Instituto Politécnico da Maia

Provas Públicas para atribuição do Título de Especialista

IDEALIZAÇÃO, DESENHO E IMPLEMENTAÇÃO DE INFRAESTRUTURA DE REDE INFORMÁTICA NO AGRUPAMENTO DE ESCOLAS MADEIRA TORRES

Pedro Fernando Morais Martins Crispim

ISTEC

2022

Instituto Politécnico da Maia

Provas Públicas para atribuição do Título de Especialista

CNAEF 481 - Ciências Informáticas

Portaria n.º 256/2005, de 16 de março

IDEALIZAÇÃO, DESENHO E IMPLEMENTAÇÃO DE INFRAESTRUTURA DE REDE INFORMÁTICA NO AGRUPAMENTO DE ESCOLAS MADEIRA TORRES

Pedro Fernando Morais Martins Crispim

ISTEC

2022

DEDICATÓRIA

À minha mulher e filhos

A minha alegria e gozo, a maior bênção de Deus,

para os quais todo o esforço e empenho vale a pena.

PREFÁCIO SOBRE O AUTOR

Pedro Fernando Morais Martins Crispim nasceu em Torres Vedras, em 1970, onde frequentou todo o ensino básico e secundário, com exceção dos 8.º e 9.º anos, que foram realizados na EB23 de Freiria. Licenciou-se em Engenharia de Informática, em 1997 (parte curricular em 1996), na COCITE – Cooperativa de Ensino Superior de Técnicas Avançadas de Gestão e Informática (posteriormente designada por ISIG – Instituto Superior de Informática e Gestão, respeitando a nova legislação do Ensino Superior Particular e Cooperativo).

Tendo sido o melhor aluno do curso, cedo foi alvo de várias ofertas de trabalho, mesmo antes de terminar o mesmo. Contudo, como lecionava em part-time no ensino público para pagar os estudos (o que o fez em 1994-1995 e 1995-1996), decidiu terminar o curso e só depois analisar essas ofertas. Uma dessas propostas veio do cônjuge de uma professora da instituição de ensino superior, que lhe apresentou um projeto muito apelativo, uma vez que, nessa altura, se começava a falar dos Planos Diretores Municipais (PDM) e da sua digitalização, bem como da necessidade de catalogação de várias topologias de terrenos, edifícios, estruturas, utilizando Sistemas de Informação Geográfica (PTE

Plano Tecnológico da Educação

RDN *Relative Distinguished Name*

RFC *Request For Comments*

RID *Relative ID Master*

SAM *Security Accounts Manager*

SID *Security Identifier*

SIG).

Como sempre teve gosto por obter novos conhecimentos e de novos desafios, considerou que tal oferta poderia alargar o leque de conhecimentos e desenvolver o currículo, pelo que aceitou essa oferta (por parte da AmbiSIG, Lda.) iniciando o seu percurso nesta empresa assim que terminou o curso. Durante alguns meses, desempenhou o papel de responsável de produto (ArcView), e foi formador do pessoal técnico e apoio na implementação dos Sistemas de Informação Geográfica (PTE

Plano Tecnológico da Educação

RDN *Relative Distinguished Name*

RFC *Request For Comments*

RID *Relative ID Master*

SAM *Security Accounts Manager*

SID *Security Identifier*

SIG) em vários serviços da Câmara Municipal de Lisboa, tendo também participado na correção e adaptação da cartografia existente no Departamento de Desporto da CML, para efeitos de cadastro das infraestruturas desportivas por meio de um PTE Plano Tecnológico da Educação

RDN *Relative Distinguished Name*

RFC *Request For Comments*

RID *Relative ID Master*

SAM *Security Accounts Manager*

SID *Security Identifier*

SIG. Ainda nesta empresa, fez parte da equipa que efetuou a correção cartográfica dos PDM de Abrantes, Figueiró-dos-Vinhos, Tomar e Vila-de-Rei, ao abrigo do programa PROSIG. Esteve nesta empresa até fevereiro de 1997.

Obteve a certificação de *Microsoft Certified Professional* em junho de 1997 e a de *Microsoft Certified Systems Engineer* em setembro do mesmo ano.

Entretanto, através de um familiar, recebeu um convite para ir para Angola implementar a primeira rede wireless nesse país, no edifício da ENDIAMA, situado na Rua Major Kanhangulo nº 100, em Luanda, em regime de outsourcing, através de uma empresa angolana de consultoria informática, designada EMOSIST. Novamente a vontade de explorar novas valências e novos desafios, levou-o a aceitar o convite, tendo iniciado funções nesta empresa em março de 1997. Desempenhou, posteriormente, funções como administrador de redes Microsoft na ENDIAMA, em Luanda, até abril de 1998, em regime de *outsourcing*. Nesta instituição, implementou ainda uma Intranet e realizou um estudo de organização e de planeamento do Gabinete de Organização e Informática. Por motivos de saúde, regressou a Portugal, não mais regressando a Angola.

Após recuperar, começou a dar apoio a uma empresa de um amigo (COSASI, Lda.), em Torres Vedras, em regime de voluntariado até julho do mesmo ano. Lecionou durante mais um ano (ano letivo 1998-1999), acabando por ser convidado pelos responsáveis da COSASI, por terem gostado do trabalho anteriormente aí desenvolvido. Começou a desempenhar funções em setembro de 1999, como diretor de informática, sendo o responsável técnico de desenvolvimento de um sistema de quiosques multimédia (mupis) para implementar em diversos municípios (razão que tinha levado à sua contratação). Um ano depois, devido a problemas financeiros nesta empresa, motivados pela fraca comercialização do projeto, decidiu não continuar a sobrecarregar a folha salarial desta e, uma vez que a parte técnica do projeto se encontrava praticamente concluída, ofereceu-se para deixar a mesma (sem quaisquer compensações financeiras), o que foi aceite pelos responsáveis da mesma.

Tendo anteriormente experimentado e ficado apaixonado com o ensino, mais concretamente o ensino secundário público, decidiu enveredar definitivamente por esta carreira, tendo concorrido e sido colocado na Escola Secundária com 3.º Ciclo de Madeira Torres, em setembro de 2000.

Como detinha habilitações próprias, mas não suficientes para lecionar (faltavam as designadas "disciplinas pedagógicas"), assim que terminou 5 anos de ensino, conforme estipulado por lei, candidatou-se à profissionalização em serviço, a qual terminou em agosto de 2003, concedendo-lhe uma classificação profissional de 16,5 valores, pelo que passou a possuir habilitação própria e suficiente para o ensino. Ficou como efetivo nessa escola, no ano letivo 2003/2004, onde sempre lecionou e continua a lecionar até ao presente.

Nesta instituição de ensino, quer ainda como Escola Secundária com 3.º Ciclo de Madeira Torres - ESMT, quer depois como Agrupamento de Escolas Madeira Torres (junho de 2011), sempre foi responsável por todos os projetos tecnológicos (diretor de instalações de informática entre 2003 e 2007, coordenador TIC entre 2006 e 2009, responsável pela componente técnica da Equipa PTE entre 2009 e 2013, coordenador de projetos entre 2013 e 2015, responsável pelo Plano TIC desde 2015 até ao momento e membro da Equipa de Transição Digital, onde é responsável pela área de ação Tecnológica e Digital), fazendo a gestão de toda a rede e parque informático da mesma, coordenação de projetos na área das TIC, coordenando a parte tecnológica do Plano de Transição Digital, bem como das plataformas de apoio ao ensino (Moodle, Google Apps, Office 365). Devido ao confinamento em resultado da pandemia (COVID-19), em 2020 implementou toda a plataforma de e-learning, que implicou a migração da plataforma Google Apps para o Office 365 para Educação, de forma a unificar o ensino à distância em torno do Microsoft Teams.

Paralelamente, e até 2011, desempenhou também funções de formador em vários Centros de Formação de Escolas (inclusivamente nos Açores), hospitais, associações, com centenas de horas de formação dada a professores (é formador com Certificado de Aptidão Profissional n.º EDF 13174/99 DL para exercer a profissão de FORMADOR e também reconhecido pelo Conselho Científico-Pedagógico da Formação Contínua de Professores com o registo n.º CCPFC/RFO-06582/98).

É sócio-gerente de uma empresa (Cacto Digital Unipessoal Lda) desde 2012, onde desenvolveu trabalhos variados de consultoria informática, auditoria e segurança informática e gestão de sistemas informáticos, bem como de gestão e atualização de plataformas de e-learning (tendo sido um cliente de referência o Instituto Camões, até este ser englobado no sistema central de gestão dos ministérios portugueses).

Além do que atrás foi apresentado, também realizou, a título pessoal (em regime de voluntariado) consultoria informática a várias instituições e organizações (escolas e igrejas).

Fez diversas formações, em várias áreas: Dreamweaver/Fireworks/Flash; Internet; *Microsoft Office User Specialist* – Excel; Imagem digital; Plataformas de Ensino à Distância; Windows 2003 e ISA Server 2004; Coordenação, Animação e Dinamização de Projetos TIC nas Escolas; Azure (MOC M20533) + Azure AZ-900; Segurança Digital; Políticas e Orientações das TI e SI nas escolas; programação (Java), Microsoft Visio, entre outras.

Em 2020 obteve o título *Microsoft Certified: Azure Fundamentals*.

Fruto de uma destas ações de formação e do trabalho nela desenvolvido, foi convidado pelo Presidente do Conselho Técnico-Científico do ISTEC (Instituto Superior de Tecnologias Avançadas), Prof. Pedro Brandão, para desenhar, em conjunto com este, os conteúdos curriculares de algumas cadeiras do curso de Pós-Graduação em Virtualização e *Cloud-Computing*. Leciona nesse curso desde 2014 e até ao presente.

Fruto da aceitação desta Pós-Graduação, e dando continuidade a este projeto, o ISTEC lançou o Mestrado em Informática, no ano letivo de 2019-2020, tendo dois ramos: Computação em Nuvem; e Dispositivos Móveis e Multimédia. Leciona no Mestrado, no ramo de Computação em Nuvem, desde o início deste também.

Endereço de correio eletrónico: pcrispim@gmail.com.

RESUMO

Este documento contextualiza e apresenta um trabalho profissional idealizado, desenhado, concebido, desenvolvido, implementado, liderado e gerido pelo autor, de criação e implementação de uma rede informática (hardware, software, serviços, utilizadores, instalações, manutenções, etc.), incluindo a sua gestão e manutenção, numa instituição de ensino público (a partir de 2003, inicialmente apenas na Escola Secundária com 3.º Ciclo de Madeira Torres - ESMT, e a partir do ano letivo 2012-2013, no então criado Agrupamento de Escolas de Torres Vedras).

Tendo em conta os seus conhecimentos de organização de instituições a nível de sistemas de informação, bem como aos seus conhecimentos práticos sobre redes, em especial redes Microsoft, desde que iniciou funções como professor de informática na Escola Secundária com 3.º Ciclo de Torres Vedras, começou a configurar os poucos computadores que existiam em pequenas redes de área local (tudo fora das horas de trabalho, em regime de voluntariado). Ao implementar um pequeno sistema de redes locais com acesso à Internet nas salas de informática existentes (a partir de recursos que tinham sido colocados na escola através de projetos como o MINERVA, Nónio-Século XXI, uARTE – Internet na Escola, entre outros, mas que não tiveram continuidade por não haver ninguém que efetivamente tivesse capacidade para os desenvolver), apresentou-a como prova de conceito aos órgãos de direção, sendo o seu trabalho reconhecido. A partir desse instante, iniciou um conjunto de sugestões de aumento de produtividade, através do desenvolvimento dos sistemas de informação da escola, como fator de melhoria significativa dos métodos de trabalho e do processamento efetivo de dados como forma de apoio à decisão. Apesar de ser reconhecido o valor dos mesmos, as limitações orçamentais nunca possibilitaram o seu desenvolvimento.

Coincidente com o ter passado a exercer funções na escola como Professor do Quadro de Nomeação Definitiva, em 2003, foi lançado em 2004 o programa “1000 Salas TIC”, que “visou apoiar escolas dos ensinos básico e secundário no lançamento do ensino obrigatório das TIC nos 9.º e 10.º anos escolares”. Deste programa resultou o equipar as escolas com equipamento informático que possibilitaram a implementação de laboratórios de informática onde essa disciplina pudesse ser lecionada. No caso do AEMT, foram implementados 2 laboratórios de informática. Foi então a partir daí que começou a ter funções de coordenação técnica na escola (como Diretor de Instalações de Informática, entre os anos letivos 2003/2004 e 2006/2007), para além da atividade letiva, onde então pode idealizar, desenhar, conceber, desenvolver, implementar, gerir e liderar todo o processo, ao longo dos últimos anos, resultando naquilo que é uma das três maiores redes informáticas do ensino público, em Portugal.

O processo desenvolveu-se em 3 grandes fases:

1. Utilização do programa "1000 salas TIC" para iniciar o processo de gestão centralizada de utilizadores (*Active Directory*), implementar um LMS (*Learning Management System*), e um serviço de gestão de acesso de alunos e aquisições no bar através de um sistema de cartões (para todo o corpo docente e discente).
2. Utilização do "Plano Tecnológico para a Educação" (PTE), para iniciar o processo de virtualização de servidores, criação de novos serviços (implementação de sumários digitais), acesso à rede através de um servidor RADIUS, disponibilização de acesso à Internet por cabo em todas as salas, disponibilização de Internet por Wi-Fi em toda a escola (a toda a comunidade escolar), implementação de endereços de correio eletrónico para todos os professores e assistentes operacionais e técnicos, melhoria dos laboratórios de informática (equipamentos mais potentes, com capacidade de virtualização local), sistema de reposição de imagens do sistema operativo e aplicações para todos os computadores, aumento do tamanho da rede (passagem para Agrupamento de Escolas), aumento da resiliências dos sistemas (backups e redundância de equipamentos) bem como a proteção física do *datacenter*.
3. Início do processo de replicação entre servidores virtualizados – processo que foi interrompido devido a necessidades mais urgentes que nasceram a partir dos confinamentos por causa da COVID-19. Implementação de sistema de autenticação de utilizadores com nome de utilizador e password únicos nas várias plataformas). Migração do *Google Apps for Education* para Office 365 (email passou do GMail para o Outlook 365), em virtude da adoção do Microsoft Teams como plataforma de e-learning do Agrupamento de Escolas. Aumento da segurança dos utilizadores, com implementação de *Multi-Factor Authentication* (MFA).

São os pontos 2 e 3 que constituem, primariamente, o trabalho desenvolvido nos últimos anos, e que é apresentado pelo autor, não deixando, contudo, de ser apresentado o primeiro ponto, para efeitos de contextualização do projeto.

Assim, nos capítulos 1 e 2 são apresentados os projetos que permitiram equipar a escola, e nos capítulos seguintes, já sem a componente cronológica, é apresentado o processo técnico que levou à implementação do projeto (ou seja, o planeamento e execução do trabalho em si).

Palavras-chave

Active Directory, AEMT, computadores, correio eletrónico, *datacenter*, e-learning, escolas, ESMT, Fogproject, Google apps, Internet, Linux, LMS, MFA, Moodle, Office 365, POS, RADIUS, redes

informáticas, redundância, replicação, segurança, servidores, Teams, virtualização, VLAN, VoIP, Windows

ABSTRACT

This document contextualizes and presents a professional work conceived, designed, developed, implemented, led and managed by the author, of the Implementation of a management and maintenance system for a computer network (hardware, software, services, users, facilities, maintenance, etc.), in a public educational institution (from 2003, initially only in the *Escola Secundária com 3.º Ciclo de Madeira Torres - ESMT*, and beginning in the school year 2012-2013, in the then created *Agrupamento de Escolas de Torres Vedras*, a cluster of schools).

Considering his knowledge of organization of institutions in terms of information systems, as well as his practical knowledge of networks, especially Microsoft networks, since he started working as a computer teacher at *Escola Secundária com 3.º Ciclo de Torres Vedras*, he began to configure the few computers that existed on small local area networks (all outside working hours, on a voluntary basis). By implementing a small system of local networks with Internet access in the existing computer rooms (from resources that had been placed in the school through projects such as *MINERVA*, *Nónio-Século XXI*, *uARTE* – Internet at School, among others, but that did not continue because there was no one who effectively had the capacity to develop them), presented it as a proof of concept to the management bodies, and their work was recognized. From that moment on, he started a set of suggestions to increase productivity, through the development of the school's information systems, as a factor of significant improvement in working methods and in the effective processing of data as a form of decision support. Despite the recognition of their value, budgetary limitations never made their development possible.

Coinciding with having started to work at the school as a member of the schoolteachers, in 2003, the "1000 ICT Rooms" program was launched, in 2004, which "aimed to support elementary and secondary schools in the launch of compulsory ICT education in the 9th and 10th school years". This program resulted in equipping schools with computer equipment that enabled the implementation of computer labs where this subject could be taught. In the case of AEMT, 2 computer labs were implemented. It was then from there that he began to have technical coordination roles at the school (as Director of Computer Facilities, between the academic years 2003/2004 and 2006/2007), in addition to teaching activities, where he could then idealize, design, conceive, develop, implement, manage and lead the entire process over the last few years, resulting in what is one of the three largest public education computer networks in Portugal.

This process was developed in 3 major phases:

1. Use of the "1000 ICT classrooms" program to start the process of centralized user management (Active Directory), implement an LMS (Learning Management System), and a

service for managing student access and purchases at the bar through a card system (for all faculty and students).

2. Use of the "Technological Plan for Education" (PTE), to start the process of server virtualization, creation of new services (implementation of digital summaries), access to the network through a RADIUS server, provision of Internet access via cable in all classrooms, provision of Internet via Wi-Fi throughout the school (to the entire school community), implementation of e-mail addresses for all teachers and operational and technical assistants, improvement of computer labs (more powerful equipment , with local virtualization capability), a system for replacing images of the operating system and applications for all computers, increasing the size of the network (changed to a Cluster of Schools), increasing the resilience of the systems (backups and equipment redundancy) and also the datacenter physical protection.
3. Start of replication process between virtualized servers – process that was interrupted due to more urgent needs that were born from the confinements because of COVID-19. Implementation of a user authentication system with a unique username and password on the various platforms). Migration from Google Apps for Education to Office 365 (email moved from GMail to Outlook 365), due to the adoption of Microsoft Teams as the School Group's eLearning platform. Increased user security, with implementation of Multi-Factor Authentication (MFA).

It is points 2 and 3 that constitute, primarily, the work developed in recent years, and which is presented by the author, although the first point is also presented, for the purposes of contextualizing the project.

Thus, in chapters 1 and 2 the projects that allowed equipping the school are presented, and in the following chapters, without the chronological part, the technical process that led to the implementation of the project is presented (that is, the planning and execution of the work in yes).

Keywords

Active Directory, AEMT, computers, email, datacenter, eLearning, schools, ESMT, Fogproject, Google apps, Internet, Linux, LMS, MFA, Moodle, Office 365, POS, RADIUS, computer networks, redundancy, replication, security, servers, Teams, virtualization, VLAN, VoIP, Windows.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS E SÍMBOLOS

ACL	*Access Control Lists*
AD	*Active Directory*
AD DS	*Active Directory Domain Services*
AEMT	Agrupamento de Escolas Madeira Torres
AEPFS	Agrupamento de Escolas Padre Francisco Soares
BECRE	Biblioteca Escolar / Centro de Recursos Educativos
BRI	Basic Rate Interface (configuração ISDN para linhas telefónicas de subscrição)
CEE	Comunidade Económica Europeia
CFETVL	Centro de Formação de Associação de Escolas de Torres Vedras
CN	*Common Name*
DAP	*Directory Access Protocol*
DC	*Domain Controller* (computador da *Active Directory* que tem funções de controlador de domínio)
DDoS	*Distributed Denial-of-Service* (ataque distribuído de negação de serviço)
DGE	Direção-Geral da Educação
DGEEC	Direção-Geral de Estatísticas da Educação e Ciência do Ministério da Educação e Ciência (agrega os extintos GEPE e GPEARI)
DIT	*Directory Information Tree*
DN	*Distinguished Name*
DNS	*Domain Name System*
EBPFS	Escola Básica Padre Francisco Soares
EB1	Escola Básica do 1.º Ciclo
EMAIL	Correio eletrónico
EMOSIST	EMOSIST – Consultoria, Organização, Informática, Lda
ENDIAMA	Empresa Nacional de Diamantes de Angola, E.P.
ESMT	Escola Secundária com 3.º Ciclo de Madeira Torres
FQDN	*Fully Qualified Domain Name*
FSMO	*Flexible Single-Master Operations*
GC	*Global Catalog*
GEPE	Gabinete de Estatísticas e Planeamento da Educação
GPEARI	Gabinete de Planeamento, Estratégia, Avaliação e Relações Internacionais do Ministério da Ciência, Tecnologia e Ensino Superior

GPO	*Group Policy Object* (objeto de políticas de grupo)
GUID	*Globally Unique Identifier*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol* (protocolo de comunicação para encaminhamento de dados que funciona na camada 3 do modelo OSI, a camada de rede)
ISDN	*Integrated Services Digital Network* (Rede Digital com Integração de Serviços – conjunto de padrões de comunicação para transmissão simultânea de voz, vídeo, dados e outros serviços sobre linhas telefónicas comutadas).
ISO	*International Organization for Standardization* (Organização Internacional de Normalização)
JI	Jardim de Infância
LAMP	Linux, Apache, MySQL/MariaDB, PHP/Perl/Python
LAN	*Local Area Network* (Rede de Área Local)
LDAP	Lightweight Directory Access Protocol (protocolo da camada de aplicação do modelo OSI que permite aceder e manter serviços de informação de diretório através de uma rede IP)
LMS	*Learning Management System* (Sistema de Gestão de Aprendizagens)
MAC	*Medium Access Control* (protocolo de controlo de acesso ao meio, que constitui uma subcamada da camada 2 do modelo OSI, onde se define o endereço físico, também designado por endereço MAC, que permite a comunicação entre sistemas diretamente ligados)
MFA	*Multi-Factor Authentication* (autenticação em dois passos)
MINERVA	Meios Informáticos no Ensino Racionalização Valorização Actualização
MOODLE	*Modular Object-Oriented Dynamic Learning Environment* (LMS em código aberto para trabalho colaborativo, que utiliza a filosofia denominada de "pedagogia sócio construtivista")
MOPT	Ministério das Obras Públicas e Transportes
NDS	*Novell Directory Services*
NIC	*Network Interface Card* (adaptadores de rede)
NOS	*Network Operating System*
NSO	Núcleo de Suporte a *Outsourcing*
OS	*Operating System* (em português, SO)
OSI	*Open System Interconnection*
OU	*Organizational Unit*
PDM	Plano Diretor Municipal

POS	*Point of sale* ou *Point of Service*
PROSIG	Programa de Apoio à Criação de Nós Locais do Sistema Nacional de Informação Geográfica
PTE	Plano Tecnológico da Educação
RDN	*Relative Distinguished Name*
RFC	*Request For Comments*
RID	*Relative ID Master*
SAM	*Security Accounts Manager*
SID	*Security Identifier*
SIG	Sistemas de Informação Geográfica
SO	Sistema Operativo
TCP	*Transmission Control Protocol* (protocolo de controlo de transmissão que funciona na camada 4 do modelo OSI, a camada de transporte)
TIC	Tecnologias da Informação e Comunicação
UE	União Europeia
UNC	*Uniform Naming Convention*
UPN	*User Principal Name* ou *Universal Principal Name*
VLAN	*Virtual Local Area Network* (Rede de Área Local Virtual)
VoIP	*Voice over IP* (sistema de telefonia baseado no protocolo IP)
WSUS	*Windows Server Update Services*
X.500	Padrão de diretório (última versão definido pela norma ISO/IEC 9594-1:2020)

1. SITUAÇÃO INICIAL

Até ao início do programa "1000 Salas TIC", em 2004, diversas iniciativas e projetos foram desenvolvidos em Portugal, que visavam a adoção de sistemas informáticos e tecnologias digitais no sistema de ensino português. Estas tiveram início com a adesão de Portugal à União Europeia (então designada por Comunidade Económica Europeia, ou **Erro! A origem da referência não foi e ncontrada.**), da qual se tornou membro, formalmente, em 1 de janeiro de 1986 (Porto Editora, s.d.)[1].

A utilização pedagógica do computador era algo que vinha a ser ensaiado em Portugal desde o início dos anos 80 do século XX, através de vários programas e projetos criados pelo Ministério da Educação (Patrocínio, 2001)[2].

Foi entre 1985 e 1994 que decorreu o projeto MINERVA, a primeira iniciativa com financiamento por parte do Ministério da Educação, para se caminhar em direção a esse propósito (Rapp, 2017)[3]. De acordo com Patrocínio:

> *"O Projecto MINERVA foi muito mobilizador dos docentes e dos alunos, tendo também proporcionado uma notável interacção, uma parceria única, com uma dimensão nacional (de ampla cobertura geográfica incluindo o norte e o sul, o interior e o litoral) de contornos interessantes, entre o ensino superior e os ensinos básico e secundário. Permitiu o desenvolvimento de investigação e desenvolvimento em Educação raramente identificável em projectos ou programas de natureza institucional como foi relevado na avaliação desse projecto efectuada sob os auspícios da OCDE"* (Patrocínio, 2001)[4]"

No entanto, tanto Patrocínio como Rapp apresentam nos seus trabalhos que um dos principais objetivos deste projeto era o apetrechamento informático das escolas (Patrocínio, 2001) (Rapp, 2017).

Foi então desse projeto que surgiram os primeiros computadores na ESMT e onde primeiro tomei contacto com estes no ano de 1993, quando aí lecionei pela primeira vez (miniconcurso), ainda sem habilitações próprias e suficientes.

---

[1] Porto Editora – Adesão de Portugal à CEE na Infopédia [em linha]. Porto: Porto Editora. [consult. 2021-09-30]. Disponível em https://www.infopedia.pt/$adesao-de-portugal-a-cee

[2] Patrocínio, J. T. (2001). Tecnologia, educação e cidadania: (re)pensar projectos educacionais numa abordagem compreensiva da contemporaneidade. Dissertação de mestrado em Ciências da Educação: área de Educação e Desenvolvimento. Universidade Nova de Lisboa: Faculdade de Ciências e Tecnologia. Obtido em 30 de 09 de 2021, de http://hdl.handle.net/10362/281, p. 159

[3] Rapp, M. L. (2017). Integração das TIC nos processos de ensino e aprendizagem pelos professores do 1° e 2° Ciclo de uma escola portuguesa. Universidade Nova de Lisboa: Faculdade de Ciências e Tecnologia. Obtido em 30 de setembro de 2021, de http://hdl.handle.net/10362/54377, p.28

[4] Patrocínio, J. T. (2001). Tecnologia, educação e cidadania: (re)pensar projectos educacionais numa abordagem compreensiva da contemporaneidade. Dissertação de mestrado em Ciências da Educação: área de Educação e Desenvolvimento. Universidade Nova de Lisboa: Faculdade de Ciências e Tecnologia. Obtido em 30 de 09 de 2021, de http://hdl.handle.net/10362/281, p. 159

Vários programas se seguiram, virados para o apetrechamento e a capacitação de docentes e alunos, no uso das Tecnologias de Informação e Comunicação, para, conforme o ministro que tutelava o então designado Ministério da Ciência e Tecnologia, Mariano Gago, escreveu no preâmbulo do "Livro Verde para a Sociedade da Informação em Portugal", "À cabeça deste Livro Verde colocámos, como não podia deixar de ser, a questão decisiva da democraticidade e o combate à exclusão"[5]. Ainda neste livro, reforça-se a importância da existência de equipamentos informáticos nas escolas, para que efetivamente pudesse existir uma "generalização da utilização dos computadores e no acesso às redes electrónicas de informação pelos alunos de todos os graus de ensino" (idem)[6].

Tabela 1.1 - Principais projetos, programas e iniciativas educativas tecnológicas em Portugal – baseado em (Rapp, 2017) que adaptou de (Pereira & Pereira, 2011)

Designação	**Período**	**Entidade Responsável**
Projecto Minerva	1985-1994	Ministério da Educação (GEP e DEPGEF)
Programa Nónio-Século XXI	1996-2002	Ministério da Educação
uARTE- Internet na Escolas	1997-2002	Ministério da Ciência e Tecnologia
Programa Internet@EB1	2002-2005	Ministério da Ciência e Tecnologia; Escolas Superiores de Educação; FCCN
Projeto "1000 Salas TIC"	2004-2005	Ministério da Educação
Implementação da disciplina de TIC nos 9.º e 10.º anos de escolaridade	2004-2005	Ministério da Educação
Projeto EduTIC	2005	GIASE (Gabinete de Informação e Avaliação do Sistema educativo
"Equipa de Missão Computadores, Redes e Internet na escola – CRIE	2005-2007	Ministério da Educação
Criação das "Equipas TIC" e "Coordenador TIC"	2005	Ministério da Educação
Plano Tecnológico da Educação	2007-2011[7]	Ministério da Educação (GEPE)
Iniciativa e-Escolinha	2008-2011	Ministério das Obras Públicas, Transportes e Comunicações (MOPT)
Plano de Ação para a Transição Digital	2020-	Estrutura de Missão Portugal Digital
Plano de Ação para o Desenvolvimento Digital das Escolas (PADDE)	2021-	Ministério da Educação

Tabela 1.2 - Principais projetos, programas e iniciativas educativas tecnológicas em Portugal – baseado em (Rapp, 2017) que adaptou de (Pereira & Pereira, 2011)

[5] Portugal., Ministério da Ciência e da Tecnologia., Missão para a Sociedade da Informação. (1997). Livro Verde para a Sociedade da Informação em Portugal. Lisboa. Obtido em 30 de 09 de 2021, de https://dspace.uevora.pt/rdpc/bitstream/10174/12999/39/56ptlivroverdeparaasociedadedainformacaoemportugal.pdf

[6] Idem

[7] No ano de 2001 deu-se a queda do governo, ficando a continuidade deste plano sem concretização

Quando me decidi pela carreira de docente (continuando a exercer atividade profissional em regime de acumulação de funções), em setembro de 1999, rapidamente me envolvi ativamente na melhoria das condições de trabalho, em termos digitais, na ESMT, tendo como objetivo utilizar o melhor possível as tecnologias existentes, com base na experiência profissional que tinha até então adquirido.

Inicialmente, motivei os colegas do Departamento de Ensino da Informática e começamos a fazer ligações de rede entre as salas, para usufruirmos de ligação à Internet, entretanto colocada na escola no âmbito do programa "uARTE- Internet na Escolas".

Conseguimos também realçar a importância das infraestruturas tecnológicas, conseguindo que a direção da escola permitisse a atribuição de horas para a gestão do parque informático existente (disperso e sem gestão centralizada). Assim, a partir do ano letivo 2003-2004, desempenhei o cargo então designado "Director de Instalações de Informática".

No ano seguinte dá-se o primeiro grande salto tecnológico nas escolas desde que tinha chegado ao ensino, fruto do programa "1000 Salas TIC", resultante do "Plano de Acção para a Sociedade da Informação". É a partir desse ponto que, verdadeiramente, iniciei o trabalho de construção daquela que se viria a tornar uma das maiores redes de computadores das escolas secundárias de Portugal. É esse projeto de construção que pretendo apresentar, ao longo deste documento.

2. FASE 1 – "1000 SALAS TIC"

Este projeto teve origem numa parceria público-privada entre o Ministério de Educação, a Microsoft Portugal e a *Sun Microsystem*[8], tendo o seu lançamento ocorrido no ano letivo 2004/2005 (Lei n.º 55-A/2004, 2004, p. 111).

Esta iniciativa teve como fundamento criar salas (laboratórios de informática) que suportassem/apoiassem a disciplina de Tecnologias de Informação e Comunicação (TIC) que foi criada e inserida no currículo obrigatório do ensino público nesse mesmo ano letivo, e que abrangia os 9.º e 10.º anos de escolaridade.

Em termos de implementação, o projeto previa a instalação de 1220 laboratórios em 1072 escolas (tendo, efetivamente, sido instalados 1182 servidores[9]), e tinha como objetivo "criar e equipar laboratórios de informática", cada um composto pelo seguinte equipamento:

- Servidor (com Windows Server 2003)
- Computadores (com sistema dual-boot entre Windows XP e Alinex, uma versão de Linux criada pela Universidade de Évora, baseada na distribuição Linex, da Junta de Extremadura de Espanha, com quem estabeleceram um protocolo)
- Projetor
- Impressora
- 1 câmara digital (webcam)

Se este projeto teve a vantagem de trazer equipamentos para as escolas, até aí mal ou nada apetrechadas para se poder lecionar uma disciplina como TIC, não tinha, contudo, o objetivo de trazer uma gestão centralizada de utilizadores e segurança a nível de toda a escola.

Assim, cada sala foi desenhada para funcionar como uma "ilha", isolada do resto. Cada sala teria o seu próprio servidor com Windows Server 2003 e *Active Directory*, mas apontava, sobretudo, para a utilização de uma das "ferramentas mais inovadoras, concebida a pensar na sala de aula"[10], o "*Class Server*", da Microsoft.

No caso da Escola Secundária com 3.º Ciclo de Madeira Torres, onde existiam 2 salas, implicava ter a necessidade de contas duplicadas e a inexistência de acesso aos ficheiros e configurações entre as duas salas, mesmo a nível do "*Class Server*".

As escolas caminhavam no sentido de utilização do digital, mas ainda sem um caminho consolidado de gestão e utilização dos recursos, o que aumentava a carga administrativa associada.

