Mestrado em Informática e Sistemas

Dimensionamento, Planeamento, Configuração e Colocação em Produção de um Data Center para uma Instituição de Ensino Superior

Dissertação apresentada para a obtenção do grau de
Mestre em Informática e Sistemas

Especialização em Tecnologias da Informação e do Conhecimento

Autor

Paulo Alexandre dos Santos Faria

Orientador

Prof. Doutor Jorge Augusto Castro Neves Barbosa

Professor do Departamento de Engenharia Informática e Sistemas

Instituto Superior de Engenharia de Coimbra

Coimbra, Fevereiro, 2017

Ao Doutor Jorge Barbosa,
por todo o apoio e motivação.

À Ana, Rita e João.

RESUMO

O século XX assistiu ao nascimento e evolução das tecnologias de informação. Inicialmente estas tecnologias inovaram pela capacidade demonstrada no processamento matemático, mas nas duas décadas finais deste século, assistiu-se a uma revolução destas tecnologias ao evoluírem fortemente, nomeadamente no processamento de informação de todo o tipo.

Com a introdução da *internet* o crescimento destas tecnologias, tanto a nível da capacidade de processamento como ao nível da quantidade de utilizadores foi exponencial.

Atualmente a *internet* e *intranet* são dois ambientes indissolúveis em qualquer organização e neles estão baseados um grande número de aplicações que suportam o funcionamento da sociedade atual. Os métodos de comunicação tradicionais estão em extinção (correio, telefax, telefone analógico, etc.) tendo sido substituídos por serviços online como o correio electrónico, comunicações VoIP e outros.

É do senso comum que toda a tecnologia disponibilizada tem origem em computadores, ou mais especificamente, servidores informáticos, passando despercebido toda a engenharia necessária para o alojamento de todo o equipamento informático necessário para tal.

O espaço físico onde se efectua este alojamento do equipamento informático denomina-se Data Center, ou centro de dados, e trata-se de uma localização ou edifício com características específicas para acomodar todo o equipamento informático proporcionando as condições de segurança e ambientais necessárias a que este funcione 24 horas por dia, 365 dias por ano com uma fiabilidade e disponibilidade de – ou quase de – 100%.

Neste documento descreve-se a evolução do parque informático de uma Instituição de Ensino Superior nascida numa época anterior à das tecnologias da informação descrevendo mais em pormenor o alojamento de servidores de última geração, com técnicas de redundância, um Data Center construído de raiz para o efeito, referindo-se por todas as etapas de configuração e organização deste centro.

Palavras Chave: Data Center, Virtualização, Redundância, Segurança, Disaster Recovery

ABSTRACT

The 20th century witnessed the birth and evolution of information technologies. Initially these technologies innovated by demonstrated ability in mathematical processing, but the final two decades of this century, a revolution of these technologies to evolve strongly, particularly in the processing of information of all kinds.

With the introduction of the internet the growth of these technologies both processing capacity and the amount of users has been exponential.

Currently the internet and intranet are two environments must go together in any organization and they are fundamental to a a large number of applications that support the operation of the society. The traditional communication methods are in extinction (mail, fax, telephones, etc.) and having been replaced by online services such as e-mail, VoIP and other communications.

It's common sense that all the technology available comes from computers, or more specifically, computer servers, passing unnoticed all the engineering required for the accommodation of all the equipment necessary for such.

The physical space for this accommodation of computer equipment is called Data Center or data centre, and it is a location or building with specific features to accommodate all the equipment providing the security and environmental conditions required to work 24 hours a day, 365 days a year with a reliability and availability of – or almost – 100%.

This document describes the evolution of the server farm of a higher education institution born in an era before information technologies describing in more detail the accommodation of next-generation servers with redundancy techniques, a Data Center built from scratch for the effect, referring by all the steps for setting up and organization of such room.

Keywords: Data Center, Virtualization; Redundancy; Security; Disaster Recovery

ÍNDICE

ÍNDICE DE FIGURAS

ABREVIATURAS

BTU – British Termal Unit

CO_2 – Dióxido de carbono

DC – Data Center, centro de dados

DFM – Departamento de Física e Matemática

DRC – Disaster Recovery Center

DRP – Disaster Recovery Plan

DRS – Disaster Recovery Site

HFC227 – Gás heptafluorpropano, agente extintor

Gbps – Gigabits por segundo, 2^{30} bits por segundo

GI – Gabinete de Informática

GTMI – Gabinete Técnico de Manutenção das Instalações

I/O – Input/Output

iSCSI – *Internet Small Computer System Interface*

IPC – Instituto Politécnico de Coimbra

ISEC – Instituto Superior de Engenharia de Coimbra

kVA – kilo Voltampere

OMS – Organização Mundial da Saúde

PC – Personal Computer ou computador pessoal

SAN – *Storage Area Network*

Tbps – Terabits por segundo, 2^{40} bits por segundo

TI – Tecnologias de Informação

TIA – Telecomunications Industry Association

UPS – Uninterruptible Power Supply

VA – Voltampere

VDI – Virtual Desktop Infraestruture

VMM – Virtual Machine Monitor

VRRP – *Virtual Routing Redundancy Protocol*

W – Watt

kW –quilowatt

1. INTRODUÇÃO

O ISEC – Instituto Superior de Engenharia de Coimbra –, quando contabilizado o número de alunos, é a segunda maior escola de engenharia da região de Coimbra sendo superada apenas pela Faculdade de Ciência e Tecnologia da Universidade de Coimbra.

No ISEC são lecionados cursos de licenciatura e de mestrado nas áreas científicas de Engenharia Civil, Engenharia Eletrotécnica, Engenharia Informática e de Sistemas, Engenharia Mecânica, Engenharia Química e Biológica, Engenharia Biomédica e Engenharia e Gestão Industrial que se traduzem na seguinte comunidade (dados de 30/Junho/2013) [1]:

- 3035 Alunos;
- 220 Docentes;
- 84 Funcionários não docentes;

Na oferta formativa do ISEC incluem-se ainda cursos de especialização tecnológica. Estes cursos têm como objetivo formação de técnicos (não superiores) especializados nas diversas áreas cientificas lecionadas pelo ISEC.

Empenhado na sua missão de criação, transmissão e difusão de cultura, ciência e tecnologia através da formação de alunos para o exercício de atividade em engenharia nas diversas áreas, o ISEC tem apostado no constante recurso às tecnologias de informação para atingir os seus objetivos.

É neste âmbito que, desde meados da década de 1990, começaram a ser definidos os primeiros serviços informáticos dos ISEC para responder às necessidades administrativas e formativas da instituição.

Sendo o ISEC parte integrante e ativa na sociedade não ficou isento do crescimento exponencial dos requisitos das TI (tecnologias de informação) nas quais assentou o seu funcionamento. Se, inicialmente, um pequeno gabinete fora suficiente para albergar 3 ou 4 servidores capazes de responder às necessidades informáticas de uma instituição a despertar para as TI, alguns anos depois e sem o planeamento adequado, uma sala de $25m^2$ já não era suficiente para a instalação dos vários servidores e computadores que, sofregamente, respondiam aos requisitos de TI.

O planeamento e instalação de um Data Center é uma tarefa que, no seu aspeto global, se bem que possa ter um início bem definido, nunca terá um final determinado uma vez que o surgimento de novas necessidades é um fator constante que envolverá a instalação de novos equipamentos, cablagens adicionais podendo mesmo chegar-se a um ponto em que se torne a ser necessário proceder a alterações na infraestrutura original.

Pretende-se, com este documento, relatar as diversas etapas que foram necessárias realizar para a instalação do Data Center do ISEC e que permitiram a consolidação e instalação de sistemas informáticos que suportam toda a informação necessária ao funcionamento do ISEC de uma forma bem planeada e numa sala preparada para o efeito: o Data Center do ISEC.

2. MOTIVAÇÃO – O PARQUE DE SERVIDORES

Os serviços informáticos do ISEC iniciaram a sua atividade em meados da década de 1990. Existem memórias, entre diversos funcionários docentes e não docentes, que estes serviços iniciaram com apenas um servidor SUN a correr uma versão de Unix no qual eram disponibilizados serviços de correio eletrónico, pastas pessoais e pouco mais.

Este despertar (grandioso para a época em que aconteceu e tendo em conta todo o investimento em infraestrutura de comunicações que lhe estava inerente), em paralelo com a evolução da tecnologia informática (hardware), permitiu o acesso às tecnologias de informação no ISEC.

A cadência com a qual os requisitos de TI surgiam eram tais que, estando o ISEC sujeito a orçamentos e a regras apertadas no que respeita a aquisições, rapidamente se vieram a encontrar simples computadores pessoais – PCs ou *workstations* – a disponibilizar serviços que habitualmente deveriam estar configurados em computadores com arquitetura de servidor.

Este panorama desenrolou-se durante bastante tempo até que no final da primeira metade da década de 2000 o cenário começa a apresentar os primeiros sinais de que brevemente a configuração presente se iria tornar insustentável e começaram os primeiros estudos com o intuito da reinstalação e consolidação efetiva dos serviços informáticos. Este trabalho de análise foi interrompido durante aproximadamente 7 anos.

Apesar disto, os serviços informáticos continuaram a crescer de forma a responder às crescentes necessidades de TI mas, no entanto, as infraestruturas disponibilizadas não cresceram de acordo com esta necessidades de serviços informáticos.

2.1. Parque Informático dos Serviços Informáticos

Em 2012, os serviços informáticos do ISEC tinham ao seu dispor:

- 1 Sala de 20 m^2, aproximadamente;
- 2 Bastidores de pavimento, 42 U
- 4 Servidores Intel Dual Xeon,
- 8 Servidores Intel Dual Xeon Séries antigas
- 9 Servidores Intel Xeon QuadCore
- 7 PCs dos quais:
  - 2 Intel Quad Core
  - 1 Intel Dual Core
  - 4 Intel Pentium IV
- Armazenamento de dados local, ao nível do servidor;
- 2 Switchs 24 ports, 100/1000Base-T, com uplink 3x 1000 Base-SX
- 5 Unidades UPS com capacidade 3000VA cada
- 2 Unidades de Ar Condicionado, totalizando 21000BTU

Figura 1 - Pormenor de alguns dos servidores existentes em 2012

Em 2012 existia de um conjunto de serviços de TI básicos, capazes de garantir o normal funcionamento da Instituição, fruto de vários investimentos ao nível dos recursos de hardware necessários. No entanto, estes recursos clamavam por uma reorganização profunda, essencialmente ao nível da infraestrutura base, pois o seu crescimento deixara de ser sustentável.

Esta insustentabilidade verificava-se a vários níveis:

a) Armazenamento de dados – embora os totais possam ser enganadores (10Tbytes disponíveis e 5Tbytes utilizados), a capacidade de armazenamento de dados em cada servidor é bastante pequena e lenta não permitindo a sua partilha para a implementação de novos serviços nem existindo qualquer tolerância a falhas;
b) Espacial – deixara de existir espaço para a instalação de equipamentos.
c) Climatização – A capacidade de climatização da sala fora ultrapassada:
    a. Os equipamentos de ar condicionado não produziam arrefecimento capaz de manter a sala numa temperatura desejável;
    b. Constantes avarias dos equipamentos de ar condicionado;

c. A disposição dos equipamentos informáticos face ao arrefecimento não era minimamente eficiente;

d) Elétrica – O fornecimento de energia elétrica à sala de servidores era inconstante, tanto por se verificarem grandes oscilações na tensão elétrica disponível como por ocorrerem cortes no fornecimento de energia elétrica no edifício onde a sala estava localizada. Ainda no ponto de vista de carências do fornecimento elétrico, é de salientar que o fornecimento ininterrupto de energia era garantido por várias unidades UPS, para vários grupos de servidores e sem redundância.

e) Segurança – Com o acréscimo de armazenamento de dados críticos nos servidores da instituição era premente assegurar que o acesso físico aos servidores fosse cada vez mais controlado e mais seguro. A sala de servidores tinha janelas para o exterior bem como portas duplas (de vidro) com fechadura simples que não oferecia grande resistência a um acesso forçado.

f) Incêndios, socorro a – Praticamente inexistente. Apenas existia um detetor de fumos ligado ao sistema de incêndios do edifício e um extintor de CO2 na sala de servidores.

