

The background of the cover is a photograph of a server room, showing multiple rows of server racks in a clean, brightly lit environment. The racks are filled with various server components, and the perspective is from an elevated angle looking down the aisles.

Universidade Atlântica

Infra-estruturas Microsoft

Projecto Final de Licenciatura 2007

Gestão de Sistemas e Tecnologias de Informação

Luis Miguel Arnauth Rodrigues

Orientador: Filipa Taborda

À Claudia
e a toda a nossa família
pela compreensão e ajuda
nestes quatro anos de esforço

“O autor é o único responsável pelas ideias expressas neste relatório”

Resumo

Este trabalho trata da aplicação do *Windows Server System™ Reference Architecture* (WSSRA) à realidade de uma Universidade numa visão macro.

Índice

1.	Introdução	10
2.	Rede de Serviços UB	12
2.1.	Caracterização do serviço	12
2.2.	Arquitectura lógica	13
3.	Serviços disponibilizados pela UB.....	18
3.1.	Correio Electrónico	18
3.1.1.	Caracterização do Serviço	18
3.1.2.	Arquitectura Lógica	20
3.2.	Acesso à Internet	24
3.2.1.	Caracterização do Serviço	24
3.2.2.	Arquitectura Lógica	26
3.3.	Partilha de Informação	29
3.3.1.	Caracterização do Serviço	29
3.3.2.	Arquitectura Lógica	32
3.4.	eLearning	34
3.4.1.	Caracterização do Serviço	34
3.4.2.	Arquitectura Lógica	36
3.5.	Resumo	37
4.	Serviços de Suporte	38
4.1.	Directório, Autenticação e Autorização.....	38
4.1.1.	Caracterização do Serviço	38
4.1.2.	Arquitectura Lógica	39
4.2.	Gestão da Plataforma	42
4.2.1.	Caracterização do Serviço	42
4.2.2.	Arquitectura Lógica	45
4.3.	Sistema de Gestão de Base de Dados.....	46
4.3.1.	Caracterização do Serviço	46
4.3.2.	Arquitectura Lógica	48
5.	Conclusão	49
	Bibliografia	50

Lista de Tabelas

Tabela 1 - Rede de Serviços UB, Caracterização do serviço	13
Tabela 2 - Rede de Serviços UB, Arquitectura lógica	15
Tabela 3 - Rede de Serviços UB, Arquitectura lógica (Legenda)	17
Tabela 4 - Correio Electrónico, Caracterização do Serviço.....	19
Tabela 5 - Correio Electrónico, Arquitectura Lógica (<i>roles</i> do Exchange 2007)	22
Tabela 6 - Acesso à Internet, Caracterização do Serviço.....	25
Tabela 7 - Partilha de Informação, Caracterização do Serviço.....	31
Tabela 8 - eLearning, Caracterização do Serviço.....	35
Tabela 9 - Serviços disponibilizados pela UB, Resumo (Aplicacional)	37
Tabela 10 - Directório, Autenticação e Autorização, Caracterização do Serviço	39
Tabela 11 - Gestão da Plataforma, Caracterização do Serviço (Características do SCE)	43
Tabela 12 - Gestão da Plataforma, Caracterização do Serviço.....	44
Tabela 13 - Gestão da Plataforma, Arquitectura Lógica	45
Tabela 14 - Sistema de Gestão de Base de Dados, Caracterização do Serviço	47

Lista de Figuras

Figura 1 – Rede de Serviços UB, Arquitectura lógica	16
Figura 2 - Correio Electrónico, Arquitectura Lógica (MIIS FP)	21
Figura 3 - Correio Electrónico, Arquitectura Lógica	23
Figura 4 - Acesso à Internet, Arquitectura Lógica	28
Figura 5 - Partilha de Informação, Arquitectura Lógica	32
Figura 6 - Partilha de Informação, Arquitectura Lógica (Hierarquia de sites)	33
Figura 7 - eLearning, Arquitectura Lógica	36
Figura 8 - Directório, Autenticação e Autorização, Arquitectura Lógica	41

Glossário

<i>ActiveSync</i>	É um software de sincronização que permite um dispositivo móvel ser sincronizado com uma estação de trabalho ou um servidor Microsoft Exchange.
<i>AD</i>	Active Directory, é a implementação do directório de utilizadores e serviços da Microsoft para ambientes Windows.
<i>ADAM</i>	Active Directory Application Mode, é uma implementação menos complexa da Active Directory destinada a correr aplicações, tais como o ISA Server.
<i>ALF</i>	Application Layer Filtering, é uma implementação de filtragem de pacotes a nível aplicacional para Firewalls.
<i>Array</i>	Representa um conjunto de servidores Microsoft ISA Server 2006 que partilham a mesma configuração, diminuindo a carga de gestão necessária e permitindo uma melhoria nos tempos de resposta aos clientes.
<i>Authoring</i>	Processo de criação de conteúdos.
<i>Backend</i>	Relativamente a infra-estruturas é o termo utilizado para designar a rede de dados, com necessidades de segurança superiores.
<i>Blog</i>	Website com entradas cronológicas com comentários, notícias ou outro conteúdo qualquer.
<i>Cache</i>	Duplicação de dados originais salvaguardados em outro local de forma a acelerar o acesso aos conteúdos.
<i>Caching</i>	Acto de efectuar operações de cache
<i>CARP</i>	Cache Array Routing Protocol, é um protocolo que permite um <i>array</i> de ISA Servers partilhar uma <i>cache</i> lógica única.
<i>Cluster</i>	Grupo de servidores (nós) que trabalham em conjunto de forma a balancear carga como o NLB ou em modo passivo/activo com o objectivo de assegurar a continuidade do serviço em caso de falha de um dos nós
<i>Default Gateway</i>	É um nó numa rede de computadores que permite comunicação com outras redes.
<i>DNS</i>	Domain Name System, é um serviço que permite a tradução de nomes de servidores em endereços IP.
<i>Domain Controller</i>	Numa rede Windows são os servidores responsáveis pela autenticação e autorização de pedidos.
<i>eLearning</i>	Termo associado ao ensino utilizando o computador como assistente.
<i>Extranet</i>	É uma rede privada que permite partilhar parte da informação de uma Organização com utilizadores externos.

<i>DHCP</i>	Dynamic Host Configuration Protocol, serviço responsável pela atribuição e gestão de endereços IP.
<i>Firewall</i>	Dispositivo de hardware ou software que é configurado para permitir, negar ou efectuar serviço de proxy numa rede de computadores.
<i>Frontend</i>	Relativamente a infra-estruturas é o termo utilizado para designar a rede de acesso de contacto com o exterior, com necessidades de segurança inferiores.
<i>GAL</i>	Global Address List, é o serviço de directório do Microsoft Exchange quer permite armazenar os endereços de correio electrónico dos utilizadores, listas de distribuição e recursos do próprio Microsoft Exchange.
<i>GPO</i>	Group Policies Objects, é uma funcionalidade da Active Directory que permite a gestão centralizada de políticas de segurança e configuração de utilizadores e computadores.
<i>Hardening</i>	Todas as acções que resultam na minimização dos serviços disponíveis até aos indispensáveis, maior protecção dos recursos e informação armazenados, fecho de protocolos, serviços e respectivos portos de acesso nas comunicações com a rede, activação de mecanismos de auditoria de todos os eventos e acções relevantes nos sistemas
<i>IIS</i>	Internet Information Services, é o conjunto de serviços para suporte para a Internet como o HTTP e FTP.
<i>IMAP</i>	Internet Message Access Protocol, é um protocolo que permite um cliente local aceder à caixa de correio num servidor remoto.
<i>ISP</i>	Internet Service Provider, é uma Organização que provê acesso à Internet e serviços relacionados a consumidores particulares e corporativos.
<i>LAN</i>	Local Area Network, termo referente a uma rede de computadores numa área geográfica pequena, tal como um escritório ou um edifício.
<i>Login</i>	É o processo através do qual cada acesso a um recurso de rede é controlado, identificando o utilizador de forma a obter as suas credenciais e permitir o acesso.
<i>MAPI</i>	Messaging Application Programming Interface, protocolo de acesso às caixas de correio electrónico nativo do Microsoft Exchange.
<i>NAT</i>	Network Address Translation, é o processo de reescrever a origem ou o destino de pacotes IP aquando da sua passagem por routers ou Firewalls.
<i>NLB</i>	Network Load Balacing, é uma técnica de balancear os pedidos a diferentes equipamentos.
<i>OWA</i>	Outlook Web Access, é o serviço de Webmail do Microsoft Exchange.
<i>PKI</i>	Public Key Infrastructure, infra-estrutura onde são combinadas as chaves públicas com as respectivas identidades digitais dos utilizadores ou equipamentos.
<i>POP3</i>	Post Office Protocol Version 3, é um protocolo que permite um cliente local aceder à caixa de correio num servidor remoto.

<i>Proxy</i>	Dispositivo de hardware ou software que reencaminha os pedidos de clientes internos com destino a servidores externos.
<i>Role</i>	A arquitectura do Microsoft Exchange 2007 permite a separação de funções e colocar um role ou uma combinação de <i>roles</i> em diferentes servidores ou numa combinação de servidores na Organização.
<i>Router</i>	É um dispositivo que efectua a ligação entre redes diferentes, permitindo ter um caminho optimizado de acesso às mesmas.
<i>Routing</i>	É o processo de seleccionar os melhores caminhos para o encaminhamento de dados.
<i>RPC</i>	Remote Procedure Call, tecnologia que permite a um software correr rotinas noutros sistemas que não o próprio.
<i>RPC over HTTPS</i>	Método de efectuar a passagem de pedidos RPC dentro de HTTPS, sendo utilizado na comunicação de clientes Microsoft Outlook via rede com o Microsoft Exchange.
<i>SAN</i>	Storage Area Network, é uma arquitectura que permite ligar dispositivos de armazenamento como bibliotecas de discos a servidores.
<i>Scale-out</i>	A capacidade da solução ser redimensionada com o incremento do número de servidores.
<i>Scale-up</i>	O aumento da capacidade física dos servidores, incrementando por exemplo o número de processadores, memória e/ou disco.
<i>SCORM</i>	Sharable Content Object Reference Model, é uma colecção de standards e especificações para o eLearning via Web.
<i>Service Accounts</i>	As contas de serviço são contas de utilizadores comuns destinadas a correr serviços num contexto de segurança do domínio mas com características próprias, nomeadamente uma extrema complexidade na <i>password</i> , a não atribuição do privilégio de <i>login</i> interactivo em qualquer estação ou servidor, a conta estar desabilitada entre outras. Estas opções de segurança poderão não ser compatíveis com as aplicações. Deverá ser sempre utilizado o conceito do menor privilégio possível na atribuição de direitos às contas de serviço.
<i>Site</i>	Ver Website
<i>Site (Active Directory)</i>	Separação lógica de Domain Controllers de uma Active Directory de forma a poder ter diferentes políticas de segurança e sincronização.
<i>Site-Collection</i>	Colecção de sites no Microsoft Windows SharePoint Services 3.0, permitindo a agregação de diferente Websites no mesmo contexto de segurança.
<i>SMTP</i>	Simple Mail Transport Protocol, protocolo de comunicação de correio electrónico através da Internet.
<i>SNMP</i>	Simple Network Management Protocol, protocolo usado para sistemas de gestão de rede para a gestão e monitorização de equipamentos numa rede de computadores.
<i>Sub-site</i>	Website hierarquicamente dependente do website superior.