---

[8] (Gomes, 2010, p. 46)
[9] (Teixeira, 2011, p. 64)
[10] (Lei n.º 55-A/2004, 2004, p. 111)

A aposta no "*Class Server*", apesar de interessante, veio a mostrar-se inadequada, quer porque estava incluída a utilização apenas por um ano, passando, a partir daí, a haver necessidade de pagamento de licenças (assente num modelo hoje muito em voga, a subscrição anual, por utilizador), quer porque a Microsoft veio mesmo a descontinuar este produto. Mais tarde, surgiria um produto destinado a alunos, o *Microsoft Student* 2007, que também seria descontinuado. Mas a aposta da Microsoft no mercado da educação não terminaria, surgindo ainda o *Microsoft Classroom*[11], parte do Office 365, mas que não chegaria a sair da versão "*preview*", sendo posteriormente integrado, em termos de tecnologia, no Microsoft Teams (mais propriamente na versão de educação, disponibilizada gratuitamente para todas as instituições de ensino), essa sim, uma tecnologia que ganhou o seu espaço, tendo a sua popularidade disparado com a Covid-19, tornando-se a aplicação empresarial da Microsoft com maior adoção na história desta empresa, que fez com que o seu CEO afirmasse que tinham visto dois anos de transformação digital a ocorrer no espaço de apenas 2 meses[12].

Claramente, este projeto das 1000 Salas TIC era ambicioso, tendo em conta a realidade do sistema educativo português no que respeita à utilização de meios digitais, mas poderia ter sido muito mais ambicioso, ficando por ser um projeto fechado para a disciplina de TIC e não para as comunidades escolares.

Um passo adicional e importante foi dado no ano seguinte, através do Despacho n.º 26 691/2005 (2.ª série), que atribuía às escolas/agrupamentos a responsabilidade da criação de uma estrutura de coordenação para as TIC, que incluía a nomeação de um coordenador (Coordenador TIC), o que no caso do Agrupamento de escolas Madeira Torres, por ser um agrupamento vertical com ensino secundário, permitia atribuir um crédito de 9 horas[13].

No ponto 2 do referido Despacho, estão descritas as funções do Coordenador TIC, nomeadamente:

> "*2—Sem prejuízo de outras funções, a definir em regulamento interno, o coordenador de TIC deve orientar a sua actividade no cumprimento das seguintes tarefas:*
>
> *a) Ao nível pedagógico:*
>
> *i) Elaborar no agrupamento/escola um plano de acção anual para as TIC (plano TIC). Este plano visa promover a integração da utilização das TIC nas actividades lectivas e não lectivas, rentabilizando os meios informáticos disponíveis e generalizando a sua utilização por todos os elementos da comunidade educativa. Este plano TIC deverá ser concebido no quadro do projecto educativo da escola e do respectivo plano anual de actividades, em*

[11] (Prophet, 2016) - https://blogs.microsoft.com/blog/2016/08/18/back-to-school-with-microsoft-student-focused-teacher-inspired-innovation-with-office-365-education/

[12] (Spataro, 2020) - https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

[13] (Gabinete do Secretário de Estado da Educação, 2005), p.17973, ponto 5, alínea c)

conjunto com os órgãos de administração e gestão, em articulação e com o apoio do centro de formação da área do agrupamento/escola (CFAE) e de outros parceiros a envolver;

ii) Colaborar no levantamento de necessidades de formação em TIC dos professores do agrupamento/escola;

iii) Identificar as suas necessidades de formação, disponibilizando-se para frequentar as acções de formação desenvolvidas;

iv) Elaborar, no final de cada ano lectivo, e em conjunto com os parceiros envolvidos, o balanço e a avaliação dos resultados obtidos, a apresentar aos órgãos de administração e gestão do agrupamento/escola e à respectiva direcção regional de educação;

b) Ao nível técnico:

i) Zelar pelo funcionamento dos computadores e das redes no agrupamento/escola, em especial das salas TIC;

ii) Usar o serviço do centro de apoio TIC às escolas (call center) de forma sistemática para os problemas de ordem técnica;

iii) Ser o interlocutor junto dos serviços centrais e regionais de educação para todas as questões relacionadas com os equipamentos, redes e conectividade, estando disponível para receber a formação necessária proposta por aqueles serviços;

iv) Articular com os técnicos das câmaras municipais que apoiam o 1.o ciclo do ensino básico, quando se trata de agrupamento de escolas;

v) Articular com as empresas que, eventualmente, prestem serviço de manutenção ao equipamento informático."[14]

Desse modo, após ter desempenhado funções como Diretor de Instalações de Informática, entre os anos letivos 2003/2004 e 2005/2006, fui eu nomeado Coordenador TIC do Agrupamento de Escolas Madeira Torres, papel que desempenhei nos anos letivos 2005/2006 (a partir de fevereiro de 2006, em que efetivamente fui nomeado para o cargo), 2006/2007, 2007/2008 e 2008/2009, sendo que em 2005/2006 e 2006/2007 ainda acumulei o cargo de Diretor de Instalações de Informática com o cargo de Coordenador TIC.

[14] Gabinete do Secretário de Estado da Educação (Ed.). (27 de 12 de 2005). Despacho n.º 26 691/2005 (2.ª série). DIÁRIO DA REPÚBLICA - II SÉRIE, p.17973-17974

Projetos desenvolvidos paralelamente ao projeto “1000 Salas TIC”

Sem prejuízo de apresentar o PROJETO, como um todo, a partir do capítulo 5, é importante resumir aquilo que foi feito como resultado deste projeto, em particular.

Com base no equipamento disponibilizado no âmbito do projeto “1000 Salas TIC”, pude desenvolver uma série de iniciativas que visavam a utilização de variados recursos tecnológicos, nomeadamente:

- Criação de um domínio (esmt.local) na *Active Directory*, utilizando os dois servidores existentes, com Windows Server 2003, como *Domain Controllers*.
- Configuração da rede local (física) para passar a ser uma única rede (em vez de ilhas isoladas), instalando calha técnica dupla, com separação de correntes forte e fracas, quer nos 5 laboratórios de informática, quer nos serviços administrativos e salas da direção.
- Adicionar todos os computadores existentes (93), em que havia ligação à rede local, ao domínio criado: inicialmente apenas os dos laboratórios de informática, da direção, dos serviços administrativos e também os postos POS que, numa primeira fase, utilizavam o sistema da MicroIO, mas que alteramos para o sistema da JPMAbreu (compatível com o software de gestão escolar utilizado no AEMT).
- Criação de contas de *Active Directory* para todos os professores, assistentes operacionais, assistentes técnicos, e alunos, para que o acesso aos computadores fosse feito através destas contas.
- Criação de contas de correio eletrónico institucionais para todos os professores e assistentes técnicos, utilizando o *Google apps for Education* (não integradas com AD).
- Instalação de um servidor Linux, onde foi configurado o Moodle (que necessitava de MySQL, Apache e PHP), para a escola poder utilizar um LMS.

Nos anos seguintes, esta estrutura não sofreu grandes alterações, e foi sendo feita uma manutenção apropriada ao tamanho da infraestrutura, que incluía a criação de novas contas a cada ano escolar, as manutenções e limpeza dos equipamentos informáticos, a instalação de aplicações e atualizações necessárias ao sistema operativo e a essas aplicações, atualizações dos servidores e da versão do LMS, entre outras. Foi assim, até ao ano letivo de 2007/2008, onde foi implementado o Plano Tecnológico para a Educação, que é apresentado de seguida.

3. FASE 2 – "PLANO TECNOLÓGICO PARA A EDUCAÇÃO"

Sem prejuízo, uma vez mais, de apresentar o PROJETO, como um todo, a partir do capítulo 5, é importante resumir aquilo que foi feito, também, como resultado deste projeto, em particular, num espaço temporal de 5 anos.

Alguns anos após a implementação do projeto "1000 Salas TIC", mais concretamente em setembro de 2007, foi aprovado pelo Governo português[15], o Plano Tecnológico da Educação (PTE), que pretendia "colocar Portugal entre os cinco países europeus mais avançados em matéria de modernização tecnológica das escolas até 2010"[16].

Os objetivos definidos para o período 2007-2010 foram:

> "Atingir o rácio de dois alunos por computador com ligação à Internet em 2010;
>
> Garantir em todas as escolas o acesso à Internet em banda larga de alta velocidade de pelo menos 48 Mbps em 2010;
>
> Assegurar que, em 2010, docentes e alunos utilizam TIC em pelo menos 25 % das aulas;
>
> Massificar a utilização de meios de comunicação electrónicos, disponibilizando endereços de correio electrónico a 100 % de alunos e docentes já em 2010;
>
> Assegurar que, em 2010, 90 % dos docentes vêem as suas competências TIC certificadas;
>
> Certificar 50 % dos alunos em TIC até 2010."[17]

Este plano trabalhou em 4 eixos: Tecnologia; Conteúdos; Formação; e "Investimento e financiamento". Na parte importante para o projeto que apresento neste relatório, a "Tecnologia", o PTE pretendia "dar resposta às principais barreiras observadas em termos de infra-estruturas e acessos"[18], nomeadamente no que respeita à falta de computadores nas escolas, bem como de outros equipamentos de apoio (equipamentos de projeção, quadros interativos). Outra das vertentes a que era preciso dar resposta prendia-se com a "reduzida acessibilidade aos equipamentos por parte de alunos, docentes e não docentes"[19] bem como o acesso à Internet e a velocidade a que esta era realizada, nos equipamentos que a tinham.

---

[15] Resolução do Conselho de Ministros. (18 de setembro de 2007). *n.º 137/2007*. Diário da República, 1.ª série - N.º 180. Obtido de https://files.dre.pt/1s/2007/09/18000/0656306577.pdf

[16] DGEEC. (s.d.). Plano Tecnológico da Educação - Missão e Objetivos. Obtido em 21 de janeiro de 2022, de https://www.dgeec.mec.pt/np4/243.html

[17] Resolução do Conselho de Ministros. (18 de setembro de 2007). *n.º 137/2007*. Diário da República, 1.ª série - N.º 180, p. 6567. Obtido de https://files.dre.pt/1s/2007/09/18000/0656306577.pdf

[18] *Idem*

[19] *Ibidem*

Mas, um dos pontos identificados, apontava para a inexistência de redes locais estruturadas e eficientes, e outro para o previsível aumento significativo de equipamentos nas escolas, e das infra-estruturas necessárias a suportar tal aumento, que implicava a existência de apoio técnico para a gestão e manutenção das infraestruturas a criar, e sua segurança (equipamentos e utilizadores).

Foram então desenvolvidos e implementados vários projetos, tendo em vista dar resposta ao que fora identificado, nomeadamente:

- Projeto Kit Tecnológico Escola – visava dotar as escolas de equipamentos (computadores com ligação à Internet, quadros interativos, videoprojectores e impressoras), que permitissem atingir, até 2010, o rácio de 2 alunos por computador, um videoprojector em todas as salas de aula, um quadro interativo em cada três salas de aula; o projeto implicava ainda garantir que a proporção de equipamentos com antiguidade superior a três anos não ultrapassasse os 20 % (ou seja, previa a substituição dos mesmos, teoricamente).

- Projeto Internet em Banda Larga de Alta Velocidade – visava colocar todos os computadores das escolas com ligação à Internet e aumentar, de forma progressiva, as velocidades de acesso até aos 48 Mbps, tudo até 2010.

- Projeto Internet nas Salas de Aula – visava reestruturar as redes de área local existentes (na maioria das escolas já existiam, de alguma forma, apesar de 1/3 destas não serem estruturadas e a maioria terem alcance limitado, em termos de áreas de cobertura[20]). Pretendia-se também passar as operações de manutenção e gestão destas redes para um apoio técnico especializado, em vez de estas serem realizadas por professores e/ou auxiliares, que eram que as realizava até então. Resumindo, este projeto pretendia promover a utilização das tecnologias nos processos de ensino e aprendizagem, bem como em toda a vertente administrativa das escolas, através da criação de uma "infra-estrutura de redes de comunicação que suporte a utilização de tecnologia e de Internet de forma segura e ubíqua"[21]. Tal seria implementado com "redes de área local, com acesso remoto e separação segura de redes, em todas as escolas"[22], que incluía a implementação de pontos de acesso cablados, bem como sem fios, quer nas salas de aula, quer nas áreas de maior participação dos alunos no meio escolar. O suporte à operação e gestão destas redes seria realizado de forma centralizada.

- Projeto Cartão Eletrónico do Aluno – visava a implementação de plataformas com utilização de cartões de aluno, eletrónicos, para promover o aumento da segurança, e que

[20] Resolução do Conselho de Ministros. (18 de setembro de 2007). *n.º 137/2007*. Diário da República, 1.ª série - N.º 180, p. 6570. Obtido de https://files.dre.pt/1s/2007/09/18000/0656306577.pdf

[21] *idem*

[22] *ibidem*

possibilitassem o aumento da eficiência da gestão escolar, através da supressão de circulação de numerário, controlo das entradas e saídas dos alunos, consulta do processo administrativo, do percurso académico e dos consumos dos alunos.

- Projeto Videovigilância – visava aumentar a segurança de pessoas e bens, através da implementação de sistemas de videovigilância e de alarme, em todas as escolas.

Estava, assim, a ganhar forma, uma revolução tecnológica em meio escolar. Tendo experiência profissional na gestão de redes estruturadas, pensei que, finalmente, as escolas seriam dotadas de tecnologia pertinente, que permitisse a sua utilização de forma segura e pertinente, quer para os professores e alunos, quer para a gestão escolar.

No entanto, a gestão de todo este processo deixou muito a desejar, começando com a forma precipitada como foram feitos os "*site-surveys*", em pleno agosto e sem conhecimento do Coordenador TIC / Diretor de Instalações de Informática.

A forma apressada como o processo se desenvolveu e a falta de resposta do mercado (quantidade de empresas e mão de obra qualificada para a instalação das infraestruturas, nomeadamente a cablagem, calhas técnicas, bastidores de rede), fez com que o trabalho final realizado na escola secundária com 3.º Ciclo de Madeira Torres se parecesse algo do 3.º mundo. Coloco aqui apenas algumas imagens que retratam a forma como o trabalho foi entregue:

Figura 3.1 - Aspeto de várias áreas onde a instalação dos passivos foi efetuada de forma deficiente

Tal foram a quantidade de problemas encontrados, que apresentei um pedido de averiguação da execução dos trabalhos de acordo com o Caderno de Encargos bem como do respetivo *Site-Survey*. Foi então realizada uma auditoria informática, para averiguar o estado de execução do «*check list* de *Site*

Survey» com as alterações introduzidas pelo subempreiteiro (TRUST IN) e o documento "Redes Locais - Condições e Requisitos" ambos fornecidos pelo responsável técnico da equipa PTE da Escola.

Foram feitas correções que minimizaram aquilo que de mal tinha sido feito, mas não foi corrigido as grandes lacunas nem aquilo que foi estragado da estrutura de passivos já existente na escola.

No entanto, houve áreas onde efetivamente o PTE trouxe bastantes mais-valias à escola. O facto de existir cablagem estruturada em todas as salas, bem como a instalação de computadores em toda a escola (nesta altura, o Agrupamento de Escolas Madeira Torres era composto apenas pela Escola Secundária com 3.º Ciclo de Madeira Torres), num número perto de 250, permitia, pela primeira vez, pensar globalmente na escola como uma única unidade e desenvolver, efetivamente, um projeto consistente que permitisse utilizar as tecnologias com segurança e obter um aumento da eficiência dos *stakeholders* do Agrupamento.

Projetos desenvolvidos paralelamente ao PTE

Com base no equipamento disponibilizado no âmbito do Plano Tecnológico para a Educação, tínhamos agora equipamentos que nos permitiam dar um salto enorme: ter toda a escola ligada por cablagem estruturada, com calha técnica, bem como grande parte da mesma coberta com acessos WiFi.

Além disso, a escola pode descontinuar alguns equipamentos obsoletos (computadores), pois recebeu um total de 255 computadores HP dc7900, ficando com um total de 284 computadores, todos ligados em rede e com acesso à Internet. Além disso, recebeu 48 projetores e 12 quadros interativos, bem como um servidor HP Proliant DL180 (com sistema operativo Windows Server 2003 R2).

O projeto que desenvolvi, nos 5 anos após o PTE (ou seja, até ao ano letivo 2010/2011), consistiu em:

- Desenhar e implementar mais 2 laboratórios de informática, 2 salas de informática e remodelação da rede estruturada de um outro laboratório de informática.
- Adicionar todos os computadores ao domínio da AD existente, utilizando autenticação RADIUS/802.1x (disponibilizada pelo servidor Edgebox implementado no âmbito do PTE).
- Ampliar a infraestrutura de servidores para passar a ter servidores aplicacionais (software de administração escolar) e de ficheiros (1 acessível a alunos e outro a professores/pessoal não docente), utilizando as VLAN para segmentar tráfego e aumentar segurança da informação.
- Criação de um sistema de reposição de imagens baseado em software *open-source* (FOGProject).
- Migração de todos os computadores para o Windows 7 Enterprise.
- Criação de políticas de grupo para os utilizadores e computadores do domínio da escola.

4. FASE 3 – O PÓS PTE

Passados 5 anos da implementação do PTE, era esperado, de acordo com o que a Resolução do Conselho de Ministros n.º 137/2007 refere quanto aos objetivos do ponto 3.1.1 ("Projeto chave – Kit Tecnológico Escola", nomeadamente que é necessário assegurar "a renovação dos equipamentos, garantindo que a proporção de equipamentos com antiguidade superior a três anos não ultrapasse 20 %"[23], que tivessem chegado equipamentos à escola, mas a verdade é que nunca mais foi feito grande coisa no que respeita ao PTE (exceção talvez seja a manutenção da equipa de suporte às escolas para gestão dos ativos de rede pelo NSO, a melhoria da qualidade de acesso à Internet, e uma ou outra iniciativa pontual).

Não obstante, foi nesta fase que o projeto que desenvolvi para o agrupamento teve o maior desenvolvimento. Resumindo o que foi desenvolvido e implementado (e que será apresentado, de forma pormenorizada, a partir do capítulo 5), temos:

- Implementação do novo sistema de cartões utilizando leitores de proximidade.
- Implementação do sistema de sumários eletrónicos.
- Mudança do nome de utilizadores (professores e pessoal não docente) para podermos ter o mesmo nome de utilizador que o das aplicações de gestão administrativa (GIAE).
- Apoio ao sistema desenhado pelo PTE para que pudesse suportar mais do que 256 endereços atribuídos por DHCP (devido ao tamanho da nossa rede, tornou-se necessário).
- Em 2012 deu-se a junção dos Agrupamentos de Escolas Padre Francisco Soares com o Agrupamento de Escolas Madeira Torres (passando o novo agrupamento a ter o nome deste último), o que, devido ao facto de as escolas sede destes agrupamentos serem geminadas, levou à opção de estabelecer a ligação por fibra ótica da infraestrutura de rede da Escola Secundária com 3.º Ciclo de Madeira Torres com a da EB23 PFS e do JI+EB1 PFS (que, entre si, já estavam ligadas por fibra ótica), para otimizar a gestão desta infraestrutura unida de forma centralizada.
- Atualização dos servidores para o Windows Server 2012.
- Utilização das funções existentes nos servidores com NOS da Microsoft, para virtualizar os servidores do AEMT.
- Criação de um mini *datacenter* (com porta de segurança e corta-fogo, com sistemas de arrefecimento, de monitorização e alarme relativamente à temperatura, à humidade e a inundações, bem como deteção de intrusões, incluindo captação de vídeo com deteção

[23] Resolução do Conselho de Ministros. (18 de setembro de 2007). n.º 137/2007. Diário da República, 1.ª série - N.º 180. Obtido de https://files.dre.pt/1s/2007/09/18000/0656306577.pdf

de movimento). Este *datacenter* não tem, contudo, sistemas antifogo e de controlo de acessos eletrónico. Posteriormente, criação de sistema redundante de arrefecimento.

- Remodelação da sala 235 (passagem a laboratório de informática, com rede estruturada e colunas de calhas centrais)
- Implementação de um sistema telefónico VoIP (com carta BRI OpenVox BE400E), para redução de custos e otimização da flexibilidade de reconfigurações necessárias a nível de sistema telefónico interno dentro e interescolas germinadas.
- Aquisição de mais servidores para avançar com projeto de redundância física dos servidores do *datacenter*.
- Aquisição de 75 novos computadores (em 2 fases), com processadores e memória potentes para permitirem a hipótese de virtualização do tipo 2, para os laboratórios de informática.
- Aquisição de 4 novos computadores para apoio ao *datacenter* (simulação dos servidores, para realização de trabalho de projetos de melhoria em ambiente de testes).
- Ampliação dos recursos existentes nos servidores para dar resposta à crescente necessidade de serviços, utilizadores, inerentes a termos passado a ser um agrupamento de escolas muito maior (segundo processador, aumento da capacidade de memória, aumento da capacidade de armazenamento, aquisição de placas de rede para permitir agregação de portas de rede – NIC TEAMING)
- Atualizações no *Fileserver* dos professores e alunos (aplicação de boas práticas de segurança)
- Reconfiguração do servidor VoIP para ser utilizável na nova matriz de conetividade de rede desenhada pelos responsáveis da DGEEC.
- Reconfiguração dos equipamentos de VoIP para poderem ser adicionados de forma automática à rede, sem necessidade de configuração de portas numa VLAN específica.
- Aposta na utilização do ensino misto: criação de tutoriais para utilização do *Google Classroom*, como complemento ao Moodle, para disponibilização de recursos e criação de momentos de ensino não presencial.
- Desenho do projeto TV em vez de Projetor, e sua apresentação, tendo em vista responder à problemática dos projetores de vídeo estarem em fim de vida, sem luminosidade suficiente para permitirem dar aulas com luz natural.
- Remodelação da sala 235 (passagem para laboratório de eletrónica), que incluiu a aquisição de 16 novos computadores.
- Com o evento da pandemia e a necessidade de ensino à distância, fiz a migração do Google Apps para Office 365 (ou seja, migrei as contas de email dos professores, da Google para

o Office 365, copiando o conteúdo existente para não haver quaisquer perdas de informação).

- Sincronização das contas do domínio local (*Active Directory*) com o Azure AD, para permitir a utilização de um mesmo nome de utilizador e respetiva password entre a rede local e os serviços do Office 365.
- Configuração do Moodle para utilizar o endereço de email e respetiva password, como dados de autenticação.
- Com a adoção do Office 365, foi também feita a criação de contas de email para todos os alunos (desde o jardim de infância ao secundário) e para todos os assistentes operacionais.
- Implementação do Microsoft Teams (que implicou o desenvolvimento de scripts para permitir a criação de todas as disciplinas – mais de 1000 – de todos os anos letivos, do 1.º ao 12.º ano, incluindo cursos profissionais, e a inscrição automática dos respetivos professores e alunos em cada disciplina).
- Implementação de MFA para todos os utilizadores, como medida de segurança para o ensino a distância.
- Implementação de SSO
- Produção de tutoriais em vídeo, para apoio à comunidade escolar, na utilização do email (Outlook Online), Office 365 (Aplicações do Office Online), Teams, etc.
- Início do processo de aquisição de novos computadores (16), para renovação do laboratório da sala 302, um dos locais onde se irá realizar o projeto piloto de utilização de TV (*Smart* TV) em vez de projetor.
- Prevista a aquisição de 2 TVs para piloto do projeto TV em vez de Projetor.
- Início da implementação do PADDE, que implica o desenho de uma solução de gestão documental assente em Microsoft SharePoint.

Com esta lista concluímos a descrição resumida dos passos realizados neste projeto de implementação daquela que é, efetivamente, uma das maiores redes de computadores a nível do ensino público não superior, em Portugal.

5. O PROJETO

Este projeto foi desenvolvido em várias fases, de acordo com os equipamentos que foram sendo disponibilizados pelo Ministério da Educação através das muitas iniciativas (principalmente as apresentadas nos capítulos anteriores), bem como por investimentos próprios da escola, de acordo com projetos que eu apresentei, no desempenho dos vários cargos com responsabilidades técnicas e de instalações que desempenhei no agrupamento.

Deste modo, todo o trabalho que aqui apresento, não foi resultado do meu desempenho como docente, mas sim no decurso das atividades inerentes aos cargos técnicos para os quais fui sendo nomeado.

5.1. Uma plataforma para a gestão de acessos e partilha de recursos

A primeira parte consistiu na implementação das 2 Salas TIC na Escola Secundária com 3.º Ciclo de Madeira Torres. Germinada com esta escola existe a Escola Básica do 2.º e 3.º Ciclo Padre Francisco Soares, que era sede de agrupamento vertical do então designado Agrupamento de Escolas Padre Francisco Soares, mas que, por altura quer deste projeto das 1000 Salas TIC, quer depois no arranque e primeiros anos do PTE, era uma entidade diferente e, por isso, sob responsabilidade de outra pessoa.

Deste projeto ressalva-se a adoção de servidores em Windows (Windows Server 2003), apesar de trabalharem em ilhas isoladas (1 servidor em cada sala).

Como consta do meu currículo, detinha na altura a certificação de *Microsoft Certified System Engineer* em Windows NT 4. No entanto, esta versão, completamente baseada numa tecnologia "antiga" (apesar de, ironicamente, o nome do sistema operativo Windows NT apontar para "*New Technology*"), desenvolvida para a IBM, 10 anos antes, designada por *LanManager*[24].

Mas, desde essa minha certificação, acompanhei o aparecimento do Windows Server 2000 e Windows Server 2003 (apesar de não ter renovado a certificação MCSE, fiz ações de formação para aprender sobre as novidades e como tirar melhor partido das mesmas). Estas novas versões levaram a Microsoft na direção de uma arquitetura verdadeiramente baseada em serviços de diretório, e fê-lo através dos serviços de *Active Directory* (AD), que é um diretório de rede baseado em *standards* abertos, compatível com X.500 e LDAP[25].

[24] Lan Manager. (s.d.). Obtido em 22 de janeiro de 2022, de Wikipedia: https://en.wikipedia.org/wiki/LAN_Manager
[25] King, R. R. (2003). Mastering Active Directory for Windows Server 2003. San Francisco / London: Sybex.

Como este sistema operativo de rede (do inglês *Network Operating System* – NOS) estava licenciado nas salas TIC, e como tinha feito formação específica para a utilização do mesmo, colocou-se como primeira hipótese para a implementação de servidores de autenticação e gestão de recursos.

Assim, li e estudei diversos livros sobre o mesmo, esperando aprender as vantagens da utilização da AD, nomeadamente no que respeitava a:

- Capacidade de gestão centralizada de recursos e administração da segurança.
- Acesso a todos os recursos globais com um único início de sessão (*single logon*).
- Localização simplificada de recursos.

Nessa altura, existiam na escola computadores nas várias salas dos departamentos curriculares, bem como na sala de professores, alguns dos quais em rede, mas sem qualquer gestão centralizada de utilizadores (existiam apenas contas locais, em cada computador). Cada departamento tinha um computador e impressora diferente (em termos de marca/modelo/tipo), pelo que a gestão destes recursos era muito complexa.

No terceiro e último piso da escola, existiam 4 salas de aula (salas 304, 312, 313 e 315A) com computadores (antes dos laboratórios da iniciativa das 1000 Salas TIC serem instalados), bem como uma sala (307) na Biblioteca Escolar / Centro de Recursos Educativos (BECRE), que também tinha computadores, alguns com ligação à Internet. Toda a gestão destes equipamentos era extremamente difícil, pois todas as contas eram locais, já para não falar da heterogeneidade de hardware e software. Estes computadores tinham conetividade à Internet através de um acesso a 1 Mbps.

Foi neste piso, então, que se instalaram (nas salas 302 e 315) os 2 laboratórios para a disciplina de TIC, ficando este piso quase dedicado às salas de informática e à BECRE (a exceção é o gabinete dos Serviços de Psicologia e Orientação da escola, que também se encontram localizados neste piso).

Aproveitei, desse modo, os servidores Fujitsu Primergy que foram fornecidos e que tinham o Windows Server 2003 instalado, para iniciar o processo de configuração de uma rede com gestão centralizada através da AD.

Também os computadores destas duas salas eram todos da mesma marca/modelo e vinham com o mesmo sistema operativo (Windows XP), o que permitia uma melhor gestão dos mesmos (em termos de configuração e preparação dos mesmos).

Nessa altura, o objetivo principal que defini era ser capaz de implementar um sistema de partilha dos recursos existentes (acesso à Internet, impressoras da BCRE, ficheiros) e que permitisse uma gestão centralizada da gestão das permissões. Assim, ao utilizar o Windows Server e a AD, poderia criar contas de utilizador e implementar um servidor de ficheiros onde cada utilizador poderia armazenar os seus ficheiros, tendo acesso aos mesmos a partir de qualquer computador que estivesse registado na AD, recorrendo a configurações que realizei através de Group Policies, uma característica existente nestes serviços de diretório da Microsoft.

Havendo 2 servidores num mesmo domínio, e tendo ambos o papel de *Domain Controller*, pude implementar redundância e melhorar o desempenho dos acessos.

A escola começava a ter uma estrutura centralizada e organizada de gestão dos recursos, começando pelos laboratórios de informática.

Antes de avançar para a apresentação daquilo que foi implementado, na Escola Secundária com 3.º Ciclo de Madeira Torres, inicialmente, e posteriormente no conjunto das escolas EB Padre Francisco Soares e ES Madeira Torres, que são a oferta de 2º ciclo a secundário do Agrupamento de Escolas Madeira Torres, convém fazermos uma breve incursão teórica sobre algumas das tecnologias utilizadas neste processo.

Assim, utilizando os vários servidores (e computadores "adaptados" a essas funções), o estado da rede informática do agrupamento, em 2005, era o seguinte:

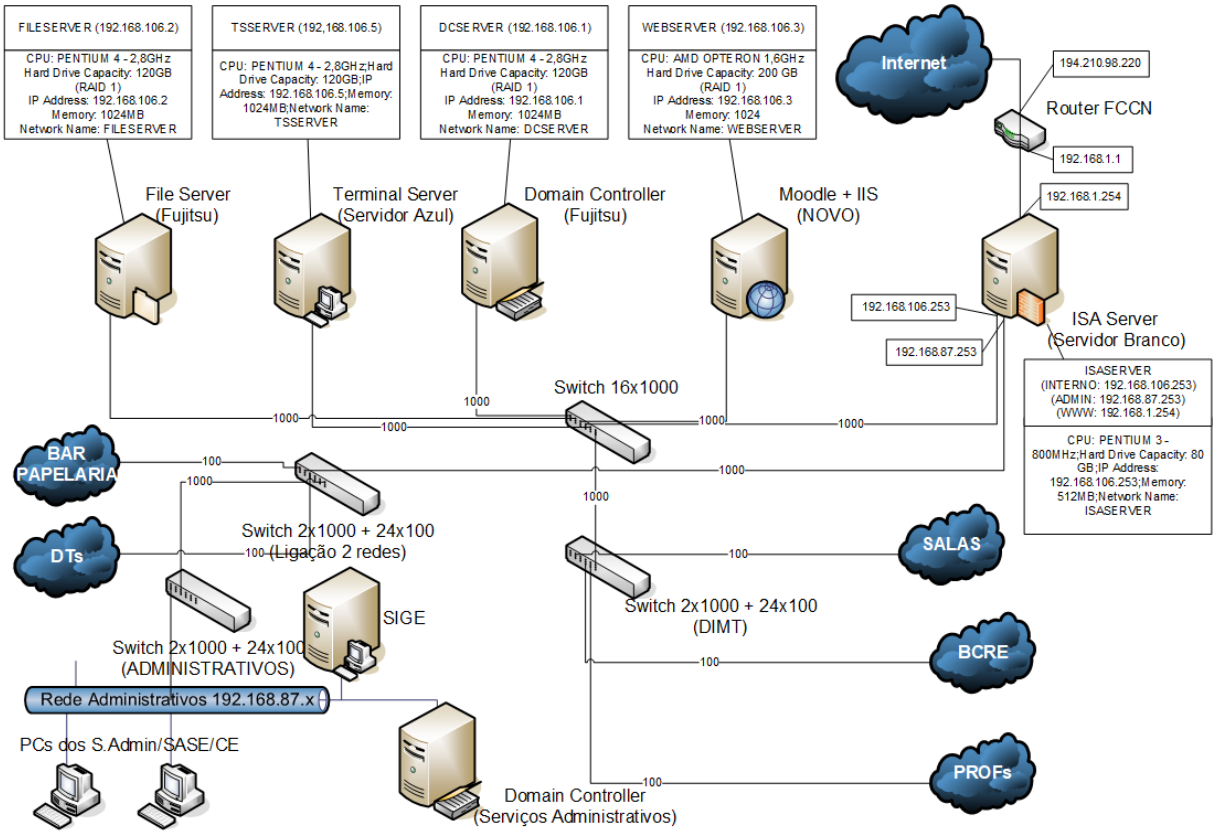


Figura 5.1 - Desenho da rede informática do AE Madeira Torres (2005)

5.2. Active Directory

Cumpre agora refletir um pouco acerca do que foi apresentado no ponto anterior, começando pela pergunta; afinal, o que é a *Active Directory* e para que serve?

Um diretório (*directory*) pode ser visto como uma lista, e é apenas uma forma fácil de procurar algo. Existem diretórios em todo o lado. Por exemplo, quando pesquisamos um número numa lista telefónica, ou quando organizamos os ficheiros e as pastas num computador, estamos a utilizar um

diretório. Tal como estes exemplos, a AD é uma coleção de informação, mais concretamente, uma coleção de informação sobre os recursos existentes numa rede Windows Server[26].

