



INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP
DELEGAÇÃO REGIONAL DO ALENTEJO
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL

Projeto final
Implementação de Rede Informática

Cliente
CEFPAL



MINISTÉRIO DA ECONOMIA
E DO EMPREGO



GOVERNO DA REPÚBLICA
PORTUGUESA



UNIÃO EUROPEIA
Fundo Social Europeu

Projeto elaborado por: Luís Santos

CET Redes e Sistemas Informáticos
2015 - Santo André

Conteúdo

Introdução.....	2
Descrição Geral do Projeto.....	4



Análise dos requisitos necessários á sua implementação.....	5
Características da rede a implementar.....	7
Desenho logico da rede.....	11
Endereçamento IP.....	12
Localização de servidores, bastidores e material activo de rede.....	13
Estratégia de gestão da rede.....	23
Desenho Físico da rede.....	24
Servidores.....	38
Descrição das políticas de segurança e salvaguarda da informação a adotar.....	40
Funcionamento do helpdesk e comunicação de avarias pelos clientes.....	43
Forma de implementação de sistemas de comunicação por voz e vídeo.....	43
Análise de custos de toda a solução apresentada.....	44

• Introdução



INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP

DELEGAÇÃO REGIONAL DO ALENTEJO

CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL

Com este trabalho pretendo aplicar conhecimentos adquiridos sobre redes informáticas durante o curso de especialização tecnológica de gestão de redes e sistemas informáticos. Foi efetuado também um grande trabalho de pesquisa para apresentar soluções para o problema apresentado. Espero com este trabalho ficar com uma noção maior do que é de facto parte do mercado de trabalho das redes informáticas.



• Descrição Geral do Projeto

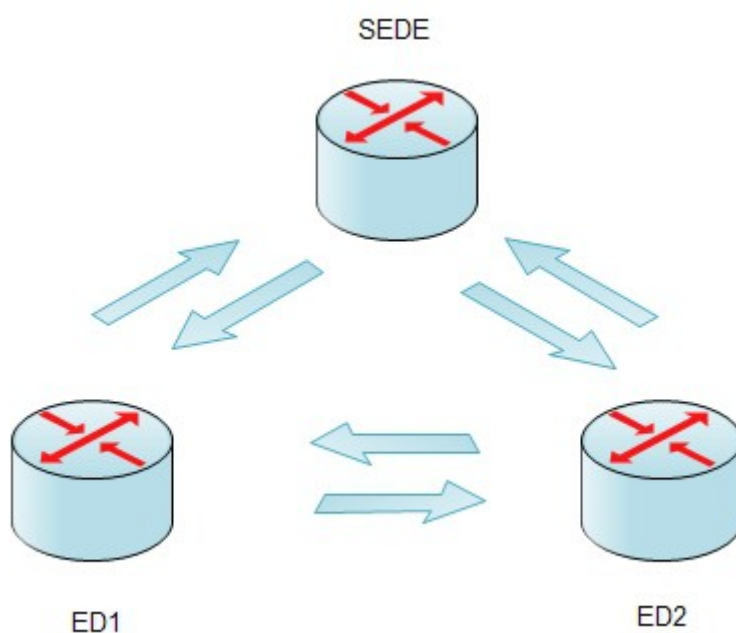
No âmbito do pedido de implementação de uma rede estruturada nos edifícios do CEFPAL, foram analisadas as necessidades da rede, que deverá suportar comunicação de informação dentro dos edifícios, mais propriamente, vídeo, voz e dados, para além da comunicação entre diferentes pisos e edifícios, para além da implementação de políticas de segurança, backup, e ergonomia. De referir que o CEFPAL é constituído por 3 edifícios, tendo o primeiro (SEDE) 4 pisos, o segundo 2 pisos e o terceiro também 2 pisos. Com este trabalho pretendo fazer um projeto mais próximo do que na realidade seria implementado.



- **Análise dos requisitos necessários à sua implementação**

Os requisitos que o cliente pediu para a implementação da rede, são:

- Rede informática que estabeleça a interconexão entre as infraestruturas do edifício:
 - A interconexão entre as infraestruturas é assegurada pela colocação de switches de layer 3 OSI em cada edifício, interconectados entre eles, com redundância de rotas, para que se falhe um canal de rede, o switch vai encontrar outra rota para chegar ao destino. Mas caso falhe o dispositivo de rede activo, poderá, caso o cliente queira, ser implementado um sistema redundante em cada edifício, como está no edifício principal.



- Todos os trabalhadores deverão ter acesso à rede da empresa, sendo que determinadas áreas ou serviços condicionado à função que desempenham:
 - Aqui entra em serviço a utilização de interVLANs, sendo permitido a aplicação das mesmas devido ao uso de switch de layer 3, que operam na camada de rede, permitindo a criação de rotas.



- Uma vez que temos vários departamentos do mesmo tipo, mas em diferentes edifícios, será necessário a criação das chamadas InterVLANs, com a configuração dos devidos switches core com canais dedicados (Trunk Link).
 - Com esta configuração, a rede será segmentada de modo a que cada departamento esteja isolado dos restantes.
 - Foi aplicada a utilização de switch core, uma vez que para além de operarem no layer 3, em relação a routers o preço cai bastante, e influencia o orçamento.
-
- Pretende-se que o acesso à informação vital da empresa seja centralizado na sua sede, com acesso autorizado em todos os pontos de rede.
 - Aqui entra a configuração das ACL (ACCESS LISTS) no switch core. Temos por exemplo um segmento de rede, no qual configuramos uma access list a essa VLAN para permitir a ligação ao datacenter localizado na sede
 - Também na sede será efectuado o acesso principal ao exterior da rede
 - Este ponto está assegurado com a instalação dos bastidores principais na sede, que irá distribuir a rede pela empresa.
 - Na zona de atendimento público providenciar o acesso wi-fi a qualquer pessoa
 - Serão criadas várias zonas de acesso wi-fi com largura de banda limitada, com hotspot público providenciado pela rede. Neste caso a rede estará isolada da rede principal, de modo a não colocar a informação da empresa em perigo.