Era urgente consolidar todo o investimento em TI, recuperando os desperdícios verificados e preparar o ISEC para os desafios do futuro.

Foi com esta perspetiva que o único rumo que havia a tomar era em direção ao Data Center.

3. O DATA CENTER DO ISEC

Neste capítulo será apresentada a definição e caracterização de um Data Center (DC) como ponto de partida para a construção do Data Center do ISEC. De acordo com a definição dos diversos aspetos que caracterizam o DC serão apresentados os trabalhos realizados nas diversas áreas.

3.1. Data Center : In-House vs OutSourcing

Ou, como se diz na gíria portuguesa, compra-se ou faz-se com a prata da casa?

Com a diversidade de oferta de serviços de alojamento de dados e aluguer de servidores, a solução de recurso ao OutSourcing não poderia passar sem ser questionada.

Para o ISEC, uma escola de engenharia de renome cuja reputação é bem reconhecida no panorama industrial português e dotada de um excelente corpo docente e não-docente o primeiro pensamento de outsourcing não passava de um sinónimo de custos acrescidos e perfeitamente dispensáveis.

Com efeito, estando reunidas as diversas especialidades de engenharia e existindo já diversos investimentos no parque de servidores e infraestrutura de rede de dados a decisão pela implementação local (in-house) do Data Center surgiu de uma forma natural e espontânea por parte da Presidência do ISEC.

ALUGAR OU COMPRAR? [10]

Tendo disponibilidade financeira, optaria por alugar ou comprar uma moradia?

Se alugasse, o senhorio seria responsável pelo bom funcionamento do imóvel. Os seus pertences ficariam guardados na moradia mas o senhorio mantem uma chave para entrar sempre que necessário.

Se comprar, a moradia é sua! Faz o que quiser e como quiser. Cuida dela da melhor forma, pode entrar e sair quando quiser mas será o único a ter a chave da porta.

Como quer guardar os seus pertences mais valiosos?

Unidos os esforços da Presidência, coordenando os gabinetes GTMI – Gabinete Técnico de Manutenção das Instalações -, GI – Gabinete de Informática – e docentes do Instituto, como consultores técnicos, rapidamente surgiu o projeto de construção, apetrechamento e implementação do Data Center do ISEC.

A implementação local do Data Center foi facilitada pela disponibilidade de um espaço com aproximadamente 50m^2 (aprox. 9x5m) situado num piso térreo, acessível por um largo corredor de acesso que facilita o transporte de cargas e que, sujeito a ligeiras obras de remodelação, ficaria com condições para a implementação do mesmo.

Em oposição à decisão da implementação *In-House*, o *outsourcing* acarretaria custos associados a aluguer de espaços, monitorização e manutenção dos equipamentos e serviços de rede dedicados. Era, assim, evidente que outsourcing traduzir-se-ia na aquisição de serviços já disponíveis no *campus* do ISEC o que resultaria na duplicação de sistemas e serviços, consequentemente, duplicação dos custos de funcionamento associados.

3.2. Caracterização de um Data Center

O Data Center é um espaço dedicado, tal como o seu nome indica, à centralização de dados e ao processamento dessa informação. Sendo os dados processados e disponibilizados por servidores informáticos, o data center é o espaço dedicado à instalação de servidores e todos os sistemas de armazenamento de dados que lhes são associados bem como os equipamentos ativos de rede que permitam a comunicação de dados entre os sistemas existentes e comunicação desses dados para o exterior.

São ainda componentes do data center todos os equipamentos que garantam o correto funcionamento do mesmo.

O objetivo do data center reside, pois, em garantir a continuidade do funcionamento da organização onde se localiza.

Em linhas gerais, qualquer data center deverá ter bem definidos os seguintes aspetos:

a) Espaço físico;
b) Infraestrutura de rede;
c) Segurança física;
d) Combate e prevenção contra incêndios;
e) Arrefecimento;
f) Energia.

A TIA (*Telecomunications Industry Association*) estabeleceu a normativa internacional TIA-942 com a definição de requisitos e recomendações do projeto de instalação de um DC desde a fase de planeamento até à sua ativação. Este conjunto de normas visa não só o projeto inicial de todo o processo de construção como permite o planeamento de um DC a longo prazo e de modo a facilitar o seu crescimento e futuras aplicações.

Compreende-se assim a escolha da norma TIA-942 como documentação de referência para o planeamento do Data Center.

3.3. Espaço Físico

A definição do espaço físico para a instalação do Data Center foi o primeiro dos desafios a ultrapassar. A tomada desta decisão teria impacto nas futuras questões relacionadas com:

a) Segurança – no que concerne aos tipos de acesso à sala, se a sala tem janelas que possam ser usadas para intrusões, etc.,
b) Fornecimento de energia elétrica – Possibilidade de instalação de uma nova linha de alimentação elétrica, independente da que existe no edifício no qual se insere a sala; disponibilidade de espaços para instalação de geradores elétricos; áreas disponíveis para a instalação de unidades de alimentação ininterruptas;
c) Climatização – Dependente do posicionamento vertical da sala também os parâmetros de temperatura e humidade poderão variar, obrigando a um maior esforço no controlo dos mesmos
d) Acesso ao backbone do campus – Facilidade de ligação da sala ao backbone do campus, incluindo ligações redundantes;

Dos vários edifícios existentes no campus do ISEC, identificaram-se 2 salas contiguas com grande potencial para a instalação do DC. Após a realização de obras resultou uma sala com 45 m^2 de área útil (9m x 5m), uma única porta de acesso e 2 pequenas janelas para o exterior (que foram fechadas sem grande dificuldade).

Esta localização, tem também uma fácil ligação redundante ao backbone da rede do ISEC.

3.3.1. Preparação do Espaço Físico

Como referido anteriormente, foram identificadas 2 sala contíguas a serem preparadas para a instalação do DC.

As obras iniciaram-se com a eliminação das paredes interiores que separavam as duas salas, remoção da caixilharia das 2 janelas existentes numa das salas e encerramento dessas janelas com recurso a alvenaria.

O piso original das salas é em mosaico, em bom estado de conservação e apresenta boa resistência pelo que não se verificou a necessidade de reparação.

Com a remoção das paredes e encerramento das janelas foi necessário serem efetuados reparações no revestimento das paredes e remates no chão.

Após escovagem e desengorduramento das paredes foi aplicado de um primário antifúngico para posteriormente serem pintadas com esmalte aquoso de cor branca.

3.3.2. Pavimento Técnico Elevado

Numa primeira observação da sala, o recurso a uma instalação suspensa – em que as cablagens seriam passadas em armações suspensas a partir do teto – seria a solução aparentemente que melhor se adaptaria às dimensões da sala.

A instalação suspensa caracteriza-se pela colocação de esteiras de cabos num nível elevado – habitualmente junto ao tecto – nas quais são instaladas as cablagens elétricas de comunicação de dados. Esta solução apresenta-se também como a mais económica e de mais fácil manutenção.

Uma vez que o projeto de climatização da sala consiste na colocação de 4 unidades de ar condicionado junto ao teto da sala, perfilados com as filas de bastidores de forma a criar um sistema de arrefecimento habitualmente designado de corredor quente e frio (em *3.7. Arrefecimento* poderá encontrar mais informação acerca do arrefecimento da sala), a colocação de esteiras suspensas poderia vir a dificultar os fluxos de ar e assim degradar a climatização da sala pelo que se procurou outra solução para a instalação da cablagem necessária.

Corredor Quente e Frio

O sistema utilizado no arrefecimento dos servidores consiste na sua ventilação interna em que várias ventoinhas fazem o ar atravessar o chassis do servidor da parte da frente para trás. Normalmente, o ar que é expelido pela traseira de um servidor foi aquecido pela transferência de calor resultante do arrefecimento dos componentes do servidor.

Uma fila de bastidores preenchidos com servidores define 2 espaços de temperatura:

- o corredor frio – na zona frontal dos bastidores
- o corredor quente – na zona traseira dos bastidores, cuja temperatura local é superior resultante da ventilação dos servidores.

Dado que a sala dispõe de uma altura, aproximadamente, de 4 metros, a instalação de um piso técnico elevado foi colocada em consideração. Com esta solução toda a cablagem é instalada num plano inferior ao dos bastidores – sob o piso – seguindo os caminhos pré-definidos por esteiras instaladas para o efeito.

Com a instalação deste pavimento, salvaguarda-se ainda qualquer incidente de inundação que possa ocorrer no edifício e que pudesse vir a afetar o DC.

Para a instalação do pavimento técnico, foram utilizadas placas de aglomerado de madeira de alta densidade revestidas com folha de alumínio na parte inferior, orla em ABS e com revestimento superior em vinílico anti estático.

As placas, com 38mm de espessura e dimensões de 600mm x 600mm, estão elevadas por pedestais de 250mm nos seus extremos ficando este conjunto com uma resistência média aproximada de 700 Kg/m^2 sabendo-se que as cargas máximas ou de ruptura poderão ascender até aos 1100 Kg/m^2. Nas áreas onde se prevê a colocação de objectos de maior peso, optou-se

por efectuar o reforço dos suportes do pavimento garantindo-se assim uma resistência mais elevada.

3.3.3. Passagem de cabos

Para a passagem de cabos elétricos para a alimentação dos bastidores e demais equipamentos bem como para a instalação da cablagem horizontal de rede foram instaladas esteiras sob o pavimento técnico existente.

A instalação das esteiras foi feita de forma dupla para separar a cablagem elétrica da cablagem de rede.

As esteiras têm 2 pontos de origem, de acordo com a sua finalidade:

1. O quadro elétrico da sala;
2. A localização do bastidor de rede da sala.

A figura seguinte apresenta uma perspetiva da instalação das esteiras de cabos sob a instalação do pavimento elevado.

Figura 2- Pormenor da instalação das esteiras de cabos

3.4. Segurança Física

O único acesso ao Data Center é feito através da sua porta.

A sala do Data Center é desprovida de janelas ou quaisquer outras aberturas para o exterior.

A entrada de cabos é subterrânea e é feita através de 3 mangas com 15 cm de diâmetro cada.

A porta de acesso ao Data Center foi especificada com dimensões que permitissem a passagem dos diversos equipamentos habituais num espaço destes, pelo que as suas dimensões são de 2000x1000x230mm. Trata-se de uma porta blindada (de ferro) com acabamento de madeira contendo dobradiças com espigões de segurança bem como com fechadura de segurança.

Na sua construção, a sala ficou preparada para a instalação de um sistema de controlo de acessos a atuar sobre a porta.

3.5. Combate e Prevenção de Incêndios

Foi instalado um sistema de deteção e combate de incêndios exclusivo para o Data Center. Este sistema é composto por 1 central de controlo, 4 detetores de incêndio, condutas metálicas com 4 difusores e 1 unidade de gás HFC227ea (ou heptafluorpropano) como agente extintor.

A unidade de controlo do sistema de combate a incêndios permite várias configurações de modo a que o sistema funcione de forma manual ou automática e com ativação ou restrição da utilização do agente extintor, permitindo assim a realização de tarefas de manutenção sem a existência do disparo acidental do agente extintor. Estão ainda disponíveis interruptores de emergência para ativação do controlo de incêndios ou interrupção do mesmo em caso de falso alarme.

Figura 3 - Central de controlo de incêndios e botões de emergência

O gás HFC227ea é fabricado pela Dupond® e actua sobre os focos de incêndio através da absorção do calor e quebra das reações químicas de combustão. No estado gasoso, este gás é praticamente inerte e sem efeitos nocivos para o ser humano o que torna a sua utilização viável nas mais diversas situações.

Figura 4 - Reservatório do agente extintor

O reservatório de gás e as dimensões das condutas foram estudados para que, em caso de ativação do sistema de extinção, a difusão do gás atinja uma concentração ideal de 7% na atmosfera local num instante não superior a 10 segundos.

Este método de extinção tem como requisito adicional a característica de estanquidade ou hermeticidade da sala em que é instalado. Ou seja, a sala deve ser o mais estanque possível de forma a manter a concentração do gás HFC227ea durante o maior período de tempo possível e assim garantir a extinção de qualquer foco de incêndio que possa ocorrer. Para aumentar a estanquicidade da sala existem apenas 3 pontos de comunicação com o exterior – porta de entrada e 2 passagens de cabos – estando estes pontos munidos de vedantes.

