os clientes empresariais, isto porque fornece uma compreensão simples, facilidade e rapidez de implementação.

A facturação por utilização é essencial para os prestadores de serviços. A baixa margem de lucro e a natureza de alto volume de negócios, significa que a automação é essencial em conjunto com outros recursos, de modo a otimizar a receita gerada por cada peça de *hardware* adquirida.

Os prestadores de serviço pretendem ter como base dos seus planos de serviços, uma oferta gratuita, de modo a cativar e adquirir clientes, e posteriormente um mecanismo de facilitar a venda de ofertas de maior valor. Além disto, a customização, integração e valorização da marca, oferecem oportunidades valiosas para alinhar recursos da nuvem com processos de negócio existentes.

A Tabela 1 mostra a simetria entre as necessidades dos prestadores de serviço e das empresas, de ter uma solução única, onde podem simples e facilmente providenciar um ambiente de alojamento em nuvem, self-service em cima de investimentos já realizados em *software* e *hardware*.

Prestadores de serviço pretendem...	Empresas pretendem...
Ganhar e facilmente adquirir/providenciar cada vez mais negócios de clientes corporativos	Flexibilidade e agilidade na escolha da nuvem por razões financeiras, comerciais ou de conformidade
Ambiente <i>multi-tenant</i> , Infra-estrutura como serviço (IaaS) em self-service.	Ambiente de computação em nuvem <i>multi-tenant</i> que possam controlar e que seja simples de utilizar.
Facturação por utilização	Facturação por utilização
Automatização extrema	Operações automatizadas e de simples execução
Optimização da monetização do <i>hardware</i>	Utilização mais eficaz dos recursos de <i>hardware</i> existentes, uso de <i>hardware</i> a baixo custo
Oportunidades para aumento de vendas e aumento da utilização dos clientes	Fornecer flexibilidade na forma que os inquilinos optam por utilizar a capacidade
Ofertas personalizadas e diferenciação de nuvem pública.	Comodidade e ofertas customizadas de computação em nuvem
Integração com o portal e customização da marca	Interoperabilidade com sistemas existentes

Tabela 1 - Necessidades dos prestadores de serviços e empresas. Retirado de (Microsoft, 2013)

2.3.3. Windows Azure

O Windows Azure é uma plataforma de computação em nuvem aberta e flexível que permite construir, colocar em produção e gerir aplicações através de uma rede global de *datacenters* geridos pela Microsoft. Podemos verificar todo o esquema de funcionamento do Windows Azure na Figura 4, dividido nas várias áreas que constituem o produto.

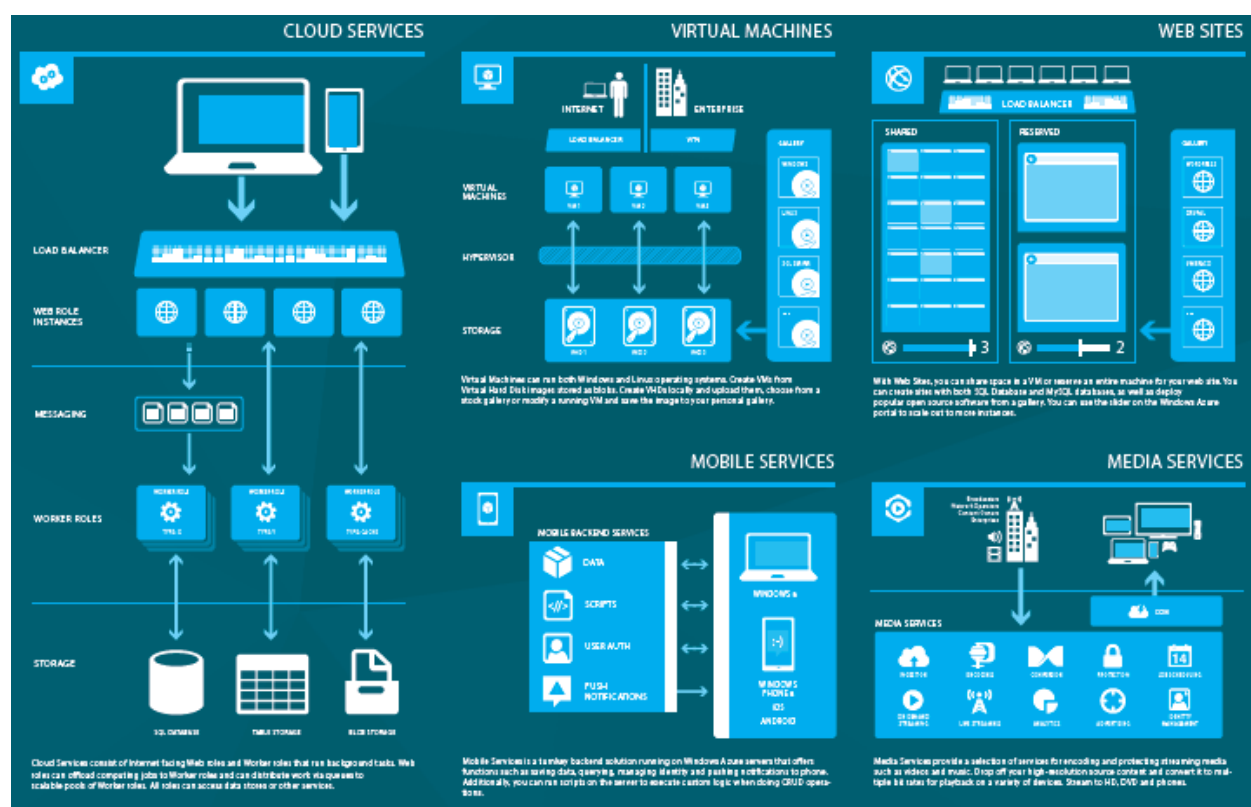


Figura 4 – Esquema de funcionamento do Windows Azure. Retirado de Microsoft Azure Poster

Os clientes do Windows Azure acedem à nuvem pública através de um *site* conhecido como portal de cliente ou gestão. Este portal funciona como uma porta de entrada para vários serviços de tecnologias de informação, entregues em cima da computação, armazenamento e recursos de rede dos *datacenters* da Microsoft, localizados em todo o mundo. A Microsoft gere os recursos do *datacenter*, contratando para o efeito pessoas especializadas na administração de sistemas.

Os *datacenters* são compostos na sua base por sistemas Windows Server e System Center, que são familiares à grande maioria das empresas. Os administradores de tecnologias de informação também podem fornecer serviços similares ao terem o seu próprio portal de administração dedicado consistente com o portal do cliente.

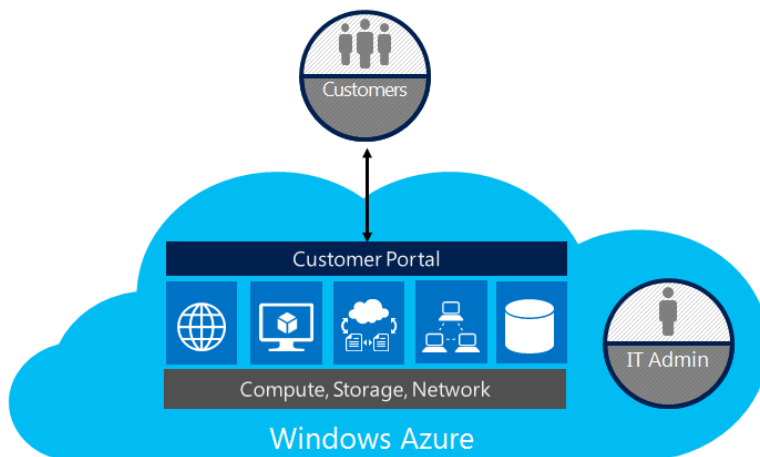


Figura 5 – Portal de cliente Windows Azure – retirado de (Microsoft, 2013)

Na Figura 5 podemos visualizar o esquema do portal de cliente do Windows Azure. Ao utilizar o portal os administradores de sistemas podem ter uma gama de capacidades de gestão, como as seguintes:

Construção de recursos de nuvem: Os administradores podem definir a computação, armazenamento, rede e outros recursos que sustentam cada um dos serviços do *tenant*.

Automatização: Os administradores podem criar *runbooks* em Windows Powershell para definir uma série de processos, que devem ser executados em circunstâncias específicas, reduzindo a necessidade de intervenção humana e os custos da gestão da nuvem.

Facturação: Os administradores podem definir estruturas de preços associadas aos serviços dos clientes

Gestão do *Tenant*: Os administradores podem lidar com tarefas associadas à gestão de contas de utilizadores do *tenant* e relatórios de actividade.

Planos de alojamento: Estes planos permitem com que os administradores possam estabelecer várias combinações de serviços, recursos da nuvem e quotas, disponibilizando-as para subscrição para grupos específicos de *tenants*.

Todas as capacidades mencionadas combinam-se para formar experiências e serviços do Windows Azure Pack. Este pacote inclui o portal do cliente, portal de gestão e serviços de administração baseados no Windows Server e System center. (Microsoft, 2013)

2.3.4. Performance

A performance da computação em nuvem é um tema com bastante relevância. São poucos, ou nenhuns os prestadores de serviço ou tecnologias que oferecerem garantias com base em dados quantitativos.

Independentemente das potenciais vantagens da computação em nuvem em comparação com aplicações empresariais implementadas localmente, as infra-estruturas da nuvem podem vir a falhar se as aplicações colocadas em produção não cumpram as exigências comportamentais esperadas. (Hill, et al., 2010)

2.4. Office 365

Segundo a Microsoft a tecnologia de computação em nuvem tem várias vantagens. Muitos podem pensar que o Office 365 é apenas uma colecção de programas de *software* para utilização profissional, mas esta tecnologia contém muito mais. Na sua designação mais simples pode-se referir que o Office 365 inclui todas as funcionalidades que uma empresa precisa para criar uma infra-estrutura de Tecnologias de Informação profissional. (Microsoft, 2013)

- Disponível em qualquer dispositivo: Os colaboradores têm acesso ao Office Web Apps quer estejam num PC de casa, num PC do escritório, num *smartphone* ou *tablet*.
- Os documentos e dados actuais estão sempre disponíveis: Graças aos serviços na *cloud*, os documentos, contactos e compromissos existentes em todos os dispositivos estão sempre disponíveis na versão mais recente.
- A colaboração é fácil: Os documentos podem ser editados por vários colaboradores em simultâneo. A introdução de dados em grupo é possível, mesmo que a equipa esteja geograficamente dispersa.
- Áreas de trabalho seguras: Uma área protegida por palavra-passe permite o acesso a informações confidenciais da empresa apenas a quem tenha a autorização adequada.
- *Web site* incluído: É possível criar e editar facilmente um sítio da empresa personalizado utilizando as ferramentas do Office.
- Conferência Web e *chat*: As reuniões com participantes em localizações diferentes podem ser facilmente planeadas e realizadas, incluindo a troca de documentos.
- Segurança de dados: A protecção actualizada contra *hackers* e vírus, bem como a capacidade de encriptar documentos privados estão incluídas.
- Administração Simples: O departamento de TI pode gerir o acesso e as permissões facilmente, bem como criar e aplicar políticas internas de forma flexível.

- **Transparência:** O Office 365 é vendido por subscrições. Isto significa que apenas paga as licenças de que realmente necessita. Saberá sempre exactamente quanto pagará de subscrição mensal.
- **Actualizações Incluídas:** As actualizações e novas versões do Office estão incluídas nas subscrições. O seu *software* está sempre actualizado.
- Os subscritores do Office 365 podem agora transferir e utilizar o Office Mobile para iPhone gratuitamente.

Segundo o *White Paper* “Office 365 Justification” realizado pela MatrixForce Corporation, o Office 365 é uma oferta de SaaS (Software as a Service), que providencia portais e aplicações para administradores de TI e utilizadores finais. O Office 365 combina a bem conhecida tecnologia de Office desktop com as versões baseadas em nuvem de comunicações de próxima geração e serviços de colaboração:

- Microsoft Exchange Online, oferece correio electrónico com funcionalidades avançadas e necessidades empresariais, agendamento e mobilidade.
- Microsoft SharePoint Online, com armazenamento de documentos avançado e integração de aplicações.
- Microsoft Lync Online, fornece disponibilidade de presença, mensagens instantâneas e partilha do ambiente de trabalho.

Este produto oferece acesso seguro em todas as plataformas e dispositivos, bem como tecnologias de *anti-spam* e antivírus superiores que são automaticamente actualizados para protecção contra as ameaças mais recentes.

As funcionalidades e serviços associados com o Office 365 são *built-in*, ou seja embutidos no próprio produto, de forma a reduzir o tempo e custo associados com a segurança dos sistemas de Tecnologias de Informação.

Ao mesmo tempo, o Office 365 permite controlar facilmente as permissões, políticas e recursos através de consolas de gestão e administração, de modo a atender às necessidades de negócio e de segurança específicas. (MatrixForce Corporation, 2012)

2.4.1. Serviços de colaboração



- Correio electrónico de classe empresarial, calendário e contactos, no PC, telefone e web
- Caixas de correio com até 50 GB de capacidade e habilidade para enviar mensagens até 25 MB
- 99,9% de tempo de actividade com compromisso financeiro ao nível de SLA
- *Backup* de dados continuo entre *datacenters* redundantes
- *Compliance* regulatória incluindo CyberTrust, SOX, SAS 70 Type II, HIPAA, ISO 27001 e 27002
- Sempre actualizado contra vírus e *spam* com o Exchange Online Protection (EOP)
- Correções automáticas eliminam o tempo e esforço de manutenção e assistência ao sistema de correio electrónico
- Políticas de segurança para reforçar o bloqueio do PIN e a limpeza automática (*wipe*) de dados para dispositivos móveis perdidos
- Políticas de arquivo e retenção de correio electrónico e opções legais para a preservação de dados
- Suporte telefónico disponível 24 horas por dia e 7 dias por semana



- Saber se os outros estão disponíveis para comunicar, com informação de presença
- Integração com várias aplicações Microsoft Office
- Criar, moderar e ligar a reuniões ou eventos pré-planeadas e de reuniões *on-the-fly* de áudio e/ou vídeo, com pessoas dentro e fora da organização
- Colaboração com *sites* Sharepoint
- Comunicar com outras organizações que utilizem o Lync
- Comunicar com contactos Skype e *Windows Live Messenger*
- Permite que outros clientes participem em *Conference calls*, mesmo que não sejam clientes Office 365
- Aumento da comunicação e produtividade com redução do correio electrónico, através de mensagens instantâneas
- Redução de custos para o negócio (despesas de viagens e telefone)



- Partilha de informação através de um ambiente altamente seguro e trabalho conjunto independente da localização
- Melhoria da produtividade da equipa com ferramentas colaborativas fáceis de usar
- Convidar utilizadores externos para trabalhar em projectos, documentos, e outros dados importantes
- Gestão fácil de documentos e ajuda na integridade do conteúdo
- Informação sempre actualizada relativa à empresa
- Ter os colaboradores rapidamente actualizados
- Redução da complexidade de assegurar informação de negócio
- Elevar a capacidade de partilhar ficheiros através de capacidades robustas de armazenamento
- Integração com várias versões do Microsoft Office (2007/2010/2013)

2.4.2. Gestão e administração

A gestão e administração da plataforma Office 365 pode ser realizada de duas formas de acordo com (Microsoft, 2014), ou pelo portal baseado em tecnologia Web ou pela consola Powershell.

Conceito de Tenant – No nosso mundo de serviços partilhados o termo tenant tem sido amplamente utilizado. No Office 365 este termo é constantemente referido, porque é um excelente exemplo de um sistema multi-tenant, ou seja tal como um apartamento onde temos o nosso próprio espaço, mas partilhamos corredores, elevadores, escalas, cave, entre outros.

O centro de administração (*admin center*) do Office 365 é constituído pelas seguintes áreas:

Painel de “Como começar” – Este painel está disponível nos primeiros 30 dias. Inclui ligações e assistentes para ajudar e aprender a utilizar o Office365, incluindo vídeos, um assistente de configuração e *software* para descarregar.

Painel de instrumentos – Esta é a página de início para os administradores do Office 365. Pode verificar um pequeno resumo da saúde e utilização do serviço, e variados recursos de administração do *tenant*.

Instalação – Inclui opções de configuração básica e customizada, bem como guias de configuração passo a passo.

Utilizadores e grupos – Este é o local central para a maioria das tarefas relacionadas com utilizadores e grupos. Podemos adicionar, editar ou apagar utilizadores, reiniciar palavras-chaves, assignar licenças, configurar grupos de seguranças e gerir os restantes administradores delegados.

Domínios – Podemos adicionar ou remover os domínios, verificar as definições de DNS, e solucionar problemas relacionados com domínios.

Licenciamento – Verificar detalhes das subscrições e datas de término, número de licenças assignadas e renovação de subscrições.

Configurações de serviço – O centro de administração contém ligações para as configurações mais comuns do Exchange Online, participação na comunidade e configurações móveis. Os serviços adicionais são geridos nos centros de administração das restantes tecnologias (Exchange, Lync e Sharepoint).

Saúde do serviço – Verificar a saúde de todos os serviços, visualizar o histórico de incidentes que afectaram o *tenant*, e avisos de manutenção planeada.