• Características da rede a implementar

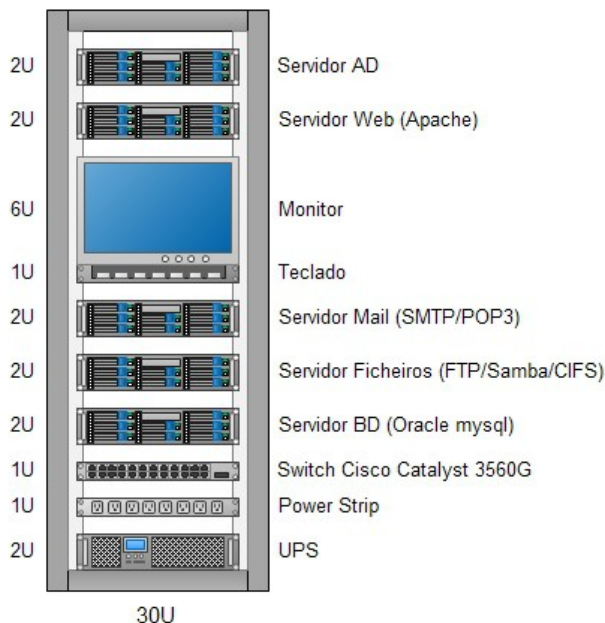
A rede a implementar terá que ser flexível, confiável, segura, de alto desempenho e economicamente viável. Para isso definiu-se uma margem de expansão de cerca de 50 % na rede, para além da implementação de uma DMZ para serviços ao exterior com regras nas firewalls, para além da implementação de um domínio e vlans. Quanto à segurança veremos mais abaixo as características implementadas. O desempenho estará assegurado por dispositivos activos de grande capacidade e passivos também, como é o caso da utilização de cabos CAT6 E para giugabit e fibra para interligação dos dispositivos de rede. Em termos qualidade/preço foi aplicado por exemplo switch layer 3 em vez de routers nos edifícios o que vai baixar bastante o orçamento, mas manter a rede de alto desempenho e segura.

A rede estará assente num domínio, denominado de cefpal.pt

- Serviços de rede: partilha de ficheiros, AD, internet, email e bases de dados
 - Os serviços acima descritos serão disponibilizados por servidores Dell Xeon com Windows server 2012 montados em RACK com cada uma das características necessárias, tirando o servidor de base de dados que será em baseado em unix (oracle Linux com mysql). Temos então o servidor active directory, que é um sistema de domínio no qual se irá controlar os acessos dos computadores na rede, o servidor Web com apache e php. O servidor de base de dados estará montado num outro servidor com ligação entre eles, e irá usar o mysql apenas disponível aos sectores de vendas e financeiros. Depois temos o servidor de mail, configurado o SMTP e POP3, onde irá funcionar sistema de



emails dos funcionários da empresa. Depois temos o servidor de arquivos que ira estar ligado ao datacenter da empresa. Este servidor estará configurado com FTP (em conjunto com o servidor web), Samba e CIFS.



Bastidor Servidores

- Comunicação por email entre todos os postos de trabalho
 - Estará assegurada pelo servidor SMTP/POP3 implementado no servidor de email
- Implementação de uma intranet para divulgação de informação interna da empresa, apenas acessível dentro da rede e em todos os postos de trabalho
 - No servidor web será configurado numa porta 8080 um segundo website com toda a informação da empresa a disponibilizar. Esta porta estará bloqueada ao exterior, de modo a que o acesso seja apenas possível dentro da empresa
- Implementação do site para acesso ao exterior, contemplando também o acesso via ftp a informação a disponibilizar aos utentes
 - No servidor web, na porta 80, será aberta ao exterior, com implementação de servidor de FTP para disponibilizar ficheiros aos utentes.
- Implementação de mecanismos de armazenamento redundantes, e politicas de backup de informação



- Neste campo está a implementação de um datacenter, onde vai guardar de forma segura a informação da empresa. O datacenter terá vários tipos de RAID (espelhado e redundante e o misto de ambos) e os backups serão feitos de forma regular (diário para ficheiros alterados e mensal para o sistema completo) ou antes de ser feita alguma actualização aos sistemas. Para além disso vai ser usada o Hadoop da apache, open source para a manipulação da informação em grandes quantidades do datacenter.
- Todos os utilizadores deverão ter acesso à Internet
 - Este campo está assegurado com servidor de Internet, onde cada posto de trabalho terá o endereço de DNS e IP atribuído automaticamente.
- Acesso não autorizado e propagação de vírus (mecanismos de segurança)
 - Neste campo deverá ser dada formação base aos trabalhadores sobre políticas de segurança, para além dos sistemas implementados de firewall com antivírus e controlo de tráfego. Caso o problema venha de dentro da rede, como uma pen com vírus, os computadores estarão devidamente actualizados, tanto a nível de sistema, como antivírus e software, e para impedir a propagação de vírus temos o servidor de email com antivírus, para além da rede segmentada, caso um vírus ataque determinado departamento a ameaça estará limitada ao segmento de rede em que se encontra.
- Todas as secções deverão ser isoladas das outras, do ponto de vista logico da rede
 - Assegurado com a criação de VLANs
- Validação de utilizadores
 - Estará assegurado pela utilização de um domínio, quanto à validação wireless, cada ponto de acesso, para além da rede destinada ao publico, terá um mecanismo com utilizador e password para os trabalhos da empresa
- Entre as direcções de cada edificio implementar videoconferência
 - Assegurado pela transferencia de dados pela rede por IP, com a instalação de uma camera IP de alta resolução e Televisor LCD como output em cada secção de direcção.
- Dentro de cada edificio deverá ser possível o estabelecimento de comunicação de voz pela rede
 - Implementado o acesso a rede de voz através de VOIP, usando switches POE, com PBX na sede para saída para o exterior.
- Projecto deverá prever escalabilidade