<i>TCP</i>	Transmission Control Protocol, protocolo orientado à conexão que garante a resposta relativamente à entrega de dados da origem para o destino.
<i>Trust (Active Directory)</i>	Método de assegurar ligações de confiança entre directórios logicamente distintos.
<i>Unified Messaging</i>	Integração de diferentes tipos de mensagens como o correio electrónico, Fax e correio de voz num único servidor que permite o acesso de diferentes clientes aos recursos partilhados.
<i>Virtual Server (WSS)</i>	Método para armazenar múltiplos Websites num servidor.
<i>VOIP</i>	Voice Over IP, processo de routing de conversações voz através de redes IP.
<i>VPN</i>	Virtual Private Network, rede de comunicação segura e dedicada estabelecida através da Internet de forma a ter acessos a recursos numa rede privada.
<i>WAN</i>	Wide Area Network, termo referente a uma rede de computadores numa área geográfica ampla, que ultrapasse os limites metropolitanos, regionais ou nacionais.
<i>Web Farm</i>	Conjunto de servidores que suportam as necessidades de um serviço Web em que um único equipamento não teria capacidade.
<i>Webmail</i>	Serviço de correio electrónico acedido através de um browser da Internet.
<i>Website</i>	É uma colecção de páginas Web, imagens, vídeos e outros conteúdos armazenados em servidores Web.
<i>Wiki</i>	Website colaborativo que poderá ser editado por qualquer utilizador que lhe tenha acesso e sem conhecimentos de HTML.
<i>Wireless</i>	Rede de comunicação de dados sem fios.
<i>Workgroup</i>	Conjunto de estações de trabalho e servidores que não se encontram ligados a qualquer tipo de directório.

1. Introdução

A Infra-Estrutura de Tecnologias de Informação (IETI) de uma Organização é um recurso estratégico e o alicerce sobre o qual diversos tipos de software podem disponibilizar serviços e aplicações de negócio necessárias ao funcionamento óptimo da Organização.

O crescimento das Organizações é acompanhado pelo crescimento da IETI que se torna mais complexa e difícil de gerir, com o consequente aumento dos custos associados e o possível desalinhamento com as necessidades estratégicas do negócio, tornando mais árduo o retorno do investimento efectuado na IETI.

O caso em estudo, Universidade da Barra (UB) no distrito de Lisboa, é um espelho desta realidade, tendo como estratégia delineada pela sua Reitoria a criação de uma Secretaria Electrónica, que irá disponibilizar determinados serviços online, pelo que a IETI terá que estar enquadrada com as necessidades desta nova estratégia.

Considerando que a UB já tem uma IETI estabelecida era intenção deste projecto a optimização da mesma, utilizando para tal o *Infrastructure Optimization Model (IOM)* da Microsoft, um modelo que permite a optimização da IETI para a eficiência e controle de custos, conseguindo conciliar a segurança com a disponibilidade obtendo assim uma IETI mais madura e alinhada com o modelo de negócio da Organização.

Um dos objectivos principais desta abordagem seria o de proporcionar à UB uma perspectiva crítica sobre o actual estado da IETI e identificar as áreas que poderiam beneficiar de intervenção, quer no sentido de optimizar as mesmas ou, em alternativa, promover a sua evolução, podendo no limite identificar-se ainda características e serviços não existentes e que poderão constituir uma mais-valia para a UB.

De acordo com o IOM foram elaborados dois questionários direccionados aos docentes e equipa de gestão da IETI, de forma a melhor compreender as necessidades, dificuldades e realidade da UB.

No entanto não foi possível conseguir em tempo útil uma resposta por parte da UB relativamente à sua IETI pelo que a adopção do IOM para este caso de estudo não será o apropriado.

Dadas as contingências foi adoptado um outro modelo, o *Windows Server System Reference Architecture* (WSSRA) que é uma iniciativa, promovida pela Microsoft, com a colaboração de parceiros de todo o mundo e líderes de mercado, cujo objectivo é o de desenvolver e testar, em condições reais, soluções integradas de infra-estruturas e serviços.

Em consequência desta alteração de metodologia este trabalho o tratamento dos questionários previamente referidos não será considerado uma vez que o WSSRA é uma metodologia de referência que busca a standardização no planeamento e implementação de soluções, nomeadamente nas áreas de disponibilidade, segurança, escalabilidade e gestão.

Este relatório encontra-se dividido em quatro capítulos, sendo o primeiro a introdução, onde se contextualiza o trabalho. O segundo capítulo define e apresenta a Rede de Serviços UB. O terceiro capítulo abordará os Serviços disponibilizados pela UB aos seus utilizadores (docentes e alunos), nomeadamente o Correio Electrónico, o Acesso à Internet, a Partilha de Informação e o eLearning. O capítulo quatro irá abordar os Serviços de Suporte aos Serviços disponibilizados pela UB, designadamente o Directório, Autenticação e Autorização, Gestão da Plataforma e por fim o Sistema de Gestão de Base de Dados. Em cada um dos capítulos irá ser caracterizado o serviço, bem como uma perspectiva da arquitectura lógica.

Foram assumidos como pressupostos que a UB não dispõe de localizações remotas ligadas através de uma rede Wide Area Network (WAN), tem um universo de 2000 utilizadores, sendo que os utilizadores concorrenciais dependem do tipo de serviço caracterizado. A independência das infra-estruturas da entidade gestora, universidade e laboratório foram pressupostos assumidos, dado serem desconhecidas as opções estratégias da entidade gestora da UB, tais como a criação de novas universidades com currículo académico distintos dos actuais ou mesmo a alienação da UB a uma entidade gestora terceira.

Não foram considerados quaisquer serviços dedicados ou de suporte às estações de trabalho, como o Dynamic Host Configuration Protocol (DHCP), concentrando-se este trabalho nas infra-estruturas servidor para a Rede de Serviços UB.

2. Rede de Serviços UB

A arquitectura da Rede de Serviços UB é uma peça essencial no conjunto de serviços disponibilizados pela mesma aos seus docentes e alunos, pelo que um planeamento desadequado terá consequências significativas no futuro, particularmente na escalabilidade, segurança e eficiência operacional da plataforma.

De acordo com as melhores práticas definidas pela WSSRA é proposta esta arquitectura que não poderá ser considerada como um desenho técnico detalhado pelas razões anteriormente citadas.

De acordo com a visão proposta pressupõe-se que a UB dispõe de uma série de equipamentos ou em alternativa de orçamento para os adquirir.

Este capítulo terá como âmbito a arquitectura da Rede de Serviços UB que suportará os equipamentos que irão disponibilizar todos os serviços.

2.1. Caracterização do serviço

O desenho da Rede de Serviços UB passa pela análise de aspectos de segurança, incluindo a privacidade e integridade da informação, bem como a separação entre a rede de ensino e a rede corporativa da entidade gestora da UB.

Adicionalmente este desenho tem como objectivo dotar a UB de uma rede escalável que permitirá a inclusão de novos serviços, partilhados ou dedicados, sem ser necessário alterar as redes e zonas de segurança definidas pela mesma.

A Tabela 1 ilustra os principais aspectos considerados na elaboração do desenho da arquitectura da Rede de Serviços UB.

Segurança	<p>A natureza privada da rede corporativa da UB deverá ser protegida ao máximo, considerando a rede ensino como uma <i>Extranet</i>, bem como o acesso a recursos da UB via VPN ou <i>Wireless</i>.</p> <p>A arquitectura da rede de serviços deverá seguir as boas práticas do mercado no que se refere à resistência a intrusões (internas e externas) e mitigação do impacto de intrusões bem sucedidas através de múltiplas zonas de segurança, utilização de soluções backend / frontend, separação e filtragem de tráfego entre as diferentes redes.</p>
Escalabilidade	O desenho da arquitectura deverá permitir a IETI escalar facilmente de modo suportar a inclusão de novos serviços.
Disponibilidade	A arquitectura deverá ter características de alta disponibilidade de acordo com os níveis de disponibilidade assegurados pelas arquitecturas dos serviços disponibilizados que suporta.
Gestão	Os serviços disponibilizados bem como os de suporte deverão suportar mecanismos de gestão centralizados.
Consolidação	Sempre que possível a arquitectura lógica deverá privilegiar a consolidação de serviços, otimizando os recursos físicos existentes, bem como o consumo de energia, excepção feita quando as necessidades de segurança se sobreporem a quaisquer outras.

Tabela 1 - Rede de Serviços UB, Caracterização do serviço

2.2. Arquitectura lógica

Para desenhar a arquitectura lógica presente neste documento foram definidas linhas de orientação baseadas nos vectores de qualidade descritos acima e nas boas práticas de desenho definidas pela WSSRA.

Foram considerados os seguintes princípios orientadores de forma a assegurar uma alta coerência entre as diferentes partes da arquitectura proposta, incluindo o melhor compromisso entre segurança e razoabilidade.

1. Nenhum equipamento exposto directamente a tráfego originário da Internet, deverá ter capacidade para iniciar uma sessão de comunicação para servidores que alojam informação sensível;
2. Nenhum equipamento com endereços públicos configurados ou nos quais terminem sessões de comunicações iniciadas na Internet, deverá conter informação sensível;

3. Considera-se que todos os equipamentos e redes onde existam equipamentos configurados com endereços públicos se encontram expostos a um risco alto de ataques premeditados;
4. Considera-se que a rede de ensino é igualmente uma rede com risco alto de ataques premeditados;
5. Apenas *firewalls* ou *routers* poderão ser configurados para fazer *routing* ou NAT de tráfego entre diferentes redes;
6. A zona de rede interna onde se localizam os servidores com informação sensível deve ser mantida a um nível de risco tão baixo quanto possível;
7. Todos os equipamentos de uma mesma floresta *Active Directory* (AD) devem ser considerados ao mesmo nível de risco, determinado pelo equipamento cujo nível de risco se considera mais alto;
8. Considera-se informação sensível a que se relaciona com dados pessoais dos utilizadores, informação contida em bases de dados que suportam sistemas de suporte ao negócio, caixas de correio electrónico, entre outros;
9. A segurança da solução deverá ser garantida a diversos níveis, nomeadamente através do *hardening* dos servidores e através da arquitectura lógica e física de comunicações.

Nota | Esta lista não reflecte nenhuma ordem em particular.

Com base nos princípios anteriores foram definidas as seguintes zonas de segurança presentes na Tabela 2:

Fronteira Externa	Zona que representa a transição do equipamento do ISP para a Rede de Serviços UB.
Perímetro	Zona que contém todos os equipamentos dedicados com ligação à Internet, quer oferecendo serviços para a Internet quer recebendo.
Rede Corporativa	Zona que contém todos os equipamentos clientes da rede corporativa da UB, nomeadamente os serviços administrativos da entidade gestora da UB.
Rede de Dados	Zona que contém todos os Sistema de Gestão de Base de Dados (SGBD) necessários à rede de serviços da UB, bem como a gestão dos mesmos, incluindo os corporativos.
Rede de Ensino	Zona referente a toda a rede de ensino da UB, incluindo sala de aulas, sala de professores, biblioteca, quiosques de consulta de serviços entre outros.
Rede Externa	Zona referente à rede disponível para os docentes e alunos ligarem os seus equipamentos particulares à rede de serviços da UB.
Rede Laboratório	Zona que contém todos os equipamentos necessários à investigação académica ou ao desenvolvimento de produtos e / ou serviços que a UB possa disponibilizar a terceiros.
Rede SAN	Zona responsável pelo armazenamento da maior parte da informação.