Suporte – Pesquisa de respostas e soluções relativas a problemas comuns, acesso a ferramentas de diagnóstico e resolução de problemas. Criar novos e/ou rever pedidos de suporte.

Adquirir serviços – Adquirir subscrições adicionais

O Windows Powershell é uma poderosa ferramenta de gestão que complementa o centro de administração do Office 365. Existem várias tarefas administrativas que podem apenas ser levadas a cabo através da consola de Powershell.

Como referido em (Microsoft, 2013), apesar do centro de administração providenciar todas as necessidades em termos de gestão da plataforma, nem sempre permite ter o detalhe que é necessário. Existem no mínimo seis cenários onde faz sentido utilizar o Windows Powershell como complemento, ou utilizar invés, do centro de administração.

1. O Windows Powershell pode revelar informação “escondida” que não é disponibilizada no centro de administração do Office 365. Por exemplo no centro de administração é visualizada a informação sobre os utilizadores, que é limitada a 1000 objectos. Se pretender visualizar mais do que 1000 utilizadores terá que utilizar os comandos Powershell, ou se pretender rapidamente listar, agregar ou filtrar todos os utilizadores por localização.
2. O centro de administração foi construído para que o administrador típico consiga realizar a maioria das tarefas administrativas, o que por definição significa que existem tarefas que não conseguem ser efectuadas pelo centro de administração.

Como exemplo posso referir a configuração de vários parâmetros de reuniões Lync, como o acesso de utilizadores anónimos, capacidade de gravação da sessão, ou todos os utilizadores serem designados como apresentadores quando se juntam á sessão.

3. A realização de operações em massa é mais eficiente e rápida, e caso exista algum erro é muito mais detalhado do que no interface gráfico. Por exemplo se pretender apagar um utilizador do acesso a um *site* de Sharepoint, e ao invés de ir a cada *site* alterar as permissões do mesmo, pode simplesmente automatizar que pretende apagar o respectivo utilizador em todos os *sites*.
4. A filtragem de dados pode ser muito mais detalhada, complexa e precisa quando realizada através da consola Powershell, ou seja, tem maior capacidade de customização do que no interface gráfico.
5. Os resultados dos comandos executados podem ser gravados directamente para vários tipos de ficheiros e desta forma é mais fácil recolher as informações pretendidas.
6. Permite realizar a gestão entre produtos/serviços da plataforma Office 365. Os vários componentes foram desenhados para trabalhar em conjunto, mas informação que é gerada por esses produtos ou serviços é genérica. Quando se trata de informação específica, como por exemplo a informação sobre um utilizador e respectiva caixa de correio, ou o plano de Lync associado, é aí que entra o Powershell de modo a podermos rapidamente compilar a informação sobre o utilizador (geralmente através de *scripting*).

3. Exchange Online

Neste capítulo irei-me focar na tecnologia Exchange Online, dada a variedade e complexidade do tema computação em nuvem, e mesmo do produto Office 365 da Microsoft.

O Office 365 Exchange Online foi concebido para as organizações que desejam obter os benefícios do correio electrónico baseado na nuvem, sem sacrificar as capacidades robustas de uma implementação de Exchange local. Este serviço permite o acesso ao correio electrónico a partir de qualquer parte e através de vários dispositivos, inclui protecção e conformidade dos dados enviados e recebidos, visibilidade e controlo através da consola de gestão. Fornece ao administrador de Exchange todos os aspectos de usabilidade, conformidade, segurança, controlo e familiaridade.

A Microsoft refere que o *software* foi desenvolvido por especialistas e que os seus sistemas de correio electrónico e o respectivo suporte são os mais confiáveis do mercado. O cliente pode controlar a maioria dos aspectos na sua experiência com o Exchange, e pode obter maior flexibilidade ao ter um ambiente híbrido, com uma implementação de Exchange local em conjunto com o serviço de Exchange Online.

3.1. Tipos de Migrações

Dependendo do cenário existente, podemos definir os tipos de migração que melhor se adequam a cada cenário.

Segundo a (Microsoft, 2014), para cenários apenas com Office 365, ou seja para quem pretenda migrar o correio electrónico para o Exchange Online, existem as seguintes migrações

- *Cutover*
- *Staged*
- IMAP

Para ambientes híbridos, ou seja onde exista um ou vários servidores Exchange na infraestrutura local do cliente existe a migração Híbrida com os seguintes tipos de cenário:

- Versão única
 - Exchange Server 2010
 - Exchange Server 2013
- Coexistência de versões
 - Exchange Server 2010 com Exchange Server 2007 ou 2003
 - Exchange Server 2013 com Exchange Server 2010 ou 2007

Para outras aplicações de correio electrónico, apenas a migração por IMAP é suportada.

Podemos comparar na Tabela 2 os tipos de migração disponíveis.

Organização existente	Número de caixas de correio a migrar	Gestão das contas de utilizadores a partir da organização local?	Tipo de migração
Exchange 2013, 2010, 2007, ou 2003	< 2000	Não	Cutover
Exchange 2007 ou Exchange 2003	< 2000	Não	Staged
Exchange 2007 ou Exchange 2003	> 2000	Sim	Staged ou Migração remota em ambiente de Exchange híbrido

Exchange 2013 ou Exchange 2010	> 2000	Sim	Migração remota em ambiente de Exchange híbrido
Exchange 2000 Server ou versões mais recentes	Sem valor máximo	Sim	IMAP
Sistema de mensagens local (Sem ser Exchange)	Sem valor máximo	Sim	IMAP

Tabela 2 - Comparação de tipos de migração. Baseado em Microsoft, 2014

3.1.1. Migração *Cutover*

A migração *Cutover* consiste na migração de todas as caixas de correio electrónico do servidor Exchange local para a organização Exchange Online de uma só vez. As contas de utilizadores correspondentes serão criadas e geridas no Office 365. Este tipo de migração é recomendado para clientes que não tenham mais de 2000 caixas de correio. Resumidamente este processo baseia-se no seguinte:

- O Exchange Online aprovisiona novas caixas de correio na organização de correio electrónico Office 365. Cria uma caixa de correio para cada conta de utilizador que consta na organização local. Os grupos de distribuição e os contactos também são migrados neste tipo de migração
- Após a criação das caixas de correio no Exchange Online, as mensagens, contactos, e itens do calendário de cada conta do servidor Exchange local são copiadas para a caixa de correio no Exchange Online. A este processo dá-se o nome de sincronização inicial.
- Após a sincronização inicial, as caixas de correio são sincronizadas entre as organizações a cada 24 horas, de modo a que as mensagens de correio electrónico enviadas para as caixas de correio locais sejam copiadas para as caixas de correio na nuvem. Este processo chama-se de sincronização incremental
- O Exchange Online envia uma mensagem ao administrador quando a sincronização inicial terminou. Esta mensagem lista o número de caixas de correio que foram migradas com sucesso e quantas não conseguiram ser migradas. Também inclui hiperligações para os relatórios com a estatística e erros, que contem informação mais detalhada

Após estes passos é possível alterar o registo MX correspondente do domínio de correio electrónico para o Exchange Online e apagar o lote de migração. Caso seja pretendido pode também proceder á desinstalação do servidor Exchange local.

3.1.2. Migração Faseada (*Staged*)

Este tipo de migração é tipicamente utilizada para migrar as caixas de correio electrónico para o Exchange Online durante um período algumas semanas ou meses. São utilizadas por organizações que planeiam migrar todas as contas para o Exchange Online e dessa foram transitarem da organização local para a organização na nuvem.

Este tipo de migração não é o pretendido para organizações que desejam manter permanentemente caixas de correio no servidor Exchange local como em Exchange Online, ou que planeiem que a transição seja efectuada durante um largo período de tempo. Uma implementação híbrida de Exchange é a melhor solução para manter a manutenção de caixas de correio local e na nuvem a longo prazo, pois oferece recursos como encaminhamento de mensagens de correio electrónico entre as organizações, lista de endereços unificada, *Free/Busy*, partilha de calendário e a habilidade de mover as caixas de correio na nuvem de novo para a organização local. Este tipo de migração também não deve ser utilizado para migrar de servidores Exchange 2010 ou 2013.

Para utilizar uma migração faseada (*Staged*) para o Exchange Online, temos de replicar as contas de utilizadores do serviço de directório local para a organização do Office 365. Para realizar esta tarefa, tem de se instalar e configurar a ferramenta de sincronização de serviço de directório *Microsoft Online Services Directory Synchronization* (DirSync). Após as caixas de correio terem sido migradas para a nuvem, os utilizadores ainda serão geridos pelo serviço de directório local e replicados para a nuvem pela ferramenta Dirsync.

Este processo de migração decorre da seguinte forma:

- Verificação de que a ferramenta de sincronização Dirsync está habilitada para a organização Office 365
- Verifica se um utilizador *mail-enabled* existe na organização Office 365 por cada registo no ficheiro csv
- Converte os utilizadores *mail-enabled* em caixas de correio na organização Exchange Online
- Configura o encaminhamento de correio electrónico ao popular o atributo *TargetAddress* na caixa de correio local com o endereço de correio electrónico da caixa de correio Exchange Online. Este passo permite que uma mensagem de correio enviada para a caixa de correio local possa ser reencaminhado para a caixa de correio Exchange Online
- Copia as mensagens, contactos e itens do calendário da caixa de correio local para a caixa de correio correspondente no Exchange Online. Este processo tem o nome de sincronização inicial. Após os itens da caixa de correio terem sido migrados, as caixas de correio não serão sincronizadas. As novas mensagens de correio electrónico serão automaticamente reencaminhadas para a caixa de correio no Exchange Online

- É enviada uma mensagem de correio electrónico para o administrador quando o lote de migração termina a sincronização inicial. Esta mensagem lista o número de caixas de correio que foram migradas com sucesso e quantas não conseguiram ser migradas. Também inclui hiperligações para os relatórios com a estatística e erros, que contêm informação mais detalhada

3.1.3. Migração IMAP

Este tipo de migração permite às organizações uma maneira eficiente de mover as caixas de correio de um sistema de mensagens de correio electrónico IMAP para a organização Office 365. A migração IMAP permite os seguintes servidores IMAP:

- Courier-IMAP
- Cyrus
- Dovecot
- UW-IMAP
- Microsoft Exchange (Exchange 2000 Server e versões mais recentes)

As migrações IMAP também podem ser utilizadas por pequenas e médias empresas para migrar desde um serviço de correio electrónico alojado num ISP (Prestador de Serviços de Internet)

Neste tipo de migração apenas os itens das caixas de correio são migrados do sistema de mensagens IMAP para o Exchange Online. As caixas de correio já têm de estar criadas no Exchange Online antes de se iniciar a migração, porque as mesmas não são aprovisionadas durante o processo de migração.

Este processo de migração decorre da seguinte forma:

- Os itens das caixas de correio no sistema de mensagens IMAP são copiadas para a caixa de correio correspondente no Exchange Online. A este processo dá-se o nome de sincronização inicial.
- Após a sincronização inicial, as caixas de correio no sistema de mensagens IMAP e no Exchange Online são sincronizadas a cada 24 horas, para que as novas mensagens de correio electrónico enviadas para as caixas de correio IMAP sejam copiadas para as correspondentes no Exchange Online. Este processo chama-se de sincronização incremental e é contínuo até que o lote de migração IMAP seja apagado.
- O Exchange Online envia uma mensagem de correio electrónico para o administrador quando a sincronização inicial do lote de migração IMAP termina. Esta mensagem lista o número de caixas de correio que foram migradas com sucesso e quantas não conseguiram ser migradas. Também inclui hiperligações para os relatórios com a estatística e erros, que contêm informação mais detalhada

Após estes passos é possível encaminhar directamente o correio electrónico para o Exchange Online e apagar o lote de migração.

3.2. Implementação de Office 365

Segundo a (Microsoft, 2013) existem 3 fases na implementação da solução Office 365. As fases consistem em Planear, Preparar e Migrar.

Na fase de planeamento o objectivo é o de assegurar de que o âmbito do projecto e cronograma são bem compreendidos por todos os membros da equipa de projecto, desde do *Project Manager* até ao *Executive Sponsor*.

Consiste igualmente em identificar planos para a migração, aplicações *mail-enabled*, identidade de utilizadores e opções de aprovisionamento de contas, infra-estrutura local e requisitos de *hardware*, requisitos de largura de banda de rede, sistemas operativos clientes e aplicações clientes, formação de *help* e *service desk*, formação e estratégia de comunicação para os utilizadores.

As actividades que deverão ser completadas, consistem na reunião de início do projecto, onde deverão ser acordadas a equipa de gestão de projecto dedicada á implementação, a revisão de cada área de trabalho, marcos e prazos do projecto, e respectivos compromissos.

Na fase de preparação deverá ser assegurado que todas as tarefas de preparação e configuração são terminadas, tais como a verificação e remediação de possíveis erros de sincronização de directórios, configurações específicas de serviços, implementação do Office 365 Desktop Setup, validação dos testes de migração e coexistência e integração do *Service Desk*.

Na fase de migração, os objectivos consistem no início da migração de algumas caixas de correio, e definição no critério de possível paragem da implementação, que terá de ser acordado entre as partes envolvidas. Nesta fase irão ser realizadas as tarefas de completar a migração das caixas de correio, e caso não se pretenda ter um ambiente híbrido, a tarefa de desinstalação dos serviços locais.

Antes de uma organização avançar para a implementação do Office 365, deve ter concluído alguns requisitos, tais como, a revisão da descrição dos serviços para assegurar o alinhamento das soluções com os requisitos e necessidades de negócio e de TI, e a revisão do ambiente de Active Directory.

3.3. Ambiente híbrido

Um ambiente híbrido consiste em realizar uma ligação, apelidada de federação entre duas organizações distintas, neste caso entre a organização de correio electrónico local e a organização de correio electrónico na nuvem.

De acordo com a (Microsoft, 2014) uma implementação híbrida oferece às empresas a capacidade de extensão da experiência rica em funcionalidades e controlo administrativo que têm no ambiente de correio electrónico local, para a nuvem. Um ambiente híbrido fornece a aparência e sensação de uma única organização, e pode servir como um passo intermediário para mover completamente a organização para a nuvem.

3.3.1. Terminologia chave

Transporte de correio electrónico centralizado – Esta é uma opção de configuração híbrida onde todo o fluxo de correio electrónico do Exchange Online é encaminhado através da organização de Exchange local.

Coexistência de domínios – Um domínio aceite e adicionado à organização local para o fluxo de correio electrónico híbrido e pedidos *Autodiscover* para o serviço Office 365. Este domínio é adicionado com um domínio *proxy* secundário em qualquer política de endereços de correio electrónico que tenham o atributo *PrimarySmtptAddress* preenchido com domínios seleccionados pelo Hybrid Configuration Wizard. Por omissão este domínio tem o valor de <domínio>.mail.onmicrosoft.com

Objecto *HybridConfiguration* – É o objecto da Active Directory na organização local que contem os parâmetros de configuração da implementação híbrida, definidos pelas escolhas seleccionadas durante o HCW. O HCE utiliza estes dados aquando da configuração das definições da organização local e na nuvem, para permitir as funcionalidades híbridas. Os conteúdos deste objecto são limpos cada vez que o HCW é executado.

Hybrid Configuration Engine (HCE) – Executa as acções necessárias para configurar e actualizar a implementação híbrida. Compara o estado do objecto *HybridConfiguration* com a configuração actual do Exchange local e do Exchange Online, e executa as tarefas para igualar as configurações da implementação híbrida e dos parâmetros definidos no referido objecto. Podemos verificar o esquema do HCE na Figura 6, bem como os passos do processo efectuado pelo mesmo.

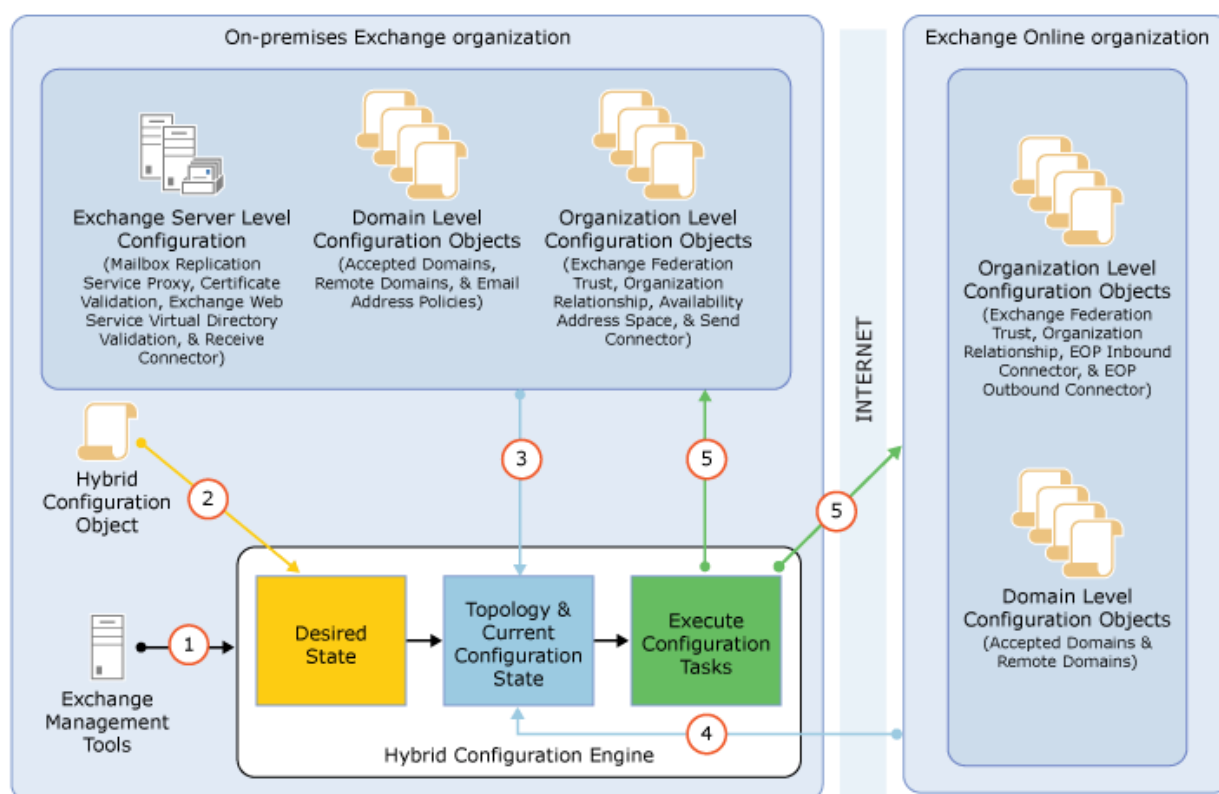


Figura 6 – Esquema do Hybrid Configuration Engine. Retirado de (Microsoft, 2014)

Hybrid Configuration Wizard (HCW) – Ferramenta que guia o administrador na configuração de um ambiente híbrido. Define os parâmetros de configuração híbrida guardados no objecto da AD *HybridConfiguration* e dá instruções ao HCE para executar as tarefas necessárias para permitir as funcionalidades híbridas.