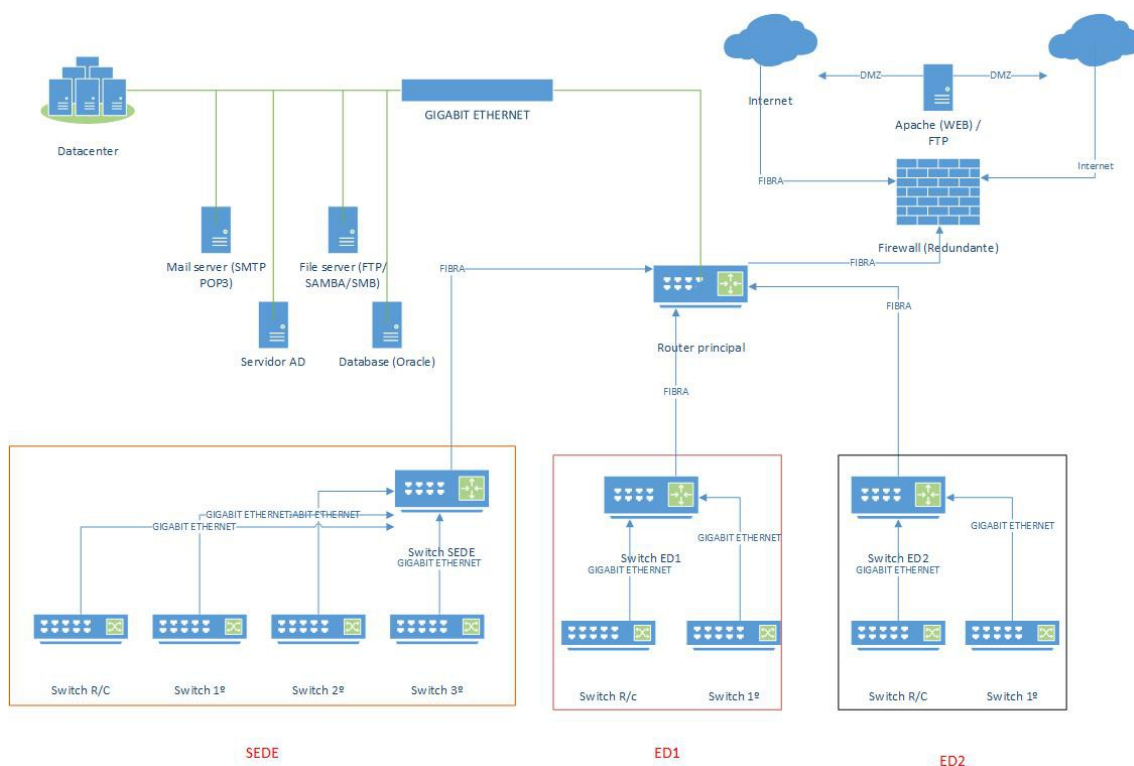


- Previsto na implementação da rede, um aumento de até 50% da rede inicial, tanto a nível lógico como a nível físico
- Deverão existir duas impressoras departamentais por cada piso de edifício acessíveis a todos os postos de trabalho
 - Deverá ser necessário um servidor de impressão onde estarão instaladas as impressoras (software e drivers), tendo duas ligadas via ethernet em cada piso, estando assim disponíveis para todos os utilizadores através do servidor de impressão
- Plotters e Sun Workstations disponíveis a trabalhadores com formação específica
 - O sistema está assegurado para trabalhar com Sun Workstations, uma vez que são sistemas baseados em unix, e a implementação no domínio Windows está prevista com a configuração do LDAP.
- Sistemas operativos dos postos de trabalho
 - Todos os sistemas instalados nos postos de trabalho serão Windows 7, à excepção da área de projecto, servidores e acessos wifi.
- Sectores financeiros e vendas acedem a base de dados oracle em unix
 - Previsto na configuração dos servidores de base de dados, que usam mysql assente no oracle linux



• Desenho logico da rede

O esquema da rede cablada resumido vai ser o que está demonstrado na imagem abaixo;



No qual temos em termos de distribuição de sinal a comunicação entre diferentes pisos de cada edifício, e a comunicação entre edifícios. Temos depois também a comunicação para o exterior, com o suporte a dual WAN, para redundância, caso falhe uma a outra entra no activo.

De salientar que os switches core de cada edifício têm rotas redundantes definidas, como já foi referido acima.

- A utilização de um switch core para cada edifício deve-se ao facto de poder fazer-se o encaminhamento de informação entre edifícios para além do facto de que se usasse um switch layer 2 em vez de um layer 3, poderia haver o facto do dispositivo principal (router) falhar e a rede toda ser afectada, para além da sobrecarga do dispositivo.