Tabela 2 - Rede de Serviços UB, Arquitectura lógica

De forma a assegurar os padrões de segurança pretendidos a transição entre zonas de segurança será sempre assegurada por um *firewall*. Privilegia-se a utilização de *firewalls* dedicados entre cada duas zonas por permitir uma maior flexibilidade na escolha da tecnologia a utilizar na sua implementação e por simplificar a configuração e operação das respectivas políticas. Este será um factor de segurança acrescido, visto que a exploração de vulnerabilidades em *firewalls* está associada a uma configuração excessivamente complexa que promove a existência de falhas nas respectivas políticas, ao invés de problemas com o funcionamento do próprio equipamento.

A Figura 1 representa a recomendação da arquitectura global da Rede de Serviços UB, que se encontram mais detalhados nos capítulos seguintes:

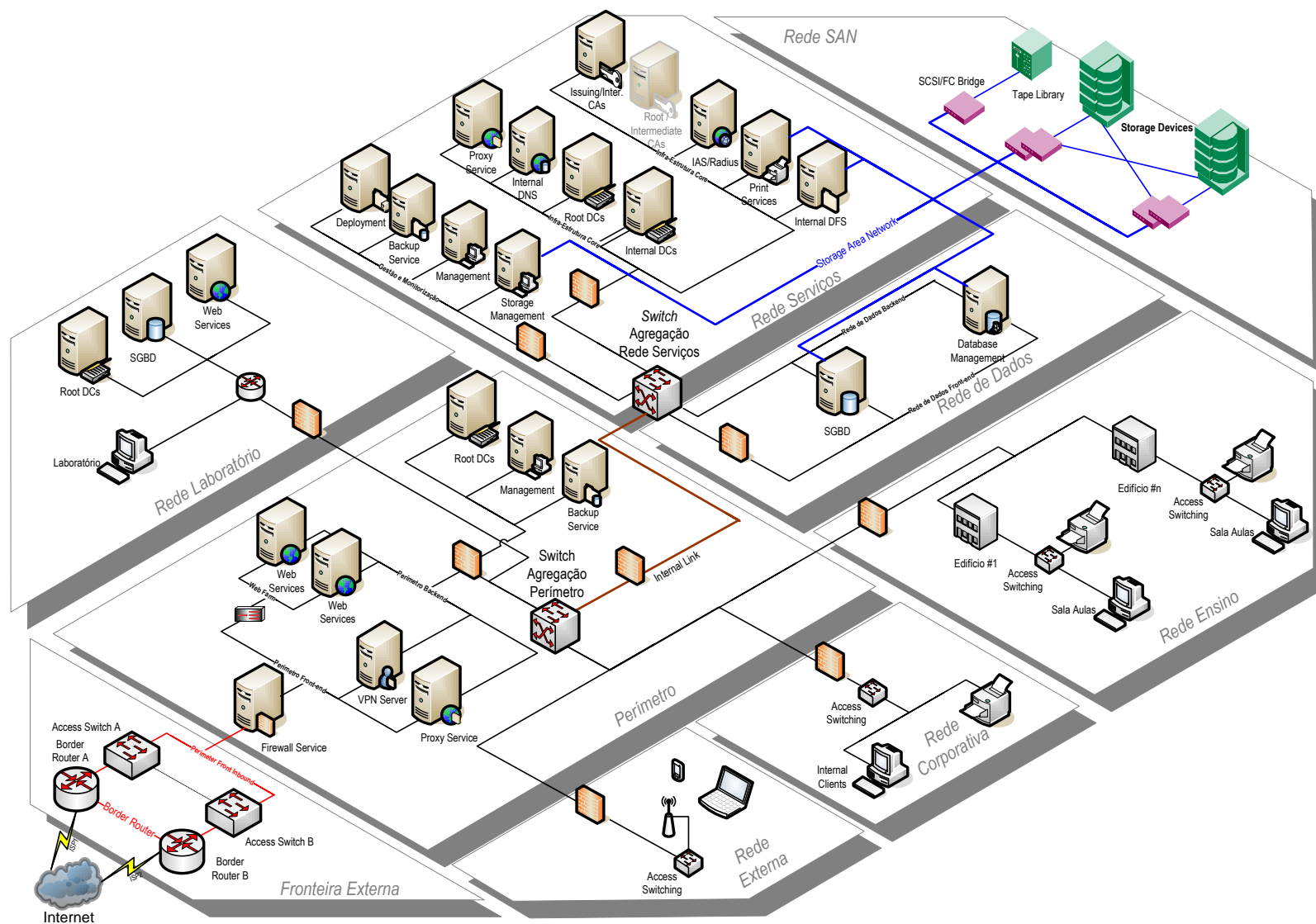


Figura 1 – Rede de Serviços UB, Arquitectura lógica

É importante voltar a referir que a arquitectura apresentada apenas se refere ao desenho lógico da infra-estrutura da Rede de Serviços UB.

Os símbolos representados na Figura 1 representam instâncias lógicas de serviço e não equipamentos físicos. A implementação física dos serviços poderá consolidar múltiplas instâncias de serviço nos mesmos equipamentos.

A Tabela 3 explica sucintamente os símbolos não relacionados com servidores e serviços, explicados no âmbito deste trabalho.

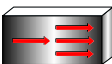






	Representa instâncias de balanceamento de tráfego implementadas com recurso a hardware ou ao serviço Network Load Balancing (NLB) incluído no Windows Server 2003.
	Representam instâncias de <i>switching Layer 2</i> . Poderão ser implementadas por múltiplos equipamentos ou por um único equipamento nomeadamente pelos <i>Switchs Agregadores</i> .
	Representam instâncias de <i>switching Layer 3</i> . Podem ser implementada por um único equipamento físico ou por múltiplos equipamentos, respeitando o princípio de criar um serviço lógico consolidado.
	Representam instâncias de <i>routing Layer 3</i> .
	Representam instâncias de serviço de <i>firewall</i> , implementadas por equipamentos de comunicações ou usando o ISA Server. Estas instâncias de serviço poderão ser implementadas por equipamentos dedicados ou através de módulos funcionais incluídos noutros equipamentos.
	Representam pontos de acesso <i>wireless</i> para acesso da rede externa.
	Representam dispositivos de armazenamento como bibliotecas de discos.

Tabela 3 - Rede de Serviços UB, Arquitectura lógica (Legenda)

3. Serviços disponibilizados pela UB

São definidas de seguida as arquitecturas dos serviços oferecidos pela UB aos seus utilizadores, sendo os serviços oferecidos:

- Correio Electrónico;
- Acesso à Internet;
- Partilha de Informação;
- eLearning.

Estes serviços são suportados pelos serviços de suporte caracterizados no capítulo 4.

3.1. Correio Electrónico

3.1.1. Caracterização do Serviço

O serviço de Correio Electrónico assume-se cada vez mais como essencial e crítico na comunicação entre docentes e alunos. A Microsoft tem no Microsoft Exchange Server 2007 uma plataforma capaz de cumprir com os requisitos de segurança, disponibilidade e escalabilidade definidos, nomeadamente na sua arquitectura de 64 bits, na capacidade de *Unified Messaging* que permite a interacção com serviços VOIP bem como serviços de Fax e correio electrónico através de telefone de modo a gerir o correio, calendário e contactos e por fim na divisão lógica dos serviços e funcionalidades por servidores (*roles*), indo além dos *roles* primários da versão 2003 que eram basicamente *front-end* e *backend*.

Os pressupostos para este serviço garantem para cada aluno da UB uma caixa de correio individual com capacidade de 50MB de capacidade, ou em alternativa e por opção do aluno, ser efectuado um reencaminhamento do correio recebido para uma caixa pessoal externa à UB. Para os docentes será dimensionada uma caixa de correio individual com capacidade de 500MB com possibilidade de efectuar o redireccionamento para uma outra caixa de correio, deixando o correio recebido na caixa corporativa da UB.

A Tabela 4 descreve os principais aspectos a considerar no desenho da arquitectura do serviço de Correio Electrónico.

Segurança	<p>Todos os servidores que disponibilizem o serviço de Correio Electrónico deverão ser protegidos e segregados fisicamente em redes distintas consoante os <i>roles</i> definidos. Ao nível lógico, devem ser aplicadas configurações de <i>hardening</i> do sistema operativo e respectivos serviços.</p> <p>A implementação dos diferentes <i>roles</i> por servidor deverá ser implementada de forma a poder maximizar o nível de segurança.</p> <p>Uma vez que este serviço necessita de contacto directo e indirecto com a Internet é fundamental que as melhores práticas de segurança relativas a esta solução sejam aplicáveis.</p> <p>Todas as caixas de correio devem ser armazenadas em servidores de <i>backend</i>, directamente inacessíveis a partir da Internet ou da zona Perímetro.</p> <p>Nenhum servidor da Organização de Exchange 2007 deverá ser exposto directamente à Internet ou ter configurado endereços IP públicos. O acesso aos serviços deverá ser sempre efectuado através da publicação do respectivo serviço, utilizando mecanismos de cifra desde o Cliente até ao servidor de Exchange.</p>
Escalabilidade	<p>A infra-estrutura deverá suportar um máximo de 500 utilizadores a utilizar o serviço em simultâneo, e um universo de 2000 caixas de correio.</p> <p>Adicionalmente, o desenho da arquitectura deverá acomodar mudanças na UB, nomeadamente o aumento do número de cursos disponíveis e consequentemente o número de utilizadores simultâneos.</p>
Disponibilidade	<p>A arquitectura deste serviço deverá ter características de alta disponibilidade, nomeadamente a utilização do serviço de <i>Cluster</i>.</p> <p>A diferenciação dos <i>roles</i> de Exchange deverá ser implementada de forma a poder aumentar a disponibilidade de serviço</p>
Gestão	<p>A gestão do serviço de Correio Electrónico bem como dos seus mecanismos deverá ser integralmente assumida pela equipa de gestão da IETI da UB.</p> <p>A gestão deste serviço será auxiliada por um conjunto de serviços de apoio, integrados nos serviços de Gestão da Plataforma.</p>
Consolidação	<p>De acordo com a política global assumida sempre que a consolidação de diversas funções num único equipamento não cause problemas para a segurança da plataforma ou limite o desempenho da solução, a consolidação deve ser favorecida.</p>

Tabela 4 - Correio Electrónico, Caracterização do Serviço

Este projecto oferece um conjunto alargado de funcionalidades como o caso do *Webmail* via *Outlook Web Access (OWA)* ou o serviço de sincronização com dispositivos móveis *ActiveSync* a acrescentar às anteriormente referidas.

3.1.2. Arquitectura Lógica

Quando se instala o primeiro servidor Microsoft Exchange 2007 numa floresta é criada uma Organização, que é a unidade lógica na arquitectura Exchange e que corresponde ao conceito de floresta em AD. A floresta corresponde, assim, ao directório da Organização de Exchange. Este factor assume maior importância relativamente à decisão de separação de florestas de AD, conforme o descrito no serviço Directório, Autenticação e Autorização.

Na sequência desta decisão terão que ser criadas duas organizações de Exchange 2007 nas duas florestas que necessitam do serviço de Correio Electrónico (*ub.local* e *ensino.local*), em que nenhuma delas será autoritária relativamente ao domínio da UB na Internet (*ub.pt*) permitindo assim a criação de conectores para as mensagens que não forem entregues no servidor do domínio *ub.local* serem reencaminhadas para o domínio *ensino.local* de forma a serem entregues. Desta forma é possível manter um único domínio para o Correio Electrónico.

A opção de uma única floresta de recursos de Exchange não permitiria manter a segurança e independência entre redes necessária, uma vez que teria que existir *trusts* bidireccionais entre as florestas e as caixas de correio ficariam sempre alojadas numa única floresta, criando constrangimentos ao nível dos pressupostos assumidos, como a independência entre florestas.