Implementação híbrida com Exchange 2010 – Configura a implementação híbrida utilizando o *Service Pack 3 (SP3)* do Exchange Server 2010, nos servidores locais, como o ponto de ligação para o Office 365 e os serviços Exchange Online. Este cenário permite a coexistência com as versões 2003 e 2007 do Exchange Server com as versões de serviço do Office 365 (*Wave 14 e 15*)

Implementação híbrida com Exchange 2013 – Configura a implementação híbrida utilizando o Exchange Server 2013, nos servidores locais, como o ponto de ligação para o Office 365 e os serviços Exchange Online. Neste cenário é permitida a coexistência com as versões 2007 e 2010 do Exchange Server, e compatível apenas com a versão de serviço mais recente do Office 365 (*Wave 15*)

Transporte de correio electrónico seguro – Característica de uma implementação híbrida automaticamente configurada, que permite às mensagens enviadas entre as organizações

(local e na nuvem) sejam seguras. As mensagens são encriptadas e autenticadas usando TLS (*Transport Layer Security*) na camada de transporte, com um certificado seleccionado no HCW. O serviço de Exchange Online Protection (EOP) no *tenant* de Office 365 é o ponto de ligação para as conexões originárias da organização local, e a fonte para ligações de transporte híbrido para a organização local desde o Exchange Online.

3.3.2. Funcionalidades

- Encaminhamento (*routing*) de mensagens de correio electrónico seguro entre a organização local e o Exchange Online
- Encaminhamento (*routing*) de mensagens de correio electrónico com um *namespace* de domínio partilhado. Por exemplo utilizar o domínio SMTP @uatla.pt tanto na organização local como no Exchange Online.
- Lista global de endereços (GAL) unificada. Também apelidada de “lista de endereços partilhada”
- Partilha de informações de estado (*free/busy*) e de calendário entre as organizações
- Controlo centralizado do fluxo de correio electrónico. Este fluxo poderá ser configurado por exemplo para todo o fluxo passar pela organização local.
- Apenas um endereço (URL) para o acesso à caixa de correio que esteja localizada tanto na organização local como na da nuvem.
- Capacidade de mover as caixas de correio entre as organizações quando necessário.
- Gestão centralizada das caixas de correio usando o Exchange Admin Center (EAC)
- Controlo de mensagens (*message tracking*), *MailsTips*, e pesquisa em múltiplas caixas de correio em ambas as organizações.
- Arquivo de mensagens baseado na nuvem, para as caixas de correio da organização local.

3.3.3. Componentes

Uma implementação híbrida contém vários serviços e componentes. Entre eles encontram-se:

- Os servidores Exchange com os *roles* requeridos de *Client Access Server* (CAS) e *Mailbox* (MBX) na organização local.
- Microsoft Office 365, que é um serviço que fornece uma organização Exchange baseada na nuvem como parte de uma subscrição de um serviço. As empresas que configuram um ambiente híbrido têm de criar e parametrizar a organização Exchange Online baseada na nuvem.
- O Microsoft Exchange Online Protection (EOP) está incluído em todos os *tenants* Office 365 para empresas por omissão e trabalha com os servidores Exchange locais com o *role* de CAS, de modo a fornecer a entrega de mensagens de modo seguro.

Dependendo de como a organização está configurada, também pode suportar o encaminhamento do fluxo de correio electrónico de recipientes externos para ambas as organizações.

- Hybrid Configuration Wizard, que está incluído nas versões de Exchange 2010 e 2013 e que providencia um processo simplificado para a configuração do ambiente híbrido.
- O sistema de autenticação Windows Azure AD, é um serviço baseado na nuvem que funciona como um *broker* confiável entre a organização local e a organização na nuvem. As organizações locais que estão a implementar um ambiente híbrido necessitam de criar uma ligação de federação (confiável) com o sistema de autenticação Windows Azure AD. Esta federação pode ser criada manualmente entre organizações locais, ou como parte da configuração de um ambiente híbrido com o HCW. Esta federação é criada automaticamente entre o *tenant* Office 365 e o Windows Azure AD, quando a conta de serviço do Office 365 é activada.
- A sincronização da Active Directory replica a informação contida na Active Directory local para os objectos *mail-enabled*, para a organização Exchange Online, de modo a suportar a lista de endereços global (GAL).

3.3.4. Pré requisitos

Single Sign-On (SSO) – Esta funcionalidade permite aos utilizadores acederem a ambas organizações com um único nome de utilizador e palavra-chave, ou seja permite aos utilizadores uma experiência familiar de acesso. O configurar do SSO permite às organizações aplicar políticas de acesso e criação de palavras-chave, e restrições de contas em ambas as organizações, e dessa forma facilitar o controlo dos acessos por parte dos administradores de sistema, utilizando as ferramentas da Active Directory na organização local. A implementação do *single sign-on* inclui vários componentes que configuram a relação de confiança entre os servidores ADFS (Active Directory Federation Services) locais e a Microsoft Federation Gateway.

Este pré-requisito é opcional.

Sincronização de directórios (Dirsync) – A sincronização da Active Directory entre a organização local e organização na nuvem, permite o uso de uma lista de endereços global unificada (GAL) e a capacidade de gerir todas as contas de utilizadores a partir da organização local. Todas as alterações efectuadas são sincronizadas automaticamente para a organização na nuvem.

Configuração do tenant – Após a configuração (opcional) do *Single sign-on* e da sincronização de directórios Active Directory entre a organização local e a organização na nuvem, é necessário verificar o funcionamento dos mesmos. Para isso é necessário realizar

uma série de testes, que incluem a criação de um utilizador na organização local e verificar a replicação desse utilizador para a organização na nuvem e a atribuição automática de uma licença, verificar se o SSO está a funcionar correctamente, ou seja se o utilizador não necessita de colocar as credenciais quando acede ao serviço na nuvem, quando já está com a sessão aberta no seu computador de domínio local.

Configuração de DNS – Para permitir que os vários clientes de correio electrónico, como o Outlook 2013, 2010 ou 2007, que se conectem às caixas de correio no Exchange Online, é necessário configurar o registo de *Autodiscover* no serviço de DNS público. O *Autodiscover* configura automaticamente os parâmetros do cliente de modo a que os utilizadores não necessitem de saber os nomes dos servidores ou outros detalhes técnicos para configurar o perfil de correio electrónico. É igualmente recomendado que seja criado um registo Sender Policy Framework (SPF) para assegurar que as mensagens enviadas do domínio local sejam confiáveis pelo EOP.

Configuração de certificados Exchange – Certificados digitais são uma parte importante na segurança da comunicação entre a organização Exchange local e o serviço Microsoft Office 365, bem como a outros servidores Exchange locais. Os certificados permitem que uma entidade confie na identidade de outra, o que ajuda a garantir que um cliente ou servidor comunica com a fonte correcta. Num ambiente híbrido, vários serviços fazem uso certificados, como o serviço de ADFS, a federação de Exchange e os serviços de Exchange. Na configuração do ambiente híbrido é também necessário configurar os certificados. É necessário adquirir certificados de uma Autoridade Certificadora (Certification Authority) externa. Pode utilizar o mesmo certificado *third-party* transversalmente por múltiplos servidores ou para cada servidor.

A Tabela 3 demonstra todos os requisitos necessários para criar um certificado externo para um ambiente híbrido de Exchange.

Serviço	Servidor	FQDN sugerido
Domínio SMTP primário	Servidores CAS e Mailbox	contoso.com
Active Directory Federation Services (ADFS)	ADFS	sts.contoso.com
Autodiscover	Servidores híbridos	autodiscover.contoso.com
Transporte	Servidores híbridos	Igual ao FQDN externo do servidor híbrido, por exemplo hybrid.contoso.com

Outlook Anywhere	Servidores híbridos	Igual ao FQDN interno do servidor híbrido, por exemplo Ex2010.corp.contoso.com
Outlook Web App (Exchange 2010 ou 2013)	Servidores híbridos	Owa.contoso.com
Outlook Web App (servidor existente)	Servidor Exchange existente	Igual ao FQDN externo do servidor existente, como por exemplo mail.contoso.com

Tabela 3 – Requisitos dos certificados para um ambiente híbrido de Exchange. Baseado em (Microsoft, 2014)

Configuração dos Exchange Web Services – O FQDN (*Fully qualified domain name*) externo de todos os servidores Exchange com a *role* CAS, necessitam de ser configurados em diversas directorias virtuais numa implementação híbrida.

3.3.5. Cenário híbrido

Para implementar e configurar o cenário híbrido e após ter revisto todos os pré-requisitos necessários e recomendados, devemos executar o Hybrid Configuration Wizard (HCW). O processo deste configurador passa por criar a fundação, ou seja, cria o objecto *HybridConfiguration* na Active Directory local. Este objecto guarda as informações da configuração da implementação híbrida.

O processo passa igualmente pela configuração da organização de Exchange local, onde vai recolher os dados sobre a topologia de Exchange e Active Directory existentes, definir vários parâmetros da organização, e só então executa a sequência de tarefas de configuração da implementação híbrida.

Durante a execução do configurador, terão de ser indicados os domínios que pretendam ser partilhados entre a organização local e a organização na nuvem. Para este efeito é necessário que para cada domínio seja criado um registo TXT no serviço de DNS externo, como prova de posse desse(s) domínio(s). Caso exista apenas um domínio partilhado, este será seleccionado imediatamente aquando da execução do configurador. Outra das opções que terão de ser definidas é como será efectuado o fluxo de transporte do correio electrónico, ou seja, se for pretendido que o fluxo seja direccionado todo para a

organização Exchange local, ou se se é pretendido que seja a organização Exchange Online a reencaminhar esse fluxo.

Em todos os *tenants* Office 365 existe um serviço de verificação de vírus, *spam*, *phishing*, esquemas e violações de políticas, que é automaticamente gerado aquando da criação do *tenant* e fica ligado a essa organização de Exchange Online.

O EOP contem vários parâmetros de transporte de correio electrónico que podem ser configurados para a organização Exchange Online.

Podem ser especificados os vários domínios SMTP e de que endereços IP são provenientes, exigem certificados TLS e SSL, podem ignorar os filtros de *anti-spam* e políticas de *compliance*, entre outros. Este serviço é a porta de entrada da organização de Exchange Online e todas as mensagens independentemente da sua origem, devem passar pelo EOP antes de serem entregues nas caixas de correio do Exchange Online, bem como todas as mensagens enviadas a partir da organização Exchange Online para a Internet. Quando configuramos o ambiente híbrido com o HCW, todas as configurações de transporte são automaticamente criadas na organização local e no EOP associado ao *tenant*. O Hybrid Configuration Wizard (HCW) configura os conectores de entrada e saída entre outros parâmetros no EOP, para proteger as mensagens enviadas entre a organização local e o Exchange Online e encaminhar as mensagens para o destino correcto.

Independentemente da configuração do referido fluxo de correio electrónico aquando da execução do HCW, todo o fluxo entre a organização local e a da nuvem é enviado através de transporte seguro. Para ajudar a proteger os recipientes em ambas as organizações e para assegurar que as mensagens enviadas entre as organizações não são interceptadas e lidas, o transporte entre a organização e o EOP é configurado para utilizar TLS forçado. O TLS utiliza certificados Secure Sockets Layer (SSL) providenciados por uma entidade externa. As mensagens entre o EOP e o Exchange Online também utilizam TLS. Quando é utilizado o TLS forçado, os servidores de envio e recepção de mensagens examinam o certificado configurado no outro servidor. O *subject name*, ou *dos subject alternative names* (SANs), configurados nos certificados tem de corresponder ao FQDN que foi explicitamente especificado no outro servidor. Por exemplo, se o EOP está configurado para aceitar e proteger mensagens enviadas pelo FQDN externo do servidor híbrido (*hybrid.contoso.com*) então o servidor de envio local tem de conter um certificado SSL com o *subject name* ou SAN de *hybrid.contoso.com*. Se este requisito não é cumprido, então a conexão é recusada.

Além de utilizar o TLS, as mensagens entre as organizações, são tratadas como internas, o que leva a que estas mensagens possam contornar os parâmetros de *anti-spam* e outros serviços.

3.4. Gestão e administração

Para a gestão e administração do Exchange Online, podemos utilizar o Exchange Admin Center (EAC) e o Windows Powershell em modo remoto.

O EAC permite que seja utilizada uma única consola unificada, que está optimizada para a gestão de uma implementação local, na nuvem ou híbrida. É uma consola de gestão baseada em web, utilizada para gerir os itens relacionados com correio electrónico que não se conseguem gerir através do centro de administração do Office 365. O EAC está disponível para acesso através do centro de administração do Office 365 ou directamente através da seguinte ligação:

<https://<Exchange Online URL>/ecp/?ExchClientVer=15>

De acordo com a Microsoft, o painel de funcionalidades do EAC está organizado nas seguintes áreas:

Recipientes – Visualizar e gerir as caixas de correio, grupos, contactos, caixas de correio partilhadas e migração de caixas de correio

Permissões – Gerir os *roles* de administrador e utilizador, e as políticas do OWA

Gestão de *compliance* – Gestão de In-Place Discovery & Hold, auditoria, prevenção de perda de dados, políticas de retenção, etiquetas de retenção e regras de *journaling*.

Organização – Gestão da partilha da organização e aplicações para o cliente Outlook

Protecção – Gerir os filtros de *malware*, de conexão, de conteúdo, *spam* externo e quarentena da organização

Fluxo de correio electrónico – Gestão de regras, relatórios de entregas, rastreio de mensagens, domínios aceites e conectores de envio e recepção.

Dispositivos móveis – Gestão dos dispositivos móveis que se irão conectar à organização. Pode-se gerir o acesso e as políticas para esses dispositivos.

Pastas públicas – Gerir as pastas públicas e respectivas caixas de correio

Sistema de mensagens unificadas – Gestão dos planos de ligação UM (Unified Messaging) e UM IP Gateways.

O Windows Powershell em modo remoto permite aos administradores conectarem-se ao Exchange Online para realizar as tarefas de gestão que não estão disponíveis, ou que não são práticos de realizar no EAC. Estas tarefas incluem a habilidade de automatizar as mais repetitivas, a extracção de dados para relatórios customizados e políticas customizadas. O

Exchange Online utiliza os mesmos comandos do que o Exchange Server 201, mas com alguns comandos e parâmetros não disponíveis, dado que algumas funcionalidades não se aplicam ao Exchange Online.

Na última contagem, havia 494 comandos do Windows PowerShell disponíveis para administração do Exchange Online, o que representa mais do que três vezes o número de comandos para o Windows Azure Active Directory, Lync Online, SharePoint Online em conjunto.

Em termos de segurança (para evitar ataques DoS – *Denial of Service*) existe um limite de três conexões Windows Powershell à organização Exchange Online.

3.5. Segurança e Compliance

No Office 365 os dados relativos ao correio electrónico que estão em “descanso” são encriptados com o *BitLocker Drive Encryption*. O BitLocker encripta os discos rígidos onde os dados estão guardados, para fornecer maior protecção contra o roubo ou exposição dos dados, ou providenciar maior segurança no apagar dos dados quando as máquinas protegidas com o BitLocker são desinstaladas ou recicladas.

O *Information Rights Management (IRM)* permite a uma organização prevenir a fuga de dados, ao restringir os direitos que os recipientes de correio electrónico têm nas mensagens e nos anexos, como por exemplo, se podem reenviar uma mensagem para outros recipientes, imprimir uma mensagem ou anexo, e copiar e colar conteúdo da mensagem ou de anexos.