Topologia

A topologia adotada na rede CEFPAL é uma topologia Híbrida, uma vez que se adapta às necessidades da rede. Esta topologia integra vários tipos de rede, por exemplo neste caso temos a rede em estrela (ponto central – router) e em malha (interligação entre switches). É um tipo de rede que permite a expansibilidade, flexibilidade e funcionalidade dos segmentos de rede implementados.

• Endereçamento IP

A estratégia de endereçamento IP da rede está assente em INTERVLAN's, uma vez que temos certos departamentos espalhados pelos edifícios, mas queremos segmentar a rede de modo a que esses departamentos fiquem ligados entre si mas isolados da restante rede. Para tal foi escolhido o catalyst 3560G, que é um switch layer 3, que permite routing, e como já referi acima se fosse usado um router para cada edifício, o orçamento disparava, quando com um switch layer 3 é permitido a criação de VLAN's entre switches, usando um trunk link entre switches. Foi usada uma rede classe B privada (172.16.0.0 (lembrando que esta classe de rede vai até 172.31.255.255)) classe essa que permite mais endereços por rede, daí a escolha da mesma, uma vez que a rede vai albergar cerca de 500 pontos de rede e ainda ter que suportar ligações wifi dos clientes.

Portanto temos como já referi acima uma rede classe B que vai ser 172.16.0.0/12, dividida em sub-redes para cada departamento.

172.16.0.0/12 Classe B Pontos de rede					
Identificação da rede	Bits/Subnet	Mascara (256 - Blocos)	Ordem	Gama	
Direção	8	255.255.240.0	11	172.16.1.185	172.16.1.201
Informática	8	255.255.240.0	10	172.16.1.168	172.16.1.184
Videoconferencia	8	255.255.240.0	9	172.16.1.151	172.16.1.167
Relações Exteriores	8	255.255.240.0	8	172.16.1.134	172.16.1.150
Recursos humanos	7	255.255.224.0	7	172.16.1.101	172.16.1.133
Impressoras	7	255.255.224.0	6	172.16.1.68	172.16.1.100
Financeiro	7	255.255.224.0	5	172.16.1.35	172.16.1.67
Marketing	7	255.255.224.0	4	172.16.1.2	172.16.1.34
Vendas	6	255.255.192.0	3	172.16.0.193	172.16.1.1
Escritorio/ Rececao	6	255.255.192.0	2	172.16.0.128	172.16.0.192
Projetos	5	255.255.128.0	1	172.16.0.0	172.16.0.127



Já em relação ao material de rede e servidores temos a rede que começa em 172.16.2.0/12 que irá ser dividida conforme abaixo descrito

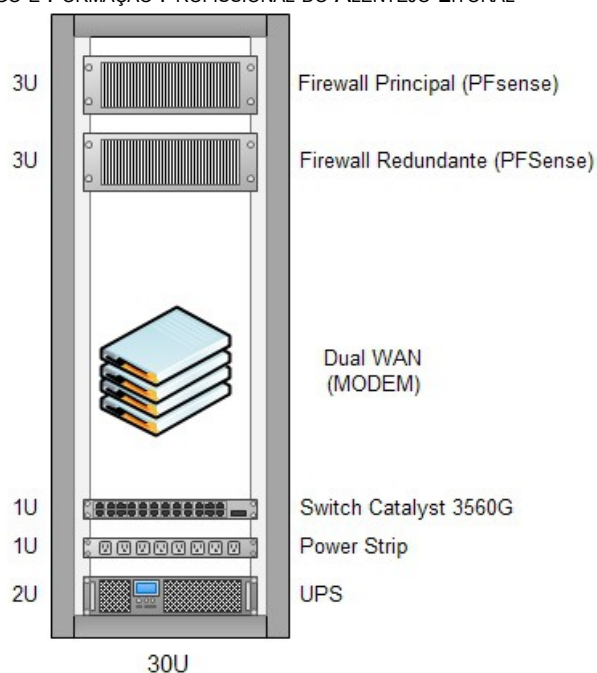
172.16.2.0/12	Classe B	Pontos de rede			
Identificação da rede	Bits/Subnet	Mascara (256 - Blocos)	Ordem	Gama	
Servidores	8	255.255.240.0	3	172.16.2.64	172.16.2.79
Switches/Routers/Firewalls	7	255.255.224.0	2	172.16.2.32	172.16.2.63
Acess Points	7	255.255.224.0	1	172.16.2.0	172.16.2.255

Para a DMZ, que terá acesso ao publico WEB e FTP, o servidor estará nesta zona com a seguinte configuração

DMZ - WEB, FTP	2	255.255.252.0	4	172.16.3.0	172.16.3.4
----------------	---	---------------	---	------------	------------

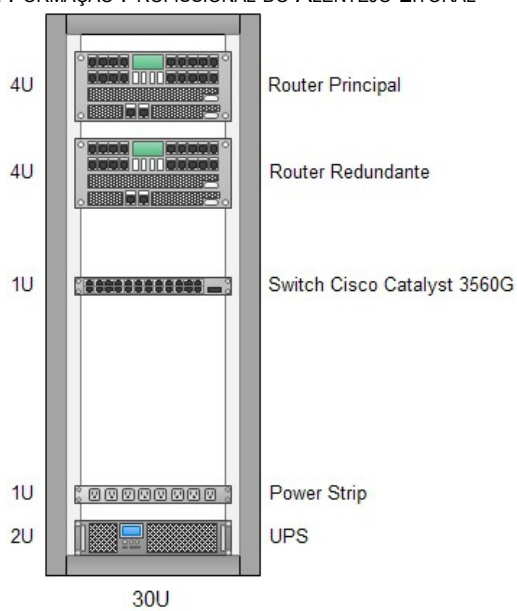
• Localização de servidores, bastidores e material activo de rede

Na sede estará no departamento de informática uma sala construída para o efeito, onde estarão localizados os bastidores principais. Primeiro temos o bastidor Firewall / WAN, que tem suporte a DUAL WAN para failover/balanceamento de carga. Daqui vem a comunicação com o exterior, que tem antes da firewall redundante da cisco, a DMZ onde está o Servidor WEB/FTP. Na firewall é onde vai filtrar os dados de forma a proteger de possíveis ataques, e prevenir a entrada de vírus na rede.