De forma a ter as *Global Address List* (GAL) sincronizadas poder-se-á recorrer ao Microsoft Identity Server Feature Pack (MIIS FP), que garante a sincronização das listas de endereços de ambas as Organizações de Exchange 2007, permitindo ter um controlo mais selectivo sobre quais os contactos que deverão passar de Organização para Organização, podendo, por exemplo, eliminar-se na floresta ensino.local os contactos pessoais dos administrativos da entidade gestora da UB, ub.local, deixando apenas as caixas de correio de serviço, como a Secretaria Electrónica entre outras. O fluxo inverso também é possível permitindo a passagem apenas das listas de distribuição desejadas e não a totalidade de caixas de correio dos alunos.

Poderá ser observado na Figura 2 o fluxo de dados MIIS entre as florestas com Organizações de Exchange.

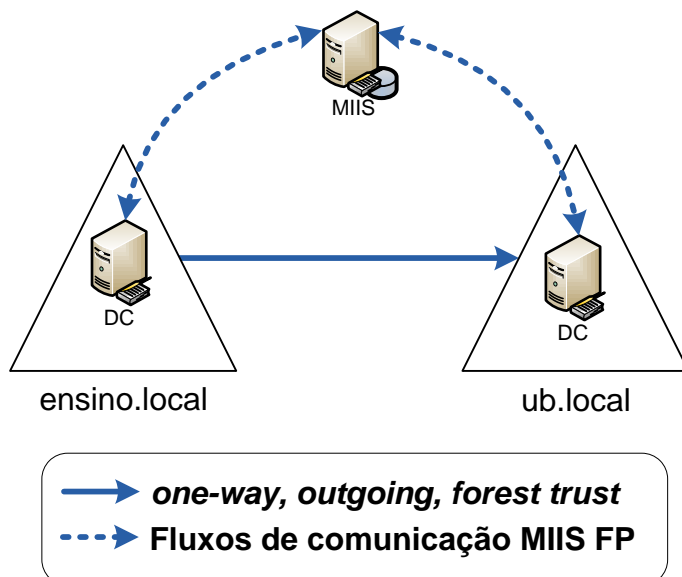


Figura 2 - Correio Electrónico, Arquitectura Lógica (MIIS FP)

O Microsoft Exchange 2007 permite uma maior segregação de funções separando os diferentes *roles* necessários à Organização como se pode observar sucintamente na Tabela 5.

Mailbox Server (MS)	Este <i>role</i> armazena todas as caixas de correio electrónico dos utilizadores, além de permitir a conexão de tráfego Messaging Application Programming Interface (MAPI), nativo entre clientes Outlook e Exchange.
Client access server (CA)	Este <i>role</i> permite a conexão de Clientes por métodos não standard à arquitectura Exchange 2007, tais como o OWA, Exchange ActiveSync, Post Office Protocol 3 (POP3) e Internet Message Access Protocol (IMAP). São os substitutos dos servidores <i>front-end</i> e podem recorrer a NLB de forma a obter uma maior redundância.
Hub Transport server (HT)	Este <i>role</i> actua como ponte do tráfego de correio electrónico entre servidores de diferentes sites da AD.
Unified Messaging server (UM)	Este <i>role</i> é novo no Exchange 2007 e permite que a caixa de correio de um utilizador seja utilizada para Fax e correio de voz.
Edge Transport server (ET)	Este <i>role</i> é igualmente novo no Exchange 2007 e permite ter um servidor em <i>workgroup</i> numa zona desmilitarizada, tal como o Perímetro. Tem como objectivo filtrar o tráfego Simple Mail Transport Protocol (SMTP) de vírus e <i>spam</i> , efectuando o reencaminhamento para os servidores HT. Estes servidores possuem uma versão da Active Directory Application Mode (ADAM) sincronizada com a infra-estrutura de AD interna.

Tabela 5 - Correio Electrónico, Arquitectura Lógica (*roles* do Exchange 2007)

A Figura 3 demonstra a colocação dos diferentes *roles* nas diferentes zonas de segurança.

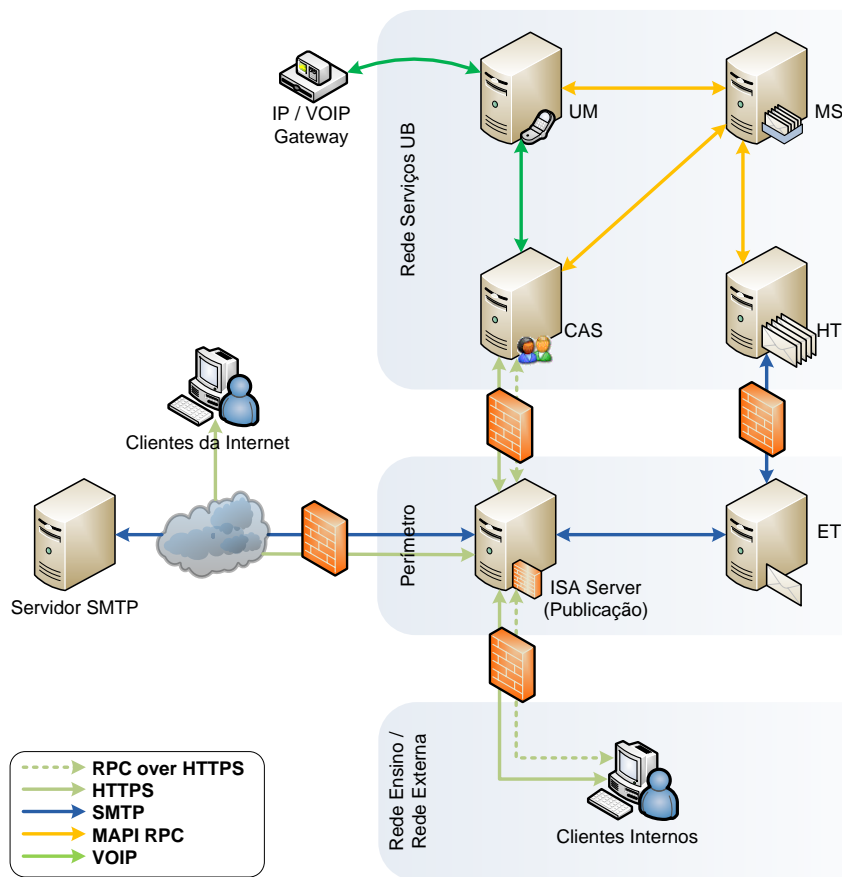


Figura 3 - Correio Electrónico, Arquitectura Lógica

Nota A arquitectura presente na Figura 3 será a mesma para ambas as florestas à excepção do *role* UM que não foi considerado na floresta ensino.local. Dado o baixo número de utilizadores da floresta ub.local e de forma a minorar os custos de implementação, gestão e manutenção poderão ser consolidados os *roles* MS, CA e HT num único servidor.

Dadas os requisitos de segurança será necessário que qualquer ligação aos servidores de *backend* seja efectuada através dos protocolos HTTPS e RPC over HTTPS na rede de ensino e rede externa e somente através de HTTPS através da Internet.

Desta forma será possível utilizar o cliente Microsoft Office Outlook (RPC over HTTPS) nas redes disponíveis na UB, bem como o OWA e dispositivos móveis através do *ActiveSync* (HTTPS). Do exterior poderão ser usados o OWA e *ActiveSync*, uma vez que o único protocolo permitido de acesso às caixas de correio será o HTTPS.

3.2. Acesso à Internet

3.2.1. Caracterização do Serviço

O acesso dos utilizadores à Internet em ambiente académico é considerado fundamental, facto pelo qual o serviço de acesso à Internet, vulgarmente conhecido por *proxy*, deverá ser optimizado e redundante.

A Tabela 6 descreve as principais características a respeitar no desenho da arquitectura do serviço de acesso à Internet.

Segurança	<p>Todos os servidores que disponibilizem o serviço de Acesso à Internet deverão ser protegidos e segregados fisicamente em redes distintas consoante os <i>roles</i> definidos. Ao nível lógico, devem ser aplicadas configurações de <i>hardening</i> do sistema operativo e respectivos serviços.</p> <p>Todos os acessos à Internet devem ser autenticados e registados. A autorização deve ser atribuída por utilizador (ou grupo de utilizadores), sendo excepcionalmente possível autorizar outros recursos, nomeadamente endereços IP de servidores. Adicionalmente, nenhum equipamento na rede interna ou nas florestas da UB deverá ter capacidade para resolver endereços públicos ou aceder a esses recursos sem utilizar a infra-estrutura de acesso à Internet.</p> <p>Sendo este um serviço com pontos de contacto com equipamentos na Internet, é fundamental que todas as precauções e boas práticas de desenho de segurança aplicáveis a este tipo de soluções sejam seguidas.</p>
Escalabilidade	<p>A infra-estrutura deverá suportar um máximo de 500 utilizadores a utilizar o serviço em simultâneo. Adicionalmente, o desenho da arquitectura deverá acomodar mudanças na UB, nomeadamente o aumento do número de cursos disponíveis e conseqüentemente o número de utilizadores simultâneos.</p>
Disponibilidade	<p>A arquitectura do serviço de Acesso à Internet deve ser dotada de características de alta disponibilidade. Em particular, em caso de falha total de um servidor individual ou no serviço, o mesmo deverá continuar disponível sem degradação de desempenho, pelo que um segundo circuito de acesso à Internet deverá ser contratado a um ISP diferente do primeiro.</p>
Gestão	<p>A gestão do serviço de Acesso à Internet bem como dos seus mecanismos deverá ser integralmente assumida pela equipa de gestão da IETI da UB.</p> <p>A gestão deste serviço será auxiliada por um conjunto de serviços de apoio, integrados nos serviços de Gestão da Plataforma.</p>
Consolidação	<p>De acordo com a política global assumida sempre que a consolidação de diversas funções num único equipamento não cause problemas para a segurança da plataforma ou limite o desempenho da solução, a consolidação deve ser favorecida.</p>

Tabela 6 - Acesso à Internet, Caracterização do Serviço

3.2.2. Arquitectura Lógica

Para o desenho de uma arquitectura deste tipo e com os níveis de disponibilidade requeridos, é essencial avaliar os seguintes factores:

- Topologia da rede WAN
- Local e largura de banda da ligação à Internet
- Serviços a disponibilizar e protocolos autorizados
- Número de sessões concorrentes a suportar

Será expectável que a larga maioria dos utilizadores autorizados apenas possam aceder a serviços acedidos usando os protocolos HTTP, HTTPS e FTP. Por outro lado, antecipa-se a eventual necessidade de alguns utilizadores virem a utilizar outros serviços, eventualmente aplicações que não tenham suporte para a utilização de um *Proxy* ou acesso a endereços que não respeitem as portas standard de HTTP (TCP 80), HTTPS (TCP 443) e FTP (TCP 20 e 21).

Dadas as características dos clientes suportados, recomenda-se a configuração da arquitectura para suportar os clientes *Web Proxy* e *Firewall Client*, com os primeiros a constituírem o tipo de cliente preferencial.

O Microsoft ISA Server 2006, utilizado na implementação deste serviço, suporta três tipos de clientes:

- *Web Proxy* – Estes clientes enviam pedidos directamente para o servidor *Proxy*, mas o acesso à Internet está limitado ao browser ou a outras aplicações cliente que suportem *Proxies*.
- *SecureNAT* – Oferecem segurança e *caching* mas não permitem autenticação ao nível do utilizador. Apenas necessitam da configuração do endereço da *default gateway* a apontar para o servidor ISA Server 2006. Qualquer cliente que utilize TCP/IP pode ser um cliente *SecureNAT*.
- *Firewall Client* – Permite autorizar o acesso com base no utilizador para todos os pedidos de saída que utilizem TCP ou UDP. Necessita da instalação de uma aplicação cliente em cada estação de trabalho.