Os administradores podem utilizar o *Azure Rights Management Services (RMS)* baseado na nuvem, ou um servidor local de *Active Directory Rights Management Services (AD RMS)* em conjunto com o Exchange Online. Se o servidor AD RMS local for implementado, o Outlook pode comunicar directamente com o servidor, permitindo aos utilizadores compor ou ler mensagens protegidas, sendo que não é necessária nenhuma interoperabilidade entre o servidor local e o Exchange Online para permitir o uso desta funcionalidade no cliente de correio electrónico.

No entanto existem várias funcionalidades avançadas em que é necessário importar a chave TPD (*Trusted Publishing Domain*) do servidor local para o Exchange Online, tais como:

Os utilizadores podem ler e criar mensagens nativamente no OWA, como em dispositivos móveis, contando para isso com Suporte para IRM no OWA e com o Exchange ActiveSync. As pesquisas de mensagens protegidas por IRM são indexadas. Os administradores podem pesquisar em múltiplas caixas de correio electrónico, e podem definir regras automáticas para serem aplicadas e protegerem as mensagens de correio electrónico. Os administradores podem ainda aplicar permissões de não encaminhamento de mensagens de voz para a caixa de correio de voz.

A encriptação de mensagens para o Office 365 é um serviço *online* que permite aos utilizadores enviar mensagens de correio electrónico para todos. Este serviço permite a definição de variadas regras de transporte para o envio e recepção das mensagens encriptadas bem como adicionar a marca da organização nessas mensagens.

O *Secure/Multipurpose Internet Mail Extension*, mais conhecido como S/MIME ajuda a proteger informação sensível ao enviar mensagens de correio electrónico assinadas e encriptadas dentro da organização. Para este serviço é necessário gerar certificados PKI na organização local.

No Exchange Online podemos utilizar o *In-Place Hold* ou o *Litigation Hold*, para quando as organizações são obrigadas a preservar dados electronicamente, incluindo o correio electrónico relevante. As organizações podem preservar todas as mensagens relacionadas a um tópico específico ou todas as mensagens para certos indivíduos. Estas duas funcionalidades permitem colocar os utilizadores “em espera” e preservar os itens da caixa de correio imutavelmente, proteger os itens da caixa de correio de adulteração, as mudanças efectuadas por um utilizador ou processos automáticos, salvando uma cópia do documento original. Pode igualmente preservar os itens indefinidamente ou por um período específico de tempo e utilizar o *In-Place eDiscovery* para procurar itens da caixa de correio, incluindo itens colocados em espera.

O Exchange Online permite aos clientes pesquisar o conteúdo de caixas de correio numa organização usando uma interface baseada na web. Os administradores e utilizadores autorizados a realizar as pesquisas através do *In-Place eDiscovery* podem procurar mensagens de correio electrónico, anexos, compromissos do calendário, tarefas, contactos e outros itens. A pesquisa pode ser efectuada simultaneamente em caixas de correio primárias e arquivos e incluem várias opções de filtragem.

Podem ser utilizados o centro de administração do Exchange ou o Windows PowerShell remoto para realizar pesquisas a múltiplas caixas de correio. O EAC permite a pré-visualização de leitura dos dados, em que posteriormente pode copiar os resultados para a caixa de correio *Discovery* criada por omissão.

A funcionalidade de prevenção de perda de dados (DLP) irá ajudá-lo a identificar, monitorizar e proteger informações confidenciais de sua organização por meio de análise de conteúdo profundo. O DLP é um recurso *premium* que é cada vez mais importante para os sistemas de mensagens corporativos, porque existem dados sensíveis que necessitam de ser protegidos sem afectar a produtividade do utilizador.

4. Estudo de Caso

Este estudo de caso realizado na Universidade Atlântica sobre a migração de correio electrónico para a plataforma Office 365 - Exchange Online, permite com que seja dado um exemplo real de uma migração híbrida, e após a análise do mesmo, sugerir possíveis melhorias e novas implementações de serviços disponibilizados no Office 365.

4.1. Perfil da Universidade

A Universidade Atlântica, que iniciou as suas actividades lectivas em 1996, foi constituída por professores universitários, investigadores, instituições financeiras, grupos institucionais, empresas de serviço e de estudos, e pela Câmara Municipal de Oeiras. A Atlântica é administrada pela E.I.A. - Ensino, Investigação e Administração S.A., entidade instituidora criada em 1993 com o objectivo de desenvolver uma instituição de ensino superior de qualidade que fosse igualmente reconhecida pela capacidade de, em paralelo, formar profissionais de excelência para o mercado de trabalho. Em 1996 tiveram início as primeiras licenciaturas na área da Gestão. Em 2001, foi criada a Escola Superior de Saúde. Desde então, a Atlântica tem alargado os seus interesses científicos e consolidou as suas vertentes de ensino e investigação em quatro áreas estratégicas: Ciências Empresariais, Saúde, Tecnologias de Informação e Comunicação, e Território, Ambiente e Desenvolvimento.

A prestação de serviços à comunidade, a investigação, a formação e os estudos pós-graduados são áreas em que a Atlântica aposta fortemente para desenvolver um ensino superior de qualidade, inovador e consistente.

É uma instituição de ensino superior privada de dimensão média, com cerca de 1200 alunos, 150 professores e 50 colaboradores.

A Universidade Atlântica ministra actualmente 13 cursos de licenciatura, 4 mestrados, e pós-graduações focadas em áreas distintas como as Ciências Empresariais e Saúde.

4.2. Situação

O Centro de Informática da Universidade Atlântica tem como função assegurar o bom funcionamento da infra-estrutura de rede no âmbito dos meios computacionais e serviços de comunicação existentes, necessários ao bom funcionamento das várias áreas de actividade administrativa, ensino e investigação.

É responsabilidade do Centro de Informática:

- Garantir o bom funcionamento da rede informática
- Configurar, gerir e administrar os recursos físicos e aplicativos instalados
- Optimizar a sua utilização e partilha das capacidades existentes
- Assegurar a aplicação de mecanismos de segurança, integridade e confidencialidade da informação armazenada

- Realizar estudos e projectos com vista à aquisição e implementação de soluções e equipamentos
- Apoiar os utilizadores disponibilizando e assegurando os meios informáticos necessários

Para melhorar os serviços prestados pelo Centro de Informática foi equacionada a alteração da solução do correio electrónico da Universidade.

A Universidade Atlântica conta praticamente desde o início com tecnologias Microsoft para oferecer mais serviços com menor trabalho, mas sempre com a preocupação de evitar quaisquer constrangimentos aos seus utilizadores.

Desde o início que estava definido que a informática seria uma vantagem competitiva e que qualquer custo teria de ser configurado como um investimento cujo retorno fizesse sentido para o negócio da universidade.

A infra-estrutura de correio electrónico da Universidade Atlântica assentava num ambiente completamente local (*on-premises*) baseado em Exchange Server 2010 SP2.

Antes da migração das caixas de correio electrónico e numa visão simplificada da rede, a UATLA tinha dois controladores de domínio (Domain Controllers) com Windows Server 2008 R2, um servidor de Exchange Server 2010 SP2 com as *roles* HUB, CAS e Mailbox na rede interna e na DMZ um Exchange Server 2010 SP2 com a *role* de EDGE, como demonstrado na Figura 7.

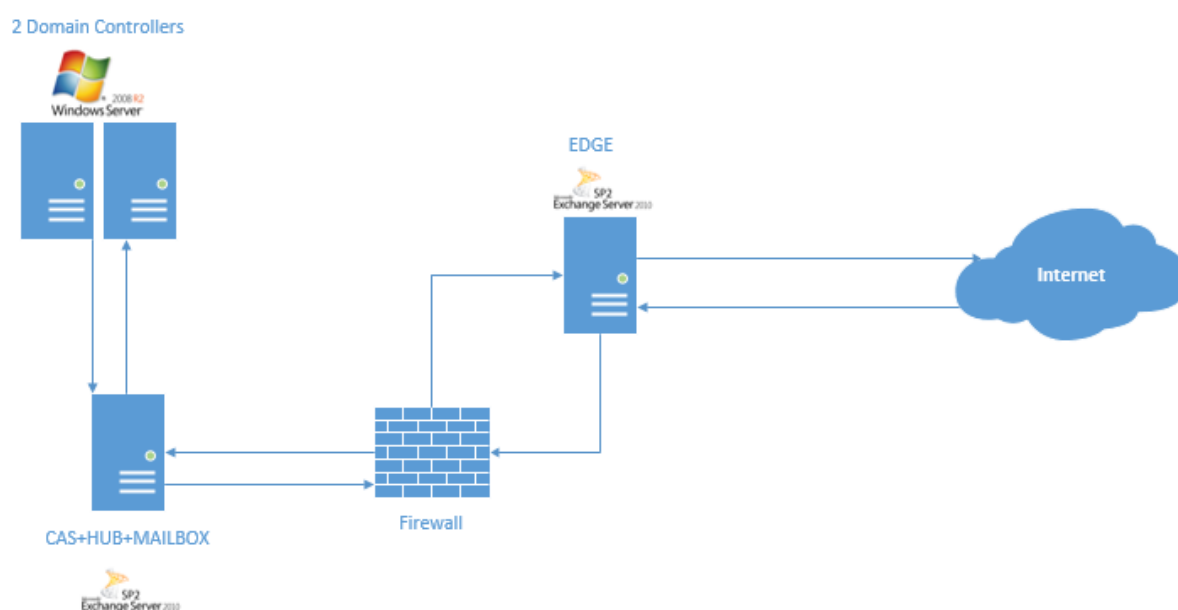


Figura 7 – Diagrama de rede simplificado da UATLA antes da migração

Porque as organizações tendem a agrupar as suas actividades de gestão em torno de um conjunto básico de funções (*roles*) de servidor, o Exchange 2010 mapeia a gestão do Exchange Server para esta mesma abordagem, de acordo com (Microsoft, 2013) A *role* de servidor é uma unidade que agrupa logicamente os recursos e os componentes necessários para executar uma função específica no ambiente de mensagens, que pode ser executada como uma unidade atómica de escalabilidade e que é composta por um grupo de características.

Na Figura 8 podemos verificar todos as *roles* da versão 2010 do Exchange Server.

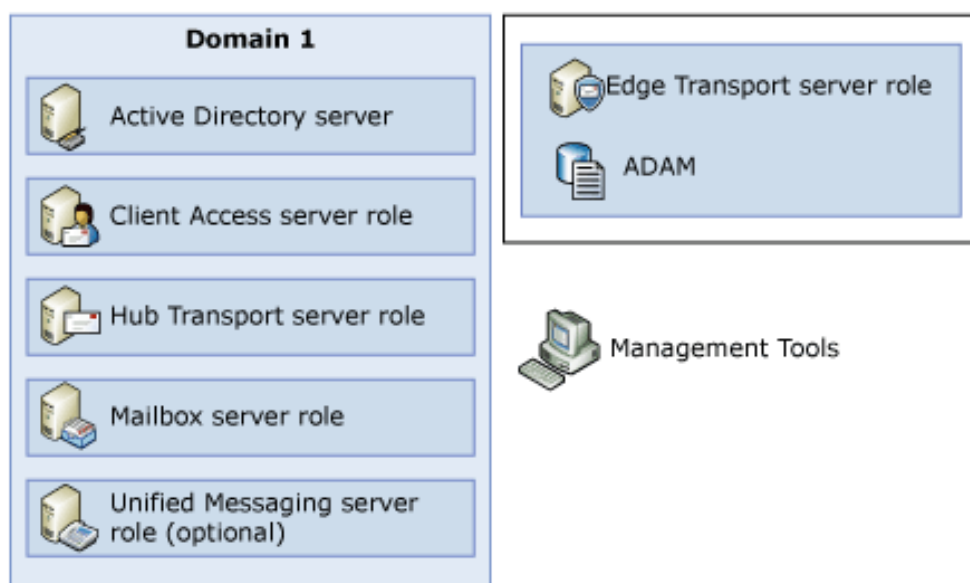


Figura 8 – Exchange Server 2010 Roles. Fonte Microsoft

A Mailbox Server Role é uma das *roles* que pode ser instalada e configurada no Exchange Server 2010 e que realiza as seguintes funções:

- Alojamento das bases de dados das caixas de correio
- Fornecer armazenamento de correio electrónico
- Alojamento das bases de dados das pastas públicas
- Calcular as políticas de endereço de caixas de correio
- Gerar listas de endereços e livros de endereços *offline* (OABs)
- Pesquisas Multi-Caixa de Correio
- Fornecer alta disponibilidade e resiliência de *site*
- Fornecer a indexação de conteúdo
- Fornecer gestão de registos de mensagens (MRM) e políticas de retenção

Um servidor com esta *role* interage directamente com vários serviços incluindo a Active Directory, os servidores com outras *roles* (Client Access Server, Hub Transport Server,

Unified Messaging Server) e com o Microsoft Outlook ou outros clientes de correio electrónico.

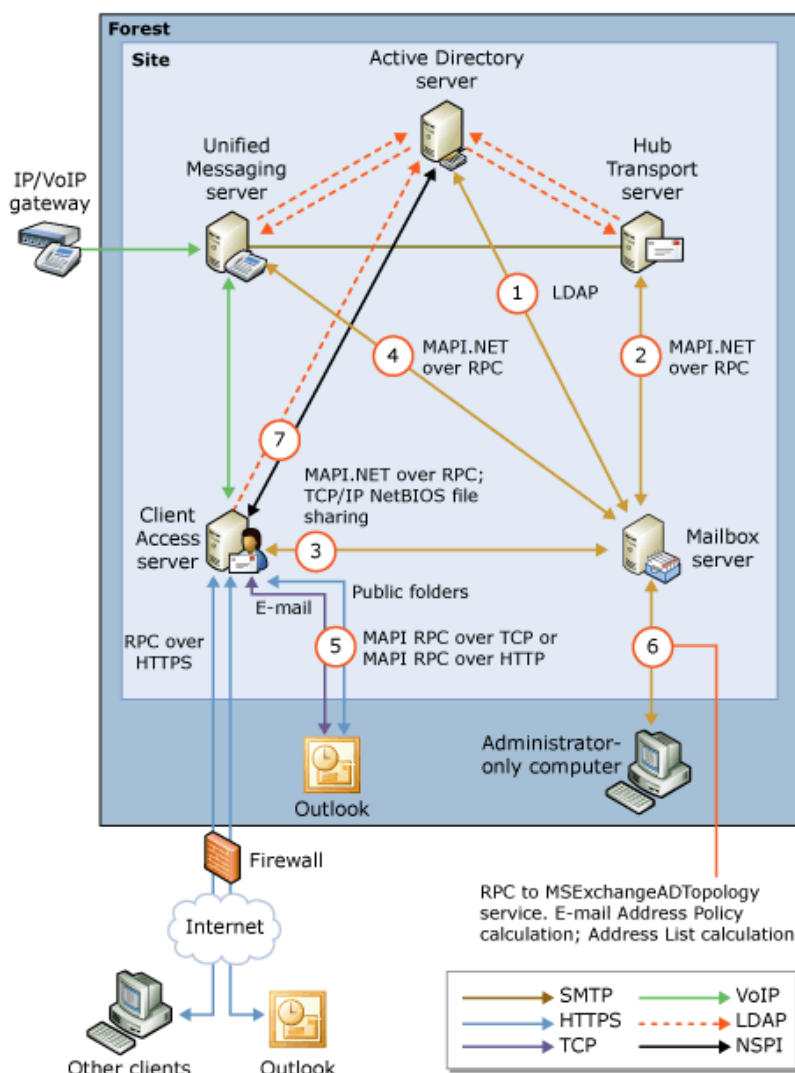


Figura 9 – Interações do Exchange 2010 Mailbox Server. Fonte Microsoft

A Figura 9 demonstra todas as interações realizadas pela role Mailbox no Exchange Server 2010, que consistem em:

1. O Mailbox Server utiliza o protocolo LDAP para aceder ao recipiente, servidor e às informações de configuração da organização na Active Directory.
2. O *store driver* no Hub Transport Server coloca as mensagens no canal de transporte, e também adiciona mensagens por enviar do remetente para o mesmo canal.
3. O Client Access Server (CAS) envia pedidos dos clientes para o Mailbox Server, e retorna os dados para os clientes. Acede igualmente aos ficheiros OAB no Mailbox

Server através da partilha de ficheiros NETBIOS. As mensagens enviadas incluem dados de *free/busy*, definições de perfil do cliente e OAB.

4. O Unified Messaging Server recupera as mensagens de correio electrónico, mensagens de voz e informações de calendário a partir do Mailbox Server para o Outlook Voice Access. Também recupera informação dos limites de armazenamento.
5. O cliente Outlook na rede interna acede ao CAS para enviar e receber mensagens. Podem aceder através do Outlook Anywhere (protocolo RPC através HTTP). No entanto se o cliente Outlook estiver a visualizar ou a modificar pastas públicas, acede por RPC através de TCP.
6. O computador utilizado pelo administrador recolhe a informação da topologia da Active Directory directamente do serviço Microsoft Exchange Active Directory Topology. Também recolhe informações da política de endereçamento de correio electrónico e listagem de endereços.
7. O CAS utiliza LDAP ou Name Service Provider Interface (NSPI) para contactar o servidor Active Directory e retirar as respectivas informações.