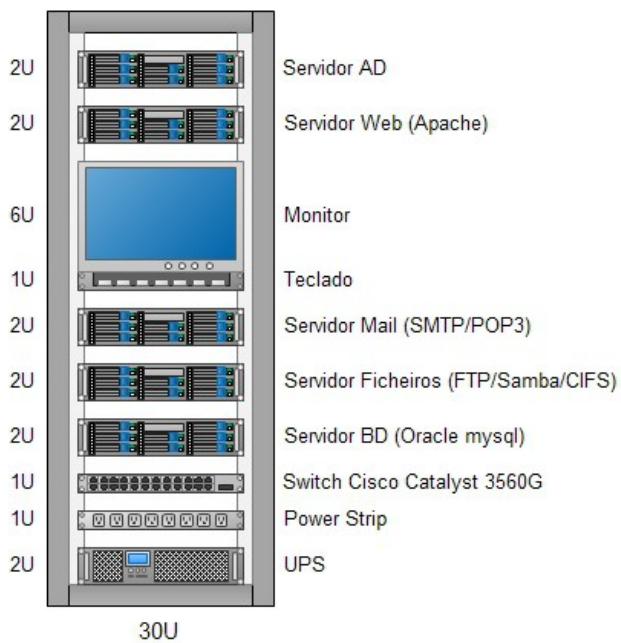
Bastidor Firewall / Wan

Depois temos o bastidor principal, que vai distribuir a rede, ou seja as ligações de internet/intranet. Este bastidor tem dois MX 400 meraki para redundância, e um Cisco Catalyst 3560G para comunicar com a rede interior.



Bastidor Principal

Depois temos o bastidor de servidores, onde estão ligados os servidores que irão providenciar os serviços necessários à rede.



Bastidor Servidores

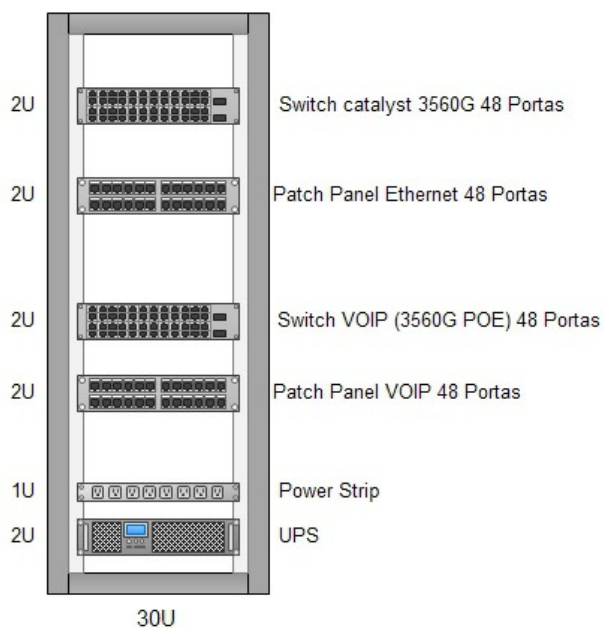


INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP

DELEGAÇÃO REGIONAL DO ALENTEJO

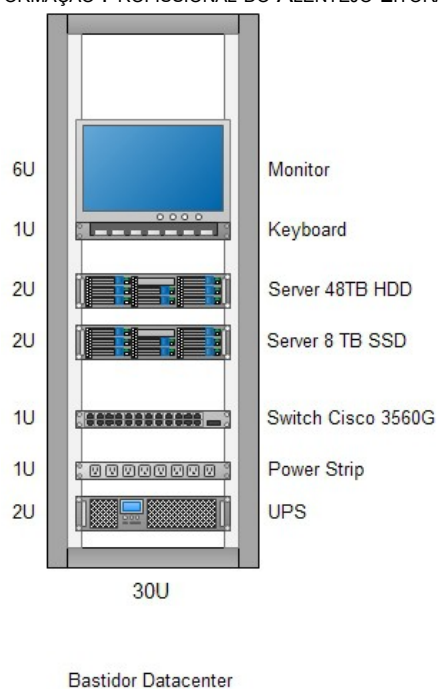
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL

Depois temos o bastidor de piso da sede r/c, que irá distribuir a rede pelo piso

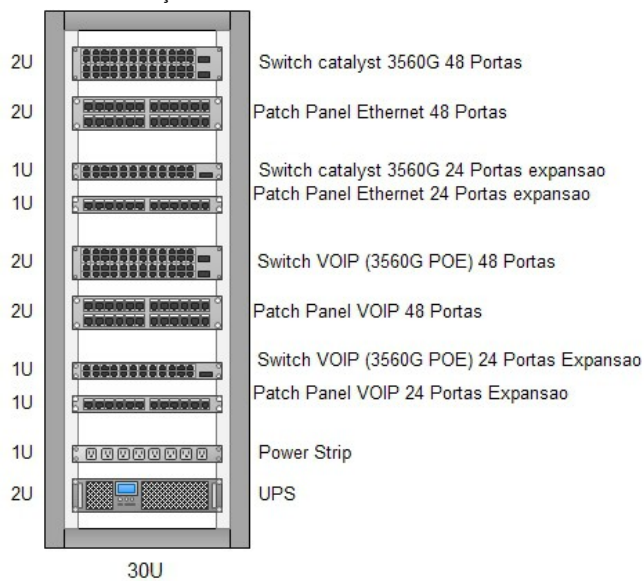


Bastidor Rede SEDE R/C

Ainda no R/C temos o pequeno DataCenter da empresa com 56 TB de capacidade assente em Hadoop.