Dadas as características dos clientes suportados, recomenda-se a configuração da arquitectura para suportar os clientes *Web Proxy* e *Firewall Client*, com os primeiros a constituírem o tipo de cliente preferencial.

De forma a suportar os níveis desejados de disponibilidade do serviço, os servidores acedidos pelos clientes deverão ser configurados em NLB. Os servidores assim configurados permitem oferecer um elevado grau de disponibilidade e desempenho, e pode ser utilizados quer pelos clientes *Web Proxy*, quer pelos clientes *Firewall Client*.

Os servidores deverão ser configurados com o Microsoft ISA Server 2006 Enterprise Edition e constituídos num *array* comum, permitindo assim usufruir de uma gestão centralizada das configurações aplicadas a todos eles.

Recomenda-se a constituição de uma *cache* de conteúdos lidos nos acessos à Internet de forma a reduzir a utilização do acesso à Internet para obtenção de conteúdos comuns e de grande procura. De forma a evitar a multiplicação do mesmo conteúdo por diversos servidores, deverá ser activado o protocolo Cache Array Routing Protocol (CARP) na rede dos servidores ISA onde são recebidos pedidos *cacheable*, nomeadamente pedidos HTTP de clientes *Web Proxy*. Através do protocolo CARP, a *cache* individual de cada servidor é partilhada com os restantes membros do *array*. No entanto o acesso a endereços onde sejam efectuados exames não deverá ser alvo de *cache*.

A Figura 4 demonstra o processo de acesso à Internet, comum para o *Web Proxy* e *Firewall Client*.

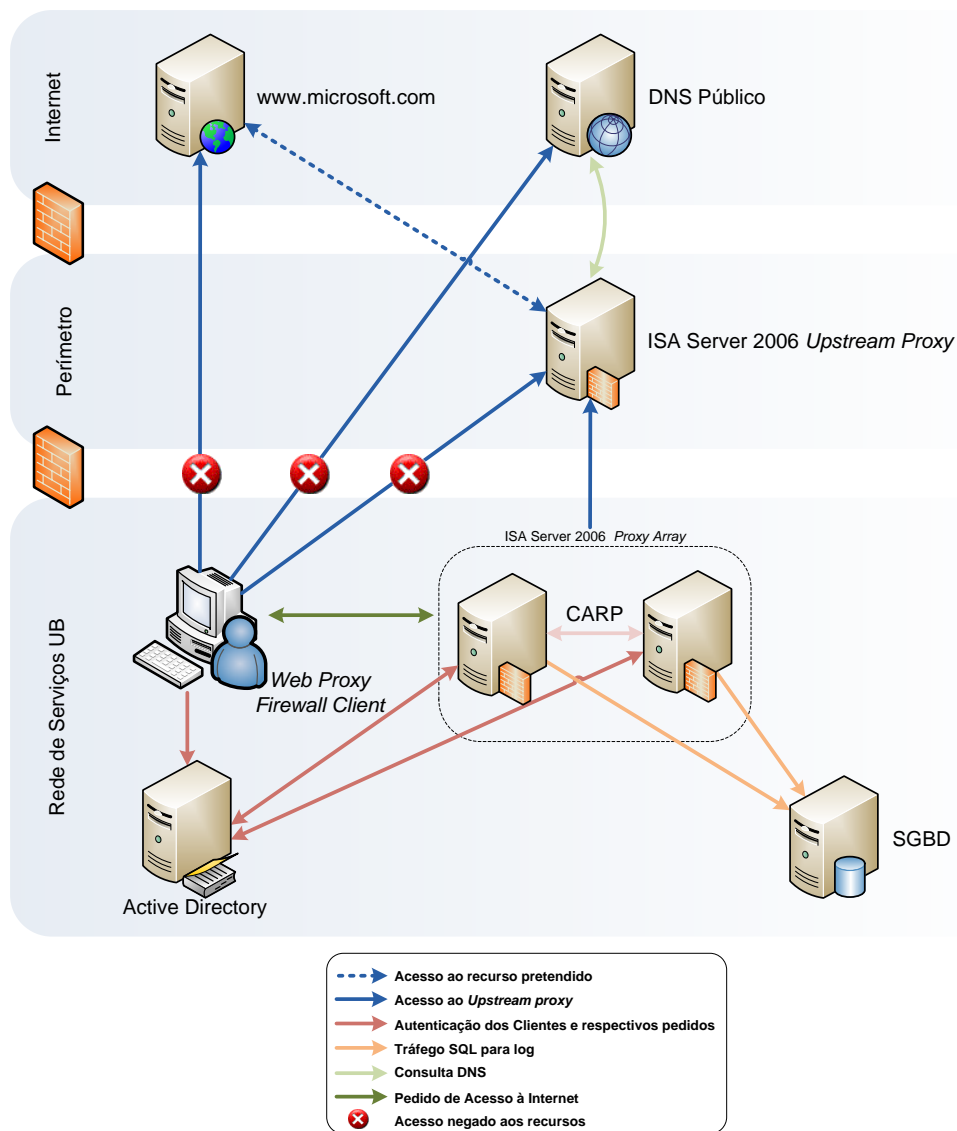


Figura 4 - Acesso à Internet, Arquitectura Lógica

A autenticação e autorização dos utilizadores são asseguradas através dos *trusts* estabelecidos entre os diferentes domínios de onde as contas de utilizadores são originárias. As contas dos utilizadores são colocadas em grupos de segurança dos diferentes domínios e autorizados a aceder aos recursos em causa, sendo a autenticação dos mesmos perante o serviço totalmente transparente. A escolha de um *proxy* de *upstream* permite aceder a recursos da Internet através da zona do Perímetro onde não existem *trusts* com nenhuma outra floresta.

Mais detalhes sobre a estrutura da floresta AD e respectivos *trusts* poderão ser consultados na secção 4.1.

3.3. Partilha de Informação

3.3.1. Caracterização do Serviço

À semelhança do Correio Electrónico e Acesso à Internet também a Partilha de Informação no meio académico é fundamental, assumindo-se como um canal preferencial na troca de ficheiros e comunicação entre docentes e alunos. A Microsoft disponibiliza o Windows SharePoint Services 3.0 (WSS) de forma gratuita¹, uma plataforma Web que oferece serviços de Partilha de Informação com características que o tornam mais adequado ao ambiente académico do que a simples partilha de ficheiros, tais como versões de documentos, aprovação dos mesmos, calendário e pesquisa de conteúdo de documentos, além de uma série de outras características que o tornam num produto Web 2.0, tais como *Wiki*, *Blogs* e *Fóruns*.

A Tabela 7 descreve os principais aspectos a considerar no desenho da arquitectura do serviço de Partilha de Informação.

¹ Será necessário licenças do sistema operativo servidor Microsoft Windows 2003 Server Standard, Enterprise ou Datacenter.

Segurança

Dado que a plataforma estará exposta a um conjunto de canais diferentes e que consequentemente têm universos de utilizadores também eles diferentes a segurança será considerada como uma qualidade indispensável à solução.

A autenticação dos utilizadores nos portais WSS será integrada na AD.

Ainda, ao nível dos sistemas, para além dos mecanismos de segurança de base do sistema operativo Windows Server 2003, disponíveis desde o primeiro momento da instalação, deverá ser realizado um *hardening* base das suas componentes.

É no entanto indispensável que, associado ao aumento do nível de auditoria a realizar, seja efectuada uma monitorização que permita analisar a informação recolhida em tempo útil.

A gestão do serviço de Partilha de Informação deverá ser totalmente assegurada pela equipa de gestão da IETI da UB, sem prejuízo da capacidade de delegação de tarefas individuais de gestão de serviço a membros da equipa.

Escalabilidade

O desenho da arquitectura deverá acomodar mudanças na UB, nomeadamente o aumento do número de cursos disponíveis e consequentemente o número de utilizadores simultâneos.

Estas evoluções pressupõem uma maior carga sobre os equipamentos, quer ao nível do número de pedidos de serviço por clientes, quer ao nível do volume de informação suportada no directório.

O desenho lógico da solução foi realizado de forma a dotar a plataforma de elevados níveis de escalabilidade. Nomeadamente *scale-out*, bem como *scale-up*.

<p>Disponibilidade</p>	<p>A arquitectura do serviço de Partilha de Informação deve ser dotada de características de alta disponibilidade. Em particular, em caso de falha total de um servidor individual, o serviço deverá continuar disponível sem degradação de desempenho.</p> <p>O serviço de Partilha de Informação será disponibilizado localmente na <i>Local Area Network</i> (LAN) da rede de serviços da UB, bem como externamente através da ligação WAN à Internet.</p> <p>O desenho lógico e físico da solução para o serviço de Partilha de Informação tomou em consideração os requisitos normais para uma solução deste género que requerem níveis de alta disponibilidade. Através das melhores práticas de desenho e implementação, definidas pelas equipas de produto e pela sua experiência de implementação de soluções semelhantes, procurou-se desenhar a melhor solução tendo em conta os requisitos pretendidos.</p> <p>Para garantir o objectivo de dotar a arquitectura de altos índices de disponibilidade, esta deverá estar equipada com as seguintes facultades:</p> <ul style="list-style-type: none"> • <i>Web Farms</i> que asseguram a disponibilidade dos serviços. Na falha de um servidor o serviço continuará a suportar os utilizadores finais através dos restantes servidores. • <i>Cluster</i> de dois servidores Microsoft SQL Server 2005 para garantir a manutenção do serviço caso haja uma eventual falha de um componente do sistema com o <i>failover</i> do serviço para o outro nó.
<p>Gestão</p>	<p>A gestão do serviço de Partilha de Informação bem como dos seus mecanismos deverá ser integralmente assumida pela equipa de gestão da IETI da UB.</p> <p>A gestão deste serviço será auxiliada por um conjunto de serviços de apoio, integrados nos serviços de Gestão da Plataforma.</p>
<p>Consolidação</p>	<p>As boas práticas de desenho deste tipo de serviços indicam que, de uma forma geral, os servidores que compõem o serviço de Partilha de Informação (WSS) não devem suportar outras funções. Caso contrário, serão comprometidos os objectivos de <i>hardening</i> dos equipamentos e serviços, para além de aumentar os riscos para a segurança e disponibilidade do serviço.</p>

Tabela 7 - Partilha de Informação, Caracterização do Serviço

3.3.2. Arquitectura Lógica

A configuração proposta no âmbito da Rede de Serviços UB consiste numa *web farm* que tenha as seguintes características:

- Existência de múltiplos servidores separados a correr o WSS e o SQL Server. Desta forma garante-se a alta disponibilidade necessária.
- Múltiplos *sites* e *sub-sites* agrupados em *site collections* em cada *virtual server* do Internet Information Services (IIS) que seja estendido com o WSS.
- Desempenho e capacidade são aumentados adicionando servidores a correr o Windows SharePoint Services e o SQL Server.
- A escalabilidade do sistema baseia-se na adição de mais *front-ends* para aumentar a qualidade de entrega dos conteúdos existentes, e pela adição de novos Web sites de topo e sub-sites com o intuito de aumentar os conteúdos.
- O balanceamento de carga é atingido com recurso à utilização de equipamento activo que efectue essas funções, ou pela utilização do NLB do Windows Server 2003.

A Figura 5 ilustra a arquitectura para o WSS numa configuração de *web farm*.