Em qualquer rede informática num ambiente empresarial, existe um tipo de base de dados com informação sobre as contas. Por exemplo, no Windows NT era designada de base de dados SAM (*Security Accounts Manager*) e nas versões iniciais da Novell NetWare era conhecida por *bindery*[27].

Os serviços de diretório vão para além da funcionalidade de um conjunto de diretórios proprietários dispersos, ao providenciarem uma fonte unificada de informação[28]. Um serviço de diretório fornece um local para armazenar informação acerca de entidades pertencentes à rede, tais como aplicações, ficheiros, impressoras ou pessoas[29] (ou seja, é uma base de dados da rede que armazena informações acerca dos recursos nela existentes).

A *Active Directory* foi introduzida no Windows 2000[30], e a Microsoft tem feito melhoramentos à AD a cada nova versão do Windows Server. No caso do Windows Server 2003, foram feitas melhorias a nível da gestão da AD, com um aumento do número de ferramentas e da facilidade de uso das mesmas.

A *Active Directory* é, então, o serviço de diretório centralizado dos ambientes Windows Server[31]. São também utilizadas como repositório central da informação relacionada com a segurança, o que inclui as identidades de segurança, os intermediários de segurança (grupos e funções), direitos (o que uma identidade de segurança pode fazer) e outros atributos de identidades de segurança, e informação acerca das políticas de segurança[32].

Segundo King[33] (King, 2003), os diretórios são um apoio aos administradores na gestão dos ambientes complexos nas seguintes vertentes:

- **Gestão simplificada** – são um ponto central de gestão e administração, que utiliza um conjunto específico de ferramentas específicas para esse fim, que permite facilitar a gestão de ambientes de rede complexos.
- **Aumento de segurança** – pelo facto de os acessos e autenticações serem controladas através de um único serviço, permitem utilizar um processo de autenticação simplificado e mais seguro.

---

[26] Glenn, W., & Simpson, M. T. (2004). *Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit.* Washington: Microsoft Press, p. 1-2
[27] King, R. R. (2003). *Mastering Active Directory for Windows Server 2003.* San Francisco / London: Sybex, p. 5
[28] Glenn, W., & Simpson, M. T. (2004). *Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit.* Washington: Microsoft Press, p. 1-3
[29] King, R. R. (2003). *Mastering Active Directory for Windows Server 2003.* San Francisco / London: Sybex, p. 5
[30] Snedaker, S. (2004). *Best Damn Windows Server 2003 Book Period.* Rockland: Syngress, p. 3
[31] Holme, D., & Thomas, O. (2004). *MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296.* Washington: Microsoft Press, p. 2-1
[32] Clercq, J. D., & Grillenmeier, G. (2007). *Microsoft Windows Security Fundamentals.* Oxford: Elsevier, p. 21
[33] King, R. R. (2003). *Mastering Active Directory for Windows Server 2003.* San Francisco / London: Sybex, p. 6

- **Promoção da interoperabilidade** – maioria dos serviços de diretório para ambientes empresariais atualmente disponíveis, são baseados em padrões da indústria (por exemplo, o X.500 e o LDAP), e a AD não foge à regra. Tal permite utilizar estes serviços com outros sistemas, de outros fabricantes.

Sem querer entrar em grandes detalhes sobre os serviços de diretório e os padrões de indústria (que podem ser consultados no site da *Internet Engineering Task Force*[34], resumo os principais na tabela que se segue:

Identificação do serviço	**Descrição**
X.500 e DAP (*Directory Access Protocol*)	Especificação da ISO que define como os diretórios globais devem de ser estruturados. O X.500 especifica como utilizar o DAP para providenciar comunicações entre os clientes e os servidores do diretório.
LDAP (*Lightweight Directory Access Protocol*)	Surgiu em resposta à crítica de que o DAP era demasiado complexo para ser utilizado na maioria das implementações de diretórios de serviço e rapidamente se tornou o protocolo padrão de diretórios utilizados na Internet.
NDS	É o serviço de diretório utilizado nas redes *Novell Netware* e cumpre o padrão X.500.
Active Directory	Parte integrante das redes Windows Server, a partir da versão 2000, que foi desenhado para cumprir o padrão LDAP.

Tabela 5.1 - Exemplos de serviços de diretório e padrões da indústria – baseado em (Glenn & Simpson, 2004)

Para Glenn e para Simpson (Glenn & Simpson, 2004), numa rede complexa, o serviço de diretório deve providenciar uma forma eficiente de gerir, encontrar e aceder a todos os recursos da rede (computadores, utilizadores, impressoras, pastas partilhadas, entre outros recursos) e, para uma boa implementação de um serviço de diretório, este deveria providenciar um conjunto nuclear de benefícios[35], tais como:

- **Centralização** – ter a informação de todos os recursos de rede num local centralizado permite fazer a sua gestão através de um único ponto, facilitando a gestão dos recursos existentes bem como permitindo a delegação de tarefas administrativas.
- **Escalabilidade** – permitir acomodar o crescimento de uma rede sem que isso traga um aumento da sobrecarga do mesmo, o que implica ser capaz de ter mecanismos de partição da base de dados do diretório.

[34] https://www.ietf.org/

[35] Glenn, W., & Simpson, M. T. (2004). *Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit.* Washington: Microsoft Press, p. 3-4

- **Padronização** – permitir aceder à informação através da utilização de padrões abertos, para que outras aplicações/serviços possam utilizar os recursos (ou publicar novos) sem terem de ter os seus próprios serviços de diretório.
- **Extensibilidade** – providenciar formas de um administrador ou uma aplicação/serviço poderem ampliar a informação contida no diretório para ir de encontro às necessidades da organização.
- **Separação da rede física** – transparência relativa à topologia de rede para que um recurso possa ser identificado e acedido independentemente do local e da forma como está conectado à rede.
- **Segurança** – providenciar uma forma segura de armazenar, gerir, obter e publicar informações acerca dos recursos de rede.

A AD foi desenhada para cumprir tudo o que atrás foi apresentado, ou seja, a AD é mais do que uma simples base de dados.

O modelo de rede do Windows que utiliza a AD é conhecido como o modelo de domínio[36]. Neste modelo, todos os recursos empresariais existem num diretório único que é confiável por todos os sistemas seguros pertencentes a esse domínio. Esses sistemas podem utilizar os atores de segurança (*security principals*) do diretório para garantir a segurança dos recursos. A AD pode ser vista, então, como uma loja de identidades (*identity store*) que fornece uma lista segura de quem é o quê no domínio[37].

Gerir a *Active Directory* de uma rede Windows Server é talvez a principal tarefa de um administrador de redes Windows. Segundo Allen, "um administrador competente da *Active Directory* tem de ter, pelo menos, conhecimentos ligeiros sobre uma mão cheia de tecnologias, incluindo DNS, WINS, *Kerberos*, LDAP e o sistema operativo Windows em si mesmo"[38]. Allen diz ainda que "tem de ser capaz de executar mais do que cem tarefas diferentes utilizando mais de trinta utilitários distintos"[39].

Uma vez que a *Active Directory* separar a estrutura lógica dos recursos da estrutura física da rede, para se poder analisar e planear corretamente uma infraestrutura assente na AD, é necessário analisar e compreender a AD segundo estas duas perspetivas também.

5.2.1. Estrutura lógica da Active Directory

O que permite à AD ser tão escalável e configurável, é mesmo o facto de separar a estrutura lógica da hierarquia de domínio do Windows Server da estrutura física da própria rede, como atrás se indicou.

---

[36] Holme, D., & Thomas, O. (2006). *Managing and Maintaining a Microsoft Windows Server 2003 Environment.* Washington: Microsoft Press, p. 1-13
[37] *Idem*
[38] Allen, R. (2003). *Active Directory Cookbook.* Sebastopol: O'Reilly, p. 3
[39] *Idem*

Fazem parte desta estrutura lógica os domínios, as árvores, as florestas, as unidades organizacionais e os vários objetos em si. Neste ponto iremos analisar cada um dos elementos desta estrutura lógica.

5.2.1.1. Objetos

Todos os recursos são armazenados na AD como objetos, ou seja, os objetos representam os recursos tangíveis que existem na rede. Os objetos são armazenados na AD numa estrutura hierárquica de contentores e subcontentores, o que possibilita encontrá-los, aceder-lhes e geri-los muito mais facilmente. Convém analisarmos os objetos sobre duas perspetivas[40]: classes de objetos e o esquema da AD:

Classes de objetos – um objeto, efetivamente, é apenas um conjunto de atributos, e os atributos que definem um determinado objeto estão especificados numa classe de objeto (a classe dos utilizadores, por exemplo, especifica os atributos que definem um objeto do tipo utilizador). Estas classes de objetos permitem organizar os objetos com base em similaridades e, quando criamos um objeto de uma determinada classe, este automaticamente herda os atributos especificados nessa classe. A Microsoft automaticamente define um conjunto de classes de objetos, definido por um objeto do tipo *classSchema* no recipiente do esquema[41]. Cada instância de uma classe de objetos tem uma propriedade com múltiplos valores do tipo *objectClass* (por exemplo, a propriedade *objectClass* de um objeto do tipo utilizador iria identificar as classes *top*, *person*, *organizationalPerson* e *user*. Cada instância de uma classe de objetos também possui uma propriedade do tipo *objectCategory*, que é uma propriedade com um único valor que contem o nome distinto (*distinguished name*) ou da classe da qual o objeto é uma instância ou de uma das suas superclasses. Ao ser criado um objeto, o sistema define a propriedade *objectCategory* do mesmo para o valor especificado na propriedade *defaultObjectCategory* da sua classe de objetos[42]. É importante referir que, antes da versão do Windows Server 2008, o atributo *objectClass* não era indexado.

O esquema (*schema*) da *Active Directory* – as definições formais das classes de objetos que podem ser criadas numa floresta da AD, bem como as definições formais de cada atributo que pode existir num objeto da AD, estão definidos no esquema (*schema*) da AD[43]. Por outras palavras, o esquema da AD (*Active Directory Schema*) pode se visto como uma coleção de dados (classes de objetos) que definem como os dados reais do diretório (atributos dos objetos) estão organizados e armazenados o que, em termos de bases de dados, se define pela forma da estrutura de tabelas e campos, bem como

---

[40] Glenn, W., & Simpson, M. T. (2004). *Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit.* Washington: Microsoft Press, p. 1-5 e 1-6

[41] *Características das classes de objeto*. (s.d.). Obtido em 30 de 01 de 2022, de Microsoft: https://docs.microsoft.com/pt-br/windows/win32/ad/characteristics-of-object-classes

[42] *Características das classes de objeto*. (s.d.). Obtido em 30 de 01 de 2022, de Microsoft: https://docs.microsoft.com/pt-br/windows/win32/ad/characteristics-of-object-classes

[43] *Esquema de Active Directory*. (s.d.). Obtido em 30 de 01 de 2022, de Microsoft: https://docs.microsoft.com/pt-br/windows/win32/adschema/active-directory-schema

a forma em como estes se relacionam. Quase tudo, na AD, é um objeto, até o esquema em si. Em termos de segurança, o acesso ao esquema (tal como aos restantes objetos) é feito através de ACL (*access control lists*), que são geridas pelo subsistema de segurança do Windows Server.

5.2.1.2. Identificação de objetos

No ambiente das redes e das aplicações de rede, existem diversas formas de identificar os recursos, pelo que, em cada ambiente singular, cabe ao administrador do sistema e aos utilizadores, saberem a forma correta de utilizar as várias formas de atribuir nomes ou identificar e encontrar determinados recursos. No que respeita a servidores e partilhas, um dos métodos mais comuns é a utilização de nomes UNC (*Uniform Naming Convention*), que utilizam o formato:

```
\\<nome do servidor>\<nome da partilha>\<caminho para o recurso>
```

Designação	Explicação
<nome do servidor>	Refere-se ao nome do dispositivo onde o recurso se encontra
<nome da partilha>	Refere-se ao nome atribuído à área que está a ser partilhada
<caminho para o recurso>	Refere-se à estrutura lógica do diretório utilizada para encontrar a informação pretendida

Tabela 5.2 - Identificação dos componentes de um UNC - com base em Allen, 2003

Ao se poderem armazenar, potencialmente, milhões de objetos na AD, cada um destes tem de ser localizável e identificável de forma única[44].

O GUID – a cada objeto existente/criado na AD é atribuído um GUID (*Globally Unique Identifier*), que é um número de 128 bit. Este GUID permanece inalterável durante o tempo de vida do objeto, independentemente de se alterar a sua localização ou o seu nome (desde que se mantenha na mesa DIT – *Directory Information Tree*).

Os ADsPath – apesar de ser um número único e resiliente, os GUID não são fáceis de memorizar, razão pela qual se utiliza, normalmente, o ADsPath para referenciar os objetos[45]. Na AD, os ADsPath são os caminhos hierárquicos que podem ser utilizados para identificar e referenciar inequivocamente um objeto. Os ADsPaths para AD são representados utilizando as regras de sintaxe e semântica definidas no padrão LDAP. Por exemplo, para identificar a raiz do domínio esmt.local, o ADsPath seria `LDAP://dc=esmt,dc=local`.

O *Distinguished Name* (DN) – é o nome utilizado para referenciar inequivocamente um objeto na DIT. Um *Relative Distinguished Name* (RDN) é o nome utilizado para referenciar, inequivocamente, um objeto dentro do contentor onde este se encontra. Por exemplo, para a conta de administrador do domínio esmt.local, os identificadores seriam:

[44] Allen, R., & Lowe-Norris, G. A. (2003). *Active Directory, 2nd edition* (2ª ed.). O'Reilly
[45] Allen, R., & Lowe-Norris, G. A. (2003). *Active Directory, 2nd edition* (2ª ed.). O'Reilly

Tipo	Conteúdo
ADsPath	LDAP://cn=Administrator,cn=Users,dc=esmt,dc=local
DN	cn=Administrator,cn=Users,dc=esmt,dc=local
RDN	cn=Administrator

Tabela 5.3 - Identificação de objetos na DIT

Todos os ADsPath, os DN e RDN utilizam um prefixo para identificar a classe do objeto que estão a referenciar (estes códigos estão normalizados e identificados no RFC 4514[46]). Todos as classes de objetos que não tenham um código explicitamente referenciado utilizam a valor padrão que é CN (*Common Name*).

String	X.500 AttributeType
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userID

Tabela 5.4 - Lista das strings dos tipos de atributos frequentemente vistos nos RDN (RFC 4514)[47]

***User Principal Name* (UPN)** – na AD, esta é a forma como um utilizador pode identificar-se para iniciar sessão na rede[48]. Assim, a conta de administrador do domínio esmt.local teria o seguinte UPN: administrator@esmt.local.

5.2.1.3. Domínios

A estrutura base de organização do modelo de rede do Windows Server é o domínio, que mais não é do que a representação de um limite administrativo onde estão inseridos todos os computadores, utilizadores e outros objetos que se pretende serem geridos como parte desse mesmo domínio[49].

[46] Zeilinga, K. (Ed.). (2006). Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names, RFC 4514. OpenLDAP Foundation. Obtido em 12 de 02 de 2000, de https://datatracker.ietf.org/doc/html/rfc4514
[47] Zeilinga, K. (Ed.). (2006). Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names, RFC 4514. OpenLDAP Foundation. Obtido em 12 de 02 de 2000, de https://datatracker.ietf.org/doc/html/rfc4514
[48] King, R. R. (2003). *Mastering Active Directory for Windows Server 2003.* San Francisco / London: Sybex.
[49] Glenn, W., & Simpson, M. T. (2004). *Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit.* Washington: Microsoft Press, p. 1-6

Todos estes objetos, existentes dentro deste limite administrativo, partilham a mesma base de dados de segurança.

É possível implementar vários domínios, como forma de possibilitar a implementação de algumas fronteiras de segurança, podendo cada domínio ser administrado de formas diferentes, com modelos de segurança distintos e independentes uns dos outros. Com a utilização de domínios, as organizações podem então dividir logicamente as suas infraestruturas de rede, atribuindo diferentes administradores e regras para cada divisão. Em organizações grandes, com vários domínios, é comum existirem diferentes divisões, cada uma responsável pelos próprios domínios[50].

Um domínio da AD é composto por[51]:

- Uma estrutura hierárquica baseada em X.500 de contentores e objetos.
- Um nome de DNS que serve de identificador inequívoco.
- Um serviço de segurança, que autentica os acessos aos recursos, utilizando contas do domínio ou relações de confiança com outros domínios.
- Uma ou mais políticas que definem as restrições de funcionalidades para os utilizadores e máquinas do domínio.

O nome de DNS (este tema será abordado mais à frente, com maior detalhe) utilizado pelo domínio é conhecido como o espaço de nomes (do inglês *namespace*) e, ao ser criado um domínio, o nome de DNS desse domínio segue a estrutura de nomes DNS. Por exemplo, um servidor com o nome DC num domínio com o nome `esmt.local` teria um *fully qualified domain name* (FQDN) de `dc.esmt.local`.

Um domínio pode ser composto por várias partições ou contextos de nomes. O DN de um objeto inclui informação suficiente para localizar uma réplica da partição onde esse objeto está localizado. Contudo, por vezes o DN do objeto de destino que se pretende identificar, ou a partição onde este se encontra, pode ser desconhecida. É aqui que entra um componente, designado por *global catalog*[52] (GC), ou catálogo global, que contém uma réplica parcial de todos os contextos de nomes do diretório, bem como o *schema* e a configuração dos contextos de nomes, permitindo, dessa forma, encontrar objetos da AD em toda a árvore de diretórios, a partir de um ou mais atributos do objeto que se pretende localizar. Isto significa que o GC contém uma réplica de cada objeto do diretório, mas apenas armazena uma quantidade pequena dos seus atributos (os mais habitualmente utilizados nas operações de pesquisa e os necessários para localizar a réplica total dos dados do objeto).

---

[50] Glenn, W., & Simpson, M. T. (2004). *Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit.* Washington: Microsoft Press, p. 1-6

[51] Allen, R., & Lowe-Norris, G. A. (2003). *Active Directory, 2nd edition* (2ª ed.). O'Reilly

[52] Microsoft (Ed.). (17 de 08 de 2020). Global Catalog. Obtido em 12 de 02 de 2022, de Microsoft Documentation: https://docs.microsoft.com/en-us/windows/win32/ad/global-catalog

5.2.1.4. Árvores

A organização de múltiplos domínios é feita utilizando uma estrutura hierárquica designada por árvores (do inglês *tree*)[53]. Mesmo que só exista um domínio na AD, existe sempre uma árvore. O primeiro domínio a ser criado numa árvore é designado como domínio raiz (em inglês *domain root*) dessa árvore de domínios. Os domínios que forem criados posteriormente serão designados como domínios filho (em inglês, *child domain*) do domínio a partir do qual são criados. Todos estes domínios utilizarão um esquema de nomes contíguo e partilharão o mesmo esquema de objetos[54].

Por exemplo, se o domínio raiz fosse esmt.local, e fosse criado um domínio abaixo deste com o nome PFS, este domínio seria identificado pelo nome `pfs.esmt.local`. Deste modo, todos os domínios da árvore de domínios teriam na sua identificação o nome do domínio raiz, que identifica toda a árvore em si (no exemplo dado, a árvore é identificada pelo nome do primeiro domínio, ou seja, `esmt.local`).

A segurança entre múltiplos domínios ou entre múltiplas florestas é estabelecido através de relações de confiança de domínios (*domain trusts*) e relações de confiança de florestas (*forest trusts*). O fluxo de comunicações entre domínios que tenham relações de confiança é indicado pela direção dessa confiança (a confiança pode ser atribuída de forma unidirecional, bidirecional, transitiva ou não transitiva)[55].

Uma característica de uma árvore de domínios é que todos os domínios têm, entre si, uma relação de confiança bidirecional e, implicitamente, transitiva entre si, o que permite que os utilizadores de cada um dos domínios possa aceder e autenticar-se nos restantes domínios.

No exemplo a seguir, podemos ver um possível desenho de uma árvore de domínios:

[53] Glenn, W., & Simpson, M. T. (2004). Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit. Washington: Microsoft Press.
[54] Allen, R., & Lowe-Norris, G. A. (2003). *Active Directory, 2nd edition* (2ª ed.). O'Reilly
[55] Microsoft (Ed.). (29 de 12 de 2021). How trust relationships work for resource forests in Azure Active Directory Domain Services. Obtido em 12 de 02 de 2022, de Microsoft Docs: https://docs.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust

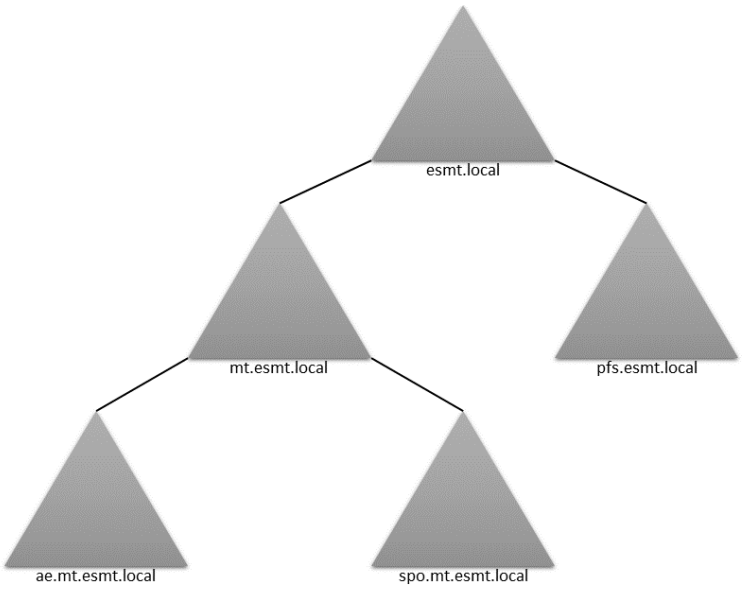


Figura 5.2 - Árvore de domínios

5.2.1.5. Florestas

Ao ser criado o domínio `esmt.local`, automaticamente é criada uma árvore, cujo nó raiz é esse mesmo domínio, como atrás foi apresentado. Na realidade, também é automaticamente criada uma floresta, onde essa árvore pertence, sendo que o domínio raiz da árvore é também o domínio raiz da floresta[56].

Uma floresta é um grupo de uma ou mais árvores de domínio que não forma um espaço de nomes contíguo, mas que podem partilhar o mesmo esquema (*schema*) e catálogo global (*global catalog*)[57].

Para organizações com mais do que um espaço de nomes DNS, o modelo de árvores tem de permitir a expansão para fora dos limites de uma única árvore[58] e é aqui que entram as florestas (em inglês, *forest*). Assim, se além da árvore de domínios `esmt.local`, uma entidade também tivesse uma outra árvore de domínios cujo nome DNS atribuído era `cfetvl.net`, como é que ambas as árvores poderiam pertencer à mesma estrutura de AD? É para isso que existem florestas.

Pegando no exemplo apresentado, do domínio `esmt.local`, se fosse adicionada outra árvore à floresta, cujo domínio raiz fosse cfetvl.local, ao pertencerem à mesma floresta, seria estabelecida uma relação de confiança bidirecional entre essas árvores de domínio.

---

[56] Allen, R., & Lowe-Norris, G. A. (2003). *Active Directory, 2nd edition* (2ª ed.). O'Reilly

[57] Glenn, W., & Simpson, M. T. (2004). Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit. Washington: Microsoft Press.

[58] Glenn, W., & Simpson, M. T. (2004). Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit. Washington: Microsoft Press.

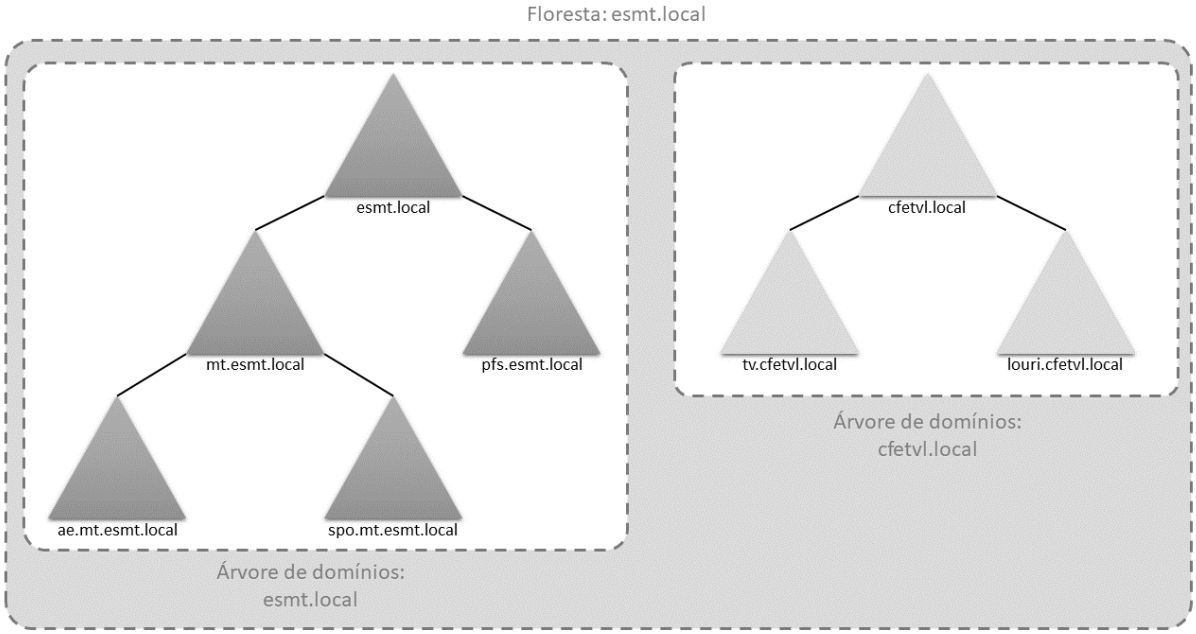


Figura 5.3 - Floresta com várias árvores de domínios

5.2.1.6. Unidades Organizacionais

As Unidades Organizacionais (ou OUs, de *Organizational Units*) são contentores no âmbito de um domínio que possibilitam agrupar objetos que partilham de uma configuração ou administração comum[59]. São, então, fronteiras administrativas que se podem criar num domínio, que além da parte organizativa, também permitem delegar tarefas administrativas. É possível, deste modo, criar várias OUs e colocar nestes objetos que tenham alguma relação entre si (que incluem utilizadores, grupos, computadores, ou outras OUs), e delegar direitos administrativos a essa OU e todo o seu conteúdo[60].

Ao se instalar um domínio de AD, são criados automaticamente um conjunto de contentores e de unidades organizacionais padrão, que incluem o contentor *Users* e o contentor *Computers*, bem como a OU *Domain Controllers*[61].

5.2.2. Estrutura física de rede da Active Directory

Depois de termos analisado a estrutura lógica da *Active Directory*, pode-se observar o quão simples é a sua estrutura física de rede, composta por Domain Controllers (alguns com funções especiais atribuídas), pelo Global Catalog Server, pelos *sites* e *site links*.

[59] Holme, D., & Thomas, O. (2006). Managing and Maintaining a Microsoft Windows Server 2003 Environment. Washington: Microsoft Press.
[60] Glenn, W., & Simpson, M. T. (2004). Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit. Washington: Microsoft Press.
[61] Allen, R., Desmond, B., Lowe-Norris, A. G., & Richards, J. (2013). Active Directory (5.ª ed.). Sebastopol: O'Reilly.

5.2.1.1. Controladores de domínio

Um controlador de domínio (*domain controller* – DC) é um servidor que tem instalado uma versão do Windows Server e onde os serviços de Active Directory foram implementados. Num domínio, podem-se adicionar os DC que se quiser a um domínio e cada um destes servidores terá uma cópia completa (uma réplica) da partição de diretório desse domínio. Por esta razão, os DCs funcionam no designado *multimaster model*, ou seja, um modelo de replicação em que cada servidor é autónomo, com a sua própria cópia do diretório, que pode, autonomamente, realizar operações padrão de alterações ao diretório e, posteriormente, replicar essas alterações para outros domínios automaticamente[62]. Torna-se evidente que esta cópia da base de dados do diretório pode ser lida ou escrita pelo servidor, o que permite, por exemplo, que seja modificada a palavra-passe de um utilizador em qualquer um dos DCs existentes no domínio, pois esta é automaticamente propagada para os restantes DCs[63].

No Windows Server antes da versão 2012, o processo era de um único passo, mas a partir do Windows Server 2012, a instalação da *Active Directory* é feita em dois passos: primeiro é adicionado o papel de *Active Directory Domain Services* (AD DS) ao servidor, através da instalação dos ficheiros (binários), que incluem os componentes do Windows necessários para permitir a um servidor poder agir como um *domain controller*[64].

Os DCs resolvem localmente os pedidos de informação acerca dos objetos do próprio domínio e reencaminham para os DCs apropriados os pedidos de informação de objetos de outros domínios[65]. Faz ainda parte das responsabilidades dos DCs, registarem as alterações à informação existente no diretório, bem como de replicar essas alterações para os restantes DCs do domínio.

Há, contudo, alguns papéis que apenas um DC pode. Estes papéis são conhecidos pela designação FSMO, do inglês *flexible single-master operations*[66] executar (pode ser escolhido qualquer um dos DC para o executar, daí a palavra *flexible*, mas apenas um o executa, daí o *single-master*).

5.2.1.1.1. FSMO

Estes papéis estão divididos em dois grupos: os papéis a nível de toda a floresta (*Forest-Wide Roles*) e os papéis a nível de domínio (*Domain-Wide Roles*)[67].

---

[62] Active Directory Infrastructure Self-Study Training Kit: Windows Server 2012 and R2. (2015). East Olympia: Stanek & Associates.
[63] Glenn, W., & Simpson, M. T. (2004). Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit. Washington: Microsoft Press.
[64] Active Directory Infrastructure Self-Study Training Kit: Windows Server 2012 and R2. (2015). East Olympia: Stanek & Associates.
[65] Glenn, W., & Simpson, M. T. (2004). Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit. Washington: Microsoft Press.
[66] King, R. R. (2003). Mastering Active Directory for Windows Server 2003. San Francisco / London: Sybex.
[67] Glenn, W., & Simpson, M. T. (2004). Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit. Washington: Microsoft Press.

Forest-Wide Roles – são dois os papéis existentes que apenas podem ser desempenhados por um único DC em toda a floresta:

Mestre de Esquema (*Schema Master*) – O primeiro DC da floresta terá este papel, que tem a responsabilidade pela manutenção e distribuição do esquema ao resto da floresta. É neste servidor que é mantida a lista de todos as classes de objetos que podem ser criados, bem como dos atributos que definem os objetos existentes na AD, sendo fundamental a sua existência e operacionalidade aquando da atualização ou alteração do esquema. Basicamente, este é o DC responsável por controlar a estrutura da base de dados da AD[68].

Mestre de Nomes do Domínio (*Domain Naming Master*) – É o DC que tem a tarefa de registar as adições ou supressões de domínios em toda a floresta, função que é vital para que a integridade do domínio não seja comprometida, pelo que este DC é questionado ao ser realizado o processo de adição de um novo domínio à floresta. Por outras palavras, sem a sua existência, ou sem estar operacional, não é possível adicionar um novo domínio à floresta. Este papel pode ser atribuído a qualquer DC da floresta.

Domain-Wide Roles – existem três papéis existentes que apenas podem ser desempenhados por um único DC em cada domínio:

Mestre de Identificadores Relativos (*Relative ID Master*, ou *RID Master*) – A sua função é distribuir blocos de RIDs a todos os DCs do domínio. Um SID (*Security Identifier*) é um identificador único que cada objeto da AD possui, composto por duas partes: uma primeira parte, comum a todo o domínio, ao qual é adicionado o RID, a segunda parte deste SID. Deste modo, o SID permite identificar de forma inequívoca cada objeto, bem como especificar onde este foi criado. Ao ser adicionado um DC, o servidor com a função de RID Master atribui-lhe um conjunto de RID (variável com a versão do Windows Server) e, quando estas se esgotam, o DC pode requerer mais ao servidor com a função de RID Master[69]. Apesar de ser possível a um utilizador iniciar sessão utilizando o UPN (User Principal Name) ou o nome de conta SAM (*Security Accounts Manager*), o sistema referenciará o utilizador para o processo de autenticação utilizando o SID[70].

Emulador de Controlador de Domínio Primário (*Primary Domain Controller Emulator*, ou *PDC Emulator*) – Originalmente criado para fornecer compatibilidade com domínios do Windows NT 4.0, é responsável por coordenar as alterações às palavras-passe, bloqueio das contas, bem como pelo sincronismo temporal. Este é também o servidor alvo da grande maioria das ferramentas de gestão de Group Policy.

[68] King, R. R. (2003). Mastering Active Directory for Windows Server 2003. San Francisco / London: Sybex.
[69] Regan, P. (2013). Administering Windows Server 2012: Exam 70-411. Hoboken: Wiley.
[70] Allen, R., Desmond, B., Lowe-Norris, A. G., & Richards, J. (2013). Active Directory (5.ª ed.). Sebastopol: O'Reilly.

Mestre de Infraestrutura (*Infrastructure Master*) – Este DC regista as alterações que digam respeito aos objetos de um domínio. Outra responsabilidade deste DC é gerir os grupos e os membros dos grupos. Deste modo, todas as alterações são, em primeira instância, comunicadas a este DC, e depois replicadas para os restantes (partindo deste DC a iniciativa de fazer essa replicação.