No Microsoft Exchange Server 2010, a *Role* de Client Access Server, suporta as aplicações clientes do Outlook Web Access e o Microsoft Exchange ActiveSync, e os protocolos Post Office Protocol version 3 (POP3) e Internet Message Access Protocol version 4rev1 (IMAP4). Esta *role* também providencia o acesso aos dados do *free/busy* ao utilizar o serviço de disponibilidade e permite com que certos clientes possam descarregar as definições de configuração automáticas do serviço de *Autodiscover*. O CAS aceita conexões de vários clientes para o servidor Exchange 2010. Esta *role* tem de ser instalada em cada organização e site de Active Directory que tenha um servidor com a *role* de Mailbox Server instalada, para evitar tráfego restrito entre servidores de Exchange, e desse modo também evitar que a funcionalidade do Exchange possa ser negativamente afectada.

Não é suportado instalar uma firewall entre servidores de Exchange ou entre um Exchange Server 2010 Mailbox/Client Access server e um servidor de Active Directory, mas pode ser instalado um dispositivo de rede, desde que o tráfego não seja restringido e que todas as portas disponíveis estejam abertas.

O Microsoft Exchange Server 2010 Unified Messaging (UM) combina mensagens de voz e correio electrónico em uma única infra-estrutura de mensagens. O UM coloca todas as mensagens de correio electrónico e de voz numa caixa de correio do Exchange 2010 que pode ser acedida a partir de vários dispositivos diferentes.

Depois dos servidores de UM serem implementados numa rede, os utilizadores podem aceder às suas mensagens utilizando o Outlook Voice Access a partir de qualquer telefone, telemóvel ou computador.

Hoje, as pessoas nas organizações normalmente gerem as suas mensagens de voz separadamente das suas mensagens de correio electrónico. Além disso, os administradores

Implementado dentro da floresta de Active Directory a *role* do Hub Transport controla todo o fluxo de mensagens dentro da organização e aplica as regras de transporte, políticas de *journaling* e entrega as mensagens para a caixa de correio dos destinatários. As mensagens que são enviadas para a internet são retransmitidas pelo HUB Transport para o servidor com a *role* de EDGE que está implementado na rede de perímetro. As mensagens que são enviadas da internet são processadas pelo EDGE antes de serem retransmitidas para o HUB Transport.

Podem ser instalados e configurados os agentes para providenciar os serviços de *anti-spam* e protecção antivírus dentro da organização, embora não seja recomendado. Esta *role* processa todas as mensagens que são enviadas dentro da organização, antes de as mesma serem entregues à caixa de entrada do destinatário ou encaminhados para utilizadores fora da organização. Não existem excepções a este comportamento. As mensagens são enviadas para o servidor de Hub Transport de três maneiras: através da submissão de SMTP, a partir do directório de recebimento, ou quando um utilizador dentro da organização envia uma mensagem.

Com uma colecção de agentes de transporte, podem ser configuradas as regras e configurações que são aplicadas á medida em que as mensagens entram e saem dos componentes de fluxo de mensagens. As políticas de mensagens podem ser alteradas conforme necessário de forma a se adaptar às exigências da organização.

A *role* de EDGE é implementada na rede de perímetro da organização. Foi projectado para minimizar a superfície de ataques. Esta função processa todo o fluxo de mensagens virado para a internet, que fornece retransmissão SMTP e serviços de *smart host* para a organização de Exchange.

As camadas adicionais de protecção e segurança de mensagens são fornecidas por uma série de agentes que são executados no EDGE e agem sobre as mensagens enquanto elas são processadas pelos componentes de transporte de mensagens. Estes agentes suportam as funcionalidades que fornecem protecção contra vírus e *spam* e aplicam regras de transporte para controlar o fluxo de mensagens.

O servidor que tem a *role* de EDGE instalada não tem acesso à Active Directory. Toda a informação de configuração e do recipiente são armazenadas na Active Directory Lightweight Directory Services (AD LDS). Para executar tarefas de pesquisa de destinatário, o servidor de EDGE exige dados que residem na Active Directory. Estes dados poderão ser sincronizadas utilizando o EdgeSync, que consiste num conjunto de processos que são executados no servidor com a *role* HUB instalada, para estabelecer a replicação unidireccional de destinatários e informações de configuração da Active Directory para a instância de AD LDS no EDGE. O serviço EdgeSync copia somente as informações necessárias para o servidor EDGE executar tarefas de configuração *anti-spam* e informação acerca da configuração do conector que é requerida para permitir o fluxo de mensagens ponto-a-ponto. Executa igualmente actualizações agendadas para que as informações no AD LDS permaneçam actuais.

4.3. Solução

A UATLA necessitava de melhorar o serviço prestado em termos de correio electrónico em conjunto com vários factores. A solução escolhida foi a plataforma de produtividade Office 365, que inclui o serviço de correio electrónico com a tecnologia Exchange Online. O Office 365 Exchange Online foi concebido para as organizações que desejam obter os benefícios do correio electrónico baseado na nuvem, sem sacrificar as capacidades robustas de uma implementação de Exchange local. Este serviço permite o acesso ao correio electrónico a partir de qualquer parte e através de vários dispositivos, inclui protecção e conformidade dos dados enviados e recebidos, visibilidade e controlo através da consola de gestão. Fornece ao administrador de Exchange todos os aspectos de usabilidade, conformidade, segurança, controlo e familiaridade.

Rafael Rocha do Centro de Informática da UATLA referiu os seguintes factores como predominantes para a mudança para o Exchange Online:

- Aumento da disponibilidade do serviço de correio electrónico aos alunos
- Disponibilização de outros serviços integrados na solução Office 365, como por exemplo o Skydrive Pro (actual One Drive)
- Poupança em recursos de computação a nível local, tais como armazenamento (storage), licenciamento e largura de banda
- 2500 Caixas de correio licenciadas (com cerca de 300 caixas de correio partilhadas)
- Disponibilização de *software* (Office)
- O tempo despendido na manutenção/configuração do servidor Exchange local, pode agora ser direccionado para outros assuntos
- Projecto de inovação na UATLA

Com o ambiente em Exchange Server 2010 foi necessário instalar todos os pré-requisitos necessários e opcionais, tais como o Single Sign On (SSO), Active Directory Federation Services (ADFS), configuração do serviço de directórios (Dirsync), configuração do tenant, e configuração de certificados de Exchange.

Esta implementação ocorreu em Julho de 2012, e na altura a versão do Office 365 Exchange Online era a 2010 (*Wave 14*)

Para instalar a solução de SSO era necessário ter o nível funcional da Active Directory no mínimo em Windows Server 2003 R2 ou superior, algo que estava acautelado pelo CI, dado que o nível funcional da Active Directory estava em Windows Server 2008 R2.

Foi equacionado ter o serviço de federação da Active Directory ADFS a suportar a solução de SSO.

Foi necessário descarregar, instalar e implementar a aplicação AD FS 2.0 num novo servidor Windows Server 2008 R2, bem como realizar todas as actualizações do sistema operativo e configurar o STS para estabelecer a ligação de confiança da federação entre o ambiente local e a Windows Azure Active Directory.

A Active Directory têm de ter determinadas configurações de forma a poder funcionar de maneira correcta com o SSO. Em particular o User principal name (UPN), também conhecido como o nome de *logon* do utilizador.

Para preparar o ambiente Active Directory foi recomendada a utilização da Microsoft Deployment Readiness Tool, que inspecciona o ambiente da AD e providencia um relatório que inclui informação se todos os pressupostos foram cumpridos. Caso não tenham sido, a aplicação lista todas as alterações necessárias para preparar o ambiente correctamente. Por exemplo a aplicação verifica se existe UPN para cada utilizador e se estão no formato correcto.

Para a funcionalidade de SSO funcionar correctamente e igualmente como um pré-requisito obrigatório para a configuração de um ambiente híbrido foi necessário configurar a sincronização de directórios (DirSync) da Active Directory. A utilização do SSO e do Dirsync asseguram que as identidades dos utilizadores são apresentadas correctamente no serviço da nuvem. Estes passos passaram pela preparação, instalação e activação da ferramenta.

Quando se configura esta aplicação, está-se definir a sincronização dos objectos (utilizadores, contas de grupo) da AD local para a Windows Azure AD, que guarda uma cópia destes objectos. Depois de activada a sincronização estes dados só poderão ser alterados no ambiente local e sincronizados continuamente para o serviço na nuvem. A sincronização de directórios deverá ser considerado como um compromisso de longo termo em cenários de coexistência entre a AD local e a AD na nuvem. A sincronização de directórios permite não só criar versões sincronizadas de cada conta de utilizador e grupo, mas também permite que a lista de endereços global (GAL) seja sincronizada da organização local do Microsoft Exchange Server para o Microsoft Exchange Online.

Vários serviços Microsoft Online, como o Exchange Online providencia funcionalidades que trabalham melhor com certas informações do directório que possam ser controladas pelo serviço na nuvem. Nestes casos os objectos do directório (como os utilizadores) que são sincronizados desde a organização local podem ser alterados na Azure Active Directory. Estas alterações serão depois reescritas para a Active Directory local de modo a poderem ser utilizadas pelas aplicações da organização local. A este processo dá-se o nome de *write back*, e terá de ser permitido ao seleccionar a opção “*Hybrid Deployment*” na aplicação Dirsync.

Para implementar e gerir o processo de sincronização foi necessário preparar o ambiente, que consistiu em verificar os requisitos de sistema, criar as permissões adequadas e compreender as várias considerações sobre performance.

Todos os clientes de Office 365 e Azure Active Directory têm um limite por omissão de cinquenta mil (50000) objectos (utilizadores, contactos *mail-enabled* e grupos). Este limite determina quantos objectos podem ser criados no *tenant*. Quando é verificado o primeiro domínio, este limite é aumentado para os trezentos mil (300000) objectos. Se a Active Directory tiver menos de 50000 objectos, a sincronização de objectos pode ser implementada com o Microsoft SQL Server 2008 Express, no entanto se a AD tem mais de 50000 objectos, a implementação da sincronização de directório deverá ser efectuada numa instância completa de SQL Server. As instâncias completas SQL Server exigidas podem ser instaladas nas versões Microsoft SQL Server 2008 Standard, 2008 R2 ou 2012. Existem vários requisitos que tiveram de ser cumpridos, tais como o sistema operativo e os seguintes são suportados:

- 64-bit Windows Server 2008 Datacenter
- 64-bit Windows Server 2008 R2 Standard ou Enterprise, Windows Server 2008 R2 Datacenter
- 64-bit Windows Server 2012 Standard ou Datacenter
- 64-bit Windows Server 2012 R2 Standard ou Datacenter

O servidor onde irá ser instalado o Dirsync deve estar associado à floresta de Active Directory que irá ser sincronizada. Para o cenário de coexistência rica, esta é uma exigência, porque o servidor DirSync enumera explicitamente todos os controladores de domínio na floresta, a fim de definir as permissões para *write-back* dos valores dos atributos. Uma floresta é um ou mais domínios de Active Directory que partilham a mesma definição de classe e de atributos, local e informações de replicação, e recursos de pesquisa de toda a floresta.

A consola de Powershell tem de estar activa, bem como a actualização mais recente do Microsoft.NET Framework.

O acesso a este servidor deverá ser limitado apenas aos utilizadores que tenham acesso aos controladores de domínio e a outros componentes de rede sensíveis. Apenas os administradores ou utilizadores que tenham as permissões necessárias para realizar alterações nos controladores de domínio devem ter acesso a este servidor.

A floresta de Active Directory deverá ter o modo funcional em Windows Server 2003 ou mais elevado, para os controladores de domínio poderem comunicar com o ambiente de Office 365.

Quando a aplicação de Dirsync é instalada, o assistente de configuração cria uma conta de serviço que será utilizada para ler da AD local e escrever na Azure AD. Este assistente cria esta conta utilizando ambas as credenciais de administração da organização local e da

organização na nuvem, que foram solicitadas durante o processo de instalação. Na primeira execução da aplicação, esta irá copiar os objectos relevantes para a Azure AD. Antes de executar esta operação, deverá se saber o número de objectos que serão copiados, de forma a se poder planear qual será o impacto desta operação no tempo de resposta da rede e dos servidores de Exchange.

De referir que os objectos que são sincronizados aparecem imediatamente na Global Address List (GAL), mas podem demorar até 24 horas a serem visualizados na Offline Address Book (OAB) e no Lync Online.

O ambiente de Active Directory deve ser correctamente configurado para que os utilizadores possam fazer o *sign-in* para os serviços Microsoft Online. Em particular, o atributo UserPrincipalName (UPN), também conhecido como o nome de *logon* do utilizador, deve ser configurado correctamente para cada utilizador de uma maneira específica. O atributo UserPrincipalName deve usar um domínio publicamente roteável, caso o domínio não seja publico, deve adicionar um sufixo alternativo na Active Directory local.

É necessário adicionar um sufixo UPN alternativo para associar as credenciais corporativas do utilizador com o ambiente Office 365. Os UPN's que são usados para SSO podem conter letras, números, pontos, traços e sublinhados, mas não podem conter outros tipos de caracteres.

Para o processo de activação da sincronização de directórios, e antes da instalação da aplicação Dirsync é necessário e recomendado executar a aplicação Microsoft Deployment Readiness Tool como referido anteriormente. É muito mais simples identificar os erros e realizar as alterações propostas pela aplicação antes de activar e instalar a aplicação de sincronização de directórios. Uma estatística interessante e a ter em conta é o numero total de objectos a serem sincronizados.

Para activar a sincronização de directórios acedeu-se ao portal de Office 365 com as credenciais de administrador, e no menu Utilizadores e na opção Sincronização da Active Directory, foi seleccionada a opção Configurar e posteriormente a opção Activar. Esta activação também poderia ter sido realizada como o seguinte comando Powershell "Set-MsolDirSyncEnabled -EnableDirSync \$true".

Num dos controladores de domínio foi instalada a aplicação Dirsync (64-bit). Foi utilizado o assistente de configuração e foram providenciadas as credenciais de Administração da organização local e da organização Office 365, e foi iniciada a sincronização dos objectos entre as organizações.

O assistente da Windows Azure Active Directory Sync cria um objecto denominado de MSOL_AD_SYNC com o seguinte nome AAD_XXXXXXXXXX, em que XXXXXXXXXXXX é uma *string* alfanumérica de 12 caracteres específica desta instalação. A sincronização de directórios usa esta conta de serviço para ler e sincronizar as informações da Active Directory local. O Assistente de configuração também configura as sincronizações

recorrentes para cada três horas a partir da Active Directory local para a Windows Azure AD. Esta conta não deverá ser movida, removida ou alteradas as permissões, para não causar falhas de sincronização.

Se não pretendermos esperar pela sincronização recorrente a cada três horas, podemos força-la a qualquer momento através do comando Powershell “Start-OnlineCoexistenceSync”.

Após a finalização da sincronização foi verificado que os objectos estavam correctamente sincronizados, ou seja, copiados para a Azure AD, e com o estado de “Sincronizados com a Active Directory”.

Após esta sincronização foi necessário activar os utilizadores no *tenant* antes de poderem começar a utilizar os serviços na nuvem. O serviço na nuvem irá mostrar os utilizadores e grupos e a informação será igualmente sincronizada para o Exchange Online. A activação significa a permissão e a atribuição de uma licença para os utilizadores poderem começar a utilizar os serviços na nuvem, como por exemplo o Exchange Online. Para realizar este processo, acedeu-se ao portal Office 365 e em Utilizadores e Grupos, foram seleccionados os utilizadores pretendidos e foi seleccionada a opção Activar utilizadores sincronizados. Foi igualmente necessário definir a localização dos utilizadores e assignar as licenças pretendidas.

A partir deste momento toda a gestão de utilizadores é realizada a partir da Active Directory local.

Apenas após a configuração anteriormente descrita da sincronização de directórios é que foi possível configurar a federação do domínio e a funcionalidade de SSO, através de AD FS.

A federação de identidade única, também conhecida como Single Sign-on, consiste no cenário de integração de directório. Um STS permite federação de identidades, ampliando a noção de autenticação centralizada, autorização e SSO para aplicações Web e serviços localizados em praticamente qualquer lugar, incluindo redes de perímetro, redes de parceiros e nuvem. Quando um STS é configurado para fornecer SSO com um serviço da nuvem da Microsoft, uma relação de confiança federada está a ser criada entre o domínio na organização local e do mesmo domínio especificado no *tenant*. A figura 11 mostra um cenário de implementação de ADFS de modo simplificado.