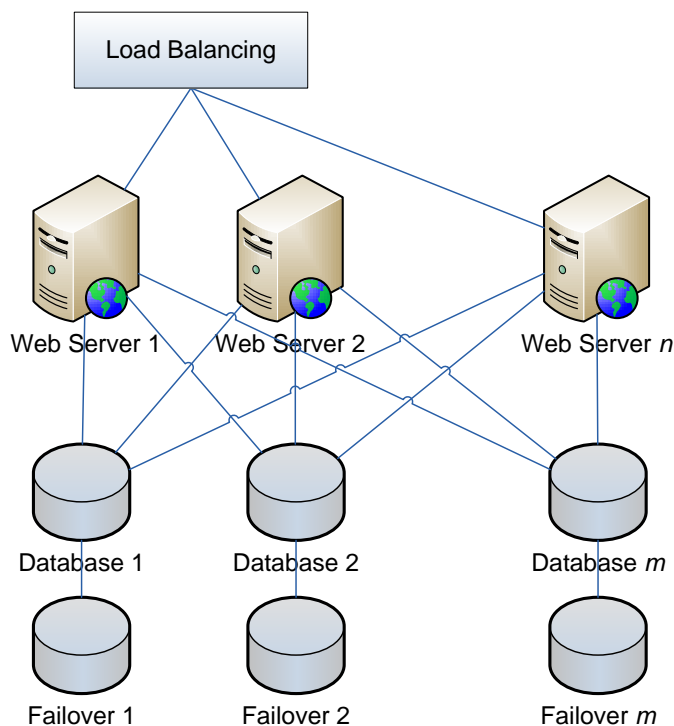


Figura 5 - Partilha de Informação, Arquitectura Lógica

Neste diagrama podem observar-se as potencialidades desta arquitectura. Como a informação dos sites é guardada directamente nas bases de dados de conteúdos, pode distribuir-se a carga por vários *front-ends* com o WSS, e todos podem comunicar com a base de dados apropriada aos conteúdos.

Numa *web farm*, cada *front-end* a correr o WSS pode ter múltiplos *virtual servers*. Cada *virtual server*, por seu lado, pode ter múltiplas *collections* de sites, que por seu turno podem conter um *Web site* de topo e múltiplos *sub-sites*.

A Figura 6 ilustra exactamente esta hierarquia.

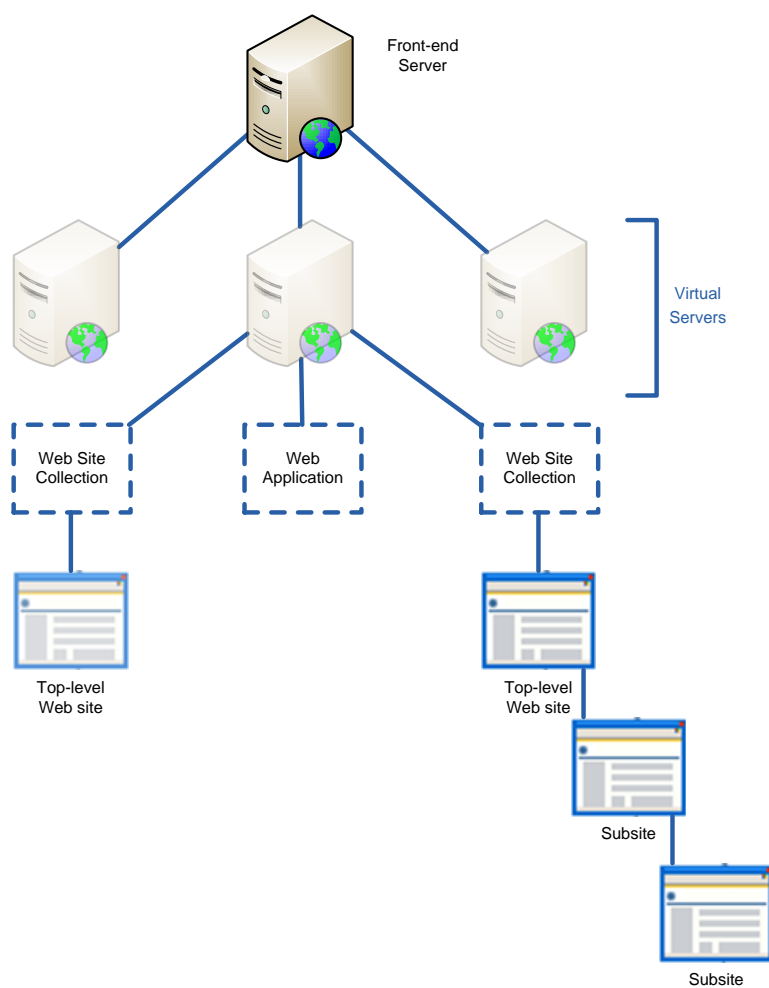


Figura 6 - Partilha de Informação, Arquitectura Lógica (Hierarquia de sites)

3.4. eLearning

3.4.1. Caracterização do Serviço

O serviço de eLearning apresenta-se como a plataforma de excelência a utilizar pela UB para oferecer formação aos seus alunos, docentes e colaboradores.

O serviço de eLearning representa a primeira evolução, baseada nos produtos e tecnologias disponíveis à data de elaboração do presente documento. No entanto, a visão para este serviço prevê a sua evolução para suportar futuras tecnologias como Microsoft Office Sharepoint Learning Kit.

Neste documento apenas serão abordados os aspectos relacionados com a arquitectura da infra-estrutura necessária para suportar o serviço de eLearning, excluindo-se os aspectos da arquitectura funcional da solução.

A Tabela 8 descreve os principais aspectos a considerar no desenho da arquitectura do serviço de eLearning.

Segurança	<p>Todos os servidores que disponibilizem o serviço de eLearning deverão ser protegidos e segregados fisicamente em redes distintas consoante os <i>roles</i> definidos. Ao nível lógico, devem ser aplicadas configurações de <i>hardening</i> do sistema operativo e respectivos serviços.</p> <p>Toda a informação que suporta o serviço, tais como documentos entre outros, deverá ser guardada em servidores de <i>backend</i>, inacessíveis directamente a partir da Internet ou da zona de Perímetro.</p>
Escalabilidade	<p>A infra-estrutura deverá suportar um máximo de 100 utilizadores a usar o serviço em simultâneo, e um universo de 2000 potenciais utilizadores.</p> <p>Adicionalmente, o desenho da arquitectura deverá acomodar mudanças na UB, nomeadamente o aumento do número de cursos disponíveis e consequentemente o número de utilizadores simultâneos.</p>
Disponibilidade	<p>A arquitectura do serviço de eLearning deve ser dotada de características de alta disponibilidade. Em particular, em caso de falha total de um servidor individual, o serviço deverá continuar disponível sem degradação de desempenho. Excluem-se as componentes relacionadas com a indexação de conteúdos cuja indisponibilidade temporária não implica uma indisponibilidade total do serviço.</p>
Gestão	<p>A gestão do serviço de eLearning bem como dos seus mecanismos deverá ser integralmente assumida pela equipa de gestão da IETI da UB</p> <p>Sendo possível a criação e disponibilização de conteúdos sem necessidade de privilégios de administração sobre a plataforma estas tarefas poderão ser delegadas aos Docentes.</p> <p>A gestão deste serviço será auxiliada por um conjunto de serviços de apoio, integrados nos serviços de Gestão da Plataforma.</p>
Consolidação	<p>De acordo com a política global assumida sempre que a consolidação de diversas funções num único equipamento não cause problemas para a segurança da plataforma ou limite o desempenho da solução, a consolidação deve ser favorecida. Em particular, a colocação de múltiplos serviços nos servidores <i>frontend</i>.</p>

Tabela 8 - eLearning, Caracterização do Serviço

3.4.2. Arquitectura Lógica

O serviço de eLearning constitui-se numa solução que integra, por sua vez, diversos produtos e serviços, alguns dos quais fazem parte dos serviços disponibilizados pela UB. A saber, o serviço de eLearning é formado pelos seguintes produtos e serviços:

- Directório (secção 4.1);
- Acesso à Internet (secção 3.2);
- Sistema de Gestão de Base de Dados (secção 4.3);
- Microsoft Windows SharePoint Services (secção 3.3);
- SharePoint Learning Kit (SLK)

A Figura 7 ilustra a arquitectura lógica da infra-estrutura de suporte ao serviço de eLearning, bem como os fluxos de comunicação.

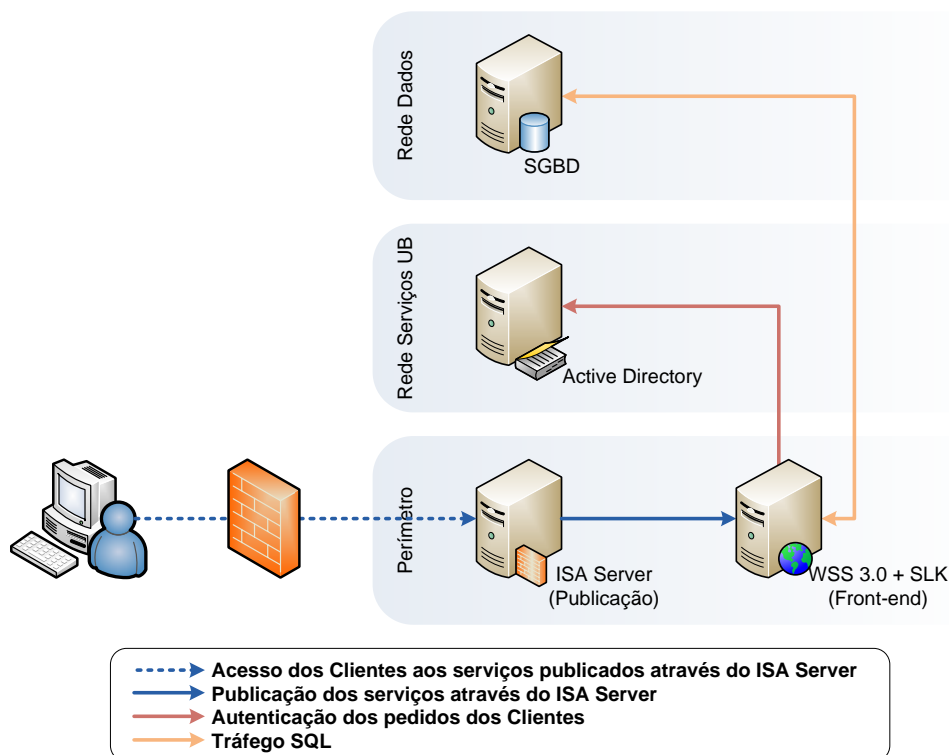


Figura 7 - eLearning, Arquitectura Lógica

O SLK² é uma aplicação de eLearning com capacidade de entrega e controlo de conteúdos, conforme a norma SCORM 2004 2nd Edition³, construída sob a forma de uma aplicação para WSS e Microsoft Office SharePoint Server 2007 (MOSS), permitindo efectuar a entrega de conteúdos de eLearning aos Alunos, possibilidade de avaliar os resultados, permitindo uma gestão praticamente isolada da do WSS.

A criação de conteúdos poderá ser efectuada através de qualquer ferramenta de *authoring* que suporte as normas SCORM 1.2 ou SCORM 2004.

3.5. Resumo

A Tabela 9 mostra de forma concisa a relação entre os serviços oferecidos e as aplicações presentes na solução.

Correio Electrónico	Microsoft Exchange Server 2007 Enterprise Edition
Acesso à Internet	Microsoft ISA Server 2006 Enterprise Edition
Partilha de Informação	Microsoft Windows SharePoint Services 3.0
eLearning	Microsoft Windows SharePoint Services 3.0 e SharePoint Learning Kit

Tabela 9 - Serviços disponibilizados pela UB, Resumo (Aplicacional)

² Mais informações em <http://www.codeplex.com/SLK>.