((Número de domínios) * 3) + 2)

Tabela 5.5 - Fórmula para cálculo do número de servidores FSMO necessários numa floresta

Utilizando a fórmula anterior[71], pode-se calcular quantos papéis são necessário atribuir em toda a floresta que, no caso extremo de se pretender atribuir cada papel em servidores diferentes, implicaria o mesmo número de DCs.

5.2.1.1.2. Global Catalog Server

Este servidor mantém um subconjunto dos atributos dos objetos da AD mais comuns de serem utilizados nas pesquisas (por exemplo, o nome de início de sessão). A sua função é muito importante e centra-se, essencialmente, em possibilitar o início de sessão em rede aos utilizadores, e permitir encontrar quaisquer objetos em toda a floresta.

O *Global Catalog Server* pode ser acedido através do protocolo LDPA (porta 3268) ou através de LDAP/SSL (porta 3269), sendo que este é acedido em modo de leitura apenas e não pode ser atualizado de forma direta[72].

5.2.1.1.3. Níveis de funcionalidade do domínio e da floresta

À medida que foram saindo novas versões do Windows Server, nem todos os DCs de um domínio ou de toda a floresta de domínios são migrados. Por essa razão, a Microsoft implementou um mecanismo que permite definir quais são as funcionalidades das novas versões que podem ser utilizadas no domínio e na floresta. A esta funcionalidade a Microsoft chamou "functional levels" e, basicamente, tem de ser configurado de acordo com a versão mais baixa existente nos controladores de domínio[73] (do domínio ou da floresta, consoante se pretenda definir o nível de funcionalidade do domínio ou o da floresta).

5.2.1.2. Site

Um *site* é um grupo de controladores de domínio existentes em uma ou mais sub-redes IP. Geralmente cada site tem as suas fronteiras definidas de acordo com a localização de uma rede de área local. Por outras palavras, se existirem múltiplas redes de área locais ligadas entre si por

[71] Snedaker, S. (2004). Best Damn Windows Server 2003 Book Period. Rockland: Syngress.
[72] Allen, R., Desmond, B., Lowe-Norris, A. G., & Richards, J. (2013). Active Directory (5.ª ed.). Sebastopol: O'Reilly.
[73] Panek, W. (2015). MCSA Windows Server 2012 R2 Administration Study Guide: exam 70-411. Indianapolis: Sybex.

conectividade WAN com ligações rápidas e estáveis, o uso de *sites* é fundamental para que possa implementar uma tecnologia de segmentação de tráfego.

Os *sites* não são parte do espaço de nomes do domínio, ou seja, ao se percorrer o espaço de nomes lógico, pode-se ver os utilizadores e computadores agrupados em domínios e OUs, sem existir quaisquer referências a *sites*. Nos *sites* encontram-se apenas referências a DCs existentes no site e ligações que permitem estabelecer conectividade com outros *sites*.

Site link – a replicação de informações dos objetos, num *site*, acontece de forma automática, mas para que esta aconteça entre vários *sites*, tem de existir uma ligação física entre esses *sites*.

5.2.3. DNS

O DNS é fundamental para que todo o ambiente de rede do Windows funcione, pois é como se fosse a linha de vida do ambiente de rede Windows[74].

Os computadores comunicam entre si de forma digital, ou seja, através de zeros e uns. Isto é válido para toda a informação utilizada pelos computadores, quer se trate de ficheiros, de páginas de Internet, de vídeos, de imagens ou de qualquer comunicação entre computadores. No que respeita à comunicação entre computadores, num ambiente de rede, o Windows utiliza endereços IP e endereços MAC, que mais não são do que representações de 32 bits em quatro grupos de 8 bits (apresentados no formato decimal) separados por um ponto (IPv4) ou de 6 bytes (apresentados no formato hexadecimal) separados pelos dois pontos (":") ou por um hífen ("-").

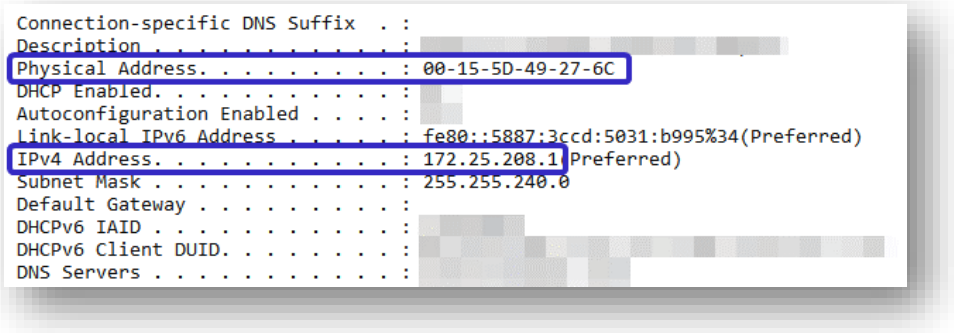


Figura 5.4 - Exemplo de endereço MAC e IP

No entanto, as pessoas preferem trabalhar com nomes, que utilizem para representar os computadores e outros recursos, pelo que tem de existir uma forma de resolver os nomes utilizado pelos humanos em números utilizados pelos computadores e vice-versa. É aqui que entra a resolução de nomes e, sem este mecanismo, não seria possível as pessoas ligarem-se aos recursos através de

[74] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). *Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System.* Rockland: Syngress, p. 3

nomes facilmente identificáveis. É, então, uma tarefa importante de um administrador de rede, desenhar e implementar uma estratégia eficiente de resolução de nomes numa rede informática[75].

O DNS é muito importante para a *Active Directory*, pois a AD utiliza os registos DNS do tipo SRV para localizar todos os serviços de que necessita para funcionar corretamente.

5.2.4. Políticas de Grupo

Uma das ferramentas mais poderosas que estão disponíveis num ambiente de *Active Directory* são as Políticas de Grupo (*Group Policy*).

Segundo Jeremy Moskowitz, o nome "Group Policy" vem da perspetiva da Microsoft de que esta se refere ao "agrupamento de políticas de configurações" (Moskowitz, 2004)[76].

Assim, as Group Policies são, na verdade, um conjunto de regras que podem ser aplicadas e forçadas em diversos níveis da AD, o que permite obter um grau elevado de capacidades de manipulação dos computadores cliente, e uma elevada eficiência na aplicação das mesmas a estes computadores. É através do uso de Group Policy que se potencializa as capacidades de gestão e administração da *Active Directory*[77].

Convém discriminar os vários termos associados às políticas de grupo, nomeadamente:

- *Group Policy* – é o conceito em si, apresentado atrás.
- *Policy setting* (configuração de política) – é apenas uma das configurações possíveis de manipular para atingir um determinado objetivo de configuração, na máquina cliente.
- GPO ou Group Policy object (objeto de política de grupo) – é um item de configuração, existente nos controladores de domínio, que é onde, efetivamente, é definido e guardado um conjunto de configurações de política.

Cada GPO, ao ser criada, tem todas as configurações definidas para o estado "Não configurado", ou seja, não afetam nenhuma configuração. Assim, uma determinada configuração pode ser definida para outros dois estados: "Ativado" ou "Desativado", que afetam, dessa forma, a maneira como essa configuração é aplicada no utilizador ou na máquina[78].

---

[75] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). *Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System.* Rockland: Syngress, p. 336

[76] Moskowitz, J. (2004). Group Policy, Profiles, and IntelliMirror for Windows 2003, Windows XP, and Windows 2000. San Francisco / London: Sybex, p. xviii

[77] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System. Rockland: Syngress.

[78] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System. Rockland: Syngress.

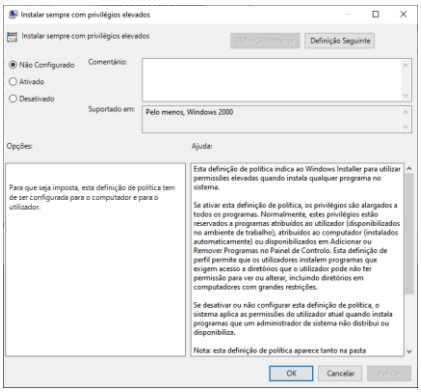


Figura 5.5 - Estados possíveis de uma configuração de política de grupo

Podemos ter, na sua forma mais granular, uma *Group Policy* que apenas especifica uma única configuração de política[79].

As políticas de grupo podem ser aplicadas a máquinas individuais, a conjuntos de máquinas, a um utilizador, a um conjunto de utilizadores, e a uma mistura entre utilizadores e máquinas. Estas permitem, então, controlar os utilizadores, os computadores e grupos de utilizadores a partir de um local centralizado[80]. Isto é conseguido, atribuindo um GPO a um contentor, que pode ser qualquer dos que Moskowitz (Moskowitz, 2004) designa como os três níveis que constituem a *Active Directory*: *site*, domínio ou OU[81] e influenciará todos os objetos nestes contidos.

No entanto, salvo algumas exceções, é às OUs que normalmente se atribuem GPOs como forma de gestão automática de uma série de configurações que se pretende que afetem um determinado grupo de utilizadores, ou de máquinas, ou de uma mistura de ambos. Aliás, as GPOs só podem ser aplicadas, ou seja, apenas afetam as definições associadas ou aos utilizadores, ou às máquinas (e de mais nenhum objeto ou contentor)[82].

Os GPOs são constituídos por dois componentes: um objeto da *Active Directory* e uma pasta armazenada no SYSVOL dos controladores de domínio[83].

[79] Holme, D., & Thomas, O. (2004). MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296. Washington: Microsoft Press

[80] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System. Rockland: Syngress.

[81] Moskowitz, J. (2004). Group Policy, Profiles, and IntelliMirror for Windows 2003, Windows XP, and Windows 2000. San Francisco / London: Sybex.

[82] King, R. R. (2003). Mastering Active Directory for Windows Server 2003. San Francisco / London: Sybex.

[83] Holme, D., & Thomas, O. (2004). MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296. Washington: Microsoft Press

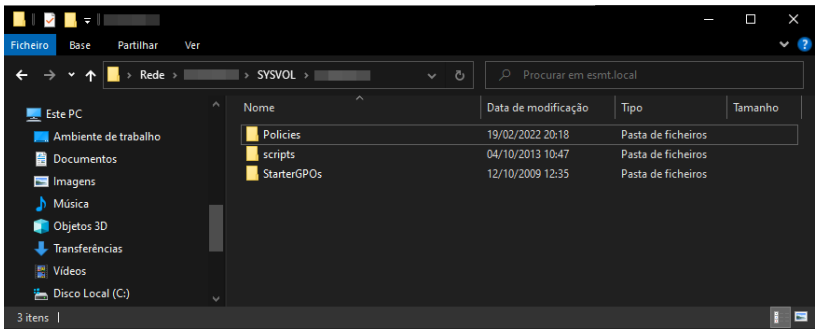


Figura 5.6 - Pasta SYSVOL onde são armazenados os ficheiros associados aos GPO

Na raiz de cada GPO existem dois nós, um para as configurações do computador e outro para as configurações do utilizador:

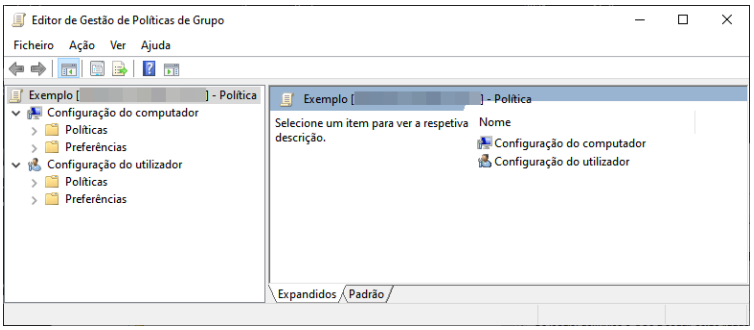


Figura 5.7 - Nós principais existentes num GPO

Desta forma, os objetos do tipo "utilizador" irão herdar as políticas definidas no nó "Configuração do utilizador", ao passo que os objetos do tipo "computador" herdarão as políticas definidas no nó "Configuração do computador"[84].

Em termos gerais, a lista apresentada de seguida apresenta os tipos de políticas que podem ser criadas (e forçadas) através do editor de políticas de grupo[85]:

Políticas de instalação de software – estas políticas afetam as aplicações que os utilizadores podem instalar a partir da rede. De uma forma genérica, a instalação pode ser realizada de uma das duas seguintes formas:

Aplicação Atribuída – A aplicação é instalada ou atualizada automaticamente, pela política de grupo. Esta instalação é despoletada quando o computador arranca, quando o utilizador inicia sessão ou quando a aplicação é utilizada pela primeira vez.

Aplicação Publicada – A políticas de grupo faz com que a aplicação seja apresentada na lista de aplicações disponíveis que o utilizador pode instalar ou remover, de forma manual.

Políticas de Scripts – Permitem que um administrador especifique um ou mais scripts que devem ser executados durante os processos de início ou término de sessão ou durante o arranque ou o encerramento do computador.

---

[84] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System. Rockland: Syngress.
[85] King, R. R. (2003). Mastering Active Directory for Windows Server 2003. San Francisco / London: Sybex.

Políticas de Segurança – Permitem variadas formas de implementar segurança na infraestrutura, quer através da restrição de acesso a ficheiros e pastas, quer por configurações de chaves do Registo para controlar serviços do sistema ou as aplicações que são executadas nos computadores, limitando certos privilégios a determinados utilizadores ou grupos de utilizadores, ou ainda definir parâmetros gerais para a complexidade ou outras configurações das palavras-passe.

Políticas de redireccionamento de pastas – Permitem alterar a localização de algumas pastas especiais do sistema (como, por exemplo, a pasta "Os meus documentos" ou a pasta "Ambiente de trabalho").

Políticas de Componentes de Software – Na sua maioria compostas por políticas baseadas no Registo, pelo que trabalham de forma idêntica às Políticas de Sistema. Estas permitem configurar vários componentes do software integrante do sistema operativo Windows, bem como muitas definições do sistema operativo em si.

As políticas irão sempre sobrepor-se a quaisquer configurações que o utilizador tenha feito, bem como a quaisquer alterações efetuadas por scripts. Além disso, como são atualizadas em intervalos de tempo definidos no sistema, não só aplicam as suas configurações como as forçam a permanecer aplicadas[86].

Desta forma, com o uso de Group Policy, podemos tirar proveito de toda a estrutura lógica da AD, nomeadamente através do domínio, de sites e da estrutura de OU, bem como da capacidade de segurança, imposição ou bloqueio das aplicações das mesmas, a qualquer nível hierárquico dessa estrutura[87].

Em termos gerais, as opções de configuração associadas aos computadores, definidas no nó "**Configuração do computador**" da política de grupo, podem ser utilizadas para[88]:

- Instalar aplicações durante o processo de arranque do computador.
- Melhorar a segurança do sistema.
- Especificar que scripts devem ser executados no arranque e no encerramento do computador.
- Definir configurações de componentes de software que sejam para aplicar a todos os utilizadores de um computador.

[86] Holme, D., & Thomas, O. (2004). MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296. Washington: Microsoft Press.

[87] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System. Rockland: Syngress.

[88] King, R. R. (2003). Mastering Active Directory for Windows Server 2003. San Francisco / London: Sybex.

Também em termos gerais, mas relativamente às opções de configuração associadas aos utilizadores, definidas no nó "**Configuração do utilizador**" da política de grupo, estas podem ser utilizadas para[89]:

- Instalar aplicações durante o processo de início de sessão do utilizador.
- Especificar que scripts devem ser executados no início e término de sessão do utilizador.
- Bloquear algumas definições do utilizador, quer ocultando ícones do ambiente de trabalho quer removendo opções de configuração.
- Definir configurações de componentes de software que sejam específicos para o utilizador.

As GPO são herdadas entre níveis hierárquicos da AD. Esta herança começa a nível da Group Policy que possa estar configurado localmente num computador e, de seguida, para a Group Policy definida a nível de *site*. O próximo nível a ser aplicado é o do domínio, seguindo-se a Group Policy que se encontra no topo da hierarquia de OUs que existam, sendo aplicados, sequencialmente, a cada nível das OUs, à medida que se desce nessa hierarquia, terminando na OU onde o utilizador ou o computador se encontram.

Caso ocorram conflitos na aplicação de políticas dos vários níveis, a política a ser aplicada é a que se encontra mais perto do local onde o utilizador ou computador efetivamente se encontra. Assim, num cenário em que uma determinada política de grupo esteja definida nos 4 níveis (computador local, *site*, domínio, OU), a da OU é a que efetivamente será aplicada[90].

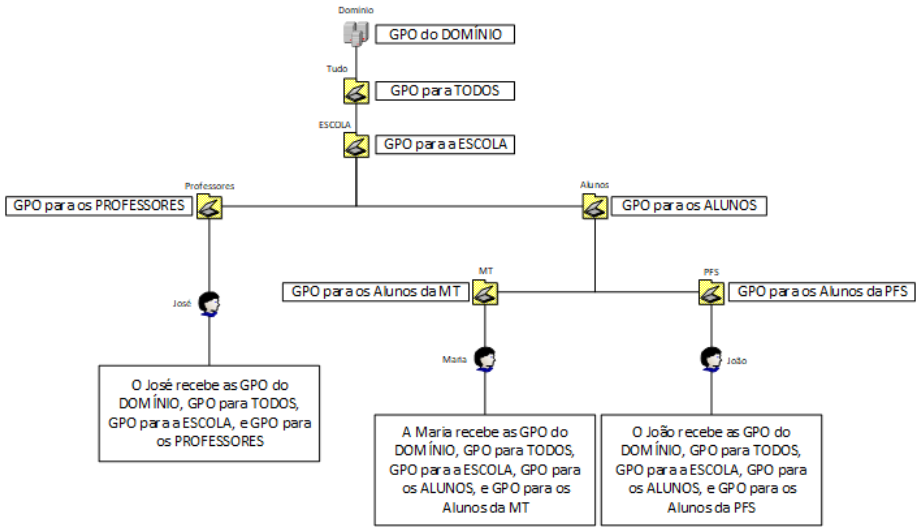


Figura 5.8 – Exemplo de aplicação de Group Policy com herança

No entanto, podemos desativar esta herança a um determinado nível da hierarquia. Por exemplo, caso se tenha aplicado uma Group Policy a nível da ESCOLA, mas se pretenda excluir os PROFESSORES dessas definições de configuração, podemos bloquear a herança de GPO para a OU Professores. Tal prática, contudo, impede que nenhuma Group Policy seja gerada, o que pode trazer alguns problemas

[89] King, R. R. (2003). Mastering Active Directory for Windows Server 2003. San Francisco / London: Sybex.
[90] Moskowitz, J. (2004). Group Policy, Profiles, and IntelliMirror for Windows 2003, Windows XP, and Windows 2000. San Francisco / London: Sybex.

de desenho no modelo de aplicação de Group Policy pretendido, razão pelo qual se recomenda[91] que se opte pelo desenho de uma estrutura de Group Policy que funcione no modelo de herança, em detrimento de um que funcione com quebras na mesma.

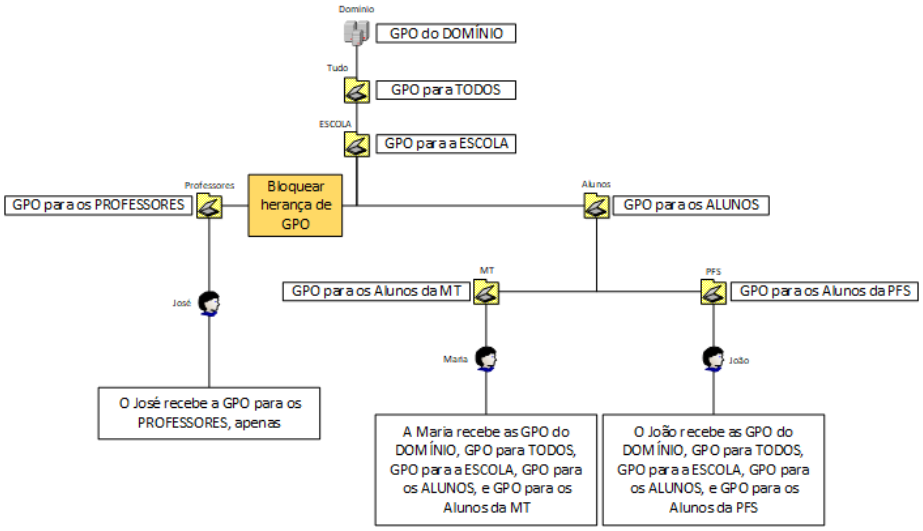


Figura 5.9 - Exemplo de aplicação de Group Policy com herança bloqueada num ramo

5.3. Moodle

Como parte da Profissionalização em Serviço, que terminei em 2003, investiguei muito acerca dos Centros de Recursos Educativos associados às Bibliotecas Escolares, e muitos dos exemplos de projetos de implementação obtive da Austrália.

Foi durante essas pesquisas que me deparei com o Moodle[92], uma plataforma de gestão de aprendizagens, em código-aberto e gratuita.

A palavra Moodle é um acrónimo para Modular Object-Oriented Dynamic Learning Environment, e este projeto tinha em mente construir uma plataforma para trabalho colaborativo, utilizando a filosofia denominada de "pedagogia sócio construtivista".

Pareceu-me claro que o futuro passaria pela utilização destas plataformas e modelo de trabalho, e poder ter uma solução gratuita e em código aberto, era algo muito adequado para a realidade da escola/agrupamento, que não tinha recursos financeiros para investir em plataformas pagas e proprietárias. Aliás, o falhanço da plataforma Class Server, da Microsoft, nas escolas, deveu-se, em grande escala, aos custos a esta associados após o primeiro ano de utilização (que foi gratuito).

[91] Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System. Rockland: Syngress.
[92] About Moodle. (2020, 08 31). Retrieved 02 27, 2022, from Moodle: https://docs.moodle.org/311/en/About_Moodle

Uma vez mais, com poucas ou nenhumas escolas a utilizar esta plataforma, em 2003, investiguei, li a documentação, e implementei o Moodle (versão 1.1) recorrendo a mais um servidor Linux, com a distribuição CentOS e o resto da plataforma LAMP[93].

Figura 5.10 - Página Moodle do AEMT

Analisei as várias hipóteses de criação de contas de utilizadores e descobri que era possível fazer a integração do Moodle com a Active Directory, o que foi "ouro sobre azul", a nível de integração. Desta forma, utilizando o nome de utilizador SAM definido na AD, e a respetiva palavra-passe, os utilizadores podiam aceder ao Moodle, evitando ter de criar novas credenciais.

Desde 2003, com a versão 1.1[94], o Moodle cresceu até à versão 3.11 e, durante esta ano, sairá a versão 4. Ano após ano fui fazendo as atualizações de versões, instalado recursos que não faziam parte da distribuição oficial (denominados plugins), especialmente os desenvolvidos pela *Open University*, de Inglaterra, que incluíam muitos tipos de questões para poderem ser utilizados nas fichas de avaliação.

Ao olhar para trás, vejo hoje o quão ambicioso este projeto foi: tentar implementar um sistema de b-learning (*blended learning* ou ensino misto, no sentido de misturar o regime presencial e o regime a distância), algo que só com a pandemia as escolas e a comunidade educativa, muito renitente à utilização destas tecnologias, se viram forçados a adotar.

Algumas versões obrigaram a reconfigurações das versões da distribuição Linux, à atualização das versões do software que constitui a plataforma LAMP, e a implementar novos visuais a nível da interface web.

[93] LAMP. (2021, 12 28). Retrieved 02 27, 2022, from Wikipédia.
[94] Moodle Releases. (2022, 03 14). Retrieved 03 20, 2022, from Moodle Docs: https://docs.moodle.org/dev/Releases

Apesar de ter iniciado a utilização desta plataforma, a nível das escolas do concelho de Torres Vedras, fruto da boa comunicação existente, principalmente com as Escola Básica de São Gonçalo e Escola Básica Padre Vítor Melícias, nas pessoas de Rui Vaz e Artur Santos, respetivamente, rapidamente também implementaram esta plataforma e, conjuntamente, fomos desenvolvendo e explorando a sua utilização, quer melhorando a componente técnica, quer, principalmente, a componente pedagógica (relacionada com uma utilização eficaz da mesma).

Com o apoio do Centro de Formação das Escolas de Torres Vedras e Lourinhã, chegámos (nessa altura, já apenas o Artur Santos e eu) a desenvolver um projeto de implementação desta plataforma, começando por juntar todos os diretores de agrupamentos destes concelhos, e depois com uma turma de formação para professores em cada escola destes agrupamentos.

No entanto, muitos diretores não conseguiram entender esta visão e nem todos deram continuidade a este projeto, mas que se manteve em muitas outras escolas em funcionamento.

Um dos grandes problemas apontados à utilização desta plataforma é o interface gráfico, algo que está a ser trabalhado nesta versão 4, prevista para este ano de 2022.

Em termos de segurança, implementei certificados SSL de acesso ao servidor (utilizando certificados Let's Encrypt[95], de uma autoridade certificadora sem fins lucrativos, que os disponibiliza gratuitamente). Estes certificados permitem a comunicação segura e encriptada da informação entre um navegador de Internet e um servidor Web (permitindo, por exemplo, enviar o nome de utilizador e a palavra-passe de forma segura).

Tendo um servidor Web na nossa infraestrutura, aberto para a Internet, e onde os utilizadores iniciam sessão com as credenciais da Active Directory, impunha a configuração de alguns mecanismos de segurança.

Entre esses, utilizei o *Fail2ban* e a proteção do acesso aos servidores através do pacote gratuito da *Cloudflare*.

O Fail2ban[96] é uma ferramenta que se instala no sistema operativo Linux dos servidores Web, que verifica os ficheiros de log e bane os IPs que demostrem alguma atividade suspeita, como falhas de palavras-passe, pesquisa por fraquezas do sistema, etc.

Quanto ao Cloudflare[97], na sua versão gratuita, permite mitigar ataques DDoS, rápida resolução de nomes DNS e certificado SSL gratuito. Como não tínhamos quaisquer capacidades de responder a este tipo de ataques DDoS, optámos por configurar a conectividade aos nossos servidores através desta plataforma.

---

[95] *Let's Encrypt*. (n.d.). Retrieved 03 20, 2022, from https://letsencrypt.org/

[96] Fail2ban Wiki. (2016, 05 28). Retrieved 02 27, 2022, from Fail2ban: https://www.fail2ban.org/wiki/index.php/Main_Page

[97] Cloudflare free plan. (2022, 02 27). Retrieved from Cloudflare: https://www.cloudflare.com/plans/free/

Resultado destas políticas de segurança, nunca tivemos quebras de serviço resultantes de ataques exteriores, e nunca tivemos os servidores comprometidos com acessos indevidos, ao longo destes quase 20 anos.

Em termos de utilização, temos uma parte considerável de professores a fazerem uso da mesma, e um número de acessos diários relevante:

Figura 5.11 - Estatísticas de acesso mensal ao Moodle

5.4. Sistema de Reposição de Computadores

Um dos problemas com o qual, desde o início, me deparei, foi a gestão das aplicações, das atualizações dos sistemas operativos, da análise de problemas que possam estar a acontecer nos computadores. Existindo uma rede informática, onde os computadores se encontram ligados, que soluções poderiam ser utilizadas para fazer esta gestão? Qual a melhor maneira de o fazer? Que custos daí adviriam?

Foram analisadas várias soluções de automatização da implantação de computadores (Microsoft System Center, Symantec Ghost, Clonezilla), mas ou os custos elevados, ou a pouca facilidade de uso, fizeram com que nenhuma destas soluções fosse a indicada.

Mas, durante a pesquisa, deparei-me com uma solução gratuita e de código aberto (*opensource*), que permitia automatizar esse processo e implementar uma série de configurações nos computadores: o FogProject[98] (ou apenas FOG), um projeto de código aberto com licenciamento GPL[99], ou seja, pode

[98] Fog Wiki. (2016, 03 09). Retrieved 02 27, 2022, from FogProject: https://wiki.fogproject.org/wiki/index.php?title=Introduction

[99] The GNU General Public License. (2022, 01 10). Retrieved 02 27, 2022, from GNU Operating System: https://www.gnu.org/licenses/gpl-3.0.en.html

ser utilizado na quantidade de computadores que for pretendida, de forma gratuita, e que o código fonte está disponível e pode ser alterado por quem o desejar.

O FOG é mais do que apenas uma solução de reposição/clonagem de imagens em computadores, é também uma solução de gestão de rede, que inclui as seguintes características:

- Ambiente de arranque em PXE (DHCP, iPXE, TFTP, e rápida transferência HTTP dos grandes ficheiros de arranque, como o *kernel* e o *initrd*)
- Solução de imagens Windows (XP, Vista, 7, 8/8.1, 10), Linux e Mac OS X
- Partições, disco na totalidade, múltiplos discos, redimensionamento dos discos, *raw*
- Extras (*snap ins*) que permitem instalar software e executar tarefas/scripts nos computadores cliente
- Gestão de impressoras
- Alteração do nome do computador e possibilidade de adicionar o computador a um domínio da Active Directory de forma automática
- Registo do acesso de utilizadores aos computadores, possibilidade de terminar as sessões automaticamente e de desligar os computadores
- Possibilidade de utilizar uma solução de antivírus
- Limpeza total e segura de discos
- Recuperação de ficheiros apagados
- Teste a blocos de disco com problemas

Os seus criadores vêm de um *background* educativo, onde muitas vezes era necessário repor as imagens dos computadores constantemente. Pareceu-me claro que era uma solução a ponderar, pelo que investiguei nos fóruns e no site do projeto como o poderia implementar no ambiente de rede do AEMT.

Sendo baseado em LAMP[100], criei, então, um servidor Linux (a distribuição CentOS), onde configurei o Apache, o MySQL e o PHP, necessários para o FOG. Configurei o servidor de DHCP do Windows para que respondesse aos pedidos de arranque em PXE e criei imagens para os modelos padrão das máquinas existentes.

[100] LAMP. (2021, 12 28). Retrieved 02 27, 2022, from Wikipédia.

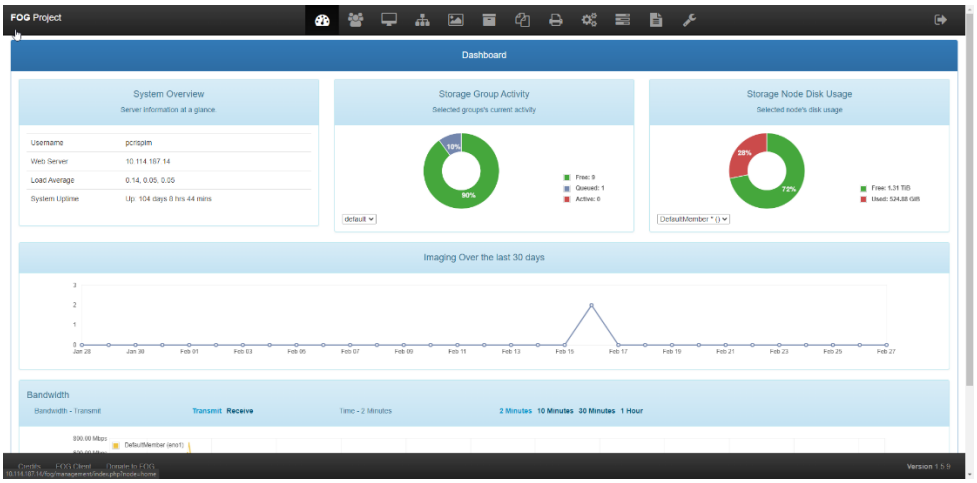


Figura 5.12 - Página de entrada do FOG

Apesar de não conseguir gerir a instalação de software, como pretendia, pelo menos conseguia criar várias imagens que poderia depois implementar nos computadores de forma automática.

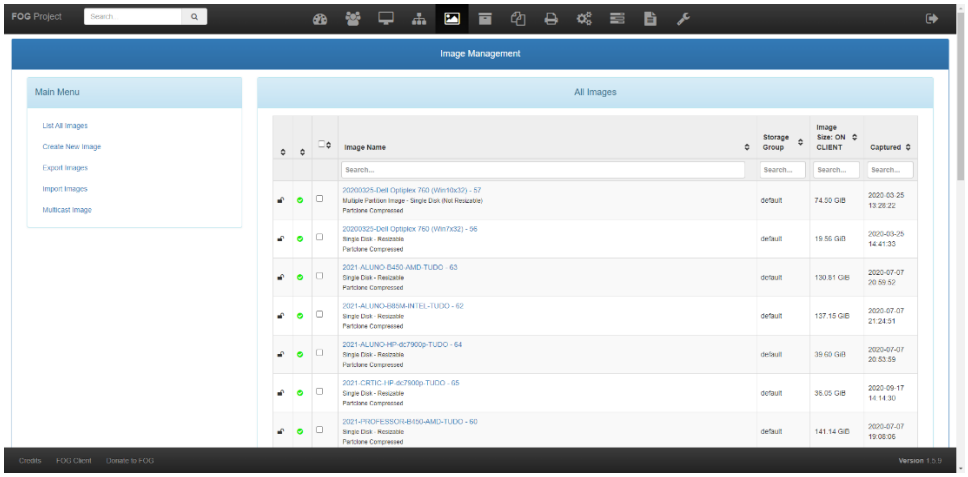


Figura 5.13 - Imagens de computadores no FOG

Nestas imagens incluía o sistema operativo desejado, as atualizações do mesmo, o Office e as aplicações padrão fundamentais (Acrobat Reader, Adobe Flash, compressão/descompressão de ficheiros ZIP, navegadores de Internet, software didático, etc.) que todos os computadores deveriam ter, bem como algum software específico para determinados computadores (os dos Cursos Profissionais e Salas TIC).