A utilização deste tipo de extinção de incêndios tem como principais vantagens:

i) Não existir danificação do equipamento existente devido a corrosão por líquidos nem choque térmicos;
ii) A descarga do gás HFC227ea é limpa e não origina resíduos;
iii) Pode ser utilizado em locais com presença humana;
iv) Não tem efeito nocivo sobre a camada de ozono.

3.6. Fornecimento de Energia Elétrica

O Data Center tem o seu fornecimento de energia elétrica feito de forma independente do edifício onde está instalado de forma a não sofrer qualquer interferência que possa condicionar o seu funcionamento.

Foi instalado um ramal elétrico para a ligação direta do Data Center ao posto de transformação do ISEC.

É do senso comum que existem, por vezes, interferências no fornecimento da energia elétrica que causam danos aos mais variados equipamentos elétricos que estejam ligados à rede elétrica. Também no Data Center existe essa preocupação e, por esse motivo, um dos requisitos para a alimentação elétrica é que esta seja filtrada e retificada.

A necessidade do fornecimento contínuo – ou sem quaisquer interrupções - de energia elétrica é outros dos requisitos indispensáveis ao DC, tendo sido satisfeito com a instalação de uma unidade de alimentação ininterrupta de dupla conversão em tempo real – vulgarmente conhecida como online UPS.

UPS de dupla conversão

Uma UPS denomina-se de dupla conversão por ter a capacidade de garantir um nível consistente e adequado da qualidade de alimentação.

Esta característica é conseguida através da conversão da corrente de entrada (AC – corrente alternada) em CC - corrente contínua. Neste processo quaisquer anomalias que existam no sinal de entrada são corrigidos.

Para fornecer energia (output) a corrente CC é novamente convertida em AC. Nesta fase a corrente de saída é produzida de forma estável, sem qualquer perturbação.

Em caso de voltagem insuficiente à entrada do sistema, a unidade de UPS recorre à carga das baterias para garantir que o sinal de saída tem a voltagem correta para o funcionamento dos equipamentos

De forma a satisfazer os requisitos de alimentação elétrica ininterrupta, a solução adotada para o fornecimento elétrico do DC implicou que o quadro elétrico da sala fosse desenhado de forma a separar as diversas fontes de energia disponíveis e permitindo assim, no hipotético caso de avaria comum e simultâneo de todos os elementos UPS existentes, a alimentação elétrica da sala a partir da rede elétrica comum ou de uma terceira fonte de energia (por exemplo, um gerador elétrico a instalar posteriormente).

Respeitando os requisitos para o fornecimento elétrico da sala, o quadro elétrico é, em suma, o conjunto de dois (2) quadros elétricos parciais:

- Quadro de entrada, onde é feito o seccionamento da alimentação da rede e construídos os circuitos de alimentação dos equipamentos de apoio ao Data Center, designadamente, a iluminação, equipamento de arrefecimento, controlo de incêndios e alimentação dos sistemas de fornecimento ininterrupto de energia aos bastidores. Este

quadro é ainda o responsável pela alimentação elétrica do quadro dos sistemas informáticos do DC.

- Quadro de UPS – ou quadro dos sistemas informáticos – onde é feito o seccionamento da alimentação de entrada em vários circuitos elétricos, cada um dedicado à alimentação de cada um dos bastidores instalados no DC.
  A alimentação deste quadro é feita através de um comutador elétrico existente no quadro de entrada de forma a ser possível escolher uma das fontes de alimentação existentes para este fornecer este quadro de energia elétrica. Normalmente a alimentação elétrica é fornecida pelas UPS (conforme requisito) mas foi prevista a possibilidade de alimentar este quadro diretamente da rede elétrica ou ainda com uma terceira fonte de energia para salvaguardar qualquer operação de manutenção ou avaria.

Na figura seguinte é mostrado o quadro elétrico instalado no DC do ISEC.

Figura 5 - Quadro elétrico do Data Center do ISEC

3.6.1. Unidades de fornecimento de energia

Foram adquiridas duas unidades APC MGE Galaxy 300 com a capacidade de 30kVA e autonomia de 25 minutos (a 75% da carga).

A aquisição destas duas unidades teve como principal objetivo a instalação em paralelo de forma a permitir a continuidade de serviço em caso de anomalia de alguma destas unidades ou mesmo permitir a manutenção de alguma delas sem necessidade de qualquer interrupção do fornecimento de energia.

A existência das duas unidades, instaladas em paralelo, vem também duplicar a autonomia do sistema no seu conjunto. Desta forma passou-se a ter, à carga atual de 75% por unidade, 50 minutos de autonomia do sistema. Uma vez que a utilização atual ronda os 15% de carga por unidade, a autonomia do sistema é, no total, cerca de 150 minutos.

A instalação das unidades requer:

i. A instalação de um módulo de "paralelismo" que permita a comunicação dos dois sistemas por forma a equilibrarem a produção de energia para o DC;
ii. A existência de dois disjuntores no quadro de entrada do DC de forma a permitirem o corte de energia de entrada de cada uma das unidades;
iii. A instalação de um quadro de bypass com o objetivo de possibilitar a saída das duas unidades de alimentação e a instalação de disjuntores que permitam isolar totalmente cada um dos sistemas da rede elétrica do DC.

As figuras seguintes mostram os pormenores da instalação do equipamento UPS no Data Center.

Figura 6- As UPS instaladas no DC

Figura 7 - Pormenor da instalação em paralelo das UPS

Figura 8- Quadro de Bypass das UPS

3.7. Arrefecimento da sala

A instalação do sistema de arrefecimento da sala é feito tendo em atenção dois aspetos primordiais: a disposição dos bastidores e a dos equipamentos de refrigeração do ar. A correta combinação destes dois aspetos é fundamental para a obtenção de um sistema eficiente. Por esse motivo é dado especial destaque a esta instalação, descrevendo-a pormenorizadamente de seguida.

3.7.1. Disposição da Sala

Considerando os princípios da convecção térmica, a disposição dos bastidores é um factor importante na tarefa de arrefecimento de uma sala de servidores.

Na grande maioria dos casos, o arrefecimento dos servidores funciona por ventilação interna dos mesmos obrigando à passagem de ar desde a sua parte frontal para a saída na traseira. Desta forma o ar será aquecido desde a entrada frontal do servidor até à sua expulsão pela traseira.

Quando o ar é aquecido as suas moléculas começam a agitar-se aumentando o volume do ar, tornando-o menos denso e mais leve. Como consequência desta alteração de estado, o ar quente tende a elevar-se ou a subir. Este fenómeno físico é o responsável, por exemplo, pela elevação dos conhecidos balões de ar quente e também se considera este fenómeno para melhorar o arrefecimento das salas de servidores.

Se for retirada a energia térmica do ar, através do seu arrefecimento, o movimento das moléculas diminuirá e estas aproximar-se-ão, a densidade do ar aumentará (bem como o seu peso) e o ar tenderá a descer.

Conhecendo-se, pois, as características dos servidores e do movimento do ar face à sua temperatura, planeou-se a disposição da sala em corredores de ar quente e frio:

- As portas frontais dos bastidores devem ser colocadas frente a frente formando um corredor que é denominado de corredor frio. As filas exteriores têm como oposição o limite da sala – o corredor aqui formado é também um corredor frio.
- As traseiras dos bastidores estão viradas uma para as outras, criando um corredor para onde é expelido o ar, aquecido, resultante da ventilação dos servidores e que constituirá o corredor quente;
- Existe, pelo menos, um equipamento responsável em retirar o ar quente existente no corredor quente, arrefece-lo e injetá-lo na zona do corredor frio para voltar a efetuar o arrefecimento dos servidores;

Esta configuração de arrefecimento da sala obriga a um requisito para os bastidores sem o qual o arrefecimento dos servidores será seriamente comprometido: a existência de portas perfuradas.

Assim, os bastidores deverão estar equipados com portas perfuradas que permitam a passagem do ar frio desde o exterior até à zona frontal do servidor e que o ar aquecido seja facilmente expelido para fora do bastidor através da sua porta traseira.

As portas deverão ter a maior área possível de perfuração, não comprometendo a sua segurança estrutural. Habitualmente esta razão situa-se perto dos 90% de área perfurada.

O fabricante de servidores Hewlett Packard® (HP®) indica como área de perfuração mínima os 65%, sendo este o valor que habitualmente aplica nos bastidores que fabrica.

A figura seguinte demonstra o comportamento do ar quente e frio numa sala com a disposta com corredores de ar quente e frio.

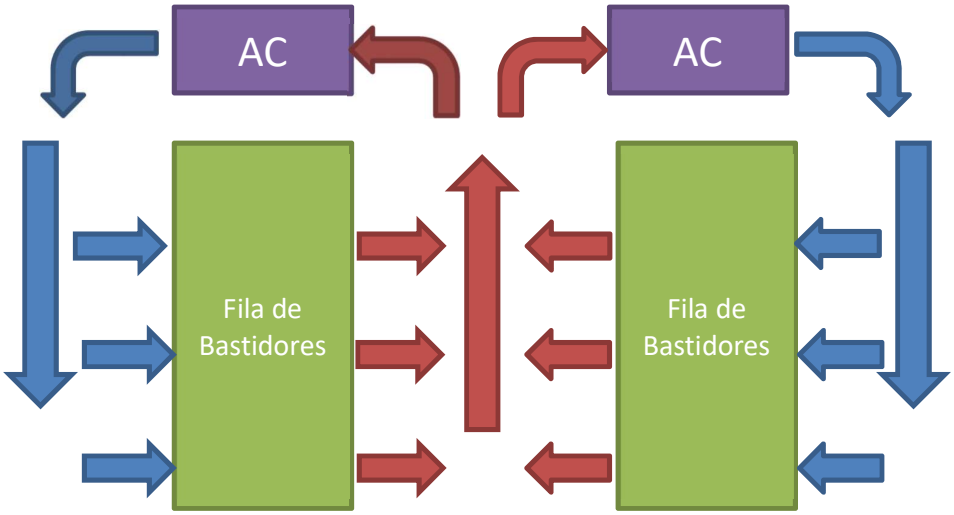


Figura 9- Movimentação natural do ar num ambiente de corredores ar quente/frio

Podemos verificar na figura 9 que, num sistema corredor quente/frio, o arrefecimento é efetuado pela colocação das unidades de arrefecimento (AC) sobre a linha de bastidores que delimita o(s) corredor(es) de quente/frio. Estas unidades vão aspirar o ar quente existente na zona do corredor quente, arrefecer esse ar e expeli-lo para a zona de corredor frio. A temperatura fria do ar é um coadjuvante ao processo de arrefecimento pois, ao arrefecer e torna-lo mais denso, o ar frio tem tendência a descer e mais facilmente atingirá as zonas inferiores dos bastidores.

Existe ainda uma segunda opção de arrefecimento possível de ser aplicada no ambiente de corredor quente/frio e é comercializada pela empresa APC/Schneider e que consiste na colocação de permutadores de calor verticalmente entre os bastidores. Desta forma o ar quente é aspirado diretamente do corredor quente, arrefecido e projetado para o corredor frio sendo este arrefecimento feito de forma igual a toda a altura dos bastidores. Esta solução seria muito mais dispendiosa que a projetada para o DC e, por isso, não foi implementada.

3.7.2. Equipamentos de arrefecimento do ar

O dimensionamento do sistema de arrefecimento foi feito tendo em conta a potência elétrica disponibilizada pelas UPS (27000 kW/h) bem como pela perspetiva da possibilidade da triplicação ou mesmo quadruplicação do parque informático.