³ Poderá consultar a certificação em <http://www.adlnet.gov/scorm/certified/Certification.aspx?ID=176>.

4. Serviços de Suporte

Os Serviços de Suporte da UB constituem a espinha dorsal dos Serviços disponibilizados pela UB.

4.1. Directório, Autenticação e Autorização

4.1.1. Caracterização do Serviço

O serviço de Directório, Autenticação e Autorização destina-se a suportar a Rede de Serviços UB bem como a autenticação de utilizadores, *service accounts*, contas de estações de trabalho e acesso aos diferentes recursos locais.

A Tabela 10 descreve os principais aspectos do desenho da arquitectura do serviço de Directório, Autenticação e Autorização.

Segurança	<p>Todos os <i>Domain Controllers</i> (DC) que disponibilizam o serviço de Directório, Autenticação e Autorização devem ser protegidos e segregados fisicamente em redes específicas. Ao nível lógico, devem ser aplicadas configurações de <i>hardening</i> do sistema operativo e respectivos serviços.</p> <p>A infra-estrutura AD que suportará o serviço de Directório, Autenticação e Autorização interno à UB deverá estar lógica e fisicamente isolada de quaisquer equipamentos que suportem serviços na Internet.</p>
Escalabilidade	<p>O desenho da arquitectura deverá desde já prever as características de escalabilidade necessárias para suportar a eventual evolução da UB, nomeadamente integração com outros organismos ou um serviço de PKI.</p> <p>Estas evoluções pressupõem uma maior carga sobre os equipamentos, quer ao nível do número de pedidos de serviço por clientes, quer ao nível do volume de informação suportada no directório.</p>
Disponibilidade	<p>A arquitectura do serviço de Directório, Autenticação e Autorização deve ser dotada de características de alta disponibilidade. Em particular, em caso de falha total de um servidor individual o serviço deverá continuar disponível sem degradação de desempenho.</p>
Gestão	<p>A gestão do serviço de Directório, Autenticação e Autorização deverá ser integralmente assumida pela equipa de gestão da IETI da UB. Por sua vez, a gestão de dados será diferenciada mediante a opção tomada pela UB.</p> <p>A gestão deste serviço será auxiliada por um conjunto de serviços de apoio, integrados nos serviços de Gestão da Plataforma.</p>
Consolidação	<p>As boas práticas de desenho deste tipo de serviços indicam que, de uma forma geral, os DCs não devem suportar outras funções. Caso contrário, serão comprometidos os objectivos de <i>hardening</i> dos equipamentos e serviços, para além de aumentar os riscos para a segurança e disponibilidade do serviço, razão pela qual os equipamentos configurados como DCs deverão ser dedicados a essa função.</p>

Tabela 10 - Directório, Autenticação e Autorização, Caracterização do Serviço

4.1.2. Arquitectura Lógica

Esta arquitectura baseia-se no directório da Microsoft, a AD, baseada no Microsoft Windows Server 2003.

A primeira decisão a tomar quando se desenha uma infra-estrutura AD prende-se com o desenho de florestas. A floresta é definida por uma base de dados que suporta o directório, segmentada em diversas partições lógicas. As diversas partições existentes numa floresta partilham:

- Um modelo de dados (*Schema*) e de configurações comuns;
- Uma única fronteira global de segurança e isolamento.

Apesar da implementação e operação continuada de mecanismos de interligação exigir habitualmente um esforço significativo e um conjunto de competências assinalável, o que por si encarece a solução de directório, a adopção de mais do que uma floresta deverá respeitar pelo menos um dos seguintes aspectos:

- Impor uma fronteira real de isolamento entre duas infra-estruturas, quer para estabelecer diferentes zonas de segurança lógica, quer para isolar completamente a actuação das respectivas de gestão de serviço;
- Permitir a implementação de diferentes aplicações que impõem modelos de dados (*Schema*) incompatíveis entre si.

A arquitectura lógica da UB define claramente três zonas distintas de segurança de acordo com a lista acima:

- Rede Corporativa;
- Rede de Ensino, que nesta perspectiva engloba a rede Externa, disponível a docentes e alunos;
- Rede Laboratório;
- Perímetro.

As boas práticas de segurança no desenho de AD recomendam que uma floresta que contém informação sobre os colaboradores da organização, ou que inclui equipamentos onde é armazenada informação sensível, não deve ser exposta a tráfego de alto risco, como o proveniente da Internet. Por outro lado, a disponibilização desejável de alguns serviços para utilizadores através da Internet cria a necessidade de autenticar esses pedidos, preferencialmente com as mesmas credenciais já usada na infra-estrutura interna. Por fim, a crescente complexidade resultante da disponibilização de mais serviços na Internet tornam desejável a utilização dos mesmos mecanismos de gestão centralizada disponíveis na rede interna, nomeadamente a aplicação de *Group Policies Objects* (GPO). Torna-se assim necessário implementar quatro infra-estruturas AD, com *trusts* entre si e associados a cada uma das zonas de segurança. De modo a minimizar os custos relativos aos equipamentos e licenciamento recomenda-se o uso de máquinas virtuais⁴.

Relativamente ao serviço de Domain Name System (DNS) o mesmo deverá ser configurado em todos os DCs de cada floresta e ser criada um reencaminhamento dos pedidos de DNS dos clientes para os servidores de DNS das restantes florestas.

A Figura 8 ilustra as diferentes florestas e respectivos *trusts* implementados.

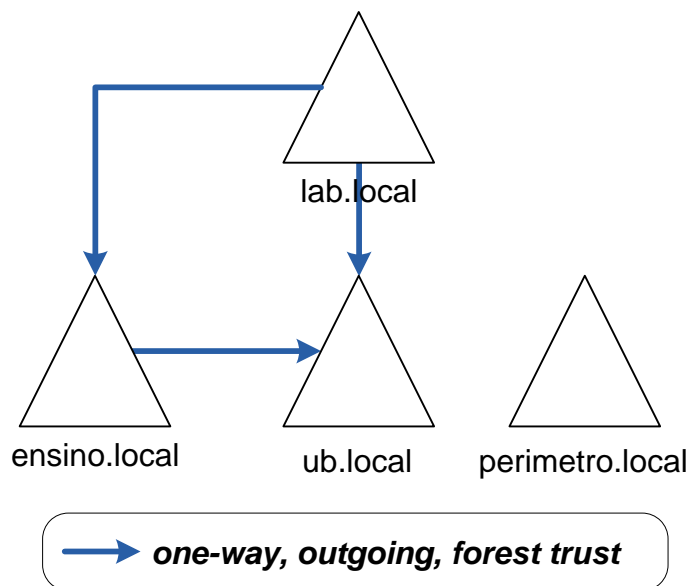


Figura 8 - Directório, Autenticação e Autorização, Arquitectura Lógica

⁴ Maiores detalhes sobre o licenciamento do Microsoft Windows Server 2003 em <http://www.microsoft.com/windowsserver2003/howtobuy/licensing2/overview.aspx#EBC>.

A floresta `perimetro.local` não deverá ter qualquer tipo de *trust* associado a qualquer outro domínio.

A escolha de *trusts* unidireccionais e não transitivos permite que recursos da floresta `ub.local` (rede corporativa) possam aceder a recursos das florestas `ensino.local` e `lab.local` não sendo possível o contrário, bem como o acesso da floresta `ensino.local` à rede `lab.local`. O facto de não serem transitivos permite aumentar o nível de segurança das florestas não permitindo que a criação de subdomínios nas florestas seja considerada *trusted*.

Este modelo apresenta uma considerável complexidade, mas as vantagens em termos de segurança e escalabilidade tornam-no numa opção viável, permitindo a criação de diferentes universidades ou mesma a alienação da UB a outra entidade gestora sem afectar quaisquer recursos das florestas.

4.2. Gestão da Plataforma

4.2.1. Caracterização do Serviço

A gestão de qualquer plataforma com a dimensão e criticidade como a apresentada nesta solução é extremamente difícil sem a utilização de ferramentas de gestão e monitorização, tendo sido identificadas duas áreas a cobrir pelos serviços de Gestão da Plataforma.

- Monitorização – destina-se a recolher informação dos equipamentos suportados, permitindo aos administradores identificar potenciais problemas antes de eles ocorrerem, ou apoiando na resolução dos mesmos quando estes se verificam;
- Gestão de actualizações (*Patch Management*) – permite a gestão centralizada e controlada do processo de obtenção e instalação de actualizações aos sistemas e aplicações instalados nos servidores;

De acordo com o portfólio de produtos disponíveis e considerando o binómio custo benefício foi decidido introduzir o novo Microsoft System Center Essentials 2007 (SCE), um pacote que combina numa única plataforma com uma consola de gestão única as necessidades acima descritas, bem como a possibilidade de estender a monitorização e gestão às estações de trabalho e equipamentos de rede, permitindo a instalação de software nos clientes.

Apesar de o SCE ter uma limitação de 30 servidores e 500 clientes este valor ultrapassa as necessidades da UB em número e tipo de equipamentos, não possuindo um número limite para equipamentos geridos por Simple Network Management Protocol (SNMP).

A componente de gestão de estações de trabalho e equipamentos de rede via SNMP não faz parte do âmbito da solução, pelo que não será considerada na arquitectura.

As principais características do SCE estão presentes na Tabela 11.

Ambiente comum de operação	Pelo facto de se tratar de uma solução única permite ter numa única consola todas as ferramentas necessárias à gestão da infra-estrutura, nomeadamente relatórios e uma base de dados de conhecimento pré carregada com a experiência da Microsoft na resolução de problemas, permitindo um maior entendimento do problema e uma resposta mais rápida.
Gestão pró-activa	Pelos motivos referidos no ponto anterior é possível acelerar a resolução de problemas e efectuar uma auto-gestão no que concerne a problemas de performance ou actualizações de segurança.
Automatização de actualizações de software e recolha de dados	Dada a interligação com o Windows Server Update Services (WSUS) permite automatizar a instalação de actualizações de segurança, drivers e aplicações de software, bem como ter um inventário do parque cliente e servidor da infra-estrutura.
Maior eficiência	Através da utilização de assistentes é possível configurar as actualizações necessárias, bem como otimizar a instalação de software sem recorrer a uma presença física nos equipamentos.
Implementação e gestão simples	Através dos mecanismos de instalação e configuração é possível configurar automaticamente os componentes necessários, como as GPO, bem como efectuar uma descoberta automática de computadores e dispositivos de rede automaticamente.

Tabela 11 - Gestão da Plataforma, Caracterização do Serviço (Características do SCE)

A Tabela 12 descreve os principais aspectos a considerar no desenho da arquitectura do serviço de Gestão da Plataforma.