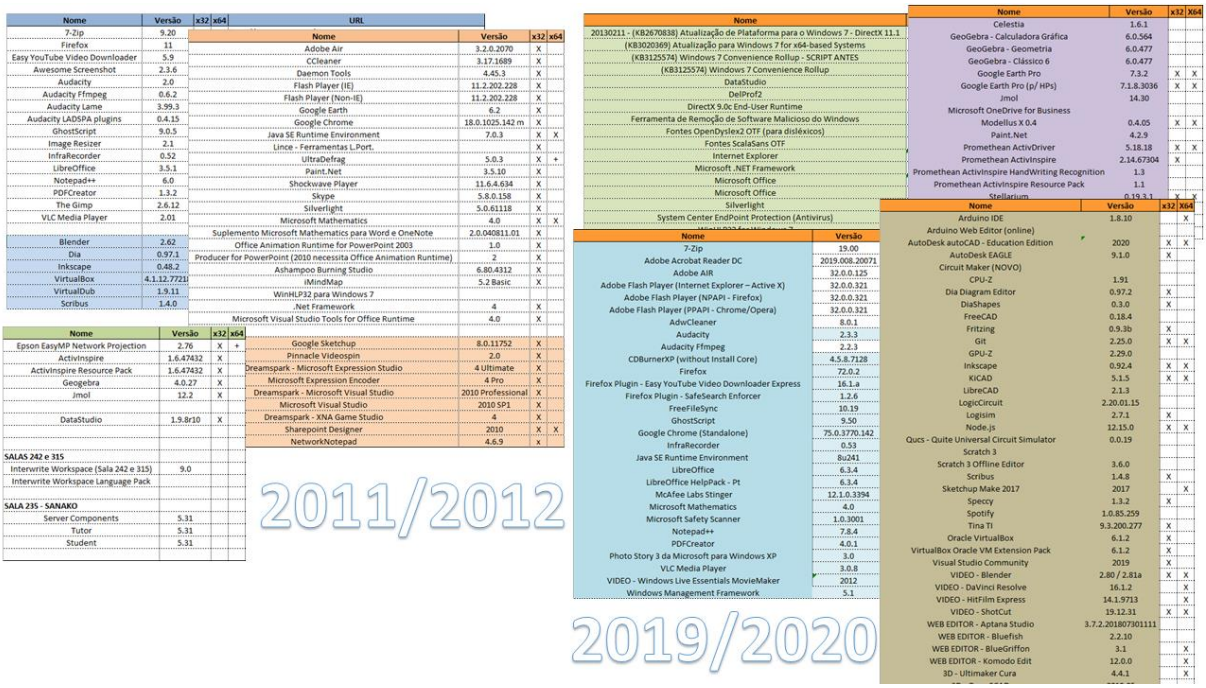


Figura 5.14 - Tabela comparativa do software instalado nas imagens dos computadores

Além disso, no FOG podia definir o nome dos computadores (que era realizado imediatamente após os computadores serem repostos) e adicioná-los ao domínio da Active Directory, bem como configurar as impressoras e proceder ao licenciamento do Windows e do Office, utilizando scripts[101].

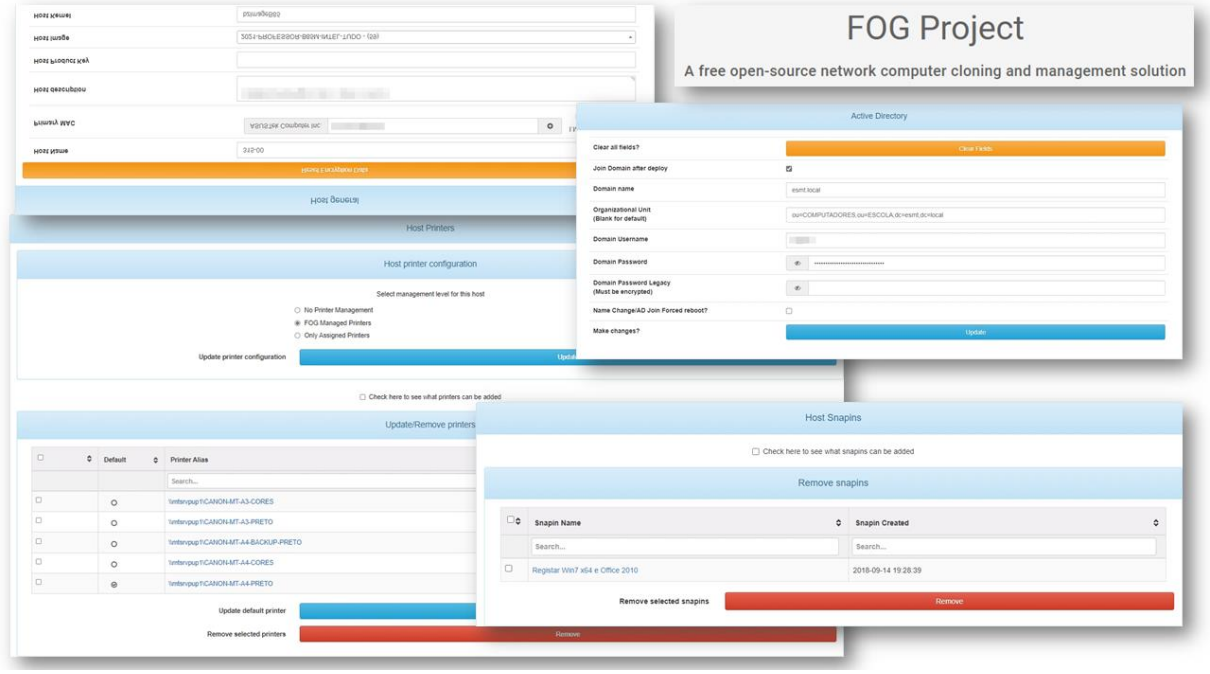


Figura 5.15 - Exemplos de ecrãs de configuração de computadores no FOG

Com a implementação deste sistema, no final de cada ano letivo consigo fazer a preparação do ano letivo seguinte, através da reposição da quase totalidade dos computadores, com imagens contendo

101 *Managing FOG*. (2020, abril 30). Retrieved março 25, 2022, from FOG Wiki: https://wiki.fogproject.org/wiki/index.php?title=Managing_FOG#Snap-ins

todo o software (sistema operativo e aplicações) necessário e atualizado, permitindo ter o computador num estado limpo de credenciais e de configurações dos utilizadores, facto que só é possível realizar porque os ficheiros dos utilizadores são armazenados na rede e não em cada computador local, como será apresentado mais à frente, neste relatório.

5.5. Sistema VoIP

Paralelamente à implementação da rede estruturada IP de que a escola foi alvo em 2007/2008, no âmbito do PTE, propus à direção da escola utilizarmos um serviço de telefonia IP, em vez do modelo tradicional e proprietário que existia.

Esta proposta visava tornar a escola mais independente do fabricante, podendo escolher entre uma variedade de equipamentos de telefonia (gateways, telefones, placas RDIS, entre outros) e ficando com capacidade de aumentar o número de pontos de telefone sem necessitar de fazer qualquer pagamento, bastando comprar e configurar os equipamentos.

Para isso, foi feita uma pesquisa de mercado e escolhida uma empresa que instalasse o sistema FreePBX[102]. Foram então adquiridas as placas de interface BRI para fazermos uso das ligações RDIS[103], um servidor e foi instalado o sistema. Criei, posteriormente, as versões traduzidas para português, dos manuais dos telefones, para os utilizadores poderem utilizar, após ter dado formação de como utilizar, e instalei um servidor de FAX virtual (necessário para os serviços administrativos, na altura).

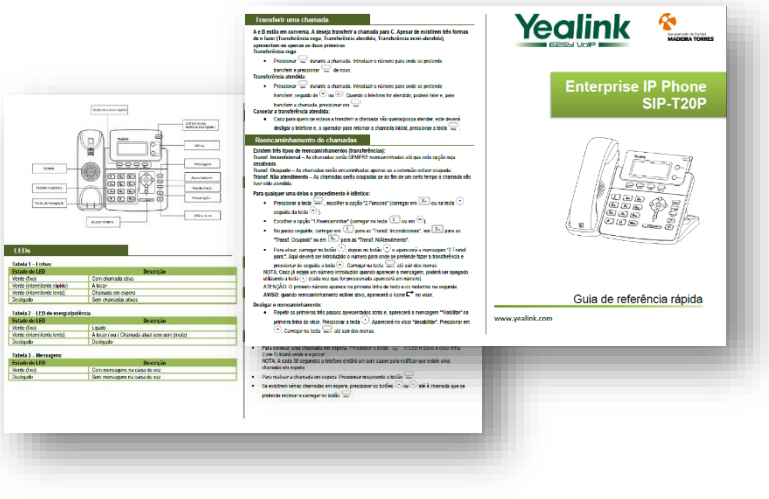


Figura 5.16 - Manuais telefones VoIP em português (traduzidos pelo autor)

Após utilização deste sistema, existe uma grande flexibilidade na utilização do sistema de telefonia, podendo as 3 escolas que se encontram ligadas por fibra ótica (JI+EB1 Padre Francisco Soares, EB23 Padre Francisco Soares e ES Madeira Torres) comunicar entre si, internamente. É ainda possível

[102] *FreePBX*. (n.d.). Retrieved 03 20, 2022, from https://www.freepbx.org/
[103] *Acesso analógico, acesso RDIS básico e acesso RDIS primário*. (2004, março 09). Retrieved março 25, 2022, from ANACOM: https://www.anacom.pt/render.jsp?categoryId=99559

deslocar qualquer extensão para qualquer ponto do edifício onde exista uma ligação de rede ou, noutros casos, utilizar telefones wireless (como no caso do campo de futebol, onde não existe nenhum ponto de rede, mas o telefone se encontra ao alcance de um ponto existente na Biblioteca Escolar).

Além desta flexibilidade, foi feita uma poupança enorme, em termos de custos, pois deixamos de ter contratos de manutenção, necessidades de intervenções técnicas (em 8 anos de serviço, foram precisas apenas 2 intervenções: uma para mudança de servidor, outra para uma atualização ao sistema, para suportar a nova matriz de conectividade da escola, e tornar o processo de configuração dos telefones VoIP ainda mais rápido).

5.6. Virtualização

5.6.1. Estudo da implementação

Alguns dos grandes desafios que se colocam nos nossos dias são a utilização eficaz em termos de custos da infraestrutura de TI, a capacidade de dar resposta a novas iniciativas e a flexibilidade na adaptação às mudanças organizacionais constantes. A virtualização é uma tecnologia que desempenha um papel fulcral no alcançar destas premissas, permitindo a implementação de soluções flexíveis e criativas que permitem dar resposta a estes desafios organizacionais[104].

Antes da virtualização

- Um único SO por máquina
- Software e hardware intimamente ligados
- Execução de múltiplas aplicações na mesma máquina geralmente cria conflitos
- Recursos subutilizados
- Estrutura inflexível e onerosa

Após a virtualização

- Independência do hardware para com o sistema operativo e aplicações
- As máquinas virtuais podem ser provisionadas em qualquer sistema
- Gestão do SO e aplicações como uma unidade através do seu encapsulamento em máquinas virtuais

[104] Virtualization Overview. (2006). *White Paper*. Palo Alto, EUA. Obtido em 09 de 04 de 2022, de https://www.vmware.com/pdf/virtualization.pdf

Figura 5.17 - Comparação de sistemas sem e com virtualização

Olhando sob uma perspetiva geral e simplificada, a virtualização é a separação de um recurso ou de pedidos de um determinado serviço, da componente física subjacente a esse pedido ou recurso. Se olharmos para a memória virtual, por exemplo, esta permite que uma aplicação tenha mais memória para a sua execução do que a quantidade real de memória instalada nesse computador. De forma similar, as técnicas de virtualização podem ser aplicadas noutras camadas da infraestrutura de TI (incluindo as redes, o armazenamento, o hardware de computadores, mesmo de servidores, de sistemas operativos e até de aplicações.

Esta mistura de tecnologias de virtualização (também designada por infraestrutura virtual), fornece uma camada de abstração entre o hardware (computação, armazenamento e rede) e as aplicações que nele são executadas[105].

Assim, por alturas da implementação do PTE, existia na EB23 Padre Francisco Soares 1 servidor Fujitsu e na ES Madeira Torres 2 servidores Fujitsu, e o sistema operativo de rede mais avançado era o Windows Server 2008 (que, posteriormente, deu lugar ao Windows Server 2008 R2). Uma das novidades deste sistema operativo foi a introdução do "Virtualization Role"[106], assente na tecnologia de virtualização Hyper-V, da Microsoft.

No entanto, não foi possível aplicar logo essa novidade, por causa das limitações em termos de recursos que existiam na ES Madeira Torres. Não havia redundância de servidores, nem dos recursos existentes no próprio servidor. Foi preciso aguardar que uma outra iniciativa governamental fosse colocada em prática, para que esta situação mudasse: a criação dos mega agrupamentos, em 2011, que no caso do Agrupamento de Escolas Madeira Torres, se efetivou na fusão com o Agrupamento de Escolas Padre Francisco Soares, mantendo o novo agrupamento a designação Agrupamento de Escolas Madeira Torres.

5.6.2. Aquisição de servidores e componentes para aumento da redundância

Assim, para possibilitar a migração para uma topologia de virtualização, foram adquiridos, no processo de agregação que decorreu no final do ano de 2011, dois servidores (HP DL180), uma UPS e um conjunto de extras para os servidores terem redundância a nível de hardware (fontes de alimentação duplas, dois processadores, aumento da memória, placas de rede redundantes). No entanto, por falta de verbas, não foi possível adquirir todo o equipamento pretendido e necessário. Só no final de 2012 existia equipamento para implementar, de forma minimamente segura, a

[105] Virtualization Overview. (2006). *White Paper*. Palo Alto, EUA. Obtido em 09 de 04 de 2022, de https://www.vmware.com/pdf/virtualization.pdf

[106] *Virtualization Role*. (2012, 02 07). Retrieved from Changes in Functionality in Windows Server 2008: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc755090(v=ws.10)

virtualização. Fundamental foi, também, a atualização a nível de sistemas operativos de rede, para o Windows Server 2012, cujas licenças também foram adquiridas no final de 2012.

5.6.3. Implementação de segurança física para os servidores (datacenter)

Para complementar as mais valias inerentes ao processo de virtualização, foi criado um mini *datacenter*, em sala própria, com ar condicionado, e com uma central de monitorização, onde era possível monitorizar os acessos, gravar em vídeo (ativado por deteção de movimento) quem entrava no *datacenter*, monitorizar a temperatura, a humidade e até a ocorrência de inundações. Foi instalado um gateway de SMS através do qual poderia receber as mensagens de aviso ou erro relativas a ocorrências no *datacenter*.

5.6.4. Interligação das redes informáticas das escolas EB23 Padre Francisco Soares e ES Madeira Torres

Outra decisão que contribuiu para se avançar com o processo de virtualização dos servidores, foi a junção, por fibra ótica, das redes informáticas das escolas EB23 Padre Francisco Soares e ES Madeira Torres. Desta forma, em vez de termos duas redes distintas, passaríamos a ter tudo numa única rede, sendo a gestão centralizada no novo *datacenter* e nos servidores do AE Madeira Torres (passando estes a estar virtualizados). Isto foi relativamente simples, uma vez que estas escolas se encontram num edifício germinado.

Começava a tomar forma a rede do agrupamento, crescendo em volume, mas também a nível de recursos e tecnologias utilizadas.

5.6.5. Link Aggregation

Com as placas de rede adquiridas para os servidores (HP NC365T 4-port NIC), que tinham 4 portas cada, podia implementar também uma série de tecnologias que aumentavam a largura de banda utilizável (as portas das placas de rede e dos *switches*, individualmente, eram de 1 Gbps), enquanto aumentavam a resiliência das comunicações (no caso de falha de uma ou mais placas de rede, o sistema permaneceria em funcionamento).

Assim, implementei esta tecnologia existente no sistema operativo de rede Microsoft Windows Server 2012 (que, no caso do Windows, toma o nome de "NIC Teaming" ou por LBFO, de "Load Balancing and Failover")[107].

Esta tecnologia pode ser implementada de duas formas distintas: *Switch-independent teaming* (que não requer que o switch faça parte desta agregação), ou Switch-dependent teaming (em que o switch faz parte da agregação e em que todas as ligações têm de ser efetuadas no mesmo *switch*). Neste

[107] Windows Server 2012 NIC Teaming (LBFO) Deployment and Management. (s.d.). Obtido de https://www.microsoft.com/en-us/download/details.aspx?id=30160

último caso, existem ainda dois modos de operação distintos[108]: agregação estática (definida pelo IEEE 802.3ad *draft* v1, que consiste em realizar as configurações manualmente, quer no lado do switch, quer no lado do *host*) e agregação dinâmica (definida pelo IEEE 802.1ax, LACP, comumente conhecido como IEEE 802.3ad[109], que permitem, em teoria, a expansão ou redução dos membros agregados; esta configuração implica ativar o LACP nas portas do *switch*).

A implementação escolhida foi com *Switch-dependent teaming*, utilizando agregação estática.

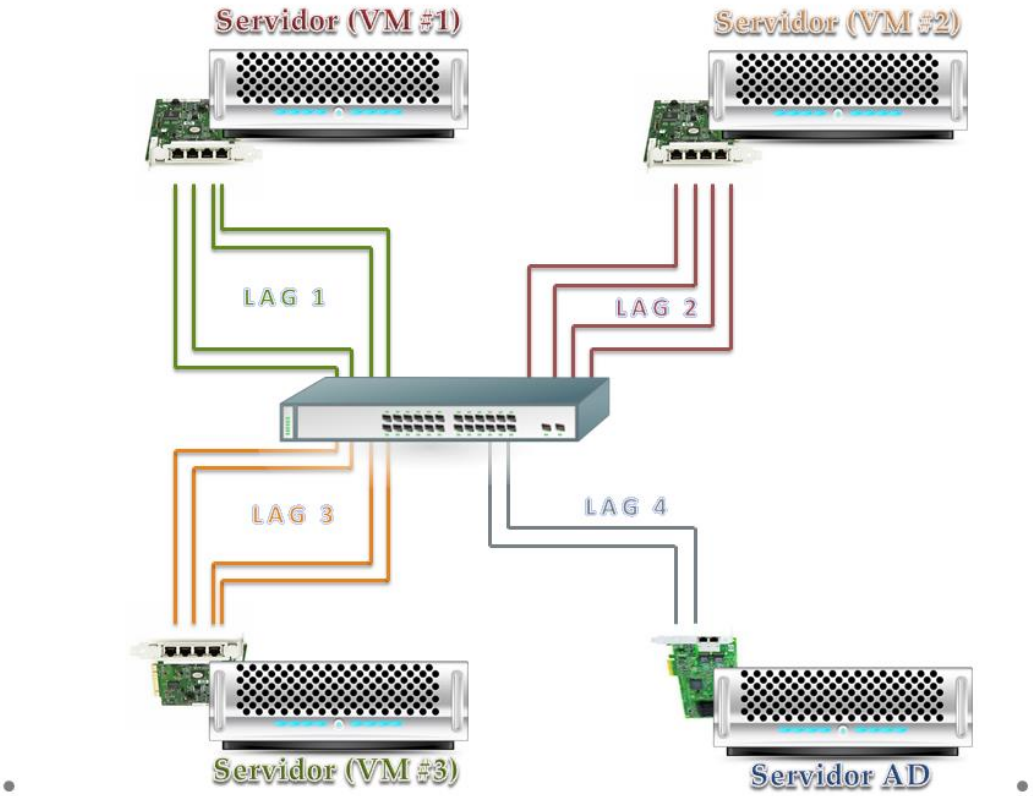


Figura 5.18 - desenho da implementação de LAG na rede do AEMT

5.6.6. Virtualização dos servidores do novo agrupamento

Após a criação do novo Agrupamento de Escolas Madeira Torres, após a junção das escolas numa única rede, após a aquisição de computadores e dos componentes que permitiam a existência de alguma redundância e resiliência (que, efetivamente, só ficaram concluídos no ano letivo 2014/2015), estava na altura de fazer a migração do sistema tradicional de servidores físicos, para o sistema virtualizado, utilizando o Hyper-V, tecnologia existente nos sistemas operativos de rede da Microsoft que o agrupamento agora dispunha (versão Windows Server 2012).

---

[108] Windows Server 2012 NIC Teaming (LBFO) Deployment and Management. (s.d.). Obtido de https://www.microsoft.com/en-us/download/details.aspx?id=30160

[109] *Link aggregation*. (25 de 03 de 2022). Obtido em 09 de 04 de 2022, de Wikipedia: http://en.wikipedia.org/wiki/Link_aggregation

6. EVOLUÇÃO DA REDE INFORMÁTICA DO AEMT

Como foi dito no ponto 5.1., o sistema existente no AEMT, em 2004, consistia em diversos computadores dispersos por toda a escola, especialmente em departamentos, nos serviços administrativos e no gabinete da direção, e ainda por alguns computadores nas salas onde eram lecionadas disciplinas dos Cursos Tecnológicos e Cursos Profissionais, bem como nas mencionadas 2 salas TIC, criadas no âmbito do projeto "1000 Salas TIC".

O que se pretendia, então, era desenvolver um sistema que possibilitasse uma gestão centralizada dos recursos e rede, a administração da segurança, a possibilidade de aceder aos recursos independentemente do computador onde se iniciava sessão, e a utilização dos recursos existentes, de forma partilhada e simples.

A solução passou por criar uma rede estruturada, quer em termos lógicos, quer em termos físicos.

Em termos físicos, foram instalados 9 bastidores de rede na Escola Secundária com 3.º Ciclo de Madeira Torres e 4 bastidores de rede na Escola Básica do 2.º e 3.º Ciclo de Madeira Torres, que, inicialmente eram duas redes fisicamente distintas. Esta implementação foi feita no âmbito do Plano Tecnológico para a Educação. Em cada bastidor de rede existem 2 switches (que podem ser Cisco 3560G ou Cisco 2960G e de 24 ou 48 portas, consoante os switches), uma UPS, uma tomada de fichas de energia, pelos patch panels e respetivos passa cabos (variando o número de acordo com o número de portas existentes).

Em termos de tecnologias, toda a rede estruturada foi criada utilizando cabos e conetores UTP, categoria 6, o que permite utilizar conexões a 1 Gbps.

Em termos de segurança, foram implementados acessos através da norma IEEE 802.1x, o que implica que cada conexão física ligada precisa de ser autenticada num servidor Radius (que no nosso caso era o Edgebox, e cujo acesso era feito utilizando o eRadManager, que "é uma Interface gráfica de utilizador, do inglês GUI - *Graphical User Interface*, que permite configurar determinados parâmetros do Servidor de Autenticação Radius"[110]). Por outras palavras, «o controle de acesso à rede é feito através de um cliente 802.1x, também chamado "*Supplicant*"»[111].

A matriz de implementação inicial, em 2009, era a que se apresenta na imagem seguinte:

[110] *eRadManager - Manual do Administrador - versão 2.2.* (2009). Critical Links.

[111] *Configuração de Clientes 802.1x - Manual de Referência - versão 2.1.* (2009). Critical Links.

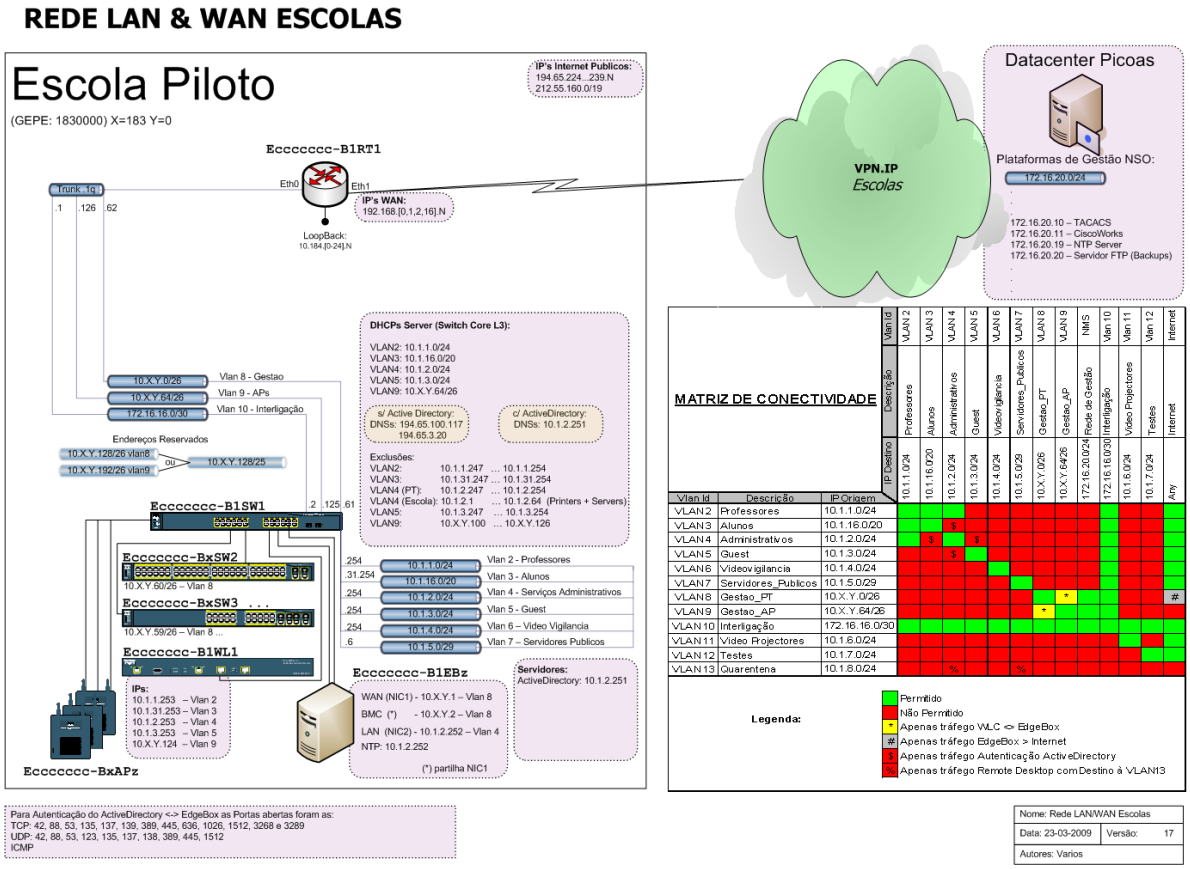


Figura 6.1 – Matriz inicial de conectividade de rede LAN & WAN das escolas

Em 2013 foi feita a primeira grande alteração da matriz, recriando algumas das VLAN co novas funcionalidades, conforme se pode verificar na imagem:

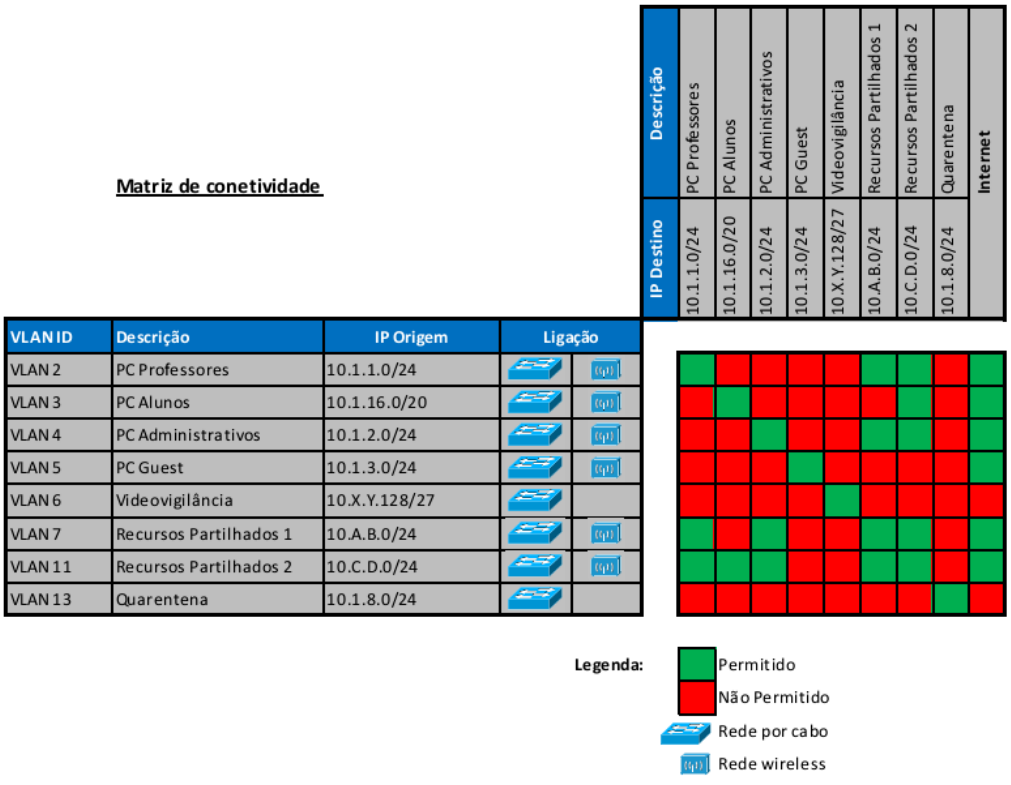
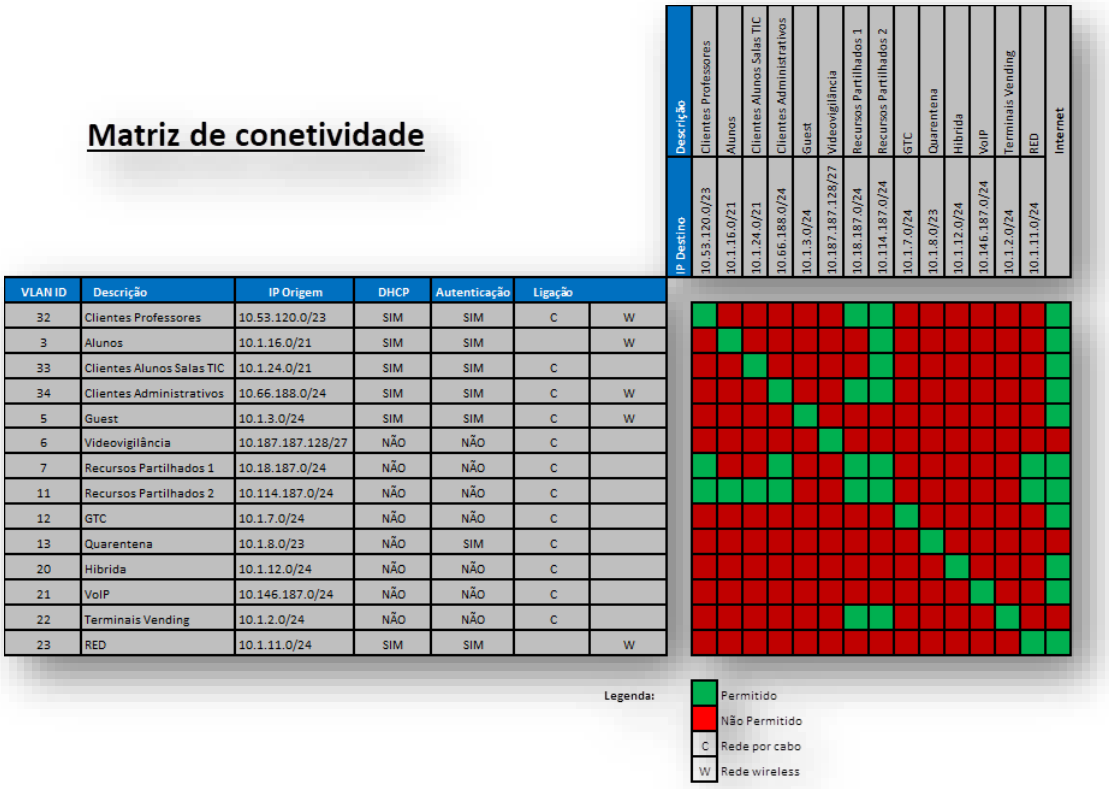


Figura 6.2 - Matriz de conectividade de rede LAN - Alteração de 2013

Em 2017 foi efetuada a alteração para o modelo que está atualmente em vigor:



VLAN ID	Descrição	IP Origem	DHCP	Autenticação	Ligação	
32	Clientes Professores	10.53.120.0/23	SIM	SIM	C	W
3	Alunos	10.1.16.0/21	SIM	SIM		W
33	Clientes Alunos Salas TIC	10.1.24.0/21	SIM	SIM	C	
34	Clientes Administrativos	10.66.188.0/24	SIM	SIM	C	W
5	Guest	10.1.3.0/24	SIM	SIM	C	W
6	Videovigilância	10.187.187.128/27	NÃO	NÃO	C	
7	Recursos Partilhados 1	10.18.187.0/24	NÃO	NÃO	C	
11	Recursos Partilhados 2	10.114.187.0/24	NÃO	NÃO	C	
12	GTC	10.1.7.0/24	NÃO	NÃO	C	
13	Quarentena	10.1.8.0/23	NÃO	SIM	C	
20	Hibrida	10.1.12.0/24	NÃO	NÃO	C	
21	VoIP	10.146.187.0/24	NÃO	NÃO	C	
22	Terminais Vending	10.1.2.0/24	NÃO	NÃO	C	
23	RED	10.1.11.0/24	SIM	SIM		W