De acordo com a formula simplificada de (*Roy Mikes[13]*) o cálculo de BTU/h necessários para o arrefecimento de uma sala de servidores resulta do total de BTU/h necessários para eliminar

o aquecimento provocado por todos os emissores de calor, considerando as seguintes constantes:

a) 1 watt/hora de consumo elétrico -> 3.412 BTU/h;
b) 1 m2 de superfície da sala -> 335 BTU/h;
c) 1 ocupante -> 400 BTU/h

Dados os equipamentos informáticos existentes para efetuar o arranque do Data Center e tendo em conta a previsão de aquisição de novos equipamentos a curto prazo foi efetuado uma previsão da capacidade de arrefecimento necessária para o arrefecimento do Data Center e que seria da ordem dos 32000 BTU/h. Este valor foi calculado baseando-se o consumo energético previsto da ordem dos 5 kW/hora.

Num cenário de utilização máxima da sala, ou seja, a potência máxima fornecida pelas UPS (27kW/hora) e atendendo que a sala não tem qualquer iluminação permanente nem a permanência de qualquer pessoa, prevê-se que a necessidade de refrigeração seja:

$$^{BTU}/_{h}\,(Sala) = 5 * 9 * 335 = 15075\,^{BTU}/_{h}$$

$$^{BTU}/_{h}\,(Servidores) = 27000 * 3.142 = 84834\,^{BTU}/_{h}$$

$$^{BTU}/_{h}\,(Total) = 15075 + 84834 = 99909\,^{BTU}/_{h}$$

A necessidade de efetuar uma separação entre os corredores quente e frio (Figura 9) e a manutenção de um fluxo de ar contínuo entre estes corredores criaram a necessidade da instalação de unidades de arrefecimento sobre as filas de bastidores como é possível ver na Figura 10.

Figura 10- Disposição das unidades de arrefecimento no DC

Sendo a climatização da sala um fator crítico para o funcionamento do Data Center foi, também, necessário garantir a redundância destes equipamentos. Este requisito foi respondido pela instalação de uma unidade adicional em cada fila de bastidores.

Optou-se então por utilizar, para o arrefecimento do Data Center, quatro unidades de ar condicionado da Mitsubishi®, modelos PEA - RP250GA/ PUHZ-RP250YHA2. Embora o mercado tenha muitas ofertas para a solução de climatização encontrou-se nestes modelos um excelente compromisso entre o custo de aquisição, o espaço necessário à sua instalação e o ruído ambiente causado pelo funcionamento destes equipamentos.

Os índices sonoros de funcionamento dos equipamentos de climatização acabaram por ser um pormenor a ter em conta uma vez que a instalação destes equipamentos é feita num campus escolar onde a existência de ruido inviabiliza o normal funcionamento das aulas.

Foi possível instalar as unidades exteriores destes equipamentos na fachada do edifício não ocupando espaço de circulação a peões nem tendo sido necessário efetuar obras adicionais.

Individualmente, estas unidades têm uma capacidade de arrefecimento da ordem dos 19800 BTU/hora, totalizando assim uma capacidade de arrefecimento da ordem dos 80000BTU/h.

3.8. A infraestrutura de rede de dados do Data Center

A infraestrutura da rede de dados do Data Center é baseada em 3 equipamentos centrais de alto desempenho e que disponibilizam ligações de rede com débitos a 1Gbps e 10 Gbps usando o cobre e a fibra óptica respetivamente.

A ligação ao backbone de rede do ISEC é efetuada através de fibra óptica monomodo com um débito de 10Gbps. Está ainda disponível uma ligação redundante em fibra óptica multimodo (com um débito de 1 Gbps) instalada num caminho de cabos alternativo de forma a salvaguardar qualquer incidente que possa ocorrer com uma das fibras. O esquema lógico destas ligações pode ser consultado no Anexo A – Infraestrutura Redundante de Rede.

4. VIRTUALIZAÇÃO DO DATA CENTER

4.1. Introdução

A aplicação da tecnologia de virtualização é uma prática que se tornou fundamental nos dias de hoje devido aos benefícios decorrentes da sua utilização: a reconfiguração dos diversos servidores de uma organização num sistema de virtualização vem permitir a rentabilização dos seus processadores e memória disponível, economia na gestão dos equipamentos ao reduzir-se o número de equipamentos, o consumo de energia bem como o espaço uma vez que, num ambiente virtualizado, será possível implementar vários sistemas operativos e vários ambientes num mesmo hardware ao mesmo tempo que os recursos do hardware (memória, armazenamento de dados, interfaces de I/O) são partilhados pelas diversas máquinas virtuais instaladas.

A virtualização de servidores já era uma prática habitual anterior a este projeto de virtualização do Data Center. Pela sua versatilidade e otimização de recursos, era possível usar alguns dos servidores mais eficientes para virtualizar serviços que exigissem menos recursos. Nessa altura as limitações eram enormes, impostas pelos recursos existentes – armazenamento, memória e capacidade de processamento – pois os servidores disponíveis não haviam sido configurados para ambientes de virtualização.

Diz-se, em bom português, que «a necessidade aguça o engenho». As necessidades que, outrora foram colmatadas com uma rudimentar solução de virtualização permitiram agora evoluir para uma solução completa de virtualização do parque de servidores já com um prévio reconhecimento dos requisitos mínimos, funcionalidade e conhecimento das soluções de virtualização – o que permitiu que este projeto avançasse de forma mais rápida.

4.2. Objetivos da Virtualização

Além de todos os benefícios já conhecidos que se podem obter com a virtualização, o ISEC recorre à solução de virtualização em duas vertentes:

- Virtualização do parque de servidores – com o objetivo de consolidar e melhorar todos os serviços instalados atingindo novos e melhores níveis de performance e segurança dos dados;
- Virtualização dos postos de trabalho – com o objetivo de garantir uma rápida reposição de um posto de trabalho em caso de avaria de hardware simultaneamente com a garantia da não existência de perda de dados do funcionário;
- Disponibilização de postos para aulas – por vezes as aulas ministradas no ISEC requerem configurações específicas de aplicações e sistemas operativos que são praticamente incompatíveis com a configuração genérica dos postos de trabalho

existentes nos diversos laboratórios. A criação de máquinas virtuais para as aulas permite a disponibilização destas soluções específicas e muitas vezes apenas temporárias sem prejuízo das restantes aulas.

4.3. Soluções de Virtualização

As soluções de virtualização definem-se, basicamente, em 2 modelos de funcionamento:

i) *Software/Hardware* – o software de virtualização é desenhado especificamente para o hardware em que será instalado. Esta tecnologia oferece um desempenho elevado quando comparada com outras. São exemplo destas tecnologias a IBM z/ VM [2] ou a HP-UX [3];
ii) *Software* – Este tipo de solução não depende do hardware em que é instalada, pois é o software que fornece todos os recursos necessários ao processo de virtualização. A grande vantagem desta tecnologia reside tanto no baixo custo de implementação como na sua portabilidade uma vez que depende apenas de requisitos comuns ou básicos de hardware servidor. As soluções VMWare ESXi , XenServer, Microsoft Hyper-V são as mais populares entre as várias soluções de virtualização existentes no mercado.

Neste projeto tomou-se em consideração apenas a virtualização baseada em *software* dado ser uma solução que não só apresenta as vantagens já citadas como possibilita a virtualização de todas as arquiteturas de software em utilização pelos serviços de informática como é ainda compatível com o parque informático existente.

4.3.1. O Hypervisor

O Hypervisor (também conhecido por VMM – *Virtual Machine Monitor*) é o mecanismo fundamental em qualquer sistema de virtualização totalmente baseado em *software*, pelo que se torna necessária uma apresentação deste mecanismo para que se possa compreender o funcionamento deste tipo de virtualização.

Sucintamente, o Hypervisor é a camada de software instalada no servidor de virtualização e que suporta cada uma das máquinas virtuais sendo responsável pela gestão e controlo dos recursos físicos (memória, processador, periféricos, armazenamento, etc..) que são partilhados nesse servidor.

O Hypervisor é o serviço responsável por:

i) Definição das máquinas virtuais;
ii) Emulação das instruções de processamento geradas pelas máquinas virtuais e respetiva coordenação e envio dessas mesmas instruções à unidade de processamento do servidor físico;

iii) Gestão de acessos ao armazenamento e memória alocados a cada uma das máquinas virtuais;
iv) Gestão dos acessos aos diversos dispositivos do servidor físico que são partilhados pelas máquinas virtuais como, por exemplo, os interfaces de rede, as unidades CDROM, dispositivos USB, etc.

De uma forma resumida pode-se afirmar que qualquer operação que uma máquina virtual necessite executar esta será transferida à camada de Hypervisor para ser processada pelo servidor físico e os seus resultados devolvidos à máquina virtual novamente através da camada de Hypervisor.

4.4. Técnicas de Virtualização

Atualmente são duas as técnicas de virtualização mais comuns e que, por esse motivo, são consideradas no processo de virtualização dos serviços do ISEC: a Virtualização total e a Para-virtualização.

4.4.1. Virtualização Total

Esta técnica baseia-se no fornecimento de uma camada de virtualização do hardware capaz de abstrair totalmente as máquinas virtuais instaladas. Neste caso, são apresentadas às máquinas virtuais todas as características físicas e recursos do servidor de virtualização não existindo necessidade de modificações dos drivers das máquinas virtuais.

Como em qualquer meio de virtualização, a camada de Hypervisor (ou VMM) está presente e encarrega-se de transferir todas as instruções de e para o sistema físico do servidor de virtualização.

Neste tipo de virtualização, o hypervisor tem um papel de abstração total de tal forma que as aplicações "julgam" lidar diretamente com o hardware do servidor.

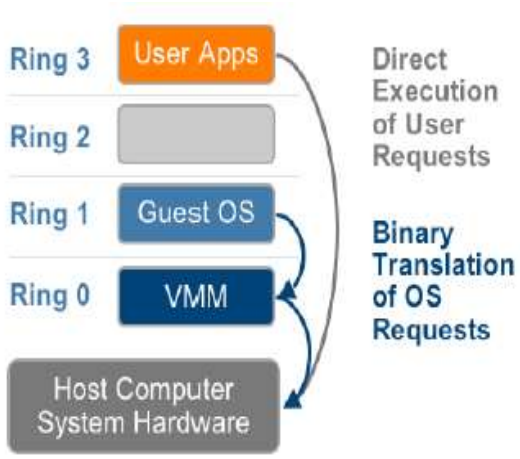


Figura 11 - Modelo de Virtualização [11]

4.4.2. Para-virtualização

O termo "para-" [4] é um prefixo de origem grega que exprime a ideia de semelhança, aproximação. Na língua inglesa, este mesmo prefixo relaciona-se com os termos "beside", "with" ou "alongside" que, em tradução para português, significam: "ao lado de", "junto a", "perto de". Desta forma, e como se mostrará, para-virtualização é uma técnica muito semelhante à técnica de virtualização total.

Na para-virtualização é inserida uma camada de virtualização com o objetivo de otimizar os acessos diretos aos recursos do servidor de virtualização através de interfaces de gestão de memória, operações de kernel, gestão de interrupções e partilha de tempo de processamento.

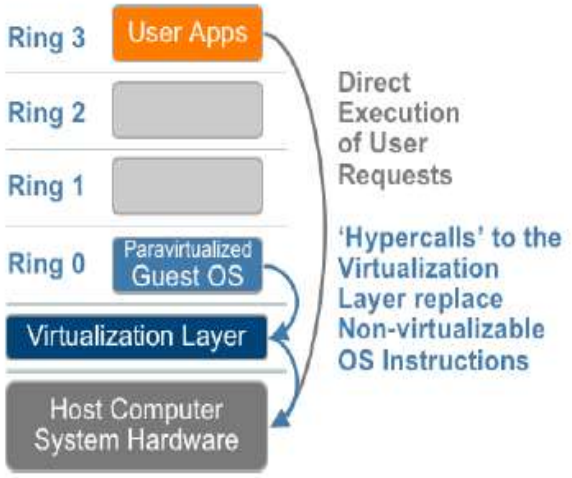


Figura 12 - Modelo de para-virtualização [11]

Com esta técnica as máquinas virtuais são sujeitas a alterações da sua configuração para que o seu processamento seja feito através do hypervisor. O virtualizador XenServer da Citrix® é um bom exemplo de utilização da técnica de para-virtualização, em que o hypervisor é baseado numa distribuição simples de Linux com o pormenor de o kernel estar ajustado para virtualização do processador e memória e em que a virtualização dos serviços de I/O é feita através de drivers de software criados para o efeito.