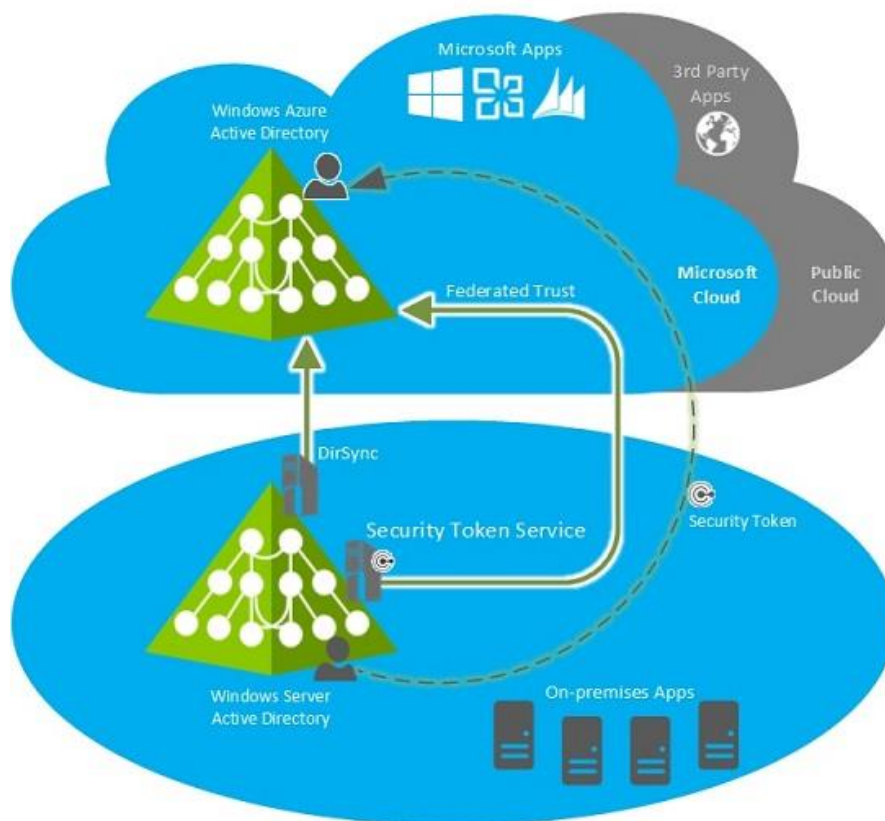


Figura 11 – Cenário de implementação de AD FS. Fonte Microsoft

Existem vários benefícios ao instalar este cenário, tais como, controlo de políticas, controlo de acessos, segurança e suporte para autenticação forte (autenticação em dois factores). A experiência dos utilizadores também será beneficiada, dado que poderão ter um ambiente similar ao de trabalhar com um computador da empresa na rede interna, quer estejam a aceder através de redes externas, como a de casa ou de uma rede pública, bem como trabalhar com um computador pessoal, com o *smartphone* ou com quaisquer clientes de correio electrónico.

Para federar um domínio partilhado entre a organização local e da nuvem, é necessário executar no servidor que contém a aplicação ADFS 2.0, na consola Powershell, o seguinte comando “New-MsolFederatedDomain –DomainName <domain>”, onde <domain> será o domínio pretendido. Após este passo será necessário criar o registo DNS correspondente, quer seja um registo TXT para verificar a propriedade do domínio, quer seja o registo MX, que ao mesmo tempo que verifica a propriedade do domínio, também altera o fluxo de correio electrónico da organização para a organização na nuvem. Se já existir um domínio partilhado entre as organizações, mas sem ser federado, bastará executar o comando Powershell “Convert-MsolDomainToFederated –DomainName <domain>”. O resultado destes comandos e respectiva operação poderá ser sempre verificado através do comando “Get-MsolFederationProperty –DomainName <domain>”. Caso as configurações não sejam idênticas poderá ser forçada a sincronização destas

configurações com o comando “Update-MsolFederatedDomain -DomainName <domain>”

Para habilitar a capacidade dos clientes de correio electrónico móveis em conectarem-se á organização de Exchange Online é necessário configurar correctamente os registos DNS, e entre eles especial destaque é dado ao Autodiscover. Este registo serve para configurar automaticamente as definições dos referidos clientes. Dependendo da configuração híbrida poderá ser necessário configurar dois ou mais dos seguintes registos públicos de DNS. O registo de DNS Autodiscover para a organização local necessita de referir os pedidos de autodiscover.dominio.com para o servidor com a *role* de CAS. Pode ser utilizado um registo CNAME ou A (Host). O registo CNAME deve referir o FQDN (Fully Qualified Domain Name) de um servidor com a *role* CAS e o registo A deve apontar para o endereço IP externo da organização, dependendo da organização.

O registo SPF utiliza o Sender ID Framework, que é um protocolo de autenticação de correio electrónico que ajuda a prevenir o *spoofing* e o *fishing* ao verificar o nome do domínio do qual as mensagens de correio electrónico são enviadas. O Sender ID valida a origem das mensagens de correio electrónico, verificando o endereço IP do remetente contra o suposto proprietário do domínio de envio.

No caso específico da Universidade Atlântica foi necessário criar o registo público de Autodiscover (autodiscover.uatlantica.pt) e de SPF (v=spf1 mx mx:exet01.uatlantica.pt ip6:2002:C189:E00A::C189:E00A -all)

Depois foi necessário adicionar a organização de Exchange Online na consola de gestão do servidor Exchange 2010 local (EMC). A organização na nuvem é adicionada como Floresta de Exchange, sendo necessário especificar um nome “amigável” e as credenciais do Exchange Online.

Para se conectar á organização na nuvem através da consola Powershell, devem ser utilizados os seguintes comandos:

```
“$O365Cred = Get-Credential”
```

```
“$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri  
https://ps.outlook.com/powershell/ -Credential $O365Cred -Authentication Basic –  
AllowRedirection”
```

```
“Import-PSSession $Session”
```

Para desconectar a sessão deve-se utilizar o comando “Remove-PSSession \$Session”, porque caso a consola seja fechada sem se utilizar o comando referido, a sessão ainda fica activa, e o número máximo de três conexões ao *tenant* poderá ser atingida, impossibilitando novas ligações, até que uma das sessões expire.

Como já referido anteriormente para realizar o processo de relação entre as duas organizações e configurar o ambiente híbrido é necessário adquirir um certificado externo. A Universidade Atlântica optou por adquirir um certificado *wildcard*, que serviu para todos os serviços existentes na organização local bem como cumpriu os pré-requisitos do ambiente híbrido.

Na EMC foi necessário importar o certificado externo adquirido e assignar os serviços pretendidos (SMTP, IIS, FTP, OA)

A próxima fase da configuração do ambiente híbrido é a configuração das várias directorias virtuais com o FQDN do servidor com a *role* de Client Access Server. Ao completar esta tarefa foi adicionado o URL externo nas directorias virtuais Exchange Web Services (EWS), Outlook Address Book (OAB), Outlook Web App (OWA), Exchange Control Panel (ECP), e Exchange ActiveSync (Microsoft-Server-ActiveSync).

O próximo passo consiste em executar o assistente de configuração híbrida (HCW) para criar as bases para a implementação híbrida. O novo assistente de configuração híbrida cria o objecto HybridConfiguration na Active Directory local. Este objecto armazena as informações de configuração híbrida para a implementação.

O HCW reúne dados de configuração do Exchange e da topologia de Active Directory, e em seguida executa uma extensa sequência de tarefas de configuração da implementação híbrida.

Como a Universidade Atlântica tinha o Service Pack 3 instalado no servidor CAS de Exchange 2010, bastou ir á consola gráfica do Exchange, seleccionar o nó Organization Configuration, de seguida seleccionar a *tab* Hybrid Configuration, e clicar na opção New Hybrid Configuration. Com estas acções foi criado o objecto de configuração híbrida na Active Directory.

Posteriormente foi necessário adicionar os dados para completar o HCW. Novamente na consola gráfica de Exchange, foi seleccionada a *tab* Hybrid Configuration, e seleccionada a opção Manage Hybrid Configuration, introduzir as credenciais do administrador da organização local de Exchange e as credenciais de administração do Exchange Online.

O passo seguinte da configuração foi a adição de domínios que queriam ser partilhados entre as organizações e para isso foi necessário criar os registos TXT correspondentes no DNS público. O registo TXT consiste em vários caracteres alfanuméricos, como pode ser verificado no seguinte exemplo:

```
“contoso.com
TXT
7Zyr2i/fE/M/T3AwCpitDbF30Fk/TdzXME6f7d11DaKGthPdoS+UF94t43D2nU5hLNnI
AP+5A3jJR2ik9HDPgg==”.
```


No HCW foi também necessário indicar o FQDN dos servidores Exchange com a *role CAS* e com a *role HUB* (neste caso era o mesmo servidor) e indicar o fluxo de correio electrónico pretendido, ou seja, se era pretendido que o fluxo de correio electrónico fosse direccionado todo para a organização local e depois redireccionado para a organização na nuvem, ou se era pretendido que o fluxo de correio electrónico fosse direccionado para a organização na nuvem e depois redireccionado para a organização local caso fosse necessário. A opção recaiu na primeira hipótese, de modo a não existirem alterações nesta fase do registo MX. Dado que a Universidade Atlântica tem um servidor com a *role* de EDGE e pretendia mantê-lo, foi necessário executar o HCW novamente e configurar o conector de Envio e de Recepção com o FQDN do servidor com a *role* de EDGE. Foi também necessário importar o certificado externo neste mesmo servidor.

Após este processo foi necessário executar testes de integração, como a criação de utilizadores a partir da organização local e verificar a sincronização, criação de caixas de correio de teste em ambas as organizações, e realizar testes de migração das caixas de correio de utilizador, bem como as caixas de correio de arquivo e caixas de correio partilhadas.

Depois dos testes realizados foi iniciada a migração. A migração em ambiente híbrido é realizada de modo a que o utilizador final apenas se aperceba dessa situação quando a mesma é finalizada e é enviado a informação para o mesmo.

Mover caixas de correio da organização local para a organização Exchange Online requer com se utilize pedidos de migração remota das caixas de correio.

Esta abordagem permite mover as caixas de correio da organização local para a organização na nuvem, ao invés de criar as caixas de correio no Exchange Online e importar o conteúdo manualmente.

A migração irá consumir vários recursos do servidor, e por isso existe o serviço MRSProxy que limita ou não a capacidade de migração, dependendo do número total de caixas de correio seleccionadas, o tamanho das mesmas e das propriedades do próprio serviço. Além de ser possível migrar as caixas de correio, também é possível criar novas caixas de correio directamente a partir da organização local. Estas caixas de correio são denominadas de remotas.

A migração foi efectuada através da consola de gestão do Exchange (EMC) através da opção “New Remote Move Request”. Esta opção abre um assistente de migração onde foi necessário indicar a(s) caixa(s) de correio a ser(em) migrada(s), seleccionar a floresta de origem (organização local) e a floresta de destino (Exchange Online), o FQDN do servidor som o serviço MRSProxy na floresta de origem e as credenciais de administração da organização local. Após estas informações foi ainda é necessário seleccionar para a opção “Target Delivery Domain” o domínio principal no Exchange Online. Depois foi necessário aguardar para que a migração ficasse concluída, sendo visualizado o estado de Completo no pedido de migração.

Este procedimento foi efectuado por fases, para limitar e não estrangular a largura de banda e serviços do servidor de Exchange, e repetido até que as caixas de correio fossem migradas na totalidade.

Durante este processo foi necessário manter os utilizadores informados, e verificar de que todas as funcionalidades do cliente Outlook estavam a funcionar correctamente após a migração das caixas de correio.

Algum tempo após a migração de todas as caixas de correio para o Exchange Online, foi decidido actualizar a versão de Exchange de 2010 para 2013 na organização local. Quando se actualiza uma organização de Exchange 2010 para 2013, existe um período de tempo em que ambas as versões vão coexistir. Esta coexistência pode ser mantida durante um período de tempo indefinido, ou pode-se concluir imediatamente a actualização, movendo todos os recursos do servidor Exchange 2010 para o servidor Exchange 2013, e depois iniciar a desinstalação do servidor com a versão 2010.

A versão Exchange 2013 trouxe várias novidades, entre as quais a arquitectura única, que podemos verificar na Figura 12, para melhorar e poder mais facilmente escalar as implementações para o Office 365. Este princípio levou a Microsoft a realizar grandes mudanças em todo o produto.

No Exchange Server 2013, ao invés das cinco *roles* existentes nas versões anteriores, existem dois blocos básicos de construção – o *array* de Client Access e o Database Availability Group (DAG)- o que resulta em duas *roles*, CAS e MAILBOX. Cada bloco proporciona uma unidade de alta disponibilidade e tolerância a falhas, que são dissociados um do outro.

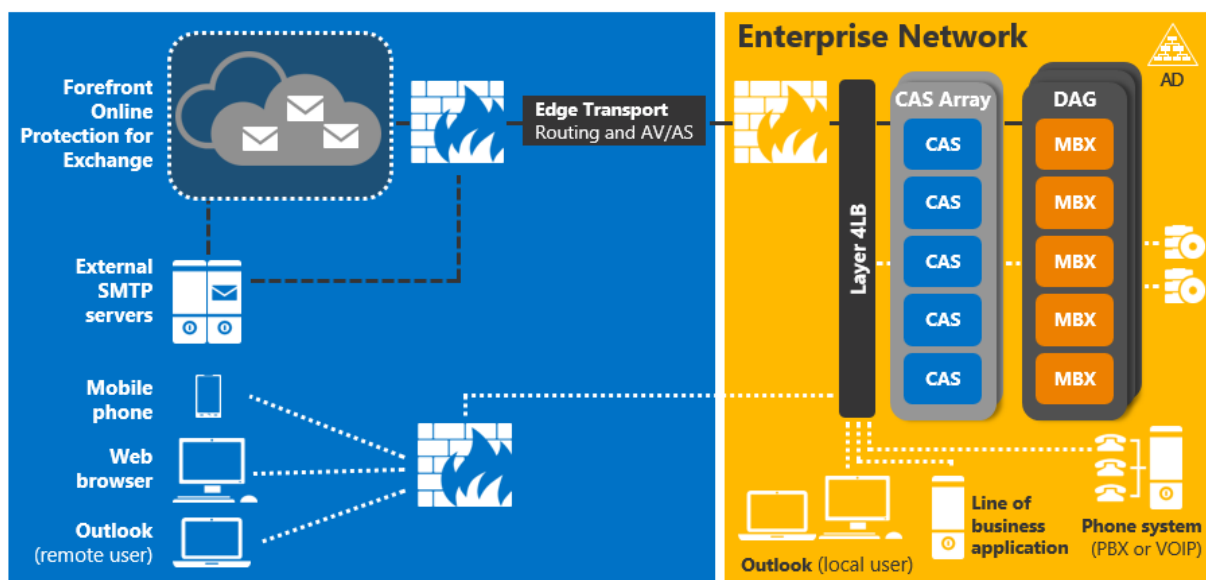


Figura 12 – Arquitectura Exchange Server 2013. Retirado de (Smith, 2013)

A *role* de CAS na versão 2013 é composta por três componentes, protocolos clientes, SMTP, e UM Call Router, e é uma sessão de protocolo sem estado de servidor, que é organizada numa configuração de balanceamento de carga. Ao contrário das versões anteriores a afinidade de sessão não é exigida no balanceador de carga, apesar de ser desejável que o balanceador de carga lide com políticas de gestão de conexão e verificação de saúde.

Este comportamento é desejável porque agora a lógica existe no CAS para autenticar o pedido e, em seguida, encaminhar o pedido para o servidor Mailbox que aloja a cópia activa da base de dados das caixas de correio.

No Exchange 2013 o Client Access Server funciona como a porta frontal, admitindo todos os pedidos dos clientes e encaminhando-os para a base de dados da caixa de correio activa, providencia também funcionalidades de segurança, como SSL e autenticação cliente, e gere as conexões de clientes através de redireccionamentos e da funcionalidade de proxy. O CAS também manuseia todas as mensagens de correio seguras enviadas entre a organização local e a organização na nuvem, bem como as regras de transporte, políticas de entrega de mensagens para as caixas de correio num ambiente híbrido. Toda a conectividade cliente, incluindo o acesso ao cliente Outlook, OWA, e o Outlook Anywhere passa através da *role* CAS. As funcionalidades da relação organizacional, como a partilha de informações *free/busy* também são tratadas pelo CAS.

A *role* Mailbox hospeda agora todos os componentes e/ou protocolos que processam, verificam e guardam os dados, as caixas de correio dos recipientes e comunica com a organização Exchange Online via proxy através do CAS da organização local. Para assegurar esta comunicação é configurado um conector de envio para suportar o transporte seguro de mensagens de correio electrónico híbrido.

Não existem conexões directas de clientes ao Mailbox Server Role, porque como referido anteriormente todas as conexões clientes são tratadas pelo CAS. Podemos verificar graficamente na Figura 13 as interações entre estas *roles*.

Os servidores com a *role* de Mailbox podem ser adicionados a um DAG (Database Availability Group), formando dessa forma uma unidade de alta disponibilidade, que pode ser implementada em um ou mais *datacenters*.

Ao contrário das versões anteriores, as funcionalidades não estão dispersas entre as várias *roles*, dado que a *role* de Mailbox interage directamente com a Active Directory, o CAS e o cliente Outlook.