Figura 6.3 - Matriz de conetividade atual (dados do AEMT)

Em termos de autenticação, o processo pode resumir-se aos seguintes passos:

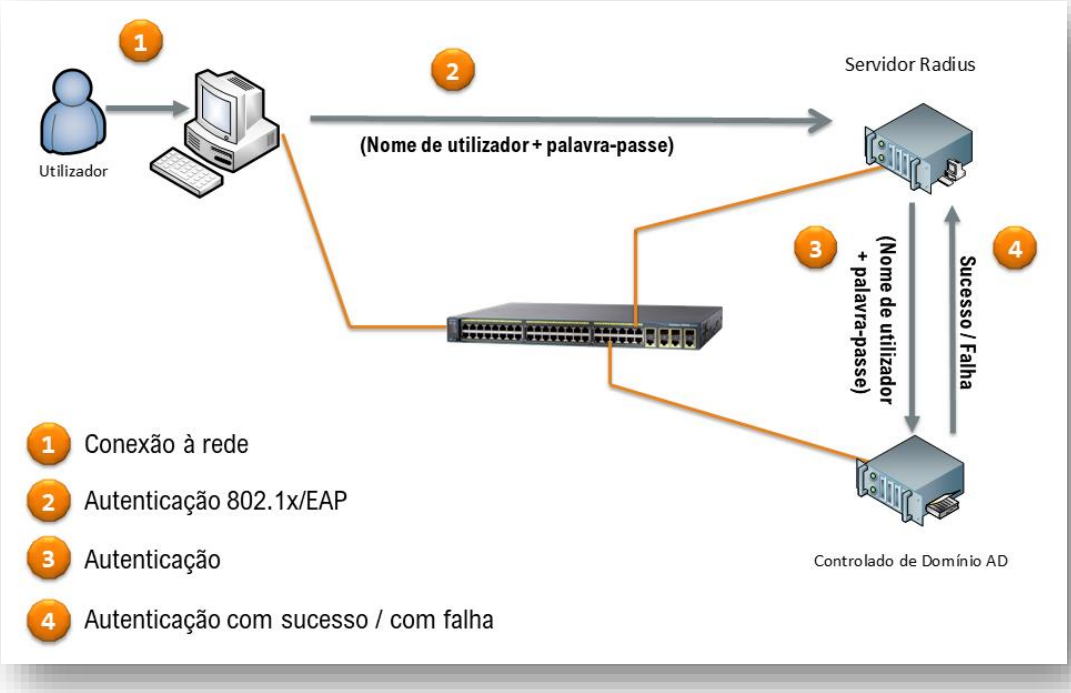


Figura 6.4 - Processo de autenticação Radius - Parte 1

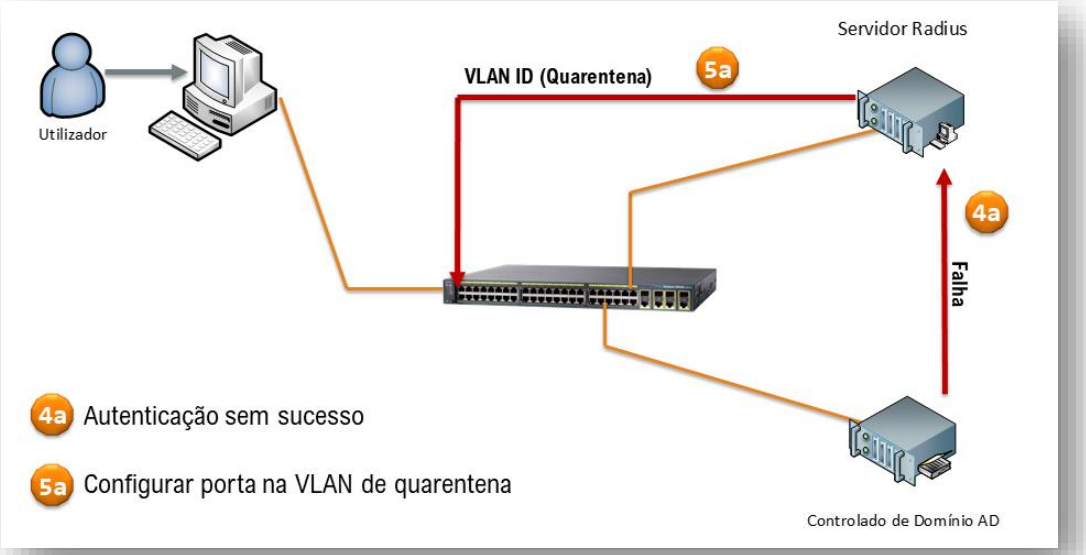


Figura 6.5 - Processo de autenticação Radius - Parte 2

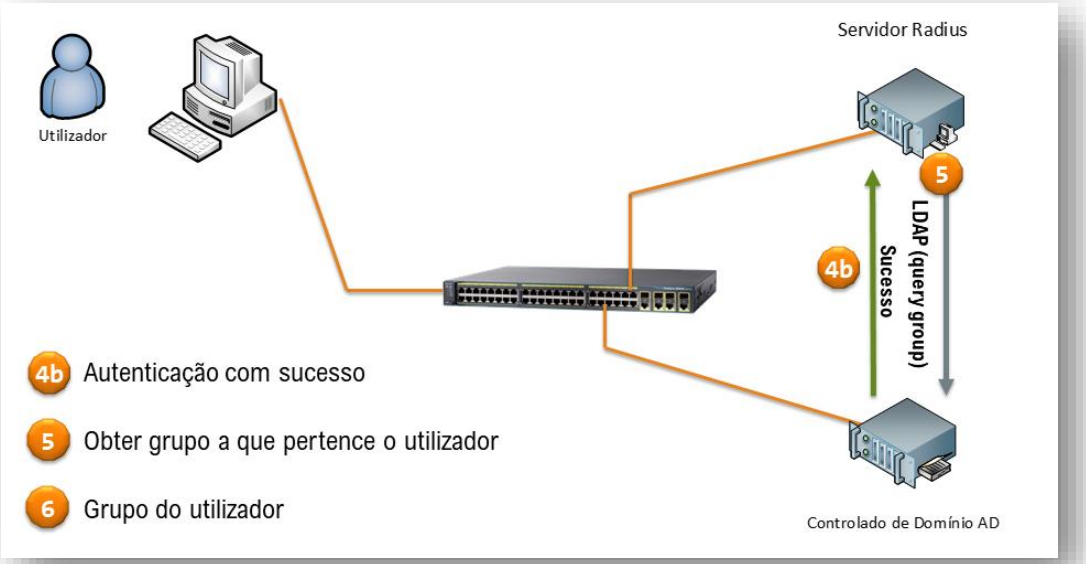


Figura 6.6 - Processo de autenticação Radius - Parte 3

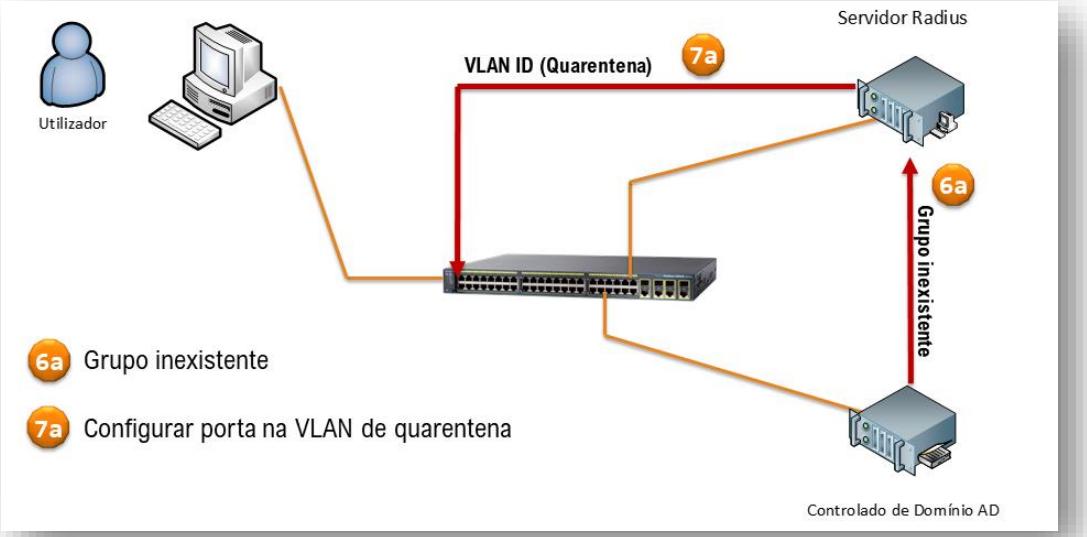


Figura 6.7 - Processo de autenticação Radius - Parte 4

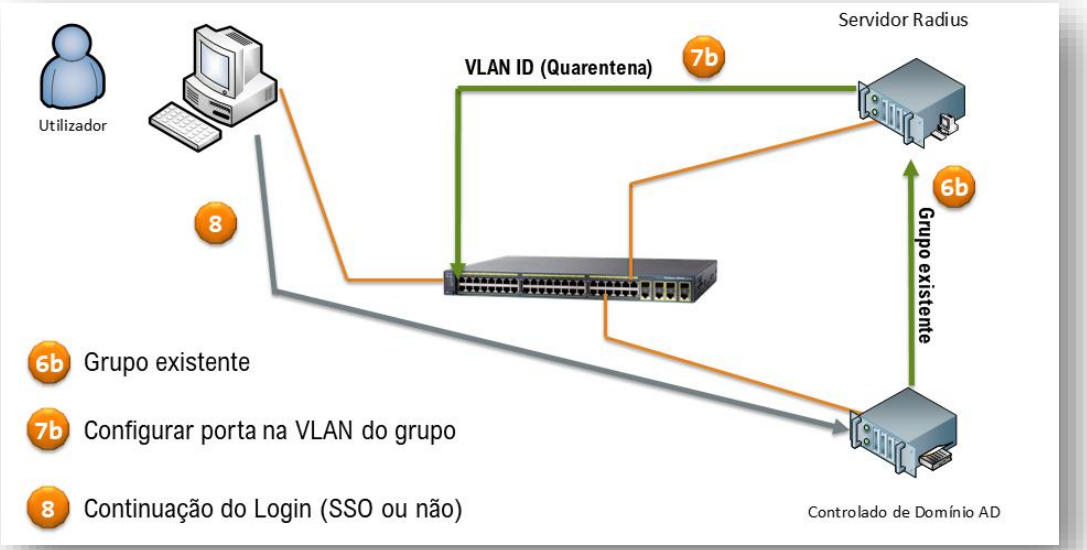


Figura 6.8 - Processo de autenticação Radius - Parte 5

Como é possível depreender das imagens acima, o modelo de autenticação é misto, ou seja, assenta num servidor RADIUS para acesso físico à rede que, por sua vez, define a VLAN em que o utilizador pode aceder. No entanto, essa VLAN é definida com base num grupo ao qual os utilizadores pertencem e que é definido na interface do eRadManager e ao qual associamos um determinado VLAN ID que, ao fim e ao cabo, é o que define o endereço IP atribuído e restantes configurações de rede.

Após essa configuração física da porta de rede, é iniciado o processo de autenticação na Active Directory que validará o utilizador, dando-lhe permissões, ou não, de acesso, com base nas definições

e políticas de grupo definidas na Active Directory. Deste modo, garante-se autenticação e segurança a dois níveis.

Nos subpontos seguintes, é apresentado, esquematicamente, tanto a estrutura lógica e física da rede como a da Active Directory.

6.1. Estrutura física de rede do AEMT

A estrutura física da rede do AEMT tem evoluído bastante, ao longo dos anos. A primeira rede, depois de pronta, tinha o seguinte desenho:

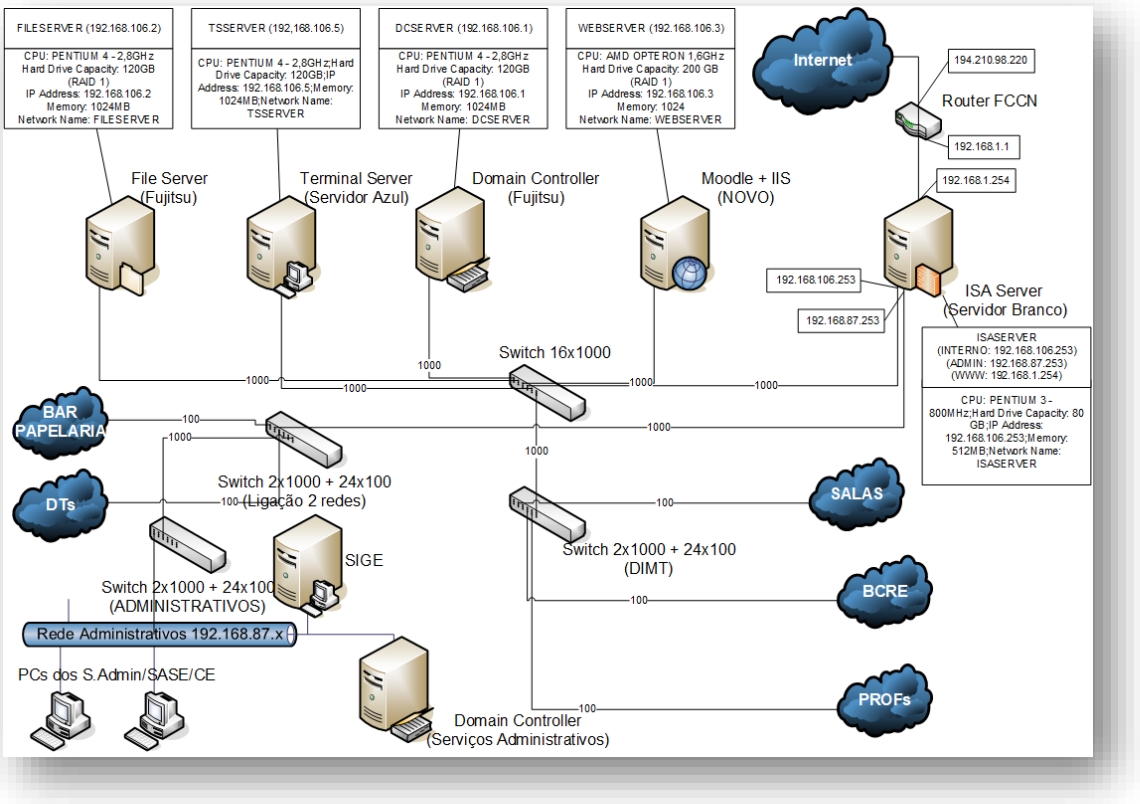


Figura 6.9 - Desenho da rede informática do AE Madeira Torres (2005)

Atualmente, a rede é composta por 13 bastidores dedicados a ligações de rede, e 2 armários com servidores.

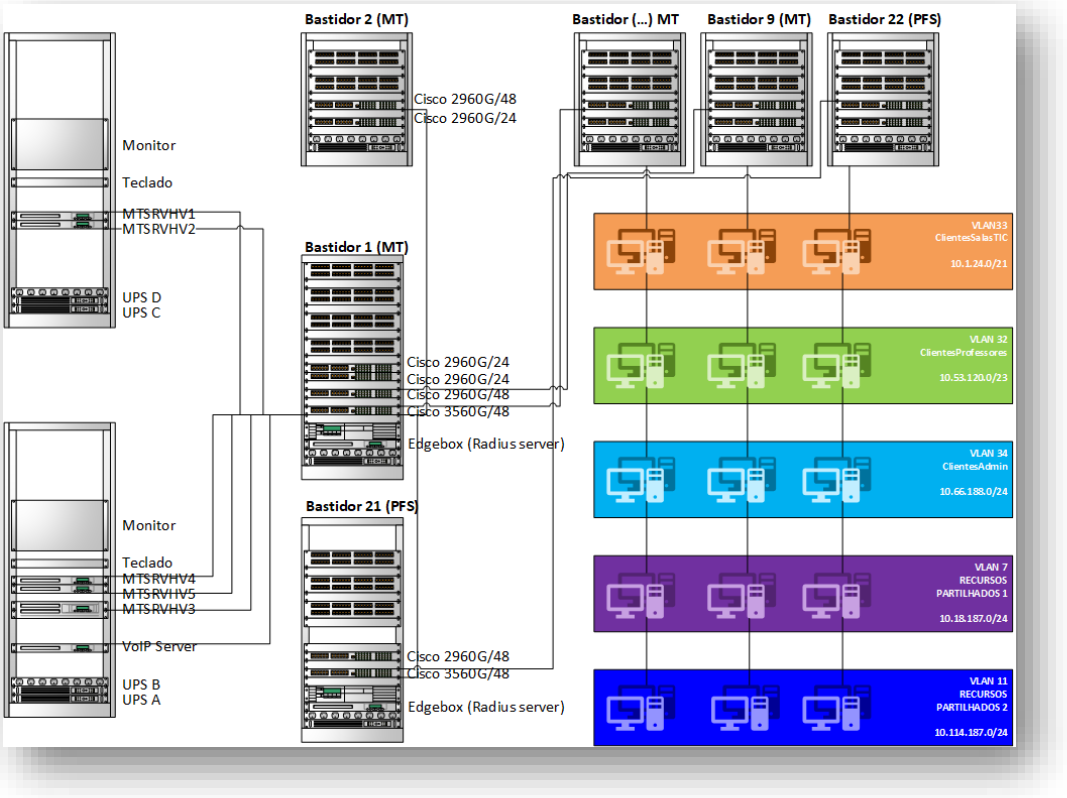


Figura 6.10 - VLANs existentes na rede do AEMT e ligações físicas

Em termos de topologia, os switches são distribuídos, nos primeiros 9 bastidores, da forma que a seguir se apresenta, sendo que o bastidor principal (B1) é aquele onde se encontra o bastidor de core, um Cisco 3560G, identificado com a designação "E1113277-B1SW1". Este é um switch que opera na camada 3 do modelo OSI:

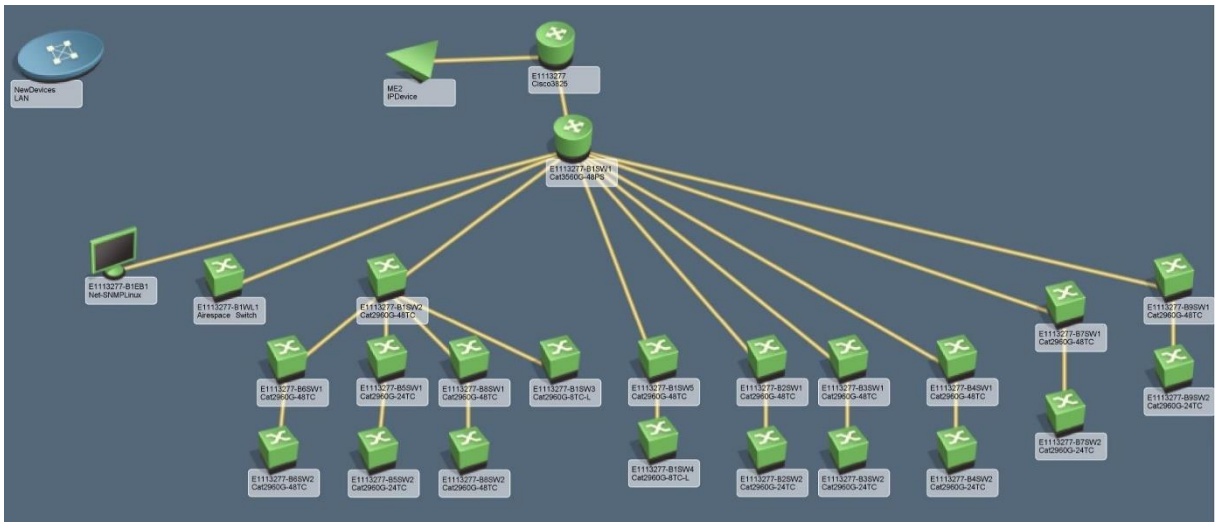


Figura 6.11 - Topologia da rede do AEMT

6.2. Estrutura lógica de rede do AEMT

A estrutura lógica assenta numa série de VLANs, onde as principais são as VLAN dos alunos, dos professores, dos administrativos (todas atribuídas a perfis de autenticação, consoante se trate de um aluno, de um professor ou de um administrativo, respetivamente):

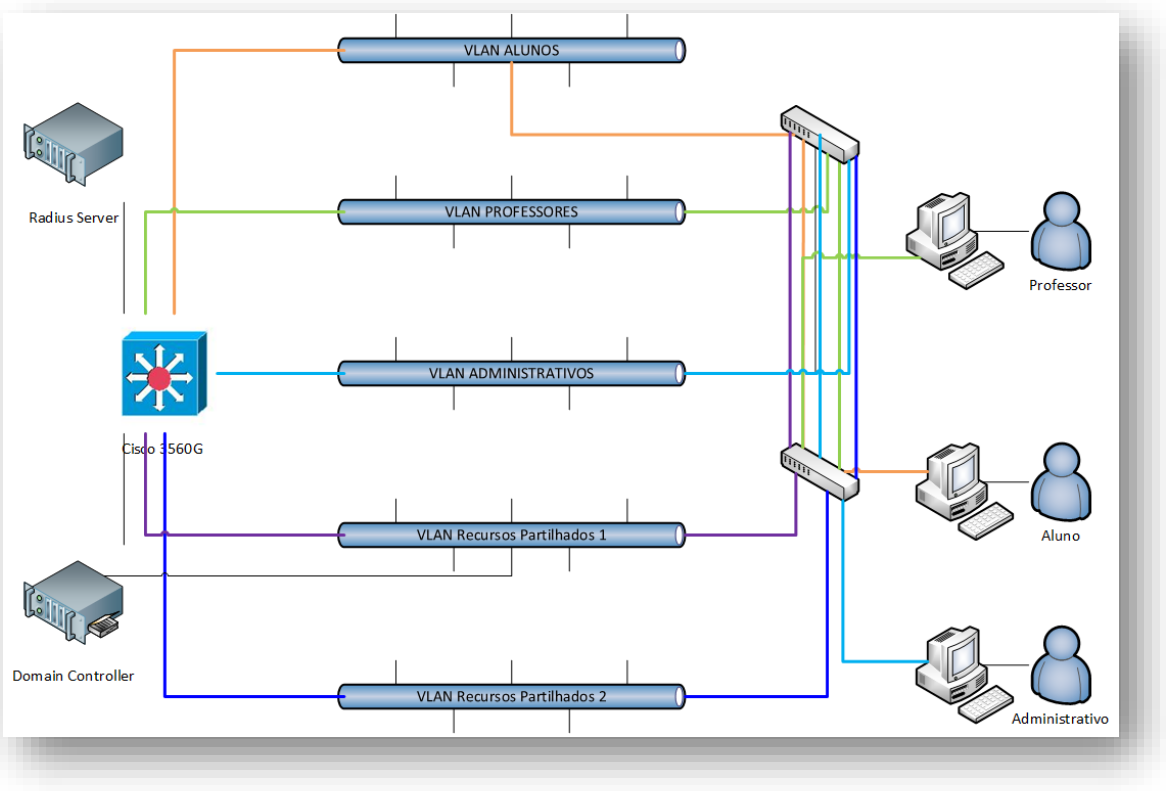


Figura 6.12 - VLANs existentes na rede do AEMT

Também existem VLANs de serviços, identificadas como "Recursos Partilhados 1" e "Recursos Partilhados 2", onde se encontram os servidores a que os utilizadores têm acesso, sendo que os alunos só têm acesso à VLAN "Recursos Partilhados 1", A conectividade entre VLANs é a que se encontra na Figura 22.

6.3. Desenho lógico da Active Directory do AEMT

O desenho da Active Directory é muito simples pois assenta numa única floresta e num único domínio. No entanto, foram criadas imensas Unidades Organizacionais, de forma a poder aplicar todas as Políticas de Grupo necessárias a uma correta configuração e definição de acessos aos recursos do computador e da rede:

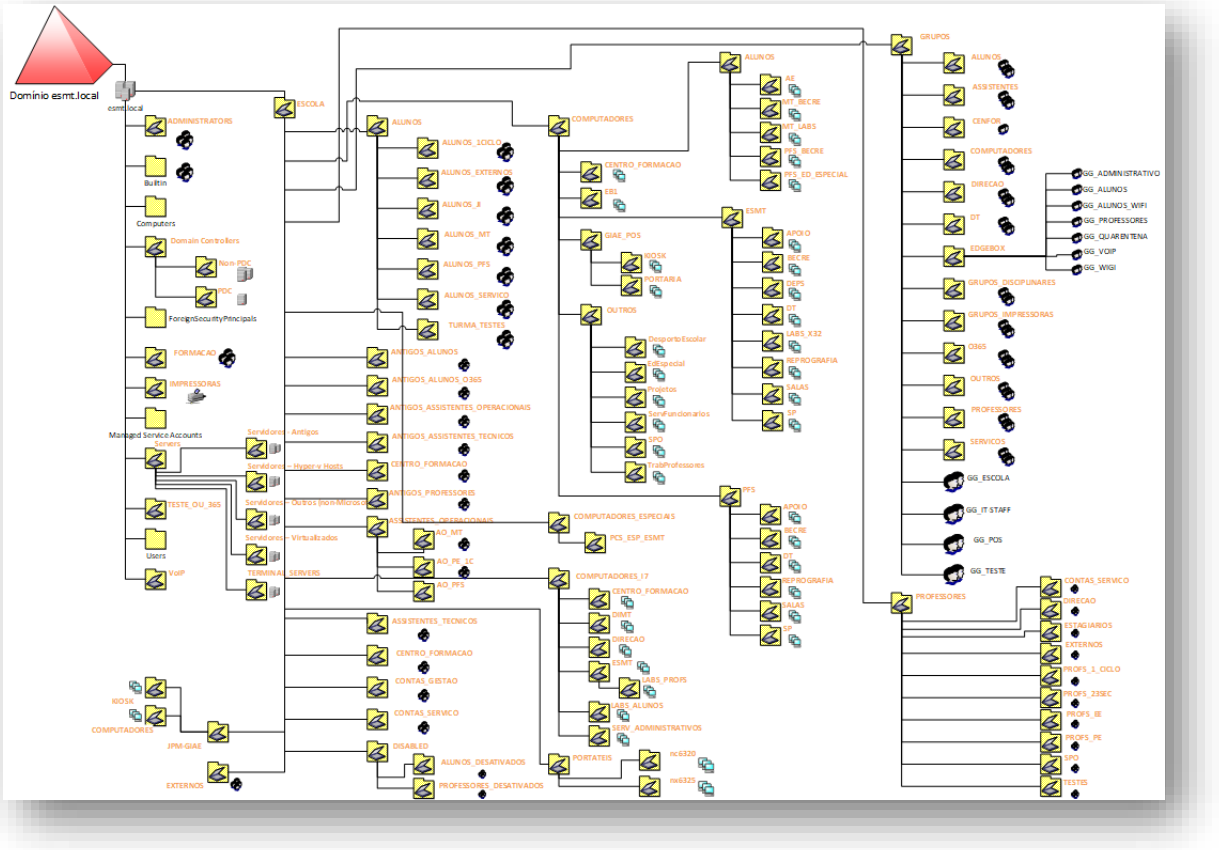


Figura 6.13 - Desenho lógico da AD do AEMT

6.4. Desenho físico da Active Directory do AEMT

O modelo físico da AD do AEMT é composto por um único domínio, onde existem 3 controladores de domínio:

- 1 controlador de domínio com o nome MTSRVDC2, colocado na VLAN 32 (para os clientes professores)
- 1 controlador de domínio com o nome MTSRVDC0, e 1 controlador de domínio com o nome MTSRVDC1, ambos colocados na VLAN 33 (para os clientes alunos)

O controlador de domínio existente na VLAN 32 (MTSRVDC2) é aquele que desempenha todas as funções FSMO.

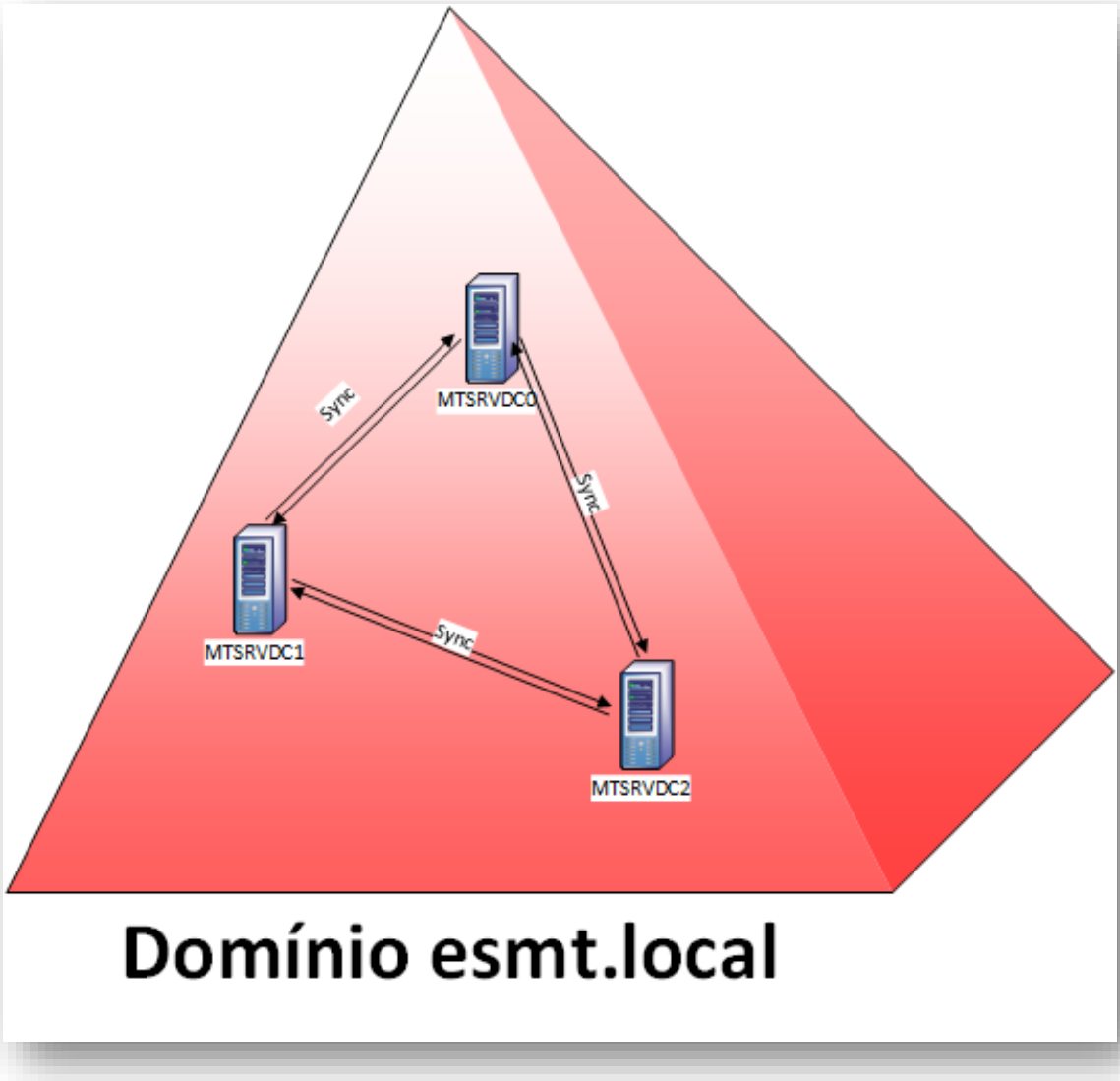


Figura 6.14 - Desenho físico da Active Directory do AEMT

6.5. Group Policy implementadas no AEMT

Foram criadas e implementadas uma série de políticas de grupo, para gestão das permissões e configurações das aplicações e dos computadores, com base no tipo de utilizador e da área a que pertence.