4.5. A Escolha da Solução de Virtualização

Os critérios para a escolha da solução [de virtualização] a adotar basearam-se basicamente em:

i) Compatibilidade do hypervisor com o hardware disponível;
ii) Compatibilidade do hypervisor com os sistemas operativos a virtualizar;
iii) Capacidade de gestão centralizada dos hypervisor's;
iv) Funcionalidade dos hypervisor's;
v) Funcionalidade vs Custo de aquisição;
vi) Suporte técnico ao sistema de virtualização.

Das soluções existentes no mercado e cuja funcionalidade é deveras reconhecida pelos profissionais de virtualização (VMWare, Citrix XenServer, Microsoft HyperV) rapidamente se

retiraram os itens i) a iv) da equação pois ambas as soluções correspondem a todas as espectativas de uma solução de virtualização.

Da análise ao item v) – Funcionalidade vs Custo de aquisição – surge de imediato a solução XenServer da Citrix (na versão *Community* ou *Open Source)* como aquela que melhor traduz o compromisso requisitado. Trata-se de uma versão semelhante à versão comercial da mesma empresa despida de suporte técnico e de ferramentas de balanceamento automático de carga entre servidores (que consiste em transferir máquinas virtuais entre hypervisor's de um mesmo grupo sempre que exista uma carga excessiva de processamento num deles – em comparação com os restantes servidores do grupo).

Dado que a Citrix® disponibiliza uma grande quantidade de documentos técnicos bem como fóruns públicos sobre o sistema de virtualização, foi da opinião do ISEC que o suporte técnico comercial poderia ser dispensado na altura da instalação dos serviços e, em caso de dificuldades acrescidas, poderia ser contratado posteriormente. Até à data todas as dificuldades sentidas com o funcionamento dos hypervisor's foram facilmente resolvidas com o conhecimento publicado pela Citrix®.

Em resposta à necessidade de virtualização de postos de trabalho surgiu a dificuldade na combinação entre o hypervisor e o software de gestão da infraestrutura de postos de trabalho virtuais (ou VDI). Esta dificuldade traduziu-se em:

- Custo de aquisição da solução de virtualização;
- Compatibilidade entre o software de gestão de VDI e os hypervisors
- Necessidade de armazenamento em disco necessário por cada posto de trabalho virtual a implementar

A solução XenServer foi a solução que apresentou mais incompatibilidades com as aplicações de gestão de VDI.

Das diversas soluções de gestão VDI, surgiu-nos a aplicação DELL® vWorkspace [5] com a melhor relação custo/funcionalidade. Embora incompatível com a solução XenServer, esta solução apresentou baixos custos de aquisição e com licenças perpétuas de utilização. A sua implementação juntamente com o hypervisor da VMWare permite uma enorme economia em armazenamento dado que todos os postos de trabalhos podem derivar de um posto de trabalho base e necessitam apenas de usar um armazenamento diferencial em relação à imagem base ou original.

A aquisição da solução VMWare ESXi na configuração básica para 3 servidores físicos e na vertente educação, foi feita a um preço promocional com uma excelente relação preço/funcionalidade.

Desta forma, a solução de virtualização implementada no ISEC é uma solução mista baseada em:

- Citrix® XenServer – 2 hypervisor's para virtualização de serviços
- VMWare ESXi – 3 hypervisor's para virtualização de postos de trabalho e *Disaster Recovery*(DR – como descrito mais à frente).

Nas figuras seguintes é possível observar o aspeto geral da configuração dos hypervisors, depois de instalados e colocados em funcionamento.

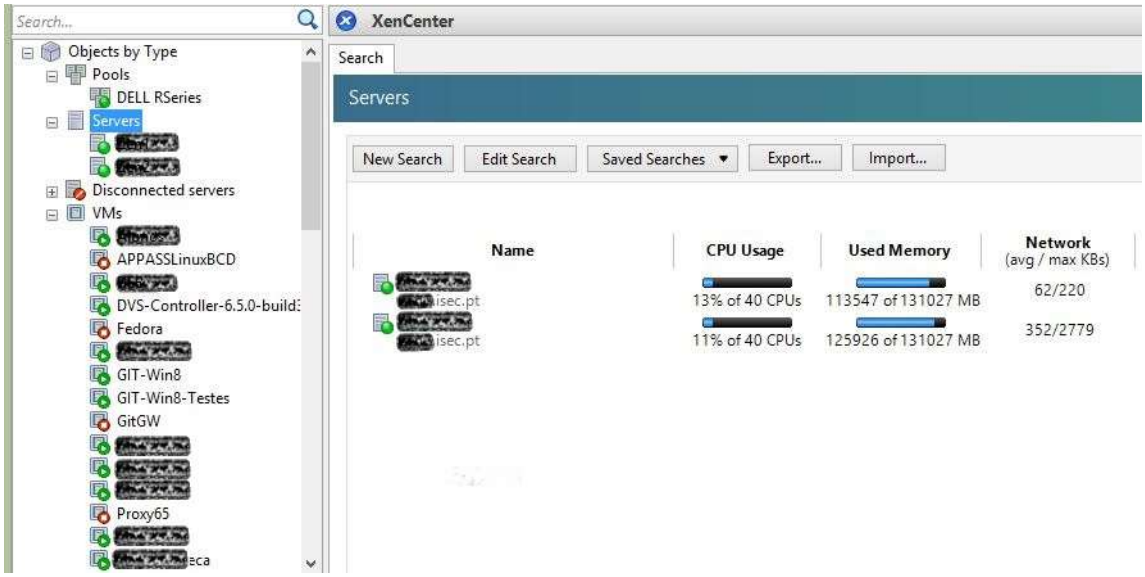


Figura 13 - Consola de configuração dos virtualizadores Xen

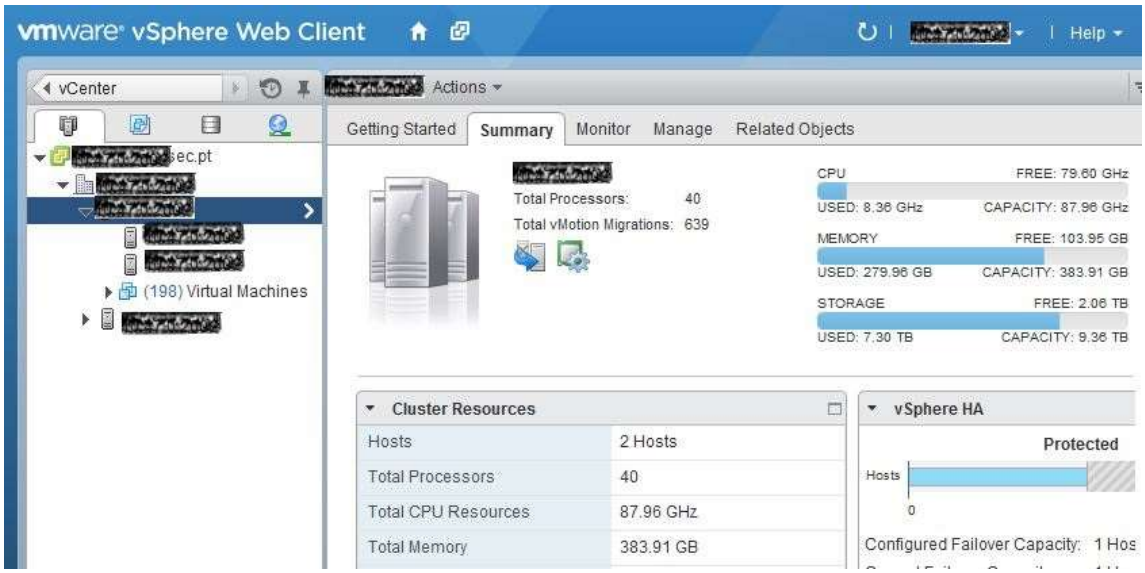


Figura 14 - Gestão dos virtualizadores Vmware ESXi

Tal como as figuras mostram, os dois sistemas de virtualização alojam mais de 2 centenas de máquinas virtuais – entre servidores e postos de trabalho virtuais.

4.6. Aquisição do equipamento para virtualização

4.6.1. Equipamento servidor

Após o levantamento dos recursos existentes à data contabilizou-se a existência de 76 núcleos (*core*) de processamento (distribuídos por 21 servidores) ao que se somam outros 8 núcleos relativos a PCs que complementavam o parque dos equipamentos disponíveis. Nestes equipamentos encontrou-se um total de 90 GB de RAM (aproximadamente).

A solução para a virtualização passou pela aquisição de um ou vários servidores que fornecessem uma quantidade igual ou superior de núcleos de processamento bem como memória disponível para a virtualização dos serviços de infra-estrutura.

Consultado o hardware disponível no mercado, encontrou-se o processador Intel® Xeon E5-2660 com 10 núcleos de processamento e capacidade de fornecer 40 cores virtuais. Embora existissem outras soluções, esta foi a identificada como tendo a melhor relação entre performance e custo.

Em relação à memória RAM a existir de base no servidor a adquirir, foi considerada a necessidade de 128 Gbyte por forma a responder à necessidade dos serviços já instalados. O aumento de memória seria possível a qualquer momento caso viesse a ser necessário.

No que respeita à virtualização de postos de trabalho, calculou-se a necessidade do funcionamento de 30 postos para serviços administrativos. Após a identificação dos recursos necessários para a sua implementação verificou-se que os requisitos de hardware são semelhantes aos requisitos para o ambiente de virtualização do Data Center.

A necessidade de redundância de hardware para garantir a continuidade dos serviços levou à aquisição em duplicado dos servidores de virtualização. Desta forma seria possível balancear a carga de processamento entre servidores e, em caso de falha ou manutenção de um servidor, transferir as máquinas virtuais para o outro servidor sem fosse necessário proceder-se a alguma interrupção de serviço.

Consultado o mercado, evidenciaram-se as propostas da DELL® e da CISCO® tanto em relação ao custo de aquisição como às características técnicas do equipamento. A decisão pendeu para a solução DELL PowerEdge R620 por esta apresentar um menor preço, melhores características em oposição à solução CISCO que apresentava uma solução modular, em chassis que acabaria por comprometer a reconfiguração e reutilização dos seus servidores.

Para o ambiente de virtualização de postos de trabalho e caso fosse necessário que estes postos de trabalho desempenhassem tarefas gráficas foram trocados os servidores Dell R620 pelo

modelo R720. A diferença entre estes modelos reside no tamanho do seu chassis: o modelo R720, por ter a altura de 2U, permite a instalação de placas de processamento gráfico.

Os servidores foram equipados com armazenamento local redundante com capacidade para a instalação do sistema operativo necessário ao funcionamento do sistema de virtualização. Esta configuração tem como objetivo salvaguardar uma possível avaria de um disco do servidor permitindo a continuidade de funcionamento do sistema operativo e até a troca do disco avariado sem necessidade de interrupção do funcionamento do servidor.

Em suma, foram adquiridos 4 servidores, cada um com as seguintes características:

- 2 processadores Intel® Xeon E5-2660 com 10 cores a 2.20Ghz, totalizando 40 cores virtuais de processamento
- 128 Gb RAM
- 2 discos de 146Gb, modelo SAS
- 4 portas de fibra óptica SFP+ (para ligação ethernet e armazenamento em rede)
- Fontes de alimentação redundantes
- Módulo de gestão remota

Na figura seguinte mostram-se os servidores adquiridos, após devidamente instalados no Data Center do ISEC.

Figura 15 - Servidores adquiridos para virtualização

4.6.2. Solução de armazenamento em rede (SAN)

Para implementar o sistema de virtualização em modo redundante foi necessário que o armazenamento dedicado aos servidores de virtualização fosse comum e partilhado. Só desta forma seria possível implementar as técnicas de redundância e de alta disponibilidade dos serviços em produção.

A aquisição de uma unidade de armazenamento em rede (vulgo *SAN – Storage Area Network*) respondeu adequadamente aos requisitos da implementação do sistema de virtualização e com garantia de redundância dos serviços.

Foi efetuado um estudo prévio às existências e necessidades de armazenamento dos servidores existentes que revelou existir um total de cerca de 10 Tbytes distribuídos pelos servidores e uma utilização de cerca de 5Tbytes de dados.