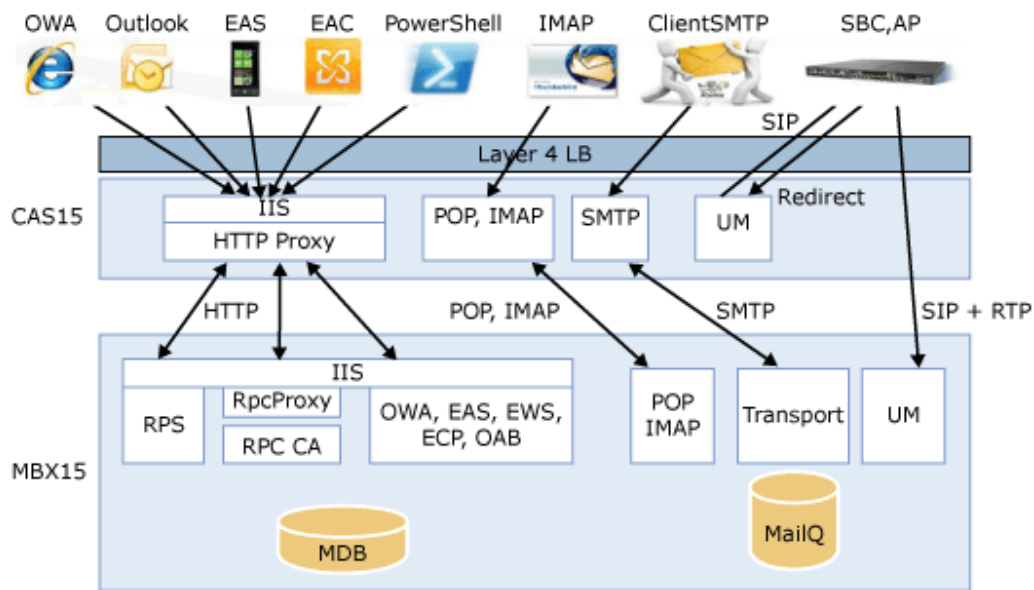


Figura 13 – Interação entre as rolas CAS e MAILBOX – Retirado de Microsoft, 2013

Após a transição para o Office 365 e após a actualização do servidor interno de Exchange para a versão 2013, a rede da universidade ficou esquematizada da seguinte forma:

Dois controladores de domínio (Domain Controllers) com Windows Server 2008 R2, um dos controladores de domínio com a aplicação de sincronização de directórios (Dirsync) instalada, um servidor também com Windows Server 2008 R2 e com a aplicação AD FS 2.0 instalada, um servidor de Exchange Server 2013 com as *roles* CAS e Mailbox na rede interna e na rede de perímetro um Exchange Server 2010 SP2 com a *role* de EDGE, como visto na Figura 14.

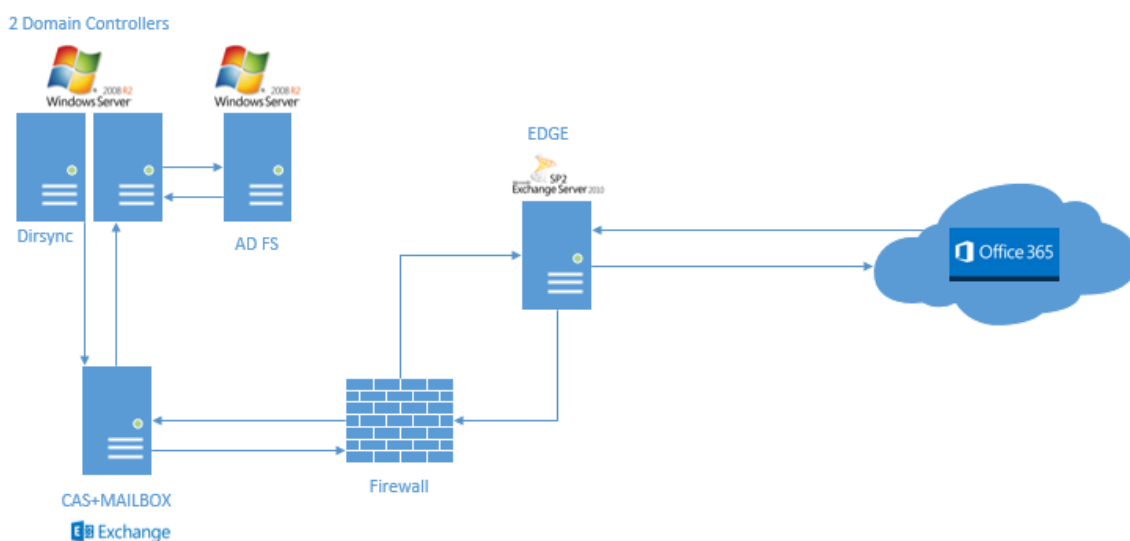


Figura 14 - Diagrama de rede simplificado da UATLA após a migração

4.4. Melhorias

Após ter revisto o processo de migração da solução de correio electrónico, identificado o estado actual da infra-estrutura da Universidade Atlântica, com especial atenção para a utilização dos serviços da tecnologia Office 365, e após toda a revisão de literatura e conhecimento adquirido sobre a mesma, descrevo as possíveis melhorias que podem ser realizadas na UATLA.

De acordo com o que me foi referido no levantamento do estudo de caso, bem como na minha apreciação das prioridades das melhorias que poderão ser efectuadas na Universidade Atlântica, construi o quadro representado na Tabela 4 para melhor exemplificar a relação entre as mesmas.

Prioridade	Alta		2013 SP1	LYO
	Média		SPO	
	Baixa	Y / OD		
		Baixo	Médio	Alto
Esforço				

Legenda:	
LYO	Lync Online
SPO	Sharepoint Online
2013 SP1	Exchange Server 2013 SP1
Y	Yammer
OD	OneDrive

Tabela 4 – Quadro de comparação de prioridades versus esforço, na implementação das melhorias do estudo de caso.

Em termos de prioridade mais elevada considerei que a instalação do Exchange Server 2013 SP1 é a mais prioritária, dado que vêm aumentar a segurança do sistema de correio electrónico, seja na implementação de novos protocolos de segurança, seja na correcção de vários problemas detectados, bem como na novidade de a *role* EDGE ser novamente disponibilizada para a tecnologia Exchange.

Instalação do Exchange Server 2013 SP1

Sugiro a instalação do Exchange Server 2013 Service Pack 1 no actual servidor Exchange 2013 com as *roles* CAS e Mailbox, bem como a actualização do servidor Exchange 2010 com a *role* de EDGE.

O Service Pack 1 da versão 2013 do Exchange Server está disponível desde o fim de Fevereiro de 2014. Além de incluir várias correcções, o SP1 fornece melhorias na segurança e conformidade, arquitectura e administração, e experiência do utilizador.

Em termos de segurança e *compliance* estas melhorias incluem a funcionalidade de DLP (Data Loss Prevention) e o regresso da encriptação S/MIME para utilizadores OWA. As *DLP Policy Tips*, que consistem em avisos que são visualizados quando um utilizador tenta enviar uma mensagem contendo dados sensíveis que correspondem a políticas criadas, foram activas para o OWA (Outlook Web Access). Estas são as mesmas *Policy Tips* disponíveis no Outlook 2013. As políticas DLP permitem detectar informações confidenciais, como dados financeiros ou pessoais, e o DLP Document Fingerprinting expande esta capacidade de detectar formulários utilizados na organização, como por exemplo, pode ser criada uma impressão digital de um documento com base no formulário de solicitação de patente da organização, para identificar quando os utilizadores estão a enviar esse documento. O DLP de seguida utiliza várias acções para controlar adequadamente a divulgação do conteúdo.

O SP1 reintroduz a funcionalidade de S/MIME para o OWA, o que permite aos utilizadores que acedem á caixa de correio por OWA, enviar e receber mensagens de correio electrónico encriptadas e assinadas. As mensagens assinadas permite ao recipiente verificar que a mensagem foi enviada pelo remetente especificado e que contem apenas o conteúdo enviado por esse mesmo remetente. Esta funcionalidade é suportada na utilização do OWA através do Internet Explorer 9 ou versão superior.

As melhorias verificadas na arquitectura e administração, ajudam a tecnologia de Exchange a estar actualizada com os requisitos solicitados pelos clientes, tais como o suporte ao sistema operativo Windows Server 2012 R2 e ambiente Active Directory para os níveis funcionais de domínio e floresta.

Outra das funcionalidades incluídas foi o Exchange Admin Center Cmdlet Logging, que consiste na verificação através do EAC dos 500 comandos mais recentes utilizados através do interface enquanto a janela de *logging* está aberta.

Uma das grandes novidades é a reintrodução da *role* EDGE, o que vem adicionar um melhor suporte a organizações que necessitem desta funcionalidade, apesar de a coexistência com a versão anterior de 2010 ser ainda suportada.

Outra grande novidade é a possibilidade de as implementações híbridas serem agora suportadas em ambientes multi-floresta de Active Directory, ou seja em organizações que

contêm servidores de Exchange implementados em várias florestas Active Directory. Para as organizações que utilizam os serviços de federação (ADFS) foi também adicionado o suporte de autenticação baseado em *claims*, o que vem permitir com que seja utilizada a autenticação multi-factor com domínios federados.

Em termos de protocolos de comunicação existem algumas novidades. Uma delas é a utilização do OAuth (Open Authorization) que permite com que a informação de colaboração entre a organização local e a organização na nuvem seja mais facilitada aquando da utilização num ambiente híbrido. Este processo de autenticação irá substituir o processo de confiança de federação (Exchange Federation trust) e habilita os processos de *Free/Busy*, *MailTips*, *Message Tracking* e *In-place eDiscovery*.

Foi também adicionado um novo método de comunicação para o Exchange e para o cliente Outlook. Este novo método de chama-se MAPI sobre HTTP (MAPI / HTTP). Este método de comunicação facilita e simplifica a resolução de problemas de conectividade e melhora a experiência do utilizador restaurando a ligação quando o computador regressa de hibernação ou quando se troca de rede. O MAPI/HTTP vem inactivo por omissão, de modo a que se possa decidir quando o mesmo é activado para a organização. Este protocolo visa substituir a utilização do RPC/HTTP (Outlook Anywhere) para a versão Outlook 2013 SP1. O Windows Server 2012 R2 introduz *clusters* de *failover* que podem operar sem um ponto de acesso administrativo, e o Exchange faz uso desta funcionalidade para utilizar os DAGs sem necessidade de ter um *cluster* de pontos de acesso administrativos, sem endereços de IP, sem recursos de nome de rede, e sem nome de objecto de *cluster*.

De referir que os DAGs com pontos de acesso administrativo continuam a ser suportados. O Exchange Server 2013 SP1 suporta agora SSL Offloading, permitindo-lhe terminar conexões SSL no servidor CAS e mover toda a carga de trabalho SSL, ou seja as tarefas de criptografia e descriptação, para um dispositivo balanceador de carga.

Em termos de experiência do utilizador foi adicionado ao OWA o mesmo editor de texto que o Sharepoint, melhorando desta forma a experiência e permitindo vários novos recursos de formatação e composição, incluindo mais opções de colar, a capacidade de criar e modificar tabelas, e pré-visualizações de conteúdo

Existe agora a possibilidade de utilizar aplicações quando se estiver a criar mensagens de correio electrónico. Este facto permite aos programadores criar aplicações para ajudar os utilizadores enquanto escrevem as mensagens. Estas aplicações podem ser adicionadas através da loja do Office ou catálogos corporativos.

Todas estas novas funcionalidades foram apresentadas na Microsoft Exchange Conference (Microsoft, 2014), realizada este ano na cidade de Austin, Texas e que tive o prazer de assistir.

Antes da instalação deste Service Pack, terá de ser actualizada a Active Directory, porque irão existir alterações no esquema da mesma. Para isso é necessário executar os seguintes comandos (preferencialmente antes da instalação do Exchange 2013 SP1):

- `setup.exe /PrepareSchema /IAcceptExchangeServerLicenseTerms`
- `setup.exe /PrepareAD /IAcceptExchangeServerLicenseTerms`

Uma vez que as etapas preparatórias acima descritas sejam concluídas, o SP1 pode ser instalado no servidor. Claro que, como sempre, se os passos descritos não forem executados separadamente, estes serão executados pelo programa de instalação.

Este procedimento irá obrigar a um reiniciar do servidor, e após a instalação deste Service Pack, a versão de Exchange não poderá ser revertida. Se o Service Pack for desinstalado o Exchange Server 2013 será removido do servidor.

Configuração/Implementação da tecnologia Lync

Como mostrado na Tabela 4 e devido à prioridade de implementação de uma solução de comunicação em tempo real e dado que a taxa de esforço do mesmo é elevada, sugiro que logo após a instalação do Exchange Server 2013 Service Pack 1, seja dada atenção à implementação e configuração da tecnologia Lync. O Lync Online providencia capacidades de comunicação em tempo real, incluindo as mensagens instantâneas e a comunicação em áudio e vídeo. As organizações podem verificar a informação de presença dos colaboradores, independentemente da localização ou fuso horário, e escolher a melhor maneira de comunicar. Tal como nos restantes serviços do Office 365, a principal função é a de conectar e melhorar a interacção entre as pessoas.

Existem três cenários de implementação possível da tecnologia Lync.

- Cenário 1 – Implementação apenas na organização local (Lync Server)
- Cenário 2 – Implementação do serviço na nuvem (Lync Online)
- Cenário 3 – Implementação de um cenário híbrido (Lync Server e Lync Online)

No cenário 1 todos os servidores são instalados e mantidos na e pela organização local. Este cenário oferece todos os recursos da tecnologia, mas dado que todas as caixas de correio da Universidade Atlântica foram migradas para o Office 365, não será o cenário mais indicado neste momento, porque seria necessário transitar de novo para a organização local todas as caixas de correio para providenciar a experiência de Single Sign-On na plataforma Microsoft, e não iriam aproveitar as vantagens de utilização da plataforma na nuvem.

No cenário 2 o método de implementação depende exclusivamente da solução Lync Online como parte do Microsoft Office 365. Os serviços Lync são fornecidos através da nuvem e a maioria das funcionalidades está disponível.

Na minha opinião este seria o cenário ideal para implementar na Universidade Atlântica devido a terem todas as caixas de correio actualmente no Office 365 e de modo a continuar a cumprir os objectivos delineados aquando da migração da solução de correio electrónico. O Lync Online permite verificar a informação de presença, onde podemos verificar o estado de disponibilidade e outras informações relacionadas com a presença no Lync ou em outras ferramentas Microsoft, como o Microsoft Outlook, e desta forma escolher qual a melhor maneira de comunicar. Permite também enviar mensagens em tempo real, transferir ficheiros com as pessoas com que estão a comunicar, bem como comunicação de áudio e vídeo, incluindo videoconferências e partilha de ecrã e aplicações. A lista seguinte apresenta as funcionalidades completas integrando a tecnologia Lync Online com a tecnologia Exchange Online:

- IM (Mensagens instantâneas) / Presença no Outlook
- Agendar e participar em reuniões *online* através do Outlook
- IM / Presença no Outlook Web App
- Agendar e participar em reuniões *online* a partir do Outlook Web App
- IM / Presença em clientes móveis
- Juntar-se a reuniões *online* em clientes móveis
- Publicar estado com base no calendário do Outlook (informações *free/busy*)
- Os ficheiros com o historial de chamadas e de conversas perdidas são escritos para a caixa de correio do utilizador
- Lista de contactos
- Foto de contacto em alta resolução no cliente Lync 2013 e Lync Web App
- Delegação de reuniões
- Arquivo do conteúdo (IM e reuniões) no Exchange
- Correio de voz

Para grande parte destas funcionalidades é necessário instalar o cliente rico Lync 2013, que está disponível com a oferta Office365 Pro Plus na subscrição para o Ensino e Educação. Existem algumas limitações no Lync Online, como poder estar dependente da localização (em Portugal não existe nenhuma restrição em termos de planos de subscrição de Lync Online) para ter acesso a todas as funcionalidades, ou a substituição/integração de uma central telefónica (PBX) não ser suportada.

Antes de configurar o Lync Online para todos os utilizadores na organização, deve-se instalar o cliente Lync para alguns utilizadores de teste (projecto piloto), executar as tarefas de planeamento e configuração que se aplicam á organização e em seguida analisar e rever os recursos de formação e treino.

Existem pré-requisitos para suportar o cliente Lync, tais como:

- Versão do sistema Operativo
 - Windows 7 ou superior
 - Windows Server 2008 R2 com o ultimo Service Pack
- Navegador de Internet
 - Internet Explorer 7 ou superior
 - Mozilla Firefox
- Cliente Microsoft Outlook
 - Versão 2010 ou 2013
- Macintosh
 - Microsoft Lync for Mac 2011
 - Microsoft Communicator for Mac 2011
- Os perfis na Active Directory não podem ser mandatórios, porque estes são apenas perfis de leitura e a PKI (Public Key Infrastructure) necessária para a utilização do Lync não pode ser escrita no perfil.

O centro de administração do Lync inclui as configurações de toda a organização, e as configurações individuais dos utilizadores. Algumas dessas configurações referem-se a:

- Federação do domínio, que permite comunicar com outras organizações que utilizem Lync
- Conectividade pública de mensagens instantâneas, para comunicar com os utilizadores Skype
- Notificações para dispositivos móveis
- Estado de presença privado, para determinar quem pode ou não verificar o estado de presença dos utilizadores Lync
- Convite para reunião, que permite adicionar o logotipo e o personalizar o rodapé, adicionar *links* para ajuda e informação legal
- Comunicação de áudio e vídeo
- Gravação de chamadas e reuniões
- Permissão de efectuar chamadas anónimas por parte dos participantes numa reunião

O cenário 3 proporciona uma combinação de uma configuração de Lync na organização local e Lync Online, em que poderão existir utilizadores em ambas as organizações usando apenas um nome de domínio. De salientar que apenas os utilizadores que estejam configurados na organização local irão dispor de todas as funcionalidades oferecidas pela tecnologia.