Em termos de políticas de grupo, apresentam-se apenas, como exemplo, as políticas de grupo criadas para Alunos e para Professores, bem como a lista de todas as existentes, para não ser demasiado extensa a explicação do que faz cada uma:

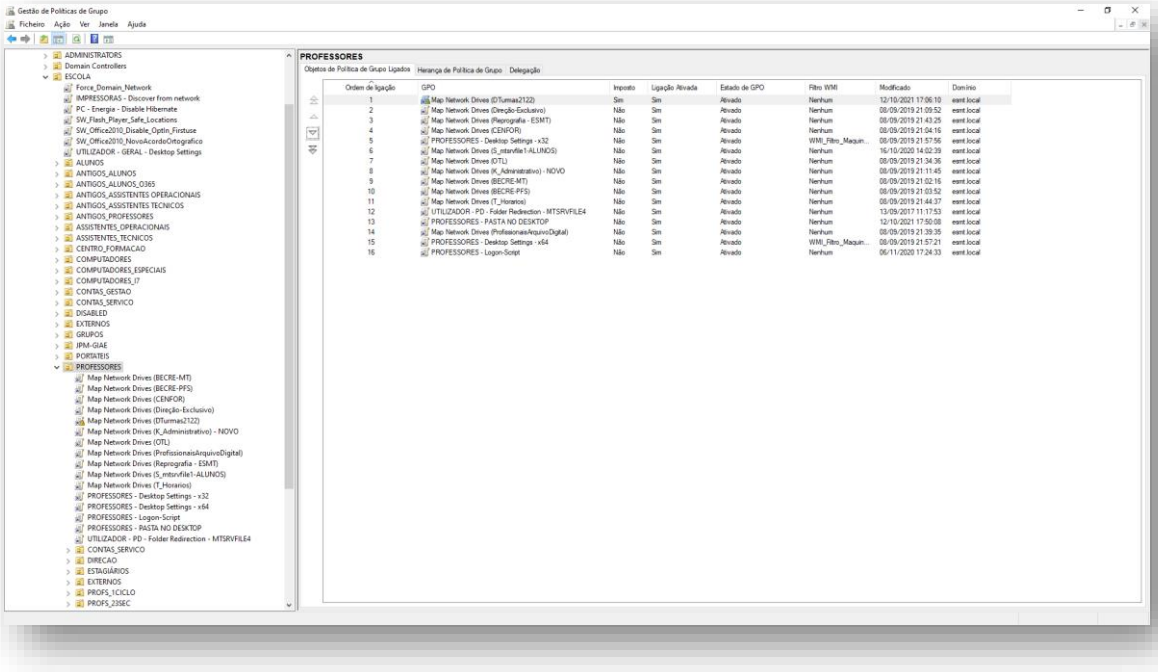


Figura 6.15 - Políticas de Grupo aplicadas a todos os alunos

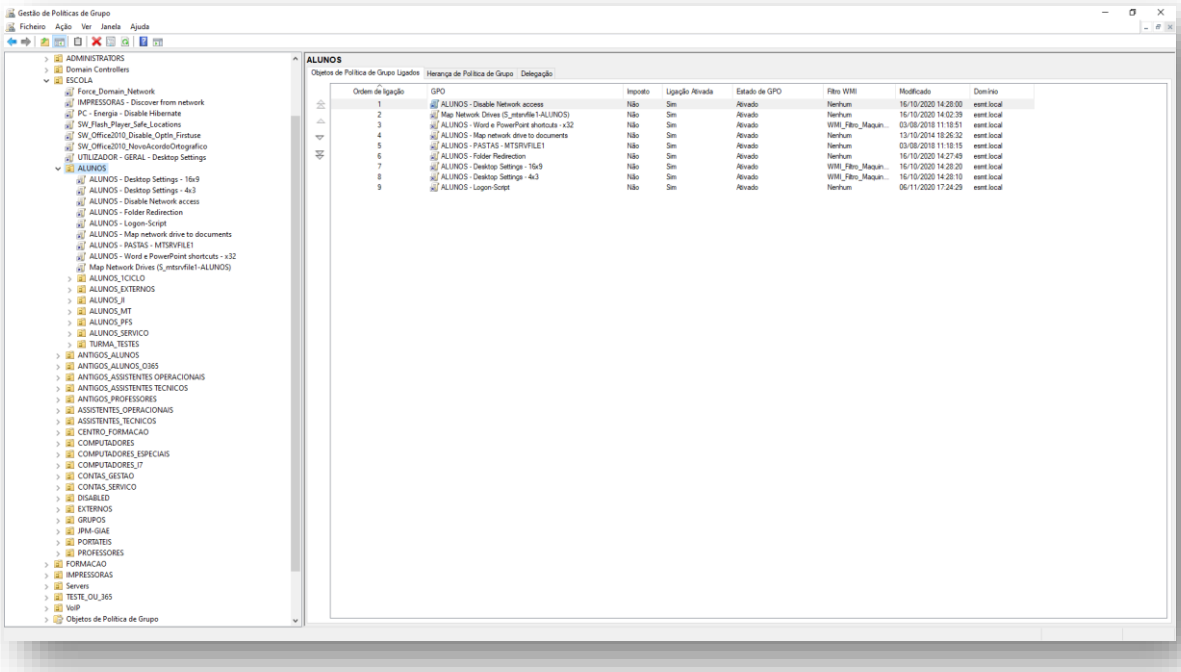


Figura 6.16 - Políticas de Grupo aplicadas a todos os professores

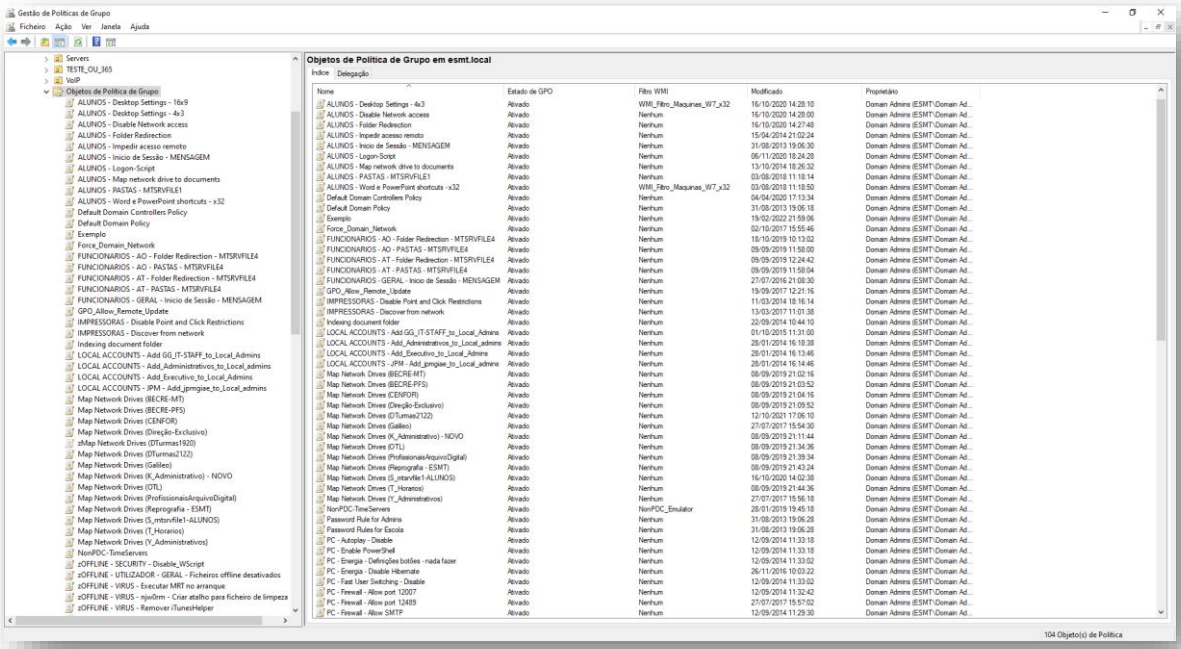


Figura 6.17 - Políticas de Grupo existentes - Parte 1

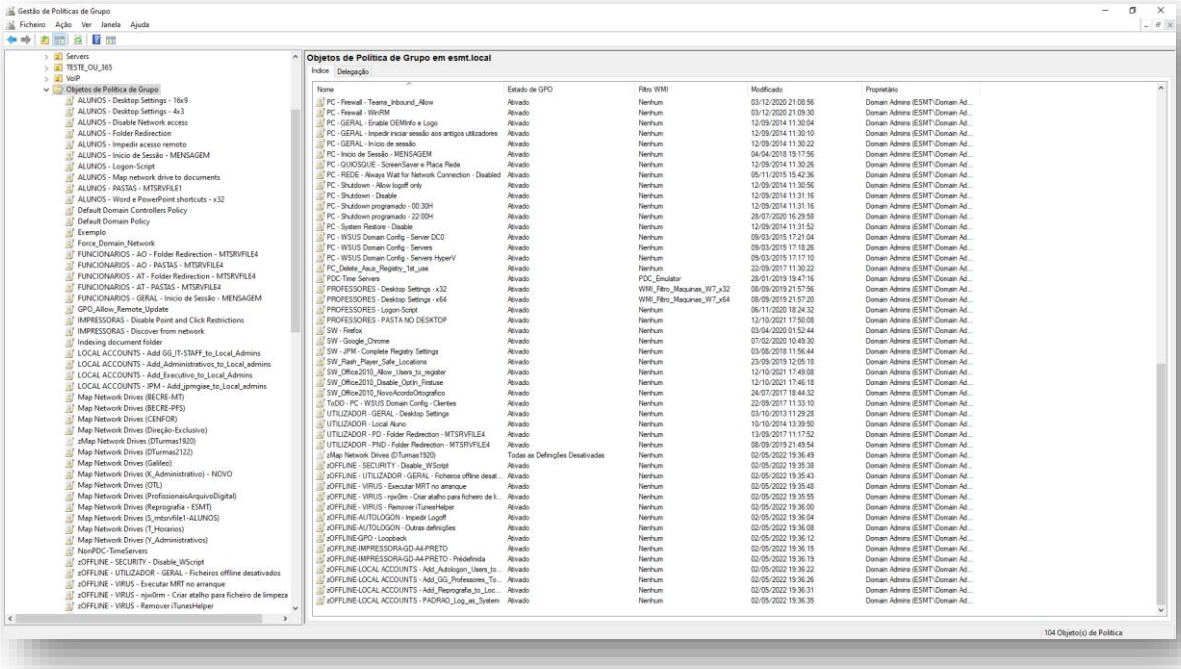


Figura 6.18 - Políticas de Grupo existentes - Parte 2

6.6. Gestão de impressoras e computadores no AEMT

Toda a gestão de impressoras é feita utilizando o FOG (software de reposição de imagens, apresentado no ponto 5.4). Nas imagens de cada computador são instalados os drivers das impressoras

existentes bem como o software cliente do FOG o que nos permite, utilizando a interface do Fog, gerir de forma centralizada as mesmas.

Para isso, começa-se por adicionar as impressoras (que, no caso do AEMT, são todas:

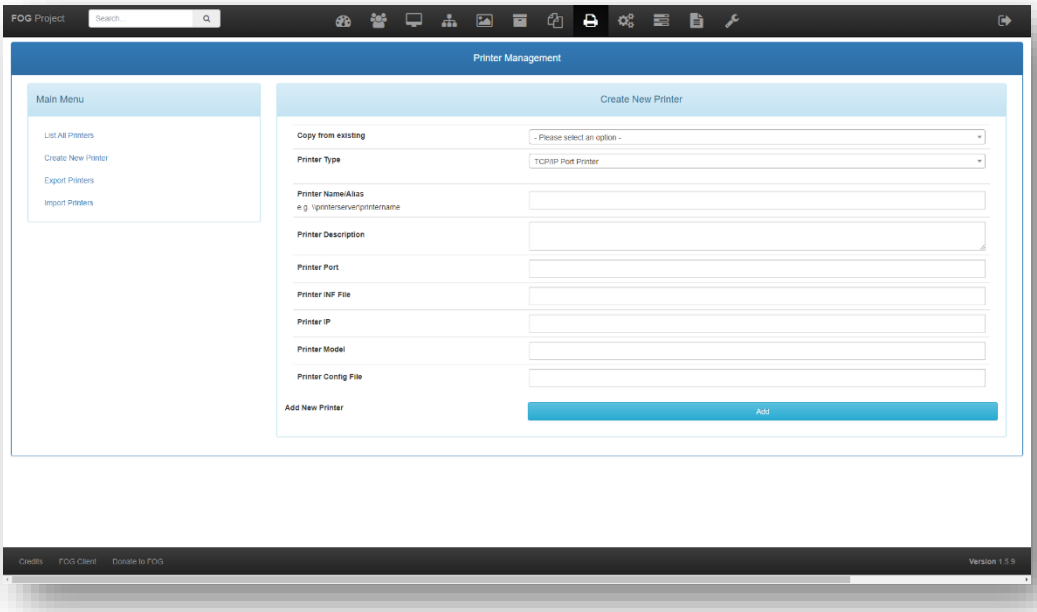


Figura 6.19 - Área do FOG onde se realiza a configuração de impressoras de rede

De seguida, podemos atribuir as impressoras a grupos, o que vai fazer, na realidade, a configuração individual de cada *host* que pertence a esse grupo:

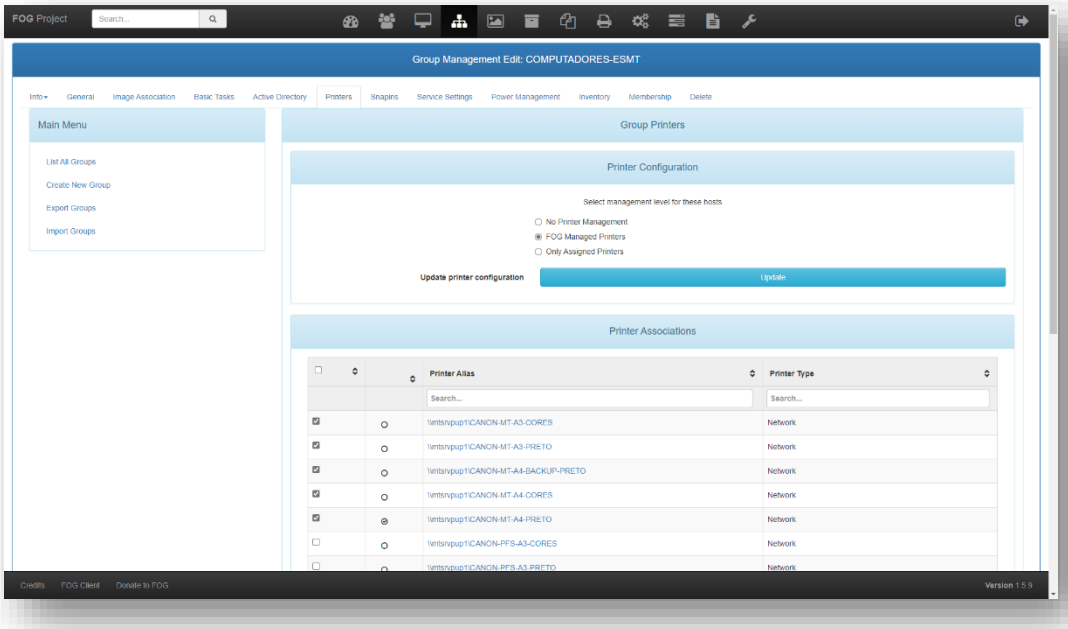


Figura 6.20 - Atribuição de impressoras a grupos de hosts

Finalmente, ao verificarmos as configurações de um determinado *host*, podemos verificar quais as impressoras instaladas e qual a impressora predefinida:

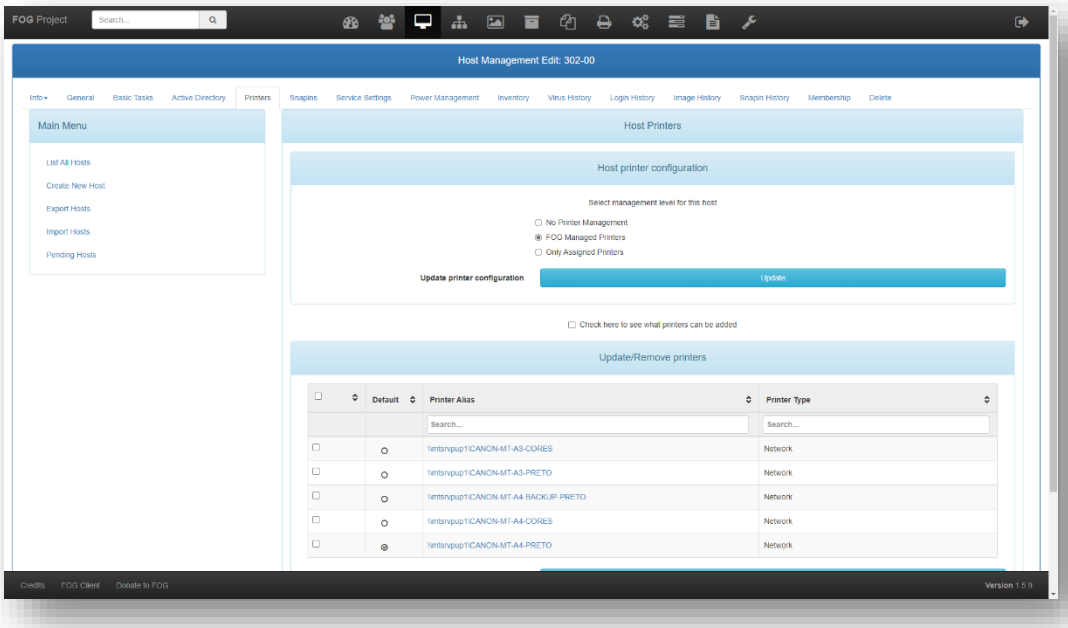


Figura 6.21 - Exemplo das impressoras configuradas num host

Desta forma, torna-se simples e muito mais fácil adicionar ou remover impressoras nos hosts, sem ter de se precisar de ir fisicamente aos computadores fazer essa configuração o que, no caso do AEMT é algo importante, devido ao elevado número de impressoras (ou variações de configurações das mesmas).

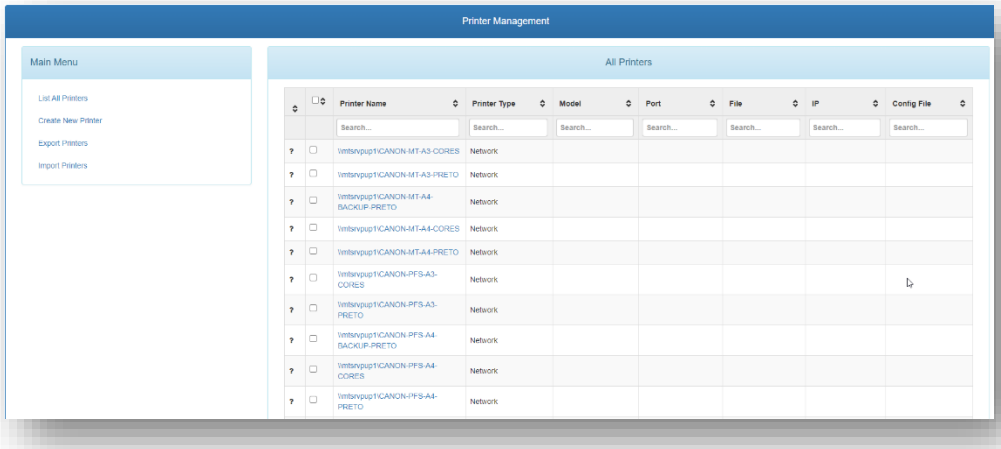


Figura 6.22 - Algumas impressoras configuradas no FOG

6.7. Virtualização no AEMT

A última parte do trabalho desenvolvido consistiu na migração dos servidores físicos para servidores virtuais. O que se pretendeu foi diminuir a dependência das configurações físicas, aumentar a resiliência dos sistemas (repor uma cópia de segurança de uma máquina virtual é um processo bastante mais rápido e simples do que fazer uma reposição *bare metal*), maximizar a utilização dos

recursos (atribuição dinâmica de memória, gestão dos núcleos de processamento), e minimizar os custos energéticos (redução do número de servidores físicos e respetivos custos de arrefecimento).

A tecnologia de virtualização utilizada foi o Hyper-V, da Microsoft, por não implicar custos adicionais aos do licenciamento dos próprios servidores Windows, e por dar resposta a todas as necessidades requeridas.

O desenho da solução passou por criar um servidor específico para os alunos (MTSRVHV1), um servidor específico para os professores e administrativos (MTSRVHV2), e um para os serviços web que dão suporta ao agrupamento (MTSRVHV3).

Entretanto, a escola foi podendo adquirir mais material, que permitiu aumentar o número de servidores virtuais em cada servidor físico, para dar resposta a todas as necessidades do AEMT, sendo, atualmente, constituído pelos seguintes servidores:

6.7.1. O servidor físico MTSRVHV1

O servidor MTSRVHV1 destina-se a todas as máquinas virtuais a que os alunos possam aceder, e inclui um controlador de domínio e servidor DNS para a resolução de nomes dos computadores que estejam na VLAN ALUNOS, um servidor aplicacional, um servidor de ficheiros (onde são armazenados as pastas “Os meus documentos”, “Imagens”, “Música”, “Vídeo” e a pasta “Transferências”, para que, independentemente do computador em que o aluno inicie sessão, possa ter acesso a todos os seus ficheiros) e a um servidor de impressões e de atualizações (onde é feita a configuração das impressoras de rede que são utilizadas, bem como onde são obtidas as atualizações que são para implementar nos computadores, e estes, através de uma política de grupo, obtêm as atualizações através deste servidor, em vez de cada um as obter da Internet, otimizando a quantidade de transferências que são necessárias transferir da Internet).

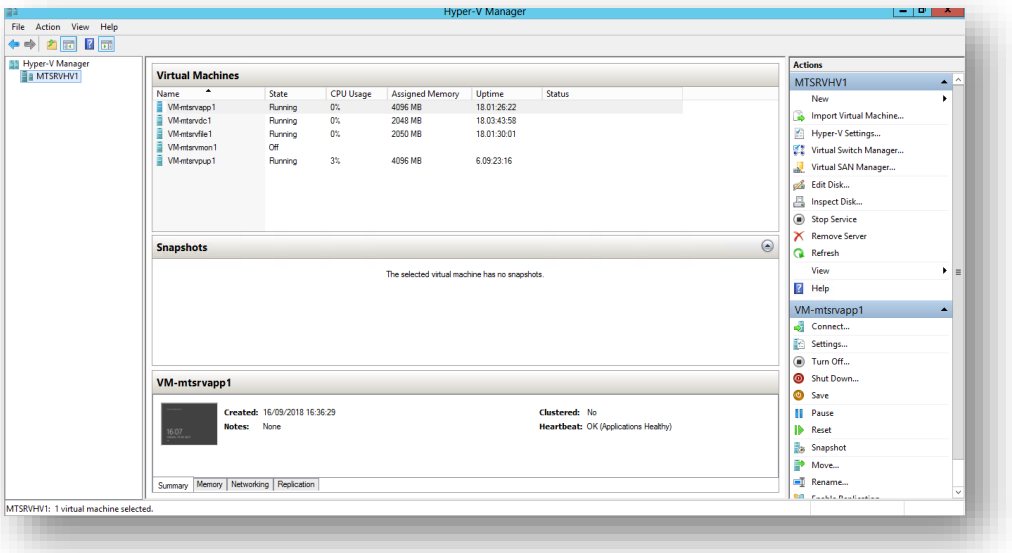


Figura 6.23 - Servidores virtuais existentes em MTSRVHV1

VM-mtsrvapp1 – servidor de aplicações para alunos

VM-mtsrvdc1 – controlador de domínio e servidor de DNS primário para os clientes da VLAN alunos

VM-mtsrvfile1 – servidor de ficheiros de alunos

VM-mtsrvpup1 – servidor de impressão e de atualizações (WSUS – Windows Server Update Services)

VM-mtsrvmon1 – por implementar (futuro servidor de monitorização)

6.7.2. O servidor físico MTSRVHV4

Inicialmente, a maioria das máquinas virtuais existentes neste servidor, estavam hospedadas no MTSRVHV2, mas com o desenho de uma solução de redundância física dos servidores físicos, foi implementado um novo servidor, o MTSRVHV4, para onde estas máquinas foram migradas.

O servidor MTSRVHV4 destina-se a todas as máquinas virtuais a que apenas os professores, assistentes operacionais e assistentes técnicos possam aceder (ou seja, os alunos não têm acesso), e inclui um controlador de domínio e servidor DNS para a resolução de nomes dos computadores que estejam na VLAN PROFESSORES ou VLAN ADMINISTRATIVOS, dois servidores aplicacionais (necessários para armazenar as aplicações legadas e as novas aplicações de gestão escolar), um servidor de ficheiros (onde são armazenados as pastas “Os meus documentos”, “Imagens”, “Música”, “Vídeo” e a pasta “Transferências”, para que, independentemente do computador em que o professor/assistente inicie sessão, possa ter acesso a todos os seus ficheiros).

Estão aqui virtualizados também os antigos servidores físicos que existiam (com aplicações descontinuadas), para efeitos de acesso e consulta a processos antigos.

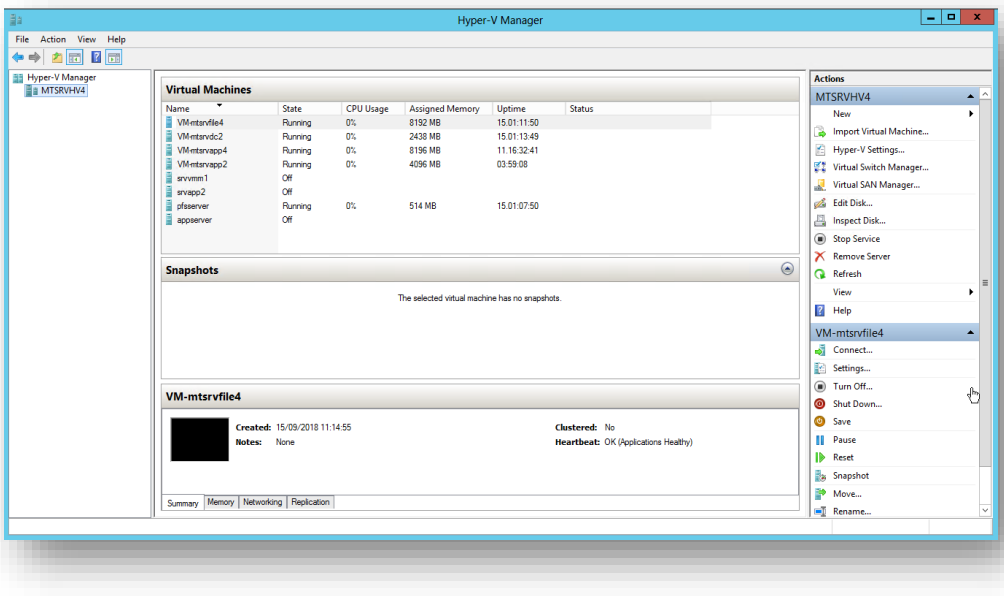


Figura 6.24 - Servidores virtuais existentes em MTSRVHV4

VM-mtsrvfile4 – servidor de ficheiros de professores, assistentes técnicos e assistentes operacionais

VM-mtsrvdc2 – controlador de domínio e servidor DNS principal das VLAN de professores e administrativos

VM-mtsrvapp2 – servidor de aplicações administrativas

VM-mtsrvapp4 – servidor de aplicações administrativas

6.7.3. O servidor físico MTSRVHV3

O servidor MTSRVHV3 destina-se a alojar as máquinas virtuais onde estão implementados servidores de páginas Internet, nomeadamente o servidor Moodle do AEMT, o servidor Joomla do Centro de Formação das Escolas de Torres Vedras e Lourinhã, e os servidores de projetos desenvolvidos por alunos no âmbito das PAP.

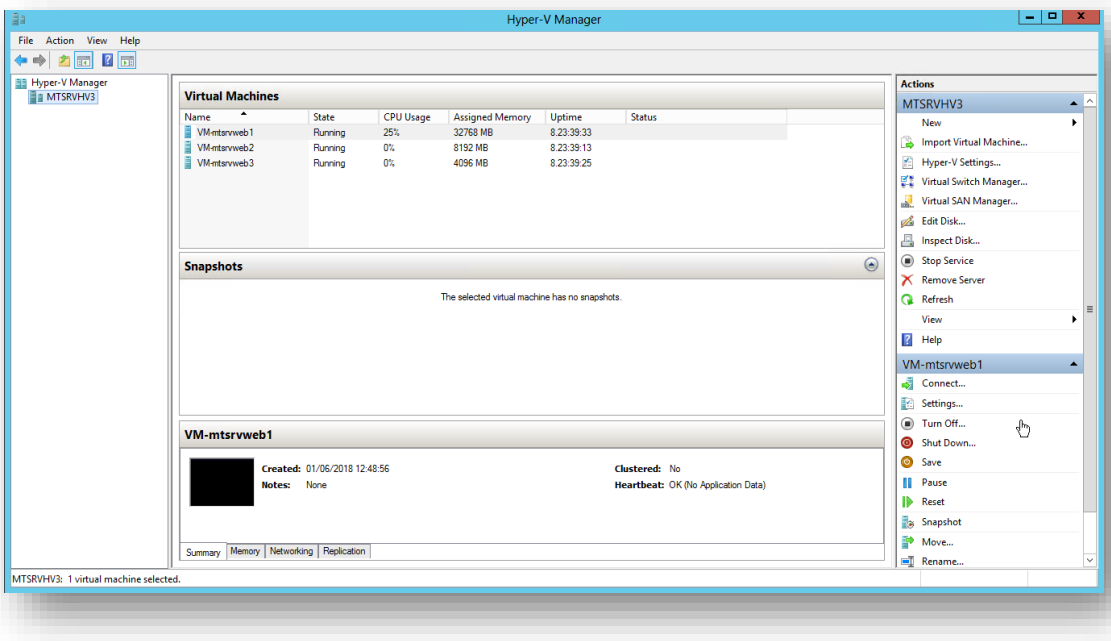


Figura 6.25 - Servidores virtuais existentes em MTSRVHV3

VM-mtsrvweb1 – servidor Moodle do AEMT

VM-mtsrvweb2 – servidor Web de trabalhos de alunos

VM-mtsrvweb3 – servidor Web do Centro de Formação de Escolas de Torres Vedras e Lourinhã

6.7.3.1. Servidores Web (Linux)

Todos os servidores Web foram implementados utilizando o LAMP, acrónimo que designa o sistema operativo Linux, e os servidores/serviços Apache (servidor web), MySQL/MariaDB (servidor de base de dados), PHP/Perl/Python (linguagens web suportadas).

No caso do AEMT, a distribuição Linux utilizada foi o CentOS, que assenta no tipo de distribuições com base no RedHat. O servidor Web é o Apache, a base de dados escolhida foi o MariaDB e a linguagem de programação o PHP.

Quanto ao Moodle, o sistema de implementação escolhido foi o GIT, que permite fazer as atualizações de forma prática e simples, através de uma linha de comandos.

6.7.4. Virtualização: próximos passos

O processo atual do projeto está no ponto de criação de réplicas de cada um dos servidores de virtualização, sendo a primeira fase deste processo a criação das réplicas dos servidores MTSRVHV1 e MTSRVHV4 (para os servidores MTSRVHV2 e MTSRVHV5, respetivamente).

Para tal ser possível, aos inicialmente dois servidores HP Proliant DL180, foram adicionados dois Lenovo RD640. Cada dois servidores de cada modelo são praticamente iguais, apenas existindo alguma diferença nos discos existentes em ambos os servidores HP.

Como inicialmente o MTSRVHV2 é que alojava as máquinas virtuais dos professores e sistemas de gestão escolar, comecei por criar um novo servidor (MTSRVHV4) para onde estas máquinas foram migradas (o MTSRVHV2 estava num HP Proliant DL180 e o MTSRVHV4 está num Lenovo RD640), libertando, deste modo, o HP Proliant DL180 para ser configurado como réplica do MTSRVHV1. Quanto ao atual MTSRVHV4, este será replicado para um outro Lenovo RD640 (o MTSRVHV5).

Este processo encontra-se parado, pois decidi, em primeiro lugar, fazer a atualização dos sistemas operativos Windows Server, da versão 2012 para a versão 2019, uma vez que a data final de suporte (data já estendida) é o dia 10 de outubro de 2023[112]. Esta atualização vai implicar uma atualização temporária, ou par a versão Windows Server 2012 R2 ou para a versão Windows Server 2016, conforme consta na documentação oficial da Microsoft[113]:

[112] https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012
[113] https://docs.microsoft.com/en-us/windows-server/upgrade/upgrade-overview

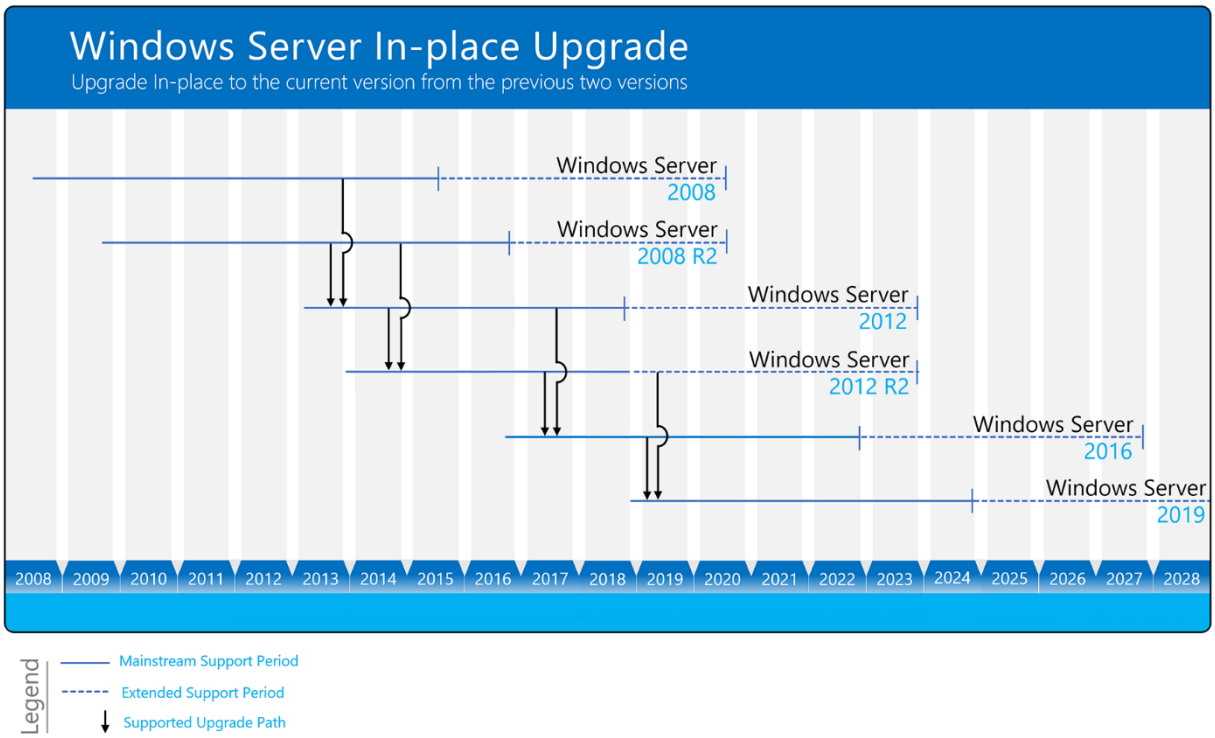


Figura 6.26 - Mapa de possibilidades de atualização das versões do Windows Server

Estes são então os passos seguintes de todo este processo, que visa criar um sistema robusto, resiliente e atual, que sirva todas as necessidades do AEMT.