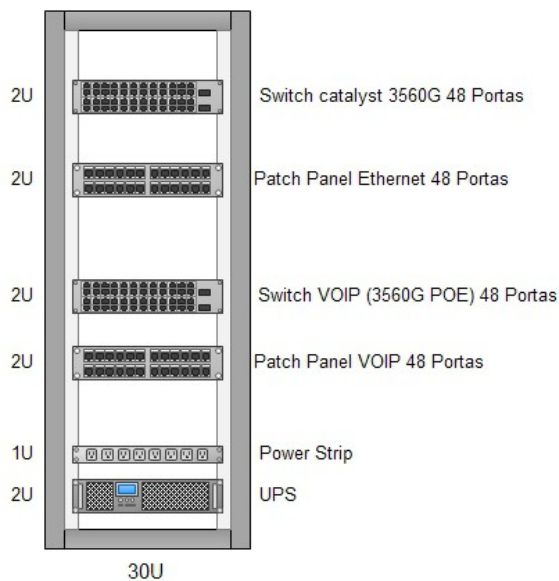


Depois temos no primeiro piso da sede o bastidor de piso, que irá ligar ao bastidor do R/C



Bastidor Rede SEDE 1º

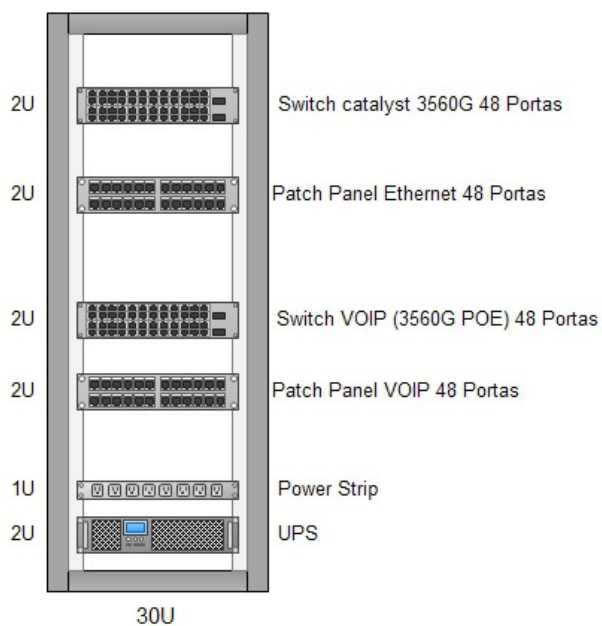
No 2º andar temos o bastidor de piso conforme a figura



Bastidor Rede SEDE 2º

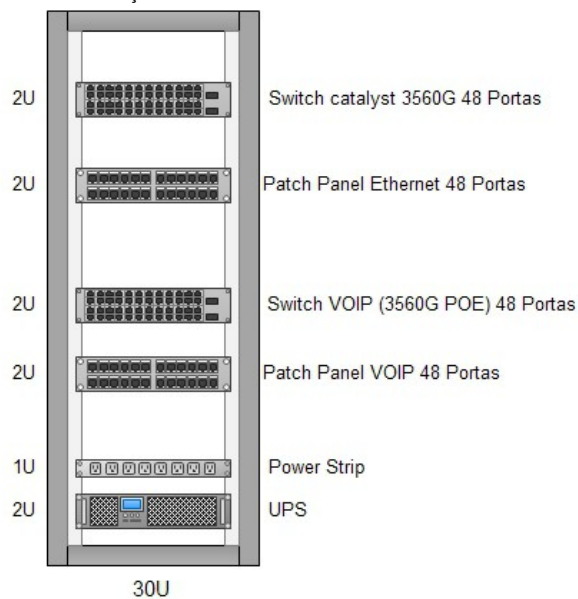


Finalmente temos no 3 andar o bastidor de piso conforme a figura



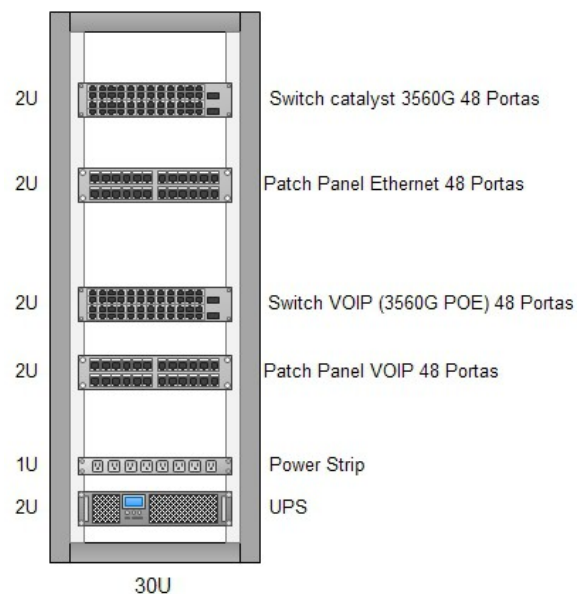
Bastidor Rede SEDE 3º

No edifício 1 temos o bastidor de piso/edifício que vai distribuir a rede pelo edifício e ligar aos outros edifícios