Iniciou-se então o processo de consulta do mercado com vista à aquisição de uma unidade de armazenamento com uma capacidade útil de, no mínimo, 10Tbyte. Foi ainda decidido que o sistema deveria funcionar em iSCSI sobre ethernet de forma a ser facilmente compatível com os servidores mais antigos existentes no parque informático pois esta infraestrutura de iSCSI permitiria a partilha de toda a infraestrutura da rede de dados local e interfaces ethernet dos servidores para estabelecer as ligações de armazenamento remoto.

Foram apresentadas propostas da NetApp, HP e DELL.

Ambas as unidades apresentaram mecanismos de redundância, tais como fontes de alimentação e controladores redundantes. Em ambos os casos, a ligação à rede de dados é realizada através de ligações em fibra óptica com débito de 10Gbps.

A proposta da DELL apresentou uma solução com capacidade de 27Tbytes composta por duas unidades SAN: uma unidade de elevado desempenho e outra unidade de maior capacidade. Em grupo estas unidades são vistas como uma única e existem mecanismos internos para a distribuição dos dados entre as unidades.

A proposta da HP tinha um custo extremamente elevado e a proposta da NetApp apresentou uma solução tecnicamente inferior à solução DELL ao ser constituída apenas por uma unidade de processamento e possibilidade de expansão através de gavetas de discos apresentando ainda um custo/TByte mais elevado.

Assim, foram adquiridas duas unidades DELL Equallogic 6010 sendo uma equipada com discos SAS (acesso rápido) e outra com discos SATA. Este conjunto de unidades de armazenamento apresenta 2 unidades de processamento conjugadas num grupo de armazenamento (superando tecnicamente a solução da NetApp).

A gestão das unidades DELL num grupo de armazenamento permite retirar a melhor performance combinada:

- O acesso ao grupo é feito através de 4 ligações a 10Gigabit
- Os blocos de dados de acesso mais frequente são ;
- Os restantes blocos de dados são armazenados na unidade SATA;
- Existe uma monitorização constante do acesso aos dados, fazendo com que estes sejam transferidos continuamente entre as unidades SAS e SATA de forma a que o acesso seja o mais rápido possível;

Na figura seguinte são mostradas as unidades de armazenamento adquiridas.

Figura 16 - Unidades de armazenamento instalada

5. O *Disaster Recovery Center*

5.1. Introdução

Qualquer que seja a infraestrutura informática estudada e implementada, mesmo recorrendo a todas as técnicas de redundância existe, pelo menos, um ponto de falha que poderá colocar em risco o funcionamento de toda a organização que assenta nessa infraestrutura informática.

Claro está que esse ponto de falha, não previsto na infraestrutura redundante, refere-se a uma situação cujo controlo é impossível: um terremoto, uma explosão… Ou seja, uma calamidade (ou desastre) capaz de destruir a sala ou edifício onde é instalado o centro de dados de uma instituição. Nestas situações todos os mecanismos de redundância no Data Center falharão conjuntamente com o DC.

A implementação de um Disaster Recovery Site (DRS) tem como objetivo o restauro imediato dos dados e serviços que existiam no Data Center (em falha) permitindo que a organização retome o seu funcionamento sofrendo minimamente com o impacto da destruição do seu centro de dados principal.

5.2. Definições – Desastre, DR Center, DR Site e DR Plan

Vulgarmente conhecido como DRC – Disaster Recovery Center – esta unidade só terá significado conhecendo-se as 4 componentes, julgadas essenciais: o Disaster, o Disaster Recovery Center, o Disaster Recovery Site e o Disaster Recovery Plan. Em seguida são apresentadas as suas definições gerais.

5.2.1. Disaster

Disaster, em inglês, ou “desastre” na língua portuguesa é um termo para o qual são propostas várias definições dependendo do contexto a que se referem.

No *Business Dictionary* [6] é proposta uma definição para “Desastre” capaz de descrever o evento tanto no contexto social como organizacional (onde se enquadram os serviços de IT). Neste dicionário “desastre” é definido como resultado de efeitos calamitosos, angustiantes, ou ruinosos de um evento desastroso (tais como secas, inundações, incêndios, furacões, guerra) de tal escala que interrompem (ou ameacem perturbar) funções críticas de uma organização, sociedade ou sistema, por um período longo o suficiente para prejudicá-lo significativamente ou provocar a sua falha. É as consequências de um evento desastroso e da incapacidade de suas vítimas para lidar com eles que constituem um desastre, e não o próprio evento.

Esta definição é corroborada pela definição adotada pela Organização Mundial da Saúde (OMS) traduz desastre [7] como "uma grave perturbação do funcionamento de uma comunidade ou uma sociedade causando perdas humanas, materiais, económicas ou ambientais generalizados

que excedem a capacidade da comunidade ou sociedade afetada para lidar com recursos próprios ".

5.2.2. Disaster Recovery Center

Sendo um termo habitualmente utilizado pelos serviços de proteção da população, o DRC - Disaster Recovery Center - [8] ou centro de recuperação de desastres ou catástrofes é o lugar onde se reúnem os esforços logísticos para a recuperação de desastres. Pode ser um lugar onde as pessoas e os equipamentos são reunidos após um desastre, ou um lugar onde as pessoas podem ir para obter informações ou ajuda na recuperação de desastres.

No âmbito dos sistemas informáticos e focando-se num ambiente institucional ou empresarial, a definição do DRC passará pelo lugar onde serão reunidos os ativos centrais relacionados com o DC, equipamentos servidor e administradores do sistema competentes para realizar e monitorizar as operações de recuperação dos desastres.

A atividade de uma instituição ou negócio de uma empresa deverá ser retomada no menor curto período de tempo depois da ocorrência do desastre. Nesta situação as instituições recorrem às suas estratégias de recuperação que poderão passar pela transferência de informação contida em backups e arranque de aplicações que asseguram o funcionamento institucional durante ou imediatamente após uma situação de desastre. O DRC será a localização indicada para a gestão e monitorização de todos estes processos.

5.2.3. Disaster Recovery Site

Um site de recuperação de desastres (DRS – Disaster Recovery Site) [8] é um recurso de backup alternativo, que é usado quando um local principal torna-se inutilizável devido a falha ou desastre. Ele contém os equipamentos e infraestrutura de recursos necessária ao restauro das aplicações e informação imprescindíveis à continuidade da atividade da instituição afetada pelo desastre. Estes recursos deverão estar em produção apenas durante o período de recuperação do Datacenter e infraestrutura afetados pelo desastre.

O DRS complementa o Disaster Recovery Center ao ser o local onde estão instalados os equipamentos necessários ao restauro dos serviços afetados pelo desastre. Após a recuperação do desastre e o restauro dos serviços e infraestrutura da instituição ocorrerá o encerramento das atividades em produção no DRS.

5.2.4. Disaster Recovery Plan

O DRP – Disaster Recovery Plan – [8] é o plano concebido para cada organização que descreve a forma mais rápida, eficaz e eficiente para que a atividade da organização seja reposta com a máxima brevidade após a ocorrência de um desastre. Este plano fará parte do plano geral de

continuidade de operação da organização e a sua área de aplicação será dedicada aos recursos informáticos, e sua infraestrutura, necessários para o funcionamento da organização.

Pretende-se com o DRP a elaboração de um plano com as diretivas necessárias que permitam ao pessoal técnico dos serviços informáticos a reposição de dados e funcionalidade do sistema necessários e suficientes de forma a garantir o funcionamento (mesmo que a um nível mínimo) da organização.

5.3. Implementação do DRC

Não existe Disaster Recovery Center sem um Disaster Recovery Plan. Na altura da elaboração deste documento, os mecanismos de recuperação de dados não iam além de procedimentos de backup (dados e máquinas virtuais) e ainda não estava disponível a localização remota e segura para a implementação da sala do DRS – Disaster Recovery Site. Existiam ainda grandes restrições à implementação do DRS pois não existiam armazenamento em disco capaz de dar resposta às políticas mais básicas de backup dos dados da instituição.

A implementação do DRC foi então pensada e distribuída em fases de forma a superar todas as dificuldades orçamentais e de disponibilidade de espaço, infraestrutura de rede e equipamento servidor disponíveis para a sua implementação.

Não estaremos perante uma solução de Disaster Recovery completa – o que será facilmente constatável – mas a solução implementada até à data já será capaz de suprir as necessidades decorrentes de desastres associados com servidores individualmente ou grupos de servidores.

O faseamento da implementação do DRC é sucintamente descrito a seguir:

i. **Fase 1** – Aquisição de hardware de virtualização, armazenamento de dados, solução de backup de dados e conectividade de rede. Simultaneamente foi efetuada a escolha do local de implementação do DRC;
ii. **Fase 2** – Implementação de serviço de backup de dados com transferência destes para o DRS. Incluído no serviço de backup está a conversão dos servidores virtualizados para o servidor principal do DRS e respetiva configuração.
iii. **Fase 3** – Configuração da infraestrutura de rede no DRC (a implementar em breve). Pretende-se que a nova infraestrutura complemente a infraestrutura de rede do ISEC de forma a torna-la redundante e garantir a continuidade do serviço de rede em caso de desastre no DC.
iv. Em aberto. Os aspetos relacionados com a redundância dos equipamentos do DRS, climatização, fornecimento de energia, segurança dos acessos e outros deverão ser atendidos assim que existir disponibilidade financeira para a sua realização.

5.3.1. O Espaço

À data da instalação do Disaster Recovery Site foi identificado um o espaço que, por estar munido de ligações à infraestrutura de dados da rede do ISEC, foi considerado como o local ideal para esta implementação.

Sabendo-se, à partida, que a sala necessitaria de diversas alterações para que nela funcionasse o DRS existiu logo recetividade por parte da Presidência do ISEC para a realização das obras de requalificação que fossem necessárias para o seu funcionamento em segurança.

5.3.2. O Hardware

Equipamento Servidor

Para a implementação do DR foi adquirido um servidor DELL R720, semelhante aos servidores utilizados na virtualização, apenas com a diferença em ter o dobro da memória RAM disponível. Desta forma será possível alojar, neste único servidor, a virtualização dos servidores críticos e indispensáveis ao funcionamento mínimo da instituição.

Para que a recuperação, em caso de falha, seja o mais fidedigna possível é necessário que os dados (no DR) estejam sincronizados com os dados em produção no DC. Para que sincronização de dados aconteça é necessário que exista, no DR, uma unidade SAN semelhante à existente no DC. Por razões económicas não foi possível avançar, ainda, com este cenário, pelo que surgiu a necessidade de se explorar soluções alternativas.

No âmbito do hardware foi então necessário equipar o servidor existente com mais discos para armazenamento de dados, tendo-se atingido um total de 40Tb de capacidade disponível.

O servidor dispõe ainda de 4 ligações de rede, em cobre, que podem funcionar até 1Gbps e 2 ligações de rede em fibra óptica capazes de debitar 10 Gbps.

Equipamento de Rede

Para suporte do serviço de rede, foram disponibilizados 2 switches DELL N3000 instalados de forma redundante e com ligações de 10 Gbps. Desta forma estas unidades ficarão ligadas diretamente ao DC – permitindo uma rápida transferência de dados – e, por caminhos alternativos à restante rede do ISEC garantindo o funcionamento da rede e serviços em caso de falha do DC.

Foi decidido, pelos administradores de rede, que a implementação do serviço VRRP – Virtual Routing Redundancy Protocol – e que permitirá a continuidade do serviço de rede (sem qualquer tipo de configuração adicional) mesmo quando o equipamento de routing existente no Data Center fique inoperacional.

Este tipo de redundância adicional permitirá ainda que as operações de manutenção aos equipamentos de routing possam ser efetuadas a qualquer hora do dia pois, desta forma, a operacionalidade do serviço continuará assegurada.

No Anexo A – Infraestrutura Redundante de Rede está esquematizada a proposta de implementação da solução redundante para o backbone de rede do ISEC.

As ligações entre os departamentos/serviços ao DC serão asseguradas pelas ligações a 10Gbps (2) e a 1Gbps(3). O protocolo Spanning Tree assegurará que apenas uma das ligações ficará ativa escolhendo sempre a mais eficiente.