7. O COVID E A NECESSIDADE DE UMA PLATAFORMA DE ENSINO A DISTÂNCIA

Apesar de não constar neste relatório (dava para um projeto completamente à parte), devido à COVID-19, o AEMT viu-se na necessidade de implementar um sistema de suporte ao ensino à distância.

Como já me encontrava a estudar as várias plataformas existentes (Google Classroom, Moodle + BlueButton, Microsoft 365 + Teams), não fui completamente apanhado de surpresa, mas não tinha previsto ter de implementar, de forma tão rápida, uma solução desse tipo.

Esta foi a razão pela qual a implementação de réplicas dos servidores Hyper-V, bem como a atualização das versões dos servidores Windows Server, acabaram por ficar relegados para uma altura posterior.

A decisão de avançar para uma plataforma específica não foi tomada isoladamente, uma vez que existem vários agrupamentos de escolas no concelho de Torres Vedras, onde se insere o AEMT e porque, já há algum tempo, tem vindo a ser desenvolvido um trabalho de uniformização das plataformas.

A escolha recaiu sobre o Microsoft 365 + Teams, por várias razões:

- Gratuitidade – a Microsoft oferece esta solução às escolas.
- Recursos disponíveis – o Teams tem uma versão específica para ensino e existe a possibilidade de utilizar as versões online gratuitas do Word, Excel e PowerPoint
- Integração com a Active Directory – torna possível integrar as contas existentes localmente e sincronizá-las com o Azure AD.
- Segurança – disponibilização de sistemas de autenticação em dois fatores, que podem ser utilizados de forma gratuita; painéis de gestão da identidade.
- Possibilidade de integrar o Moodle – sendo a plataforma de LMS que era utilizada nos vários agrupamentos, existir a possibilidade de integração com a solução a implementar, era um fator determinante para a escolha.

Por alturas do COVID, as plataformas e autenticações eram feitas de forma algo díspar:

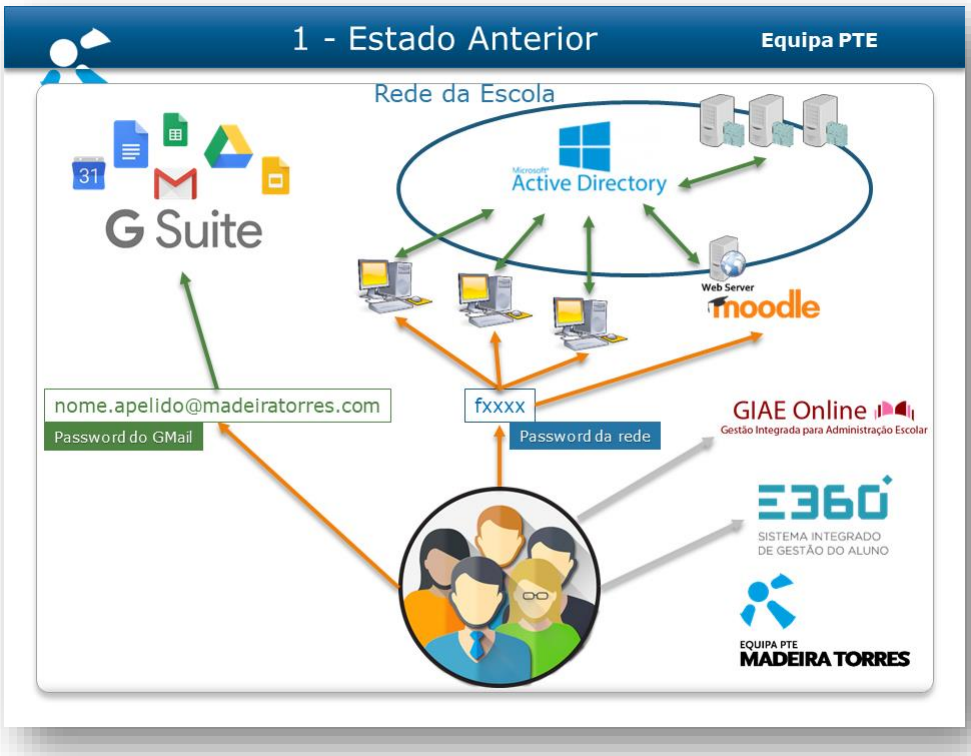


Figura 7.1 - Estado inicial dos serviços do AEMT e respetivas autenticações

Também já desenhada e prevista era a hipótese de se conseguir alcançar a meta de ter uma única forma de autenticação para todos os serviços. A necessidade de migrar do Google Mail para o Outlook (ou seja, da plataforma Google apps para a plataforma Microsoft 365), veio impor essa necessidade, pelo que a fase seguinte consistia em:

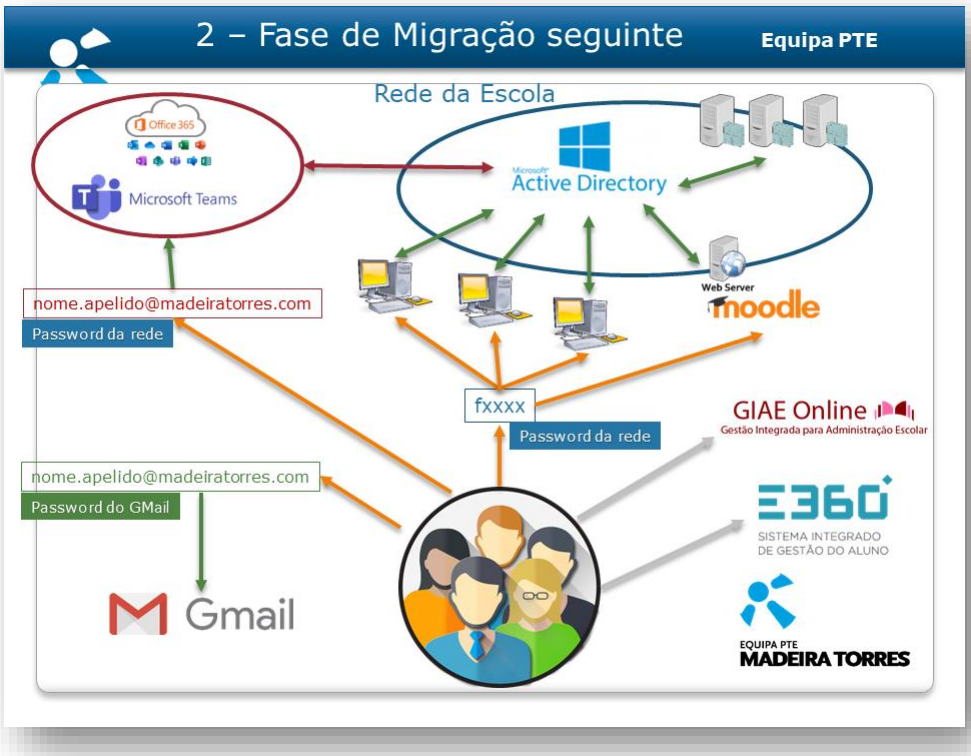


Figura 7.2 - Estado dos serviços do AEMT e respetivas autenticações com o Microsoft 365

Na imagem acima, não tinha ainda sido feita a migração do Google Apps para o Microsoft 365 na totalidade, pelo que o processo foi apenas temporário.

No entanto, como vimos, as contas de email existentes eram suportadas na plataforma da Google, pelo que o processo de migração total implicou:

- Migração de todos os emails de professores e assistentes técnicos do Google Apps para o Office 365/Outlook (processo moroso e complicado, pois foi necessário migrar todo o conteúdo que existia nos emails da Google, para ninguém perder nenhum email)
- Compatibilização das contas locais da Active Directory para poderem ser sincronizadas com o Microsoft 365 e serem criados, automaticamente, os emails de novos utilizadores.
- Criação, através de scripts, de mais de 1000 disciplinas no Teams, inscrevendo os professores e alunos nas mesmas.
- Criação de vídeos de suporte à utilização do Teams (para professores, para alunos e para encarregados de educação).

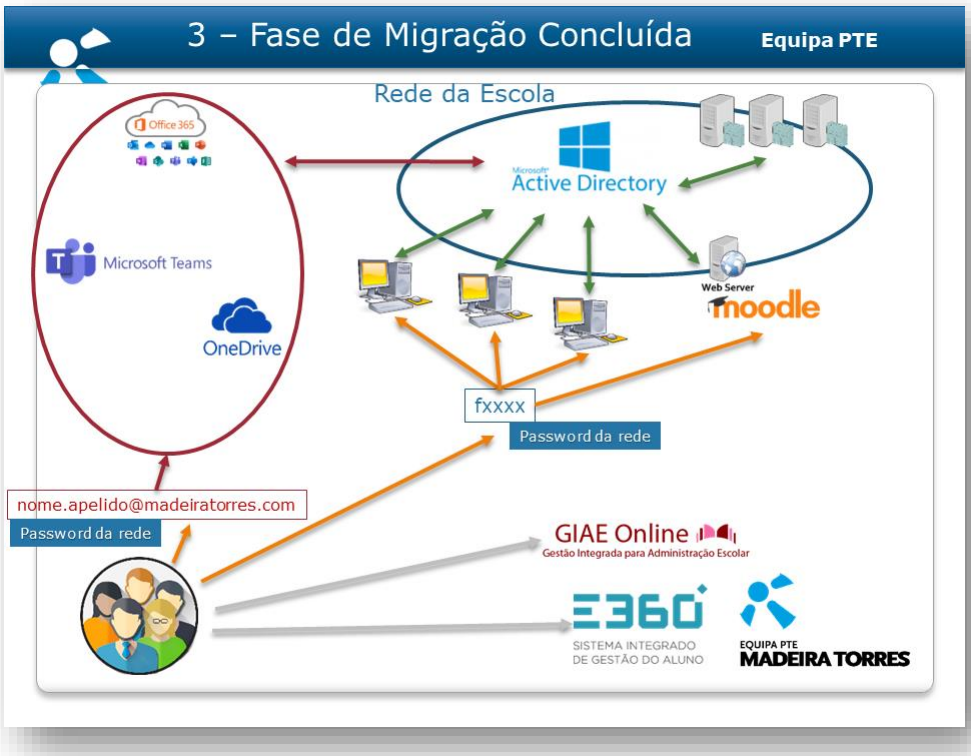


Figura 7.3 - Estado dos serviços do AEMT e respetivas autenticações com integração total no Microsoft 365

Foram necessários muitos outros processos intermédios, mas não é esta a área de interesse do atual relatório. Apenas consta aqui para se entender a necessidade de atrasar algumas das soluções previstas e que não foram ainda implementadas.

O resultado final, contudo, apenas foi possível, graças a todo o trabalho de base que foi desenvolvido a nível de configurações de rede e serviços no AEMT, que permitiram chegar ao pretendido, mesmo passando por uma pandemia: ter os sistemas completamente integrados, debaixo de uma autenticação única, mas segura:

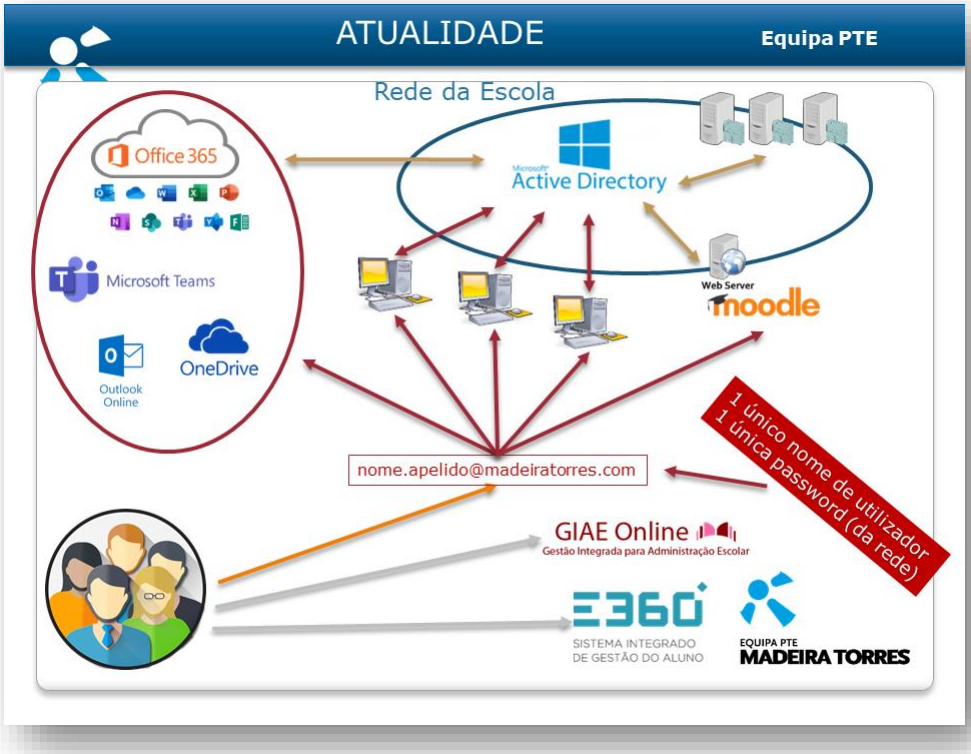


Figura 7.4 - Estado atual da autenticação nos vários dos serviços do AEMT

8. CONCLUSÃO

Este foi um processo moroso e desenvolvido no âmbito das funções por mim desempenhadas ao longo dos anos no Agrupamento de Escolas Madeira Torres.

Resumidamente, o processo consistiu em:

- 2003 - Moodle:
    - Instalação de servidor LAMP e plataforma Moodle
- 2004 - Implementação das 2 salas TIC, no âmbito do projeto "1000 Salas TIC"
    - Servidores Windows Server 2003
    - Active Directory
    - Serviços de autenticação e acessos geridos centralmente
- 2005 – Nomeação como coordenador TIC da ES Madeira Torres
- 2005 – Mudança da linha ADSL (1 Mbps com IP fixo)
- 2005 - Moodle:
    - Hospedado em servidor LAMP da escola.
    - Contas com autenticação na AD.
- 2006 – Criação de contas na AD para todos (alunos incluídos)
- 2006 – Criação de contas no Google Apps (email) para professores e assistentes técnicos
- 2007 – Criação de local para hospedar os servidores
- 2007 – Criação de contas de email institucional (inicialmente eram pXXXXX@madeiratorres.com)
- 2009/2010 – Criação de mais 4 laboratórios de informática (salas 201, 232, 235 e 242) e remodelação da sala 260A.
- Internet e rede de área local (ativos e passivos), incluindo acesso à Internet em banda larga (fibra ótica) – falta cobertura wireless em toda a escola (só está parcial), resolver algumas questões relacionadas com o cumprimento do caderno de encargos e existe material em falta. Já foi efetuada a migração para esta nova infraestrutura tendo a anterior sido descativada;
- Equipar salas com material recebido no âmbito do Plano Tecnológico de Educação:
    - 255 computadores fixos
    - 48 videoprojectores
    - 11 quadros interativos (com videoprojector embutido)
    - A escola já detinha, no âmbito de outros projetos:
        - 2 quadros interativos
        - 27 computadores portáteis

- Distribuição dos equipamentos pelas salas:
  - Salas de Informática
    - 235 – com 15 computadores e um quadro interativo
    - 242 – com 15 computadores e um quadro interativo
    - 260A – com 15 computadores e um quadro interativo
    - 302 – com 15 computadores e um quadro interativo (que a escola já detinha)
    - 303 – com 13 computadores e um quadro interativo
    - 313 – com 8 computadores e um videoprojector
    - 315 – com 14 computadores e um quadro interativo
    - 315A – com 8 computadores e um videoprojector
  - Restantes salas de aula – Um computador e um videoprojector.
- Quadros interativos nas salas 101, 139, 201, 202, 231, 232 e 245 (que a escola já detinha).
- Serviços:
  - Sala de professores – 10 computadores
  - Sala dos Diretores de Turma – 2 computadores
  - BE/CRE – 2 ao serviço da gestão da biblioteca e 18 para os alunos
  - Serviços Administrativos – 13 computadores
  - Direção – 7 computadores
  - CNO – 10 computadores
  - Centro de Formação – 3 computadores
  - Sala dos Servidores – 2 computadores
- Outros serviços com computador:
  - Gabinetes dos Grupos Disciplinares
  - Papelaria
  - Reprografia
  - Bar
  - Portaria
  - Refeitório
  - Sala do Encarregado dos Funcionários
  - Associação de Estudantes
  - PBX

- 2009/2010 – Ligação em fibra ótica à Internet
- 2010/2011 – Projeto de Gestão Documental

- 2011/2012 – Mudança do nome de utilizadores (professores e pessoal não docente) – sincronização com dados das aplicações do GIAE – novos nomes de utilizador (fXXXXX)
- 2011/2012 – Janeiro/2012 – implementação do novo sistema de cartões / GIAE
- 2011/2012 – 2º e 3º Períodos – Implementação e arranque da utilização de "Sumário Eletrónico"!
- 2011/2012 – Pedido ao NSO para resolução do erro com DHCP (limitado a 256 endereços).
- 2011/2012 – Instalação da Central VoIP
- 2011/2012 – Virtualização – estudo de viabilidade
- 2012 – janeiro – novo sistema de cartões + sumários eletrónicos (implicou mudança para leitores proximidade)
- 2011/2012 – Final – concurso público para aquisição de hardware e software para implementação dos servidores virtualizados
- 2011 (com aplicação em 2012/2013) - Passagem para Agrupamento – ligação da EB23 PFS e EB1+JI PFS por fibra – a EB PFS tinha um servidor Proliant ML330.
- 2011/2012 – Início do processo de virtualização de servidores e reestruturação do *datacenter*: Foram adquiridos, no processo de agregação que decorreu no final do ano de 2011, dois servidores (HP DL180), uma UPS e um conjunto de extras para os servidores. No entanto, por falta de verbas, não foi adquirido todo o equipamento que seria necessário, pelo que, nesta altura, a escola se encontrava no processo de aquisição de equipamento extra. Também a nível de software (sistema operativo de servidor) se procedeu ao concurso público para a sua aquisição.
- 2012/2013 – Ligação, em fibra, entre as EB23 PFS e ESMT (a EB23PFS já estava ligada, por fibra ao JI+EB1 PFS)
- 2012/2013 – Upgrade para Windows 2012 (5 licenças)
- 2013/2014 – Criação do *datacenter* (sistemas de arrefecimento, monitorização e deteção de intrusão)
- 2013/2014 – Remodelação da sala 235 (passagem a laboratório de informática, com rede estruturada e colunas de calhas centrais)
- 2013/2014 – Virtualização de servidores
- 2014/2015 – Upgrade de sistema telefónico VoIP (com carta BRI OpenVox BE400E)
- 2014/2015 – Aquisição de mais 2 servidores (redundância física) – Lenovo RD640 para criação de redundância física de servidores
- 2014/2015 – Aquisição de 40 novos PCs i7-4790 B85M-G (para melhoria dos laboratórios com equipamentos mais potentes e com hipótese de virtualização local)

- 2014/2015 – Ampliação dos recursos dos servidores (processadores + memórias + discos + placas de rede para serem agregadas – NIC TEAMING)
- 2015 – Atualizações no *FileServer* dos professores e alunos
- 2015/2016 – 35 novos PCs i7-4790 B85M-G + 4 Asus Z97 (apoio ao *datacenter*)
- 2017/2018 – Reconfiguração servidor VoIP (implementação da nova matriz de conetividade)
- 2019/2020 – Criação de tutoriais para utilização do *Google Classroom*
- 2019/2020 – Projeto TV em vez de Projetor (apresentação do estudo)
- 2019/2020 – Remodelação da sala 235 (passagem a laboratório de eletrónica)
- 2019/2020 – 16 novos computadores (laboratório eletrónica – 235)
- 2019/2020 – Pandemia – migração Google Apps para Office 365 (contas de email de professores e seu conteúdo)
- 2019/2020 – Criação de contas de email para TODOS os alunos
- 2019/2020 – Implementação Microsoft Teams (criação de todas as disciplinas de todos os anos letivos, do 1.º ao 12.º ano, incluindo cursos profissionais)
- 2019/2020 – Implementação de MFA para todos os utilizadores.
- 2019/2020 – Criação de tutoriais em vídeo, para apoio à comunidade escolar, na utilização do email (Outlook Online), Office 365 (Aplicações do Office Online), Teams, etc.
- 2020/2021 – Continuação do apoio ao ensino presencial e a distância (novos tutoriais em vídeo)
- 2020/2021 – Necessidade de ter um único login e password transversalmente (AD/Moodle/Email)
- 2021/2022 – aquisição de 16 novos computadores (laboratório sala 302 – renovação)
- 2021/2022 – PREVISTO – aquisição de TVs para piloto do projeto TV em vez de Projetor.
- 2021/2022 – Início da implementação PADDE – formação (SharePoint/OneDrive e gestão documental)

Como dá para ver, foi um processo moroso e que envolveu muito know-how (quer em quantidade, quer em diversidade). Mas hoje, o AEMT está servido por uma infraestrutura de rede e sistemas que dão resposta às necessidades existentes, e que permite continuar este processo de crescimento, melhorando ou ampliando as características já existentes.

Foi com o trabalho desenvolvido ao longo destes anos, recorrendo a todos os projetos nacionais e infraestruturas que estes proporcionaram, bem como com o apoio da direção, ao permitir que desempenhasse funções de coordenação técnica acumulando com as funções de professor, que permitiu hoje, no AEMT, existir uma infraestrutura de rede moderna, segura, eficaz, eficiente, e preparada para os próximos tempos, que é uma das mais avançadas a nível nacional, no que a escolas públicas de ensino não superior respeita.

9. BIBLIOGRAFIA

About Moodle. (31 de 08 de 2020). Obtido em 27 de 02 de 2022, de Moodle: https://docs.moodle.org/311/en/About_Moodle

Acesso analógico, acesso RDIS básico e acesso RDIS primário. (09 de março de 2004). Obtido em 25 de março de 2022, de ANACOM: https://www.anacom.pt/render.jsp?categoryId=99559

Active Directory Infrastructure Self-Study Training Kit: Windows Server 2012 and R2. (2015). East Olympia: Stanek & Associates.

Allen, R. (2003). *Active Directory Cookbook.* Sebastopol: O'Reilly.

Allen, R., & Lowe-Norris, A. G. (2003). *Active Directory, 2nd edition* (2ª ed.). O'Reilly.

Allen, R., Desmond, B., Lowe-Norris, A. G., & Richards, J. (2013). *Active Directory* (5.ª ed.). Sebastopol: O'Reilly.

Características das classes de objeto. (s.d.). Obtido em 30 de 01 de 2022, de Microsoft: https://docs.microsoft.com/pt-br/windows/win32/ad/characteristics-of-object-classes

Clercq, J. D., & Grillenmeier, G. (2007). *Microsoft Windows Security Fundamentals.* Oxford: Elsevier.

Cloudflare free plan. (27 de 02 de 2022). Obtido de Cloudflare: https://www.cloudflare.com/plans/free/

Configuração de Clientes 802.1x - Manual de Referência - versão 2.1. (2009). Critical Links.

DGEEC. (s.d.). *Plano Tecnológico da Educação - Missão e Objetivos*. Obtido em 21 de janeiro de 2022, de https://www.dgeec.mec.pt/np4/243.html

eRadManager - Manual do Administrador - versão 2.2. (2009). Critical Links.

Esquema de Active Directory. (s.d.). Obtido em 30 de 01 de 2022, de Microsoft: https://docs.microsoft.com/pt-br/windows/win32/adschema/active-directory-schema

Fail2ban Wiki. (28 de 05 de 2016). Obtido em 27 de 02 de 2022, de Fail2ban: https://www.fail2ban.org/wiki/index.php/Main_Page

Finn, A., Lownds, P., Luescher, M., & Flynn, D. (2013). *Windows Server 2012 Hyper-V Installation and Configuration Guide.* Indianapolis: Sybex.

Fog Wiki. (09 de 03 de 2016). Obtido em 27 de 02 de 2022, de FogProject: https://wiki.fogproject.org/wiki/index.php?title=Introduction

FreePBX. (s.d.). Obtido em 20 de 03 de 2022, de https://www.freepbx.org/

Gabinete do Secretário de Estado da Educação (Ed.). (27 de 12 de 2005). Despacho n.º 26 691/2005 (2.ª série). *DIÁRIO DA REPÚBLICA - II SÉRIE*, 17973-17974.

Glenn, W., & Simpson, M. T. (2004). *Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Self-Paced Training Kit.* Washington: Microsoft Press.

Gomes, M. A. (outubro de 2010). Análise comparativa de programas da sociedade da informação no ensino. *Tese de Mestrado*, 108. (E. S. Bragança, Ed.) Obtido de https://bibliotecadigital.ipb.pt/bitstream/10198/3987/1/Gomes_Maria.pdf

Grasdal, M., Hunter, L. E., & Cross, M. (2003). *Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System.* Rockland: Syngress.

Holme, D., & Thomas, O. (2004). *MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296.* Washington: Microsoft Press.

Holme, D., & Thomas, O. (2006). *Managing and Maintaining a Microsoft Windows Server 2003 Environment.* Washington: Microsoft Press.

Hunter, L. E., Barber, B., Craft, M., & Johnson, Jr, N. L. (2003). *Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000 Study Guide & DVD Training System.* Rockland: Syngress.

Kaufmann, R., & English, B. (2004). *MCSA/MCSE: Windows Server 2003 Network Security Administration Study Guide.* San Francisco / London: Sybex.

King, R. R. (2003). *Mastering Active Directory for Windows Server 2003.* San Francisco / London: Sybex.

LAMP. (28 de 12 de 2021). Obtido em 27 de 02 de 2022, de Wikipédia.

Lan Manager. (s.d.). Obtido em 22 de janeiro de 2022, de Wikipedia: https://en.wikipedia.org/wiki/LAN_Manager

Lei n.º 55-A/2004. (30 de dezembro de 2004). *Diário da República n.º 304/2004, 1º Suplemento, Série I-A*. Assembleia da República. Obtido de https://files.dre.pt/1s/2004/12/304a01/00020160.pdf

Let's Encrypt. (s.d.). Obtido em 20 de 03 de 2022, de https://letsencrypt.org/

Link aggregation. (25 de 03 de 2022). Obtido em 09 de 04 de 2022, de Wikipedia: http://en.wikipedia.org/wiki/Link_aggregation

Managing FOG. (30 de abril de 2020). Obtido em 25 de março de 2022, de FOG Wiki: https://wiki.fogproject.org/wiki/index.php?title=Managing_FOG#Snap-ins

Microsoft (Ed.). (17 de 08 de 2020). *Global Catalog*. Obtido em 12 de 02 de 2022, de Microsoft Documentation: https://docs.microsoft.com/en-us/windows/win32/ad/global-catalog

Microsoft (Ed.). (29 de 12 de 2021). *How trust relationships work for resource forests in Azure Active Directory Domain Services*. Obtido em 12 de 02 de 2022, de Microsoft Docs: https://docs.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust

Minasi, M., Greene, K., Booth, C., Butler, R., McCabe, J., Panek, R., . . . Roth, S. (2014). *Mastering Windows Server 2012 R2.* Indianapolis: Sybex.

Moodle Releases. (14 de 03 de 2022). Obtido em 20 de 03 de 2022, de Moodle Docs: https://docs.moodle.org/dev/Releases

Moskowitz, J. (2004). *Group Policy, Profiles, and IntelliMirror for Windows 2003, Windows XP, and Windows 2000.* San Francisco / London: Sybex.

Panek, W. (2015). *MCSA Windows Server 2012 R2 Administration Study Guide: exam 70-411.* Indianapolis: Sybex.

Panek, W. (2015). *MCSA Windows Server 2012 R2 Complete Study Guide.* Indianapolis: Wiley.

Patrocínio, J. T. (2001). Tecnologia, educação e cidadania: (re)pensar projectos educacionais numa abordagem compreensiva da contemporaneidade. *Dissertação de mestrado em Ciências da Educação: área de Educação e Desenvolvimento*. Universidade Nova de Lisboa: Faculdade de Ciências e Tecnologia. Obtido em 30 de 09 de 2021, de http://hdl.handle.net/10362/281

Pereira, S., & Pereira, L. (2011). Políticas tecnológicas educativas em Portugal: do Projecto Minerva à Iniciativa e-escolinha. *Literacia, Media e Cidadania - Actas do 1º Congresso Nacional* (pp. 157-168). Braga: Universidade do Minho. Centro de Estudos de Comunicação e Sociedade (CECS). Obtido de http://hdl.handle.net/1822/27089

Porto Editora. (s.d.). *Adesão de Portugal à CEE*. Obtido em 30 de setembro de 2021, de Infopédia: https://www.infopedia.pt/$adesao-de-portugal-a-cee

Portugal., Ministério da Ciência e da Tecnologia., Missão para a Sociedade da Informação. (1997). *Livro Verde para a Sociedade da Informação em Portugal.* Lisboa. Obtido em 30 de 09 de 2021, de https://dspace.uevora.pt/rdpc/bitstream/10174/12999/39/56ptlivroverdeparaasociedadedainformacaoemportugal.pdf

Prophet, T. (18 de agosto de 2016). *Back to School with Microsoft: Student focused, teacher inspired innovation with Office 365 Education*. (Microsoft, Editor) Obtido em 11 de 01 de 2022, de Official Microsoft Blog: https://blogs.microsoft.com/blog/2016/08/18/back-to-school-with-microsoft-student-focused-teacher-inspired-innovation-with-office-365-education/

Rapp, M. L. (2017). *Integração das TIC nos processos de ensino e aprendizagem pelos professores do 1° e 2° Ciclo de uma escola portuguesa.* Universidade Nova de Lisboa: Faculdade de Ciências e Tecnologia. Obtido em 30 de setembro de 2021, de http://hdl.handle.net/10362/54377

Regan, P. (2013). *Administering Windows Server 2012: Exam 70-411.* Hoboken: Wiley.

Regan, P., Baker, E., Lorge, T., Stevens, G., & Watson, R. (2014). *Configuring Advanced Windows Server 2012 Services: Exam 70-412.* Hoboken: Wiley.

Resolução do Conselho de Ministros. (18 de setembro de 2007). *n.º 137/2007*. Diário da República, 1.ª série - N.º 180. Obtido de https://files.dre.pt/1s/2007/09/18000/0656306577.pdf

Russinovich, M. E., & Solomon, D. A. (2005). *Microsoft Windows Internals, Fourth edition: Microsoft Windows Server 2003, Windows XP, and Windows 2000.* Washington: Microsoft Press.

Shinder, D. L., & Shinder, D. W. (2003). *Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System.* Rockland: Syngress.

Shinder, T. W., Diogenes, Y., Shinder, D. L., & Hicks, R. (2013). *Windows Server 2012 Security from End to Edge and Beyond: architecting, designing, planning, and deploying Windows Server 2012 security solutions.* Waltham: Syngress.

Snedaker, S. (2004). *Best Damn Windows Server 2003 Book Period.* Rockland: Syngress.

Spataro, J. (30 de abril de 2020). *2 years of digital transformation in 2 months*. (Microsoft, Editor) Obtido em 11 de 01 de 2022, de Microsoft 365 Blog: https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

Teixeira, A. L. (março de 2011). Integração das TIC na educação: o caso do Squeak Etoys. *Tese de Doutoramento*, 254. (I. d.-U. Minho, Ed.) Universidade do Minho. Obtido de https://repositorium.sdum.uminho.pt/bitstream/1822/14206/1/TeseDout_LuisValente_2011.pdf

The GNU General Public License. (10 de 01 de 2022). Obtido em 27 de 02 de 2022, de GNU Operating System: https://www.gnu.org/licenses/gpl-3.0.en.html

Virtualization Overview. (2006). *White Paper*. Palo Alto, EUA. Obtido em 09 de 04 de 2022, de https://www.vmware.com/pdf/virtualization.pdf

Virtualization Role. (07 de 02 de 2012). Obtido de Changes in Functionality in Windows Server 2008: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc755090(v=ws.10)

Windows Server 2012 NIC Teaming (LBFO) Deployment and Management. (s.d.). Obtido de https://www.microsoft.com/en-us/download/details.aspx?id=30160

Zacker, C. (2013). *Installing and Configuring Windows Server 2012: Exam 70-410.* Hoboken,: Wiley.

Zeilinga, K. (Ed.). (2006). *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names, RFC 4514.* OpenLDAP Foundation. Obtido em 12 de 02 de 2000, de https://datatracker.ietf.org/doc/html/rfc4514