Bastidor Rede ED1 R/C

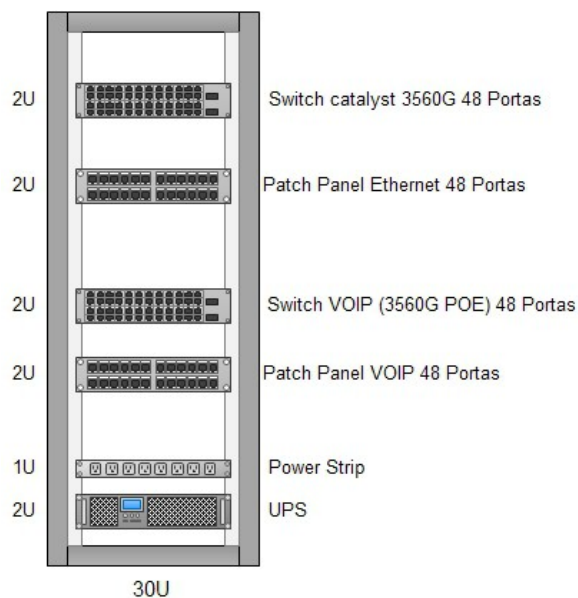
Seguindo para o edifício 1, 1º andar



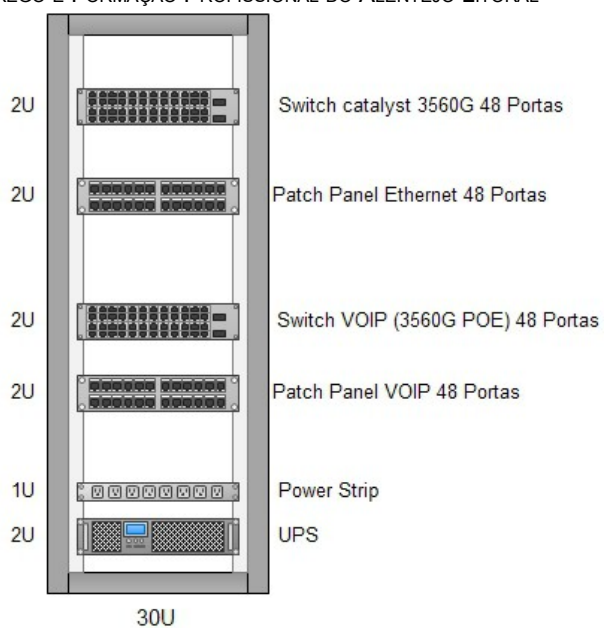
Bastidor Rede ED1 1º



Finalmente temos o edifício 2 com 1 bastidor por cada piso, sendo que no RC vai interligar com os outros edifícios