VRRP – Virtual Routing Redundancy Protocol
É um protocolo desenhado para lidar com falhas do router default de uma rede. Este processo baseia-se na utilização de 2 ou mais equipamentos que permitam routing Layer3, ambos configurados para efectuarem o trabalho de routing, sendo um deles o Master e os restantes os equipamentos de backup. O endereço de router default da rede será gerido pelo protocolo VRRP e é atribuído ao router que estiver em funcionamento. Em caso de falha do equipamento Master, o endereço do router é activado automática-mente num dos equipamentos de backup. Quando o equipamento Master voltar a ficar operacional, o controlo ser-lhe-á devolvido voltando os outros equipamentos a ficarem em estado de standby.

O serviço de encaminhamento de tráfego entre redes (routing inter-vlan) é normalmente efetuado pelo router existente no DC. A configuração do protocolo VRRP nos routers do DC e DR atribuirá o papel de *Master* ao router do DC e Standby ao router do DRC (que entrará em operação em caso de inoperacionalidade do router do DC).

5.3.3. O Software

Foi adquirida a aplicação Dell® Appassure [9], cuja principal funcionalidade é a execução de cópias de segurança – backup - da informação armazenada nos servidores do DataCenter.

Os backups dos servidores são efetuados em duas vertentes:

i. Bare Metal Backup – É efetuada uma cópia integral dos discos (físicos, lógicos ou virtuais) do servidor - também conhecida como imagem do disco. O restauro de dados deste tipo de backup permitirá reconstruir integralmente a imagem lógica do disco num suporte semelhante ou adaptá-la a um suporte que permita suportar tal quantidade de informação e assim criar uma cópia do servidor original. Uma característica que este software de backup tem é permitir fazer através da técnica de Bare Metal Backup é o backup granular dos dados simultâneo, como descrito a seguir:
    a) Backup Granular – Embora os dados sejam guardados em bloco o restauro dos mesmos pode ser feito ficheiro a ficheiro. No caso de aplicações como o Microsoft SqlServer ou Microsoft Exchange a recuperação de dados granular é possível de efetuar ao nível da base de dados ou da caixa de correio, respetivamente. A execução de cópias de segurança incrementais possibilita o restauro das várias versões dos dados conforme as datas de execução dos backups até à versão mais antiga guardada no servidor de backups;

ii. Virtual Standby – Existindo os backups Bare Metal dos servidores e existindo um servidor de virtualização, o software Appassure permite converter os backups existentes em máquinas virtuais configuradas com as características mais similares possíveis das máquinas originais e que estejam prontas a ser colocadas em produção no caso de falha dos servidores originais.
Este processo ocorre sempre que exista um aumento de informação significativo. Nessa situação o servidor de backups inicia o processo de conversão das imagens dos discos do servidor num novo servidor virtual, ficando este novo servidor em standby, pronto para ser iniciado em caso de falha do servidor original (em produção).

Os agendamentos dos backups dos servidores são feitos pelos administradores dos sistemas e de acordo com as necessidades de salvaguarda da informação.

De seguida são apresentadas imagens da solução de backups adotadas para a segurança e replicação de dados e servidores no DRS do ISEC.

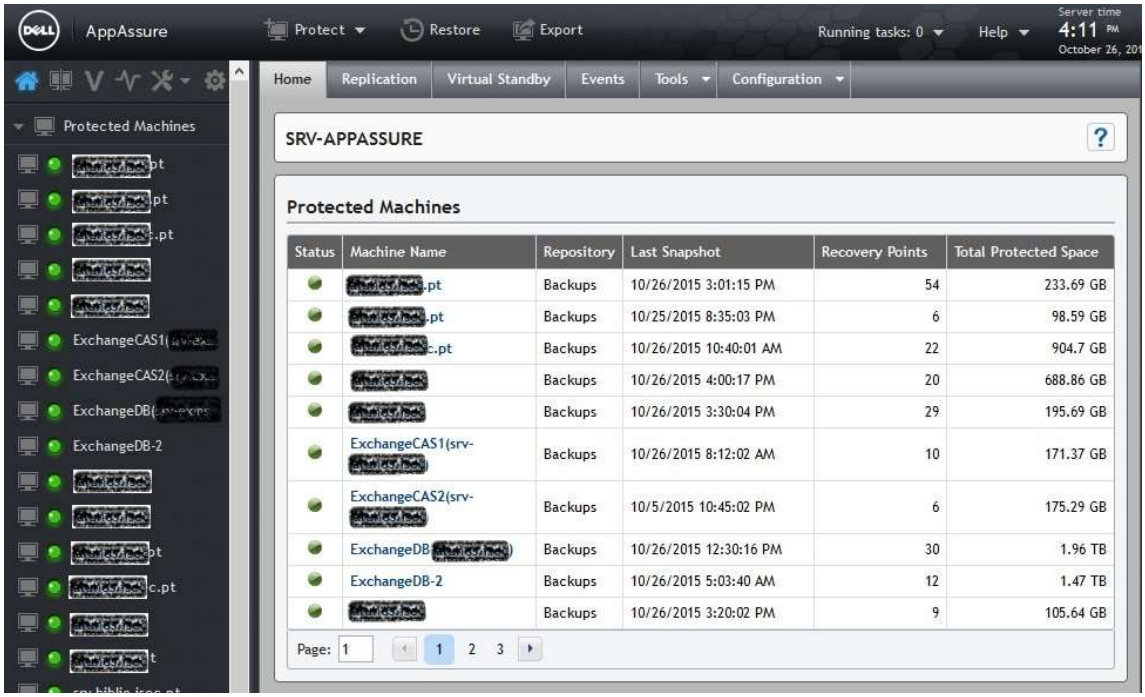


Figura 17 - Consola de administração da solução de Backups

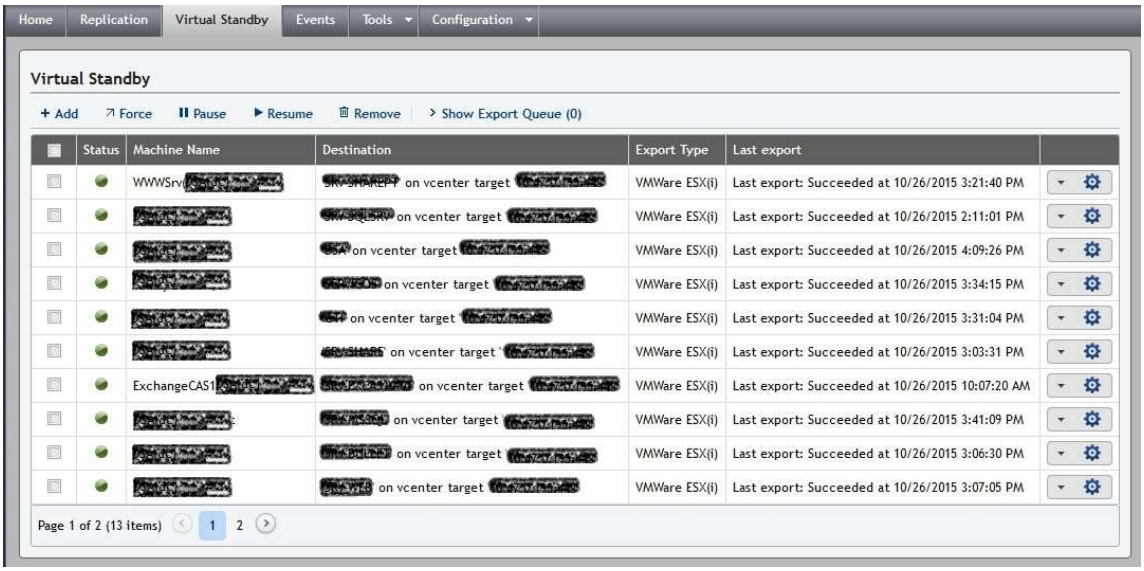


Figura 18 - Pormenor da configuração de servidores em Virtual Standby

Os processos de Virtual Standby podem não ocorrer logo após aos eventos de backup mas esta situação superar-se-á com a atualização dos dados através do restauro granular da última versão de backup se assim for necessário. Esta situação acontece porque o processo de construção de uma máquina virtual (o Virtual Standby) só acontece quando a disparidade entre a sua versão e a versão dos dados do último backup assim o justificarem. Se, a cada backup, correspondesse a criação de uma nova versão do Virtual Standby o risco de este servidor não estar disponível em caso de acidente seria elevado.

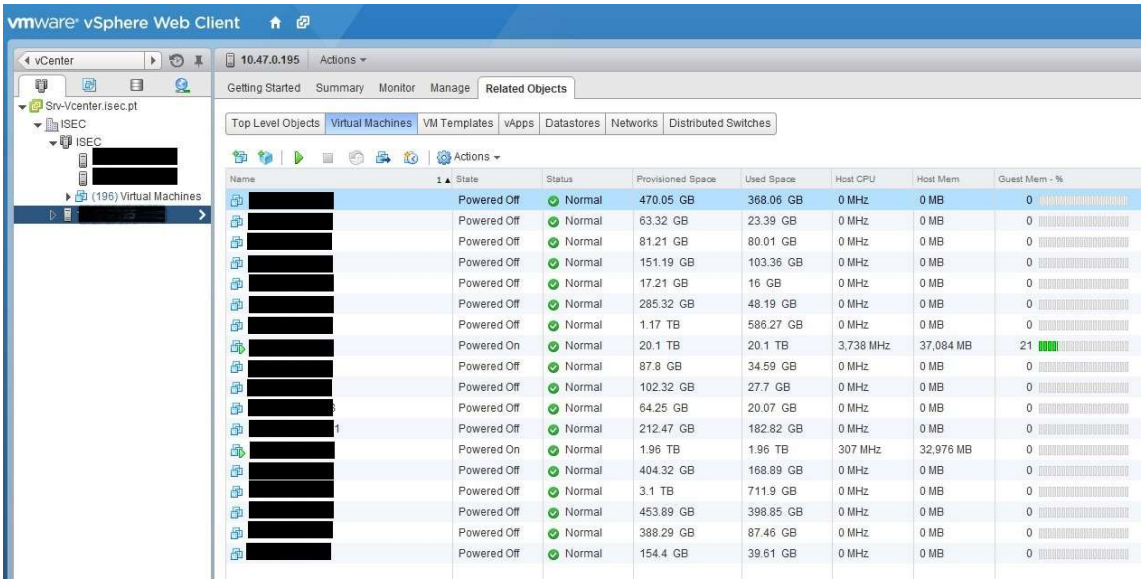


Figura 19- Listagem dos servidores em Virtual Standby no DRS

A Figura 19- Listagem dos servidores em Virtual Standby no DRS apresenta um pormenor da configuração do servidor de virtualização instalado no DRS. É neste servidor que são instaladas e mantidas cópias atualizadas das imagens dos servidores em produção para serem ativadas em caso de falha (virtual standby).

Aliado ao mecanismo de Virtual Standby pretendia-se um mecanismo que automatizasse o arranque da(s) máquina(s) em standby em caso de falha dos servidores em produção. Não só o software adquirido não dispõe de tal tecnologia como uma simples e momentânea falha de rede poderia despoletar o arranque das máquinas em standby o que poderia trazer resultados indesejáveis para o funcionamento do Data Center (duplicação de endereços IP, alteração de bases de dados, corrupção do sistema de backups, etc).

Assim o processo de Virtual Standby obriga, em caso de desastre, à intervenção de um administrador de sistemas para verificar a existência da quebra de funcionamento do servidor original, a verificação da integridade dos dados do servidor em standby, a reconfiguração dos parâmetros da rede lógica (ao nível do virtualizador) e confirmação da entrada em produção da máquina (em standby). Esta falha poderá ser ultrapassada, mas só com a existência de um mecanismo dedicado à monitorização de todas as variáveis próprias da uma infraestrutura do ISEC a fim de apurar efetivamente a existência da falha e assim dispor de dados para uma correta tomada de decisão.