Segurança	A arquitectura proposta para cada um dos componentes deste serviço deve respeitar os níveis de segurança pretendidos, não comprometendo as características globais da plataforma. Em particular, a infra-estrutura do serviço de Gestão da Plataforma deve ser configurada na mesma zona de segurança em que se encontram os equipamentos suportados.
Escalabilidade	A infra-estrutura deverá suportar um máximo de 500 estações de trabalho e 30 servidores dadas as limitações do SCE. O desenho da arquitectura deverá acomodar mudanças na UB, nomeadamente o aumento do número de cursos disponíveis e consequentemente o número de estações de trabalho e servidores, pelo que caso haja necessidade poderá ser efectuado o <i>upgrade</i> para o Microsoft System Center Operations Manager 2007 e Microsoft System Center Configuration Manager 2007 que apesar do aumento da complexidade não possuem os limites do SCE.
Disponibilidade	A arquitectura do serviço de Gestão da Plataforma deve ser diferenciada, mediante a componente específica em causa. A componente de monitorização deve ser dotada de características de alta disponibilidade, independentemente da zona de segurança a que se refere. Por outro lado, as componentes de gestão de actualizações e de instalação de servidores não apresentam requisitos de alta disponibilidade. Todas as componentes do serviço de Gestão da Plataforma deverão ser implementadas em todas as zonas.
Gestão	A gestão do serviço de Gestão da Plataforma será integralmente assumida pela equipa da IETI da UB. A componente de monitorização deverá oferecer um ponto único de operação, com uma visão global dos equipamentos e serviços monitorizados em todas as zonas de segurança.
Consolidação	De acordo com a política global assumida sempre que a consolidação de diversas funções num único equipamento não cause problemas para a segurança da plataforma ou limite o desempenho da solução, a consolidação deve ser favorecida.

Tabela 12 - Gestão da Plataforma, Caracterização do Serviço

4.2.2. Arquitectura Lógica

A arquitectura proposta para a componente de monitorização é baseada no SCE é composta pelos seguintes componentes:

- *Management Server* – Servidor onde é instalado o produto ao qual os equipamentos monitorizados reportam informação;
- *Agente* – é a componente de software que é instalada nos clientes e que permite usufruir da totalidade do serviço de monitorização. Nos equipamentos monitorizados por SNMP não é instalado o agente;
- *Management Database* – Base de dados responsável por alojar a informação recolhida pelo *Management Server*;
- *Reporting Server* – é responsável pela elaboração dos relatórios do SCE. São frequentemente utilizados em situações de análise de tendência para avaliação de desempenho.

A Tabela 13 mostra demonstra os fluxos de comunicação entre os diversos componentes do SCE nas diferentes florestas.

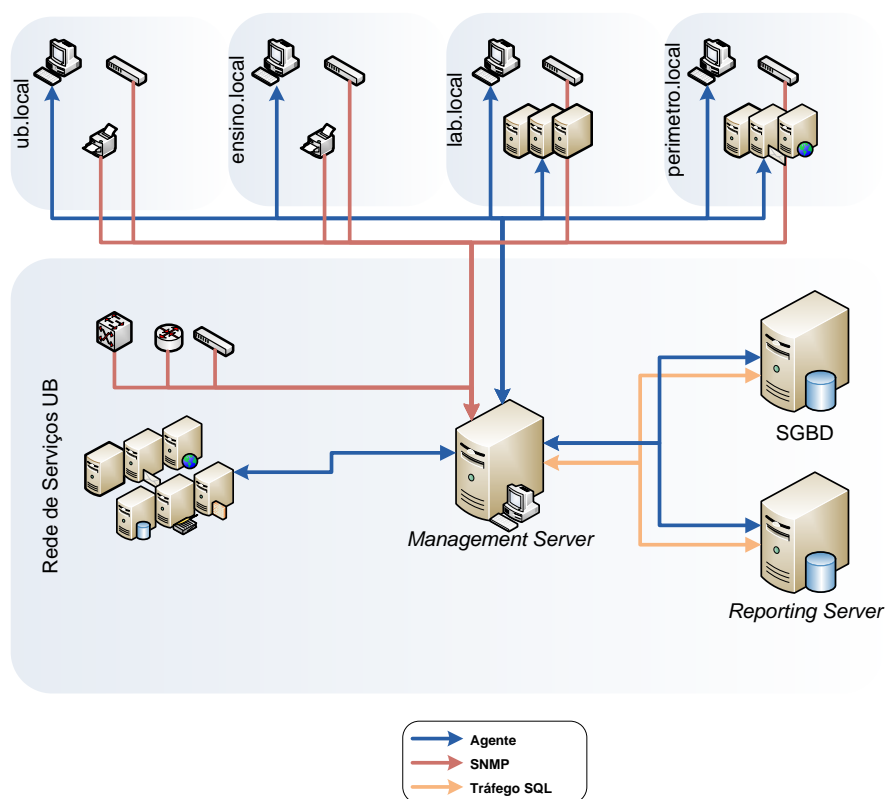


Tabela 13 - Gestão da Plataforma, Arquitectura Lógica

4.3. Sistema de Gestão de Base de Dados

4.3.1. Caracterização do Serviço

Vários dos serviços a implementar na arquitectura utilizam uma base de dados SQL como suporte para a sua informação. Por outro lado, é previsível que futuras necessidades da UB introduzam novos serviços ou funcionalidades que aumentem ainda mais a dependência em relação aos serviços de bases de dados.

Na presente arquitectura, existem já cinco serviços ou componentes destes cujas implementações dependem nalgum grau do Sistema de Gestão de Base de Dados:

- *Firewall* (Microsoft ISA Server 2006);
- *Acesso à Internet* (Microsoft ISA Server 2006);
- *Partilha de Informação* (Microsoft WSS 3.0);
- *eLearning* (Microsoft WSS 3.0 e SLK);
- *Gestão da Plataforma* (Microsoft System Center Essentials 2007).

A Tabela 14 descreve os principais aspectos a respeitar no desenho da arquitectura do Sistema de Gestão de Base de Dados.

Segurança	<p>Todos os DCs que disponibilizam o Sistema de Gestão de Base de Dados devem ser protegidos e segregados fisicamente em redes específicas. Ao nível lógico, devem ser aplicadas configurações de <i>hardening</i> do sistema operativo e respectivos serviços.</p> <p>A arquitectura proposta para o Sistema de Gestão de Base de Dados deve respeitar os níveis de segurança, pretendidos, não comprometendo as características globais da plataforma. Em particular, a segurança lógica dos dados deve ser assegurada, quer através da definição de contas com os direitos mínimos necessários para cada serviço cliente, quer através da limitação do acesso aos servidores apenas para os serviços que dependem do Sistema de Gestão de Base de Dados.</p>
Escalabilidade	<p>O desenho da arquitectura deverá acomodar mudanças na UB, nomeadamente o aumento do número de cursos disponíveis e consequentemente o número de utilizadores simultâneos, bem como o alojamento de aplicações ou serviços dependentes do Sistema de Gestão de Base de Dados.</p>
Disponibilidade	<p>A arquitectura do Sistema de Gestão de Base de Dados deve ser diferenciada, mediante a zona de segurança da plataforma cujos serviços suporta. No entanto, para ambas as plataformas deverá ser criada uma solução com características de alta disponibilidade e capacidade de suportar a falha total de um servidor sem degradação de desempenho.</p> <p>O Sistema de Gestão de Base de Dados apenas deverá ser acedido pelos serviços relevantes, e nunca a partir de uma zona de segurança diferente daquela em que os servidores estão configurados.</p>
Gestão	<p>A gestão do serviço de Sistema de Gestão de Base de Dados bem como dos seus mecanismos deverá ser integralmente assumida pela equipa de gestão da IETI da UB.</p> <p>A gestão deste serviço será auxiliada por um conjunto de serviços de apoio, integrados nos serviços de Gestão da Plataforma.</p>
Consolidação	<p>A consolidação deve ser promovida com o objectivo de auxiliar a capacidade de escala, nomeadamente <i>scale out</i>.</p>

Tabela 14 - Sistema de Gestão de Base de Dados, Caracterização do Serviço

4.3.2. Arquitectura Lógica

À semelhança da generalidade dos restantes Serviços de Suporte, a arquitectura do Sistema de Gestão de Base de Dados encontra-se intimamente ligada à definição das zonas de segurança da plataforma. Adicionalmente, como o Sistema de Gestão de Base de Dados suporta directamente um conjunto significativo dos Serviços de Suporte, a definição da sua arquitectura lógica está muito dependente da destes serviços.

A posição estratégica ocupada pelo Sistema de Gestão de Base de Dados levanta diversas dependências e restrições ao desenho da arquitectura, nomeadamente no que se refere ao domínio a que os servidores SQL pertencem. Quer no conjunto dos serviços da presente arquitectura, quer na evolução da UB, existem limites ao suporte de alguns produtos quando as suas bases de dados se encontram em domínios *untrusted*, tal como o domínio `perímetro.local`.

Assim é recomendada a constituição de duas infra-estruturas autónomas do Sistema de Gestão de Base de Dados, seguindo a filosofia já patente nos restantes serviços. As infra-estruturas serão configuradas nas zonas de segurança da Rede de Serviços UB (`ub.local`) e Perímetro (`perímetro.local`) e não deverão dispor de qualquer elo lógico ou físico entre si.

O suporte às diversas aplicações deverá ser oferecido através da criação de contar de serviço específicas para cada serviço cliente, às quais serão atribuídos os direitos estritamente necessários ao seu bom funcionamento.

5. Conclusão

Esta solução é uma visão macro da infra-estrutura de serviços a implementar na UB. Existem serviços, como os de Rede, que não foram considerados isoladamente uma vez que se encontram intimamente ligados aos Serviços de Suporte, nomeadamente ao serviço de Directório, Autenticação e Autorização como é o caso do DNS essencial para o funcionamento deste serviço.

Outros serviços, como o da presença na Internet, não foram igualmente considerados por não se encontrarem no âmbito da solução.

Esta solução pretende cumprir com as melhores práticas do mercado em termos de soluções Microsoft, nomeadamente em relação à segurança e escalabilidade.

A metodologia escolhida, WSSRA, permite a uma Organização de uma forma rápida e eficiente planear, implementar e gerir uma infra-estrutura de serviços que suporte e dê resposta às suas necessidades estratégicas.

Bibliografia

- Corbin, Wendy, e Kurt Hudson. *Designing a Microsoft Windows Server 2003 Directory and Network Infrastructure (70-297)*. Redmond: Microsoft Press, 2004.
- English, Bill. *Microsoft® Office SharePoint® Server 2007 Administrator's Companion*. Redmond: Microsoft Press, 2007.
- Glenn, Walter, Scott Lowe, e Joshua Maher. *Microsoft® Exchange Server 2007 Administrator's Companion*. Redmond: Microsoft Press, 2007.
- Microsoft Corporation. *Windows Server System Reference Architecture*. 5 de Agosto de 2005.
<http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/default.mspx> (acedido em 4 de Junho de 2007).
- Minasi, Mark, e Byron Hynes. *Administering Windows Vista Security: The Big Surprises*. Sybex, Incorporated, 2007.
- Minasi, Mark, e John Paul Mueller. *Mastering Windows Vista Professional*. Sybex, Incorporated, 2007.
- Minasi, Mark, Lisa Justice, e Rhonda Layfield. *Mastering Windows Server 2003, Upgrade Edition for SP1 and R2*. Sybex, Incorporated, 2006.
- Noel, Michael. *Microsoft ISA Server 2006 Unleashed*. Pearson Education, 2007.
- Northrup, Tony, e Martin Grasdahl. *Designing Security for a Microsoft® Windows Server™ 2003 Network (70-298)*. Redmond: Microsoft Press, 2005.
- Reimer, Stan, e Mike Mulcare. *Active Directory® for Microsoft® Windows® Server 2003 Technical Reference*. Redmond: Microsoft Press, 2002.
- Tisseghem, Patrick. *Inside Microsoft® Office SharePoint® Server 2007*. Redmond: Microsoft Press, 2007.
- Whalen, Edward, Patel, Marcilina S. Garcia, e Stacia Misner. *Microsoft® SQL Server™ 2005 Administrator's Companion*. Redmond: Microsoft Press, 2006.
- Zacker, Craig. *Implementing and Administering Security in a Microsoft® Windows Server™ 2003 Network (70-299)*. Redmond: Microsoft Press, 2005.