Bastidor Rede ED2 R/C



Bastidor Rede ED2 1º

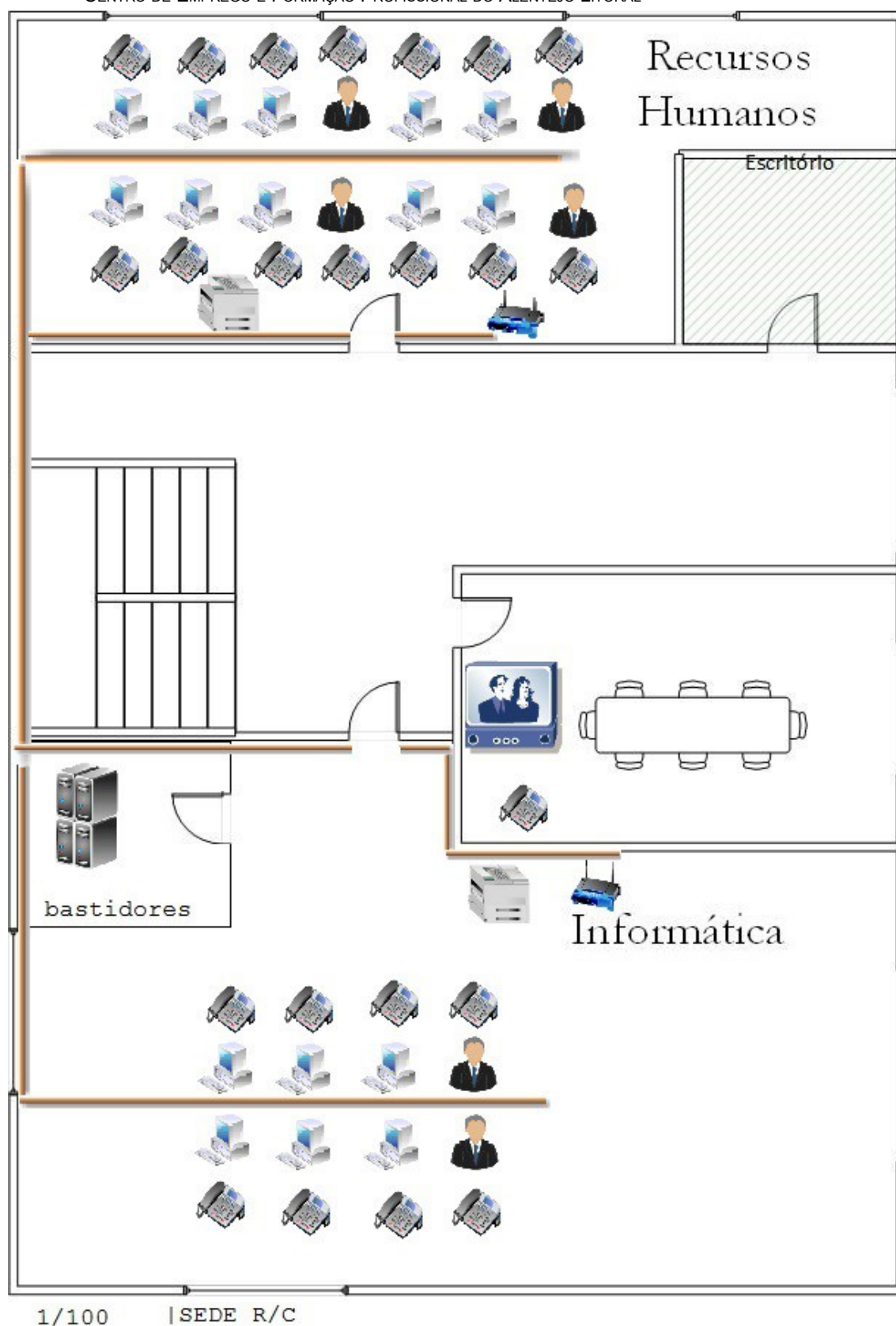


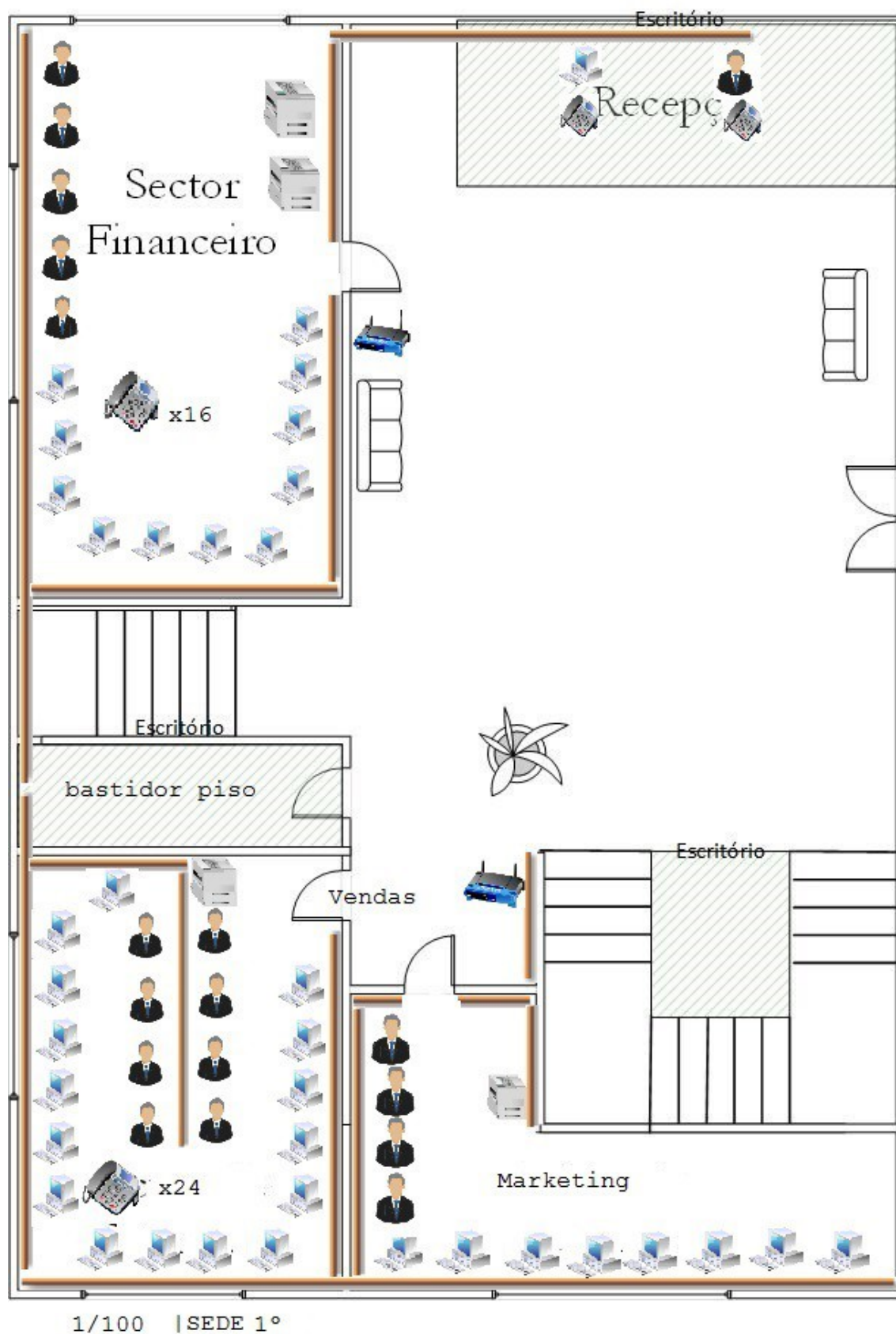
- **Estratégia de gestão da rede**

Quanto à estratégia de gestão de rede, deve estar um funcionário especializado a administrar e controlar a rede permanentemente. Isto vai fazer com que a rede esteja sempre sobre “vigilância”, e