Além da complexidade da tomada de decisão no arranque das máquinas em Virtual Standby existe a necessidade da execução de tarefas de reposição de dados nestas máquinas de modo a garantir que a continuidade do serviço é feita com dados atualizados. Este conjunto – tomada de decisão e reposição de cópia de segurança – deve ser analisado caso a caso (ou servidor a servidor) o que torna impraticável a definição de um procedimento genérico para a ativação dos Virtual Standby. Desta forma fica justificada a não implementação de um mecanismo automatizado para a ativação dos Virtual Standby em caso de falha dos servidores originais.

5.4. O Disaster Recovery Plan

O plano de backup dos dados do Data Center, as características do software utilizado para a execução das cópias de segurança, as características do servidor adquirido para a realização destas tarefas e a infraestrutura de rede implementada conseguem definir, parcialmente, o plano de Disaster Recovery:

- Os backups dos servidores do ISEC são feitos continuamente e esta informação é transferida para o Disaster Recovery Site;
- É permanentemente construída uma cópia virtual dos servidores críticos do ISEC, ficando esta cópia armazenada e configurada no DRS, pronta a ser ativada;

- A existência de uma infraestrutura de rede redundante controlada através dos protocolos Spanning Tree e Virtual Router Redundancy permitem que a rede se adapte automaticamente de forma a suprimir uma falha dos equipamentos do DataCenter;

Tomando como base o plano de salvaguarda da informação critica do ISEC, o Disaster Recovery Plan define-se, para qualquer que seja o evento que interrompa o funcionamento dos serviços informáticos do ISEC, na seguinte lista:

1. Identificação do evento ou desastre;
2. Em caso de uma simples perda de ficheiros, efetuar as reposições necessárias a partir das cópias de segurança alojadas no DRS;
3. Em caso de inoperacionalidade do DataCenter ou dos equipamentos do core de rede do DataCenter: configurar os parâmetros de rede e ativar as máquinas virtuais em standby no DRS;
4. Em caso de inoperacionalidade de um ou mais servidores deverá ser classificado o seu impacto na infraestrutura de TI e, de acordo com a sua classificação:
    a. Crítico – configurar os parâmetros de rede da imagem virtual standby existente no DRS e efetuar o startup da máquina;
    b. Não crítico – Decidir acerca da criticidade do servidor em questão e optar entre:
        i. Recriar na íntegra o servidor em falha, a partir do bare metal backup existente;
        ii. Construir, no DRS, uma cópia virtual do servidor em falha e colocá-la em produção. Posteriormente esta máquina deverá ser transferida para o DC.

Espera-se que, num futuro próximo, se consigam reunir os recursos que possibilitem a reposição na íntegra de todos os serviços de TI no DRS e assim simplificar o DRP ao ponto de transformar o plano de DR na simples decisão da ordem de arranque dos servidores em standby. Este futuro chegará quando:

i. For disponibilizado, no DRS, equipamento de armazenamento em rede da mesma série e capacidade igual ou superior que o equipamento existente no Data Center;
ii. For aumentada a capacidade de processamento no DRS – através da aquisição de servidores de virtualização – capazes de igualar os recursos necessários dos servidores críticos e menos críticos do Data Center
iii. For garantida a autonomia elétrica no DRS

Este "futuro" já não é presente **apenas devido às restrições financeiras a que o ISEC está sujeito.** Caso contrário a instalação e apetrechamento do DRS teria acontecido paralelamente com a instalação e apetrechamento do DC.

6. CONCLUSÃO

O projeto que é agora apresentado satisfaz os objetivos pretendidos ao ter resultado na instalação e colocação em funcionamento do Data Center do ISEC.

O Data Center do ISEC veio solucionar os problemas e dificuldades anteriormente existentes nos fornecimento de serviços informáticos ao ISEC (conforme descrito em 2. MOTIVAÇÃO – O PARQUE DE SERVIDORES), tanto na ótica dos serviços administrativos como na vertente da instituição de ensino superior.

O estudo e implementação dos mecanismos de recuperação de desastres no Data Center (ver 5.4. O Disaster Recovery Plan) vem permitir que o seu funcionamento seja redundante, ou que as falhas sejam recuperadas no imediato, de forma a garantir que os serviços informáticos de suporte ao funcionamento do ISEC não sejam afetados.

O projeto de implementação do Data Center não deve ser considerado como completo ou terminado pois a constante evolução dos serviços TI e o constante aumento dos seus requisitos originam a necessidade da alteração constante do Data Center no que respeita aos recursos de processamento ou de armazenamento.

Neste projeto ficou em falta – principalmente devido aos prazos disponíveis para a sua realização- a configuração de um sistema de monitorização centralizado dos equipamentos e serviços instalados no Data Center. Só desta forma seria possível ser apresentada uma análise quantitativa acerca dos ganhos obtidos com a instalação do DC, nomeadamente dos tempos de funcionamento sem interrupção, dos recursos utilizados e dos disponíveis para novos projetos.

A título pessoal, a realização deste projeto permitiu a aplicação das competências adquiridas ao longo da formação académicas nesta instituição, dos workshops e outras apresentações que tive oportunidade de participar bem como dos 15 anos de experiência profissional como administrador de sistemas e redes de dados. A experiência ganha na realização deste projeto permitiu ainda consolidar e renovar os conhecimentos na área de integração de sistemas e Data Centers-

O ISEC continuará a sua atividade com uma unidade de ensino superior de referência na área de engenharia e o seu Data Center deverá acompanhar e garantir o fornecimento de serviços informáticos de suporte ao funcionamento da instituição e para que tal continue a ser possível é necessário realizar, num futuro próximo, projetos para consolidar e garantir a ausência de falhas do DataCenter:

- A instalação de um sistema de monitorização de equipamentos e serviços com função alarmística;
- A aquisição de um grupo gerador capaz de assegurar o funcionamento do Data Center em caso de falha do fornecimento de energia elétrica. Uma ligeira prospeção dos equipamentos disponíveis e do seu custo de implementação permitiu expandir este

projeto a uma escala maior, podendo o grupo gerador dar suporte também aos serviços administrativos do ISEC sem grande aumento da relação kVA/€;

- O aumento dos recursos de armazenamento e virtualização de forma a garantir a normal evolução dos recursos existentes;
- A aquisição de um sistema de controlo de acessos à sala do DC que possa monitorizar todos os acessos que sejam feitos à sala;
- A instalação de um sistema de monitorização ambiental e de acessos, com registo de som e imagem, para um melhor controlo da sala do Data Center;
- A construção da sala do Disaster Recovery Site, ou seja, a construção de uma sala segura com as mesmas características da sala do Data Center, pois só assim será possível existir fiabilidade naquele que pretende ser o centro de recuperação de desastres de uma instituição.

7. BIBLIOGRAFIA

[1] IPC, "http://portal.ipc.pt/portal/portal/sobreIPC/ipcnumeros," 2013. [Online]. Available: http://portal.ipc.pt/portal/portal/sobreIPC/ipcnumeros.

[2] IBM, "IBM z/VM overview," IBM, 12 2014. [Online]. Available: http://www.vm.ibm.com/overview/. [Accessed 12 2014].

[3] HP, "Mission Critical Compute," HP. [Online]. [Accessed 12 2014].

[4] Porto Editora, "Infopédia," Porto Editora, [Online]. Available: http://www.infopedia.pt/dicionarios/lingua-portuguesa/para-. [Accessed 2014].

[5] DELL, "Dell vWorkspace Datasheet," [Online]. Available: http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Dell_vWorkspace_Datasheet.pdf. [Accessed 12 2014].

[6] Business Dictionary .com, "Business Dictionary .com," WebFinance, Inc., [Online]. Available: http://www.businessdictionary.com/definition/disaster.html.

[7] World Health Organization, "http://www.who.int," Outubro 2013. [Online]. Available: http://www.who.int/hac/about/definitions/en/.

[8] Techopedia, "Techopedia," Janalta Interactive Inc., [Online]. Available: https://www.techopedia.com.

[9] DELL, [Online]. Available: http://software.dell.com/products/appassure/.

[10] D. Alger, Build the Best Data Center Facility for Your Business, Cisco Press, 2005, p. 408.

[11] VMWare, Inc, "Understanding Full Virtualization, Paravirtualization, and Hardware Assist," 2007. [Online]. Available: http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf. [Accessed 16 01 2015].

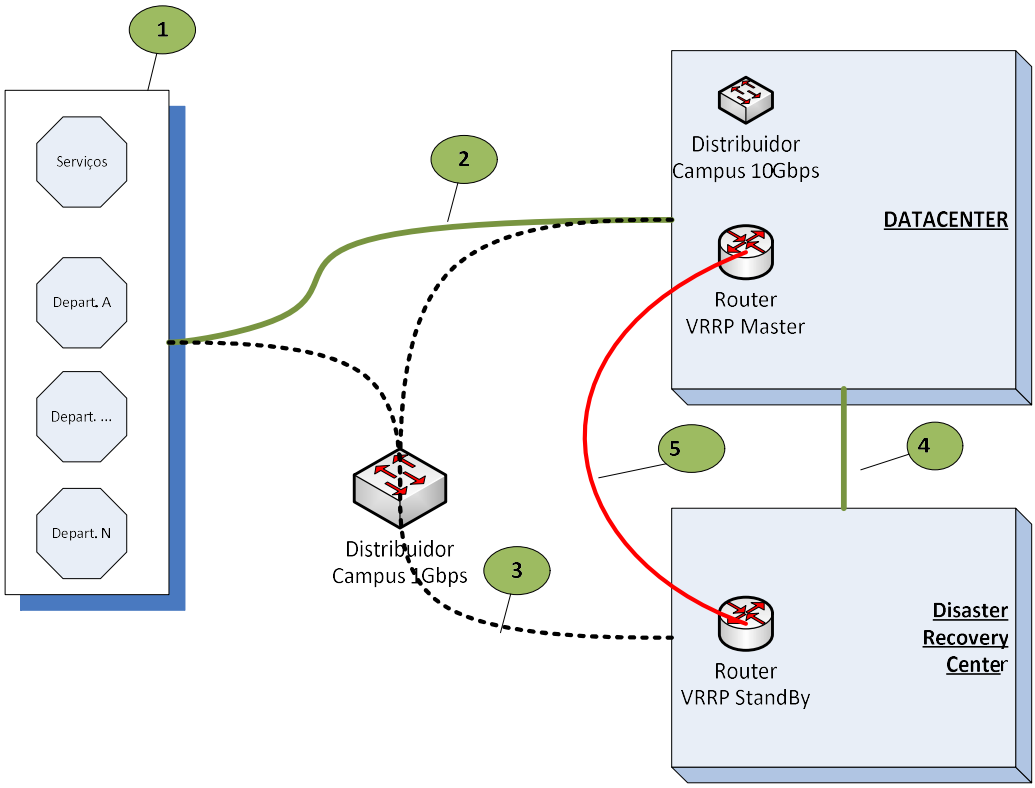
[12] DuPont, "DuPont FM200 - FIRE EXTINGUISHING AGENT," [Online]. Available: http://www2.dupont.com/FE/en_US/assets/downloads/pdf_fm/k23261_FM-200_PUSH.pdf. [Accessed 13 12 2014].

[13] Schneider Electric, [Online]. Available: www.apc.com.

[14] R. Mikes, "mikes.eu," Março 2010. [Online]. Available: http://www.mikes.eu/index.php/how-to/109-calculating-the-size-of-a-server-room-air-conditioner.html.

ANEXOS

Anexo A – Infraestrutura Redundante de Rede



1 – Representação lógica de cada um dos edifícios de serviços administrativos ou departamentos do ISEC. Cada uma destas unidades dispõe de uma ligação ao datacenter através de (2) ou (4)

2 – Ligação ao Datacenter do ISEC através de fibra óptica monomodo com débito de 10Gbps. Esta ligação é feita ao equipamento responsável pelas tarefas de inter-vlan routing e distribuidor de campus.

3 – Ligação ao Datacenter do ISEC através do [antigo] distribuidor de campus do ISEC, utilizando fibras multimodo com débito de 1Gbps.

4 – Ligação DC-DR dedicada, com débito 10Gbps, para a realização de trabalhos de backup e sincronização de dados

5 – (Simbólico) Verificação de funcionamento (heartbeat) dos equipamentos de routing do DC e DR para decisão de activação do equipamento de routing segundo o protocolo VRRP.