Mais uma vez e dado que para este cenário seria necessário migrar algumas das caixas de correio novamente para a organização local para terem acesso a todas as funcionalidades, não será na minha opinião o cenário recomendado.

Este cenário poderá ser viável e recomendado caso pretendam substituir ou implementar uma central telefónica (PBX) e efectuar todo o tipo de comunicações através da tecnologia Lync.

Para uma interacção mais segura pode-se activar a federação do domínio de Lync, caso exista uma instalação de Lync na organização local, em outras organizações externas ou para comunicar com utilizadores de Skype. Por exemplo se pretender comunicar com outros utilizadores de outras universidades que utilizem Lync ou Skype. O ambiente híbrido permite com que várias funcionalidades estejam disponíveis para os utilizadores em ambas as organizações, como por exemplo a *role* de Unified Messaging, mas existem algumas funcionalidades que estão apenas disponíveis no Lync Server. Os utilizadores podem iniciar facilmente qualquer conversa, seja por mensagem, áudio ou vídeo, verificar todos os participantes, tendo disponível várias visualizações para melhorar a experiência de utilização, bem como a possibilidade de partilhar apresentações, votações, interagir com o Microsoft Outlook para criar reuniões marcadas com antecedência, e a possibilidade de gravação das mesmas.

Além do cliente Lync local, também existe o cliente *web-based*, que tem a capacidade de poder participar em reuniões *online*.

De salientar toda a interoperabilidade existente entre o Lync Online com o Exchange (e Exchange Online) e com o Sharepoint.(e Sharepoint Online).

A integração da tecnologia Lync com a tecnologia Exchange poderá ser realizada tanto com o Exchange Server na organização local como com o Exchange Online.

Utilização do serviço Sharepoint Online

O SharePoint Online oferece os recursos poderosos do SharePoint, sem a sobrecarga associada de gestão da infra-estrutura. As opções de gestão flexíveis garantem a manutenção do controlo necessário para atender aos requisitos de conformidade das organizações.

Para a Universidade Atlântica poderia servir de incentivo para criar repositórios de partilha de informação e de colaboração para os alunos e docentes de cada disciplina e respectiva área de conhecimento, mais conhecidos como *sites* de equipa, bem como albergar os vários *microsites* existentes por cada departamento, e o próprio *site* principal da UATLA. Os *sites* de equipa do SharePoint vêm com uma abundância de recursos out-of-the-box. Pode-se personaliza-los, alterando a sua aparência e adicionando funcionalidades sem utilizar outras aplicações ou fazer qualquer tipo de programação.

Poderá também ser utilizado para gerir os projectos existentes na universidade, e permite igualmente a interacção com o Project Server e a sincronização com o Microsoft Project Professional.

A gestão e organização de documentos, bem como a pesquisa de conteúdos desses

documentos poderá ser realizada pelo Sharepoint Online, além da interacção com os restantes programas disponibilizados na oferta do Office 365 Pro Plus. A utilização deste serviço irá permitir a conexão de pessoas á informação e recursos que necessitam e melhorar a produtividade, garantir a segurança e integridade da informação, melhorar a usabilidade, adaptar as soluções às necessidades e fazer um melhor uso da informação. Um dado importante a reter é a capacidade de numa única localização ter acesso até 1 TB (terabyte) de espaço em cada *site collection*, e um potencial enorme em termos de escalabilidade. Neste espaço disponível estão contidos o espaço do conteúdo colocado no One Drive e no Yammer.

Cada vez é mais importante a disponibilização destes conteúdos para os dispositivos móveis e em que a capacidade de interacção não seja afectada ou completamente diferente entre dispositivos. Através das aplicações móveis Sharepoint este propósito é atingido.

Disponibilização do Office 365 OneDrive

Uma das facetas mais importantes para os estudantes será sempre a capacidade de terem o conteúdo necessário (e se possível a totalidade desse conteúdo) sempre disponível e acessível. O OneDrive possibilita esta capacidade, dado que com segurança consegue arquivar e partilhar com outras pessoas os valiosos ficheiros. Permite igualmente a sincronização do conteúdo em vários dispositivos, de modo a que o possa aceder sem estar ligado á internet, e qualquer alteração realizada será sincronizada na próxima vez que se conectar á internet. A gestão de partilha de ficheiros ou pastas é feita de forma simples e fácil, os utilizadores com permissões podem trabalhar nos ficheiros em tempo real, quer seja através das aplicações Office instaladas no computador, quer seja através do navegador, ou através das aplicações para dispositivos móveis. Todas as alterações realizadas podem ser facilmente controladas através do controlo automático de versões, e em caso de necessidade poderá ser revertido para uma versão anterior. O Office 365 OneDrive é *compliant* com vários *standards*, incluindo o ISO 27001, Clausulas modelos da União Europeia, HIPAA BAA, e FISMA e é verificado por auditores externos.

Os documentos que foram carregados estão disponíveis para pesquisa e preservação, ou seja o conteúdo está protegido enquanto os utilizadores continuam a trabalhar neles. Os administradores podem gerar relatórios de auditoria para os eventos mais comuns ou configurar a auditoria para gerar alertas sobre outros eventos que melhor sirvam as necessidades da organização. As funcionalidades de segurança também são centrais, de modo a permitir controlo granular, como partilha externa do conteúdo, sincronização *offline* e controlo de acessos.

O novo interface de utilizador do OneDrive permite algumas inovações e refinamentos ao incluir controlos simples (novo, enviar, sincronizar, editar, gerir, e partilhar), onde com um simples clique consegue-se criar novos documentos, realizar o envio de ficheiros para armazenamento, partilhar ficheiros para utilizadores internos e/ou externos. Estes novos

comandos estarão acessíveis em todas as livrarias de documentos. No novo interface surge também o acesso a pastas de *sites*, que permite seguir um site, seja pelo conteúdo e a facilidade de visualizar todos os documentos lá colocados, quer seja pela razão de o gerir. Outra novidade é o facto de a pesquisa ser mais inteligente, o que permite que a pesquisa seja iniciada mal comece a digitar, e é realizada em todos as pastas.

Criação de rede social privada da UATLA com o Yammer

Como sabemos as redes sociais são essenciais para promover a colaboração entre os funcionários, seja para gerar mais ideias de negócio e inovar ou melhorar o ambiente de trabalho. A utilização das redes sociais permite a conexão entre alunos e docentes, e ajuda as pessoas a socializarem aquando de uma pausa.

As organizações estão a transformar a maneira como as pessoas trabalham em conjunto com o Yammer e o Office 365, que formam o núcleo da visão da Microsoft para a rede social corporativa. Para esta integração existem três fases que necessitam de ser cumpridas e que consistem na, integração básica para reunir os serviços, conexões mais profundas para activar uma experiência sem igual, e ligar experiências que disponibilizem ao mesmo tempo as mensagens instantâneas, colaboração e correio electrónico.

O Yammer é uma rede social privada que aproxima as pessoas, conversas, conteúdo e dados de negócio. Os dispositivos móveis começam a ter cada vez mais relevância na utilização das redes sociais, porque permite aos utilizadores estarem sempre disponíveis, é uma tendência no actual mundo empresarial, marcar presença ou monitorizar os ambientes sociais da internet, e como o Yammer pode ser acedido directamente através do navegador de internet, em qualquer altura ou lugar.

Segundo a Microsoft neste momento mais de duzentas mil empresas em todo o mundo utilizam o Yammer, que como plataforma integra-se facilmente com outros sistemas para conectar-se a todas as aplicações de negócio de modo a criar uma única experiência social. Esta experiência poderá permitir á universidade ouvir as conversas mais interessantes, dada a partilha de informação, conteúdo e organização á volta de novos ou projectos existentes, entre as várias equipas, turmas e departamentos. Esta colaboração pode ser efectuada em grupos de modo flexível e num espaço de trabalho que permite discutir nas várias interacções e partilhar ficheiros. Adaptar-se e realizar decisões com maior conhecimento, porque poderão existir dados desconhecidos isso poderá com que se tenha de realizar decisões rapidamente. A colaboração entre pessoas com os mesmos objectivos, a possibilidade de dar voz a todos os colaboradores, e o aproveitar de oportunidades, faz com que a universidade possa crescer á velocidade de um mundo hiperconectado.

5. Considerações Finais

Estamos a sofrer uma alteração em termos de paradigma, em que os serviços estão a ser disponibilizados através de prestadores de serviços baseados na Internet. Aparentemente não existem dúvidas de que a computação em nuvem tem um potencial de desenvolvimento enorme. Antecipa-se um aumento significativo da procura de soluções na nuvem por parte das empresas e organizações, num processo de mudança de paradigma que está ainda apenas a começar.

Como referido anteriormente, da parte dos fornecedores a tecnologia está disponível, o ecossistema consolida-se e as ofertas são cada vez mais à medida do cliente. Mas precisam de reforçar a informação sobre o valor das suas propostas, para que os utilizadores definam estratégias sustentadas de desenvolvimento na nuvem que vão muito além da mera redução de custos.

Como referido por Paolo Campoli - Head of Service Providers Architectures e CTO Cisco EMEAR na conferência "Cloud Computing: futurologia ou inevitabilidade?" (APDC, 2013) num mundo em mudança profunda, cada vez mais digital e com dispositivos móveis cada vez mais inteligentes, que estão a gerar novos modelos de consumo, novos tipos de emprego, novas formas de viver, também nos processos se terá de mudar e de inovar. Aqui, a nuvem terá um papel fundamental, porque a confirmar isto está o facto de 50% dos CIO esperam operar em 2015 através da nuvem, com soluções cada vez mais móveis, que permitam a ligação entre pessoas e máquinas, com soluções e aplicações "*anywhere, anytime*", processos de negócio mais inteligentes, novas plataformas e uma experiência diferenciadora.

Destacando que "*a cloud* está a criar uma nova forma de ver a internet das coisas e a *internet of everything*", o autor cita as previsões de que o tráfego global de *datacenters* quadruple entre 2011 e 2016, sendo este crescimento praticamente todo gerado pelas soluções na nuvem. Este será aliás o grande driver para a criação de uma verdadeira plataforma de *cloud end-to-end*.

As economias precisam de ganhar dinâmica, as empresas precisam de otimizar e mudar modelos de negócio, criando novos produtos inovadores o mais rápido possível, e as soluções na nuvem parecem ser o caminho natural do desenvolvimento.

A universidade teve a capacidade de transformar parte dos seus serviços que tinha disponível aos colaboradores e alunos, mas pode aproveitar ainda mais as vantagens dos serviços da nuvem, neste caso com relevância para as tecnologias Microsoft presentes na solução Office 365.

Este trabalho pretendeu dar maior conhecimento sobre a computação em nuvem, e em especial do Exchange Online, e do modo como se pode adaptar a vários tipos de negócio, especialmente para o ambiente da Universidade Atlântica.

5.1. Limitações

A implementação de um ambiente híbrido de Exchange passa por cumprir todos os pré-requisitos descritos pela Microsoft e varia consoante o número de utilizadores, versão do Exchange Server e principalmente pelos serviços que se pretendem utilizar.

A realização de um projecto demonstrativo de um ambiente híbrido traria custos financeiros bastante acrescidos e por esse motivo não foi equacionado para a realização deste trabalho final de curso.

Para compensar estas limitações neste documento foi realizada uma descrição abrangente das tecnologias de computação em nuvem, dos serviços na oferta do Office 365 com especial atenção para o Exchange Online, bem como o estado da arte das mesmas, e foi realizado um estudo de caso sobre a migração do serviço de correio electrónico da Universidade Atlântica.

5.2. Trabalho Futuro

Dado que os serviços do Office 365 podem potenciar uma melhor experiência de utilização, capacidade de comunicação e interacção de todos os intervenientes na Universidade Atlântica, seria de todo recomendado apostar na divulgação destes serviços, quer na disponibilização e adopção dos mesmos em projectos bem definidos e adaptados à universidade, quer seja apenas para os colaboradores da UATLA ou também para os alunos.

Todas as possíveis melhorias apresentadas no estudo de caso poderão cumprir os objectivos de divulgação, disponibilização e adopção anteriormente referidos.

Provavelmente seria muito interessante contar com a ajuda dos alunos das licenciaturas de STI e GSC para conceber em conjunto com o Centro de Informática alguns dos projectos de implementação das melhorias propostas no estudo de caso.

Bibliografia

- APDC, 2013. *Cloud Computing: " Futurologia ou inevitabilidade?"*. Lisboa, s.n.
- Armbrust, M. et al., 2009. *Above the Clouds: A Berkeley View of Cloud Computing*, Berkeley: IEEE.
- Bhargava, S. & Samant, R. M., 2013. Alert Areas of Cloud Security. (*IJCSIT*) *International Journal of Computer Science and Information Technologies*, pp. Vol. 4 (1) , 2.
- Buyya, R. et al., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*.
- Castro, R. d. C. C. d. & Sousa, V. L. P. d., s.d. *Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança*, Ceará: Universidade Estadual do Ceará (UECE) - Centro de Ciência e Tecnologia (CCT).
- Erickson, J. et al., 2009. *Content-centered collaboration spaces in the cloud*, s.l.: HP Laboratories.
- Foster, I., Zhao, Y., Raicu, I. & Lu, S., 2008. Cloud Computing and Grid Computing 360-Degree Compared.
- Hill, Z. et al., 2010. *Early Observations on the Performance of Windows Azure*. Chicago, Department of Computer Science - University of Virginia.
- Kaplan, j., Rezek, C. & Sprague, K., s.d. *Protecting information in the cloud*, s.l.: Mckinsey&Company.
- Marcon, A., Laureano, M., Santin, A. & Maziero, C., s.d. *Aspectos de segurança e privacidade em ambientes de Computação em Nuvem*, s.l.: Instituto Federal de Educação, Ciência e Tecnologia do Paraná.
- MatrixForce Corporation, 2012. *Office 365 Justification White Paper*, Tulsa: s.n.
- Mell, P. & Grance, T., 2009. *The NIST Definition of Cloud Computing*. s.l., s.n., pp. 1-2.
- Melo, C. A. et al., s.d. *Software como Serviço: Um Modelo de Negócio Emergente*, s.l.: Centro de Informática – Universidade Federal de Pernambuco (UFPE).
- Microsoft, 2013. *Exchange Server 2010*. [Online]
Available at: [http://technet.microsoft.com/en-us/library/bb124558\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us/library/bb124558(v=exchg.141).aspx)
[Acedido em Maio 2014].

Microsoft, 2013. *Microsoft - Empresas e Negócios*. [Online]
Available at: <http://www.microsoft.com/business/pt-pt/PME-Hoje/Paginas/article.aspx?cbcid=141>

Microsoft, 2013. *Office 365 deployment guide*. [Online]
Available at: <http://technet.microsoft.com/en-us/library/hh852466.aspx>
[Acedido em Abril 2014].

Microsoft, 2013. *Why use Windows PowerShell to manage Office 365?*. [Online]
Available at: <http://technet.microsoft.com/en-us/library/dn567998.aspx>
[Acedido em Abril 2014].

Microsoft, 2013. *Windows Azure Pack for Windows Server*, s.l.: s.n.

Microsoft, 2014. *Exchange Server 2013 Hybrid Deployments*. [Online]
Available at: [http://technet.microsoft.com/en-us/Library/jj200581\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/Library/jj200581(v=exchg.150).aspx)
[Acedido em Abril 2014].

Microsoft, 2014. *Lync Server 2013 hybrid*. [Online]
Available at: <http://technet.microsoft.com/en-us/library/jj204805.aspx>
[Acedido em Junho 2014].

Microsoft, 2014. *Mailbox Migration to Exchange Online*. [Online]
Available at: [http://technet.microsoft.com/en-us/library/jj863291\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/jj863291(v=exchg.150).aspx)
[Acedido em 13 Abril 2014].

Microsoft, 2014. *Microsoft Exchange Conference*. Austin, Microsoft.

Microsoft, 2014. *Office 365 Service Descriptions*. [Online]
Available at: <http://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx>
[Acedido em Abril 2014].

Milne, R., 2014. *250 Hello*. [Online]
Available at: <http://blogs.technet.com/b/rmilne/archive/2014/02/25/exchange-2013-sp1-released.aspx>
[Acedido em Junho 2014].

Roberts, R. & Sikes, J., 2011. *Mckinsey on Business Technology*. [Online]
Available at:
http://www.mckinsey.com/client-service/bto/pointofview/pdf/MoBT22_BTO_Survey_vF.pdf

Ryan, M. D., s.d. Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM*, Vol. 54 No. 1, pp. 36-38.

Sawant, S. S. & Kalubarme, S. S., 2013. A3 (Authenticate Auditor & Avail) for Preserving Integrity of Data in Cloud Computing. *International Journal of Advanced Computer Research*, pp. 2277-7970.

Silva, A. L. J. M. d., 2012. *Cloud Computing Segurança e Privacidade da Informação na Nuvem*. s.l., IESF – Instituto Superior de Estudos Financeiros e Fiscais.

Singh, V. & Pandey, S. K., 2013. Revisiting Cloud Security Issues and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, pp. Volume 3, Issue 7, 869-875.

Smith, R., 2013. *The Exchange Team Blog*. [Online]
Available at: <http://blogs.technet.com/b/exchange/archive/2013/01/23/exchange-2013-server-role-architecture.aspx>
[Acedido em Junho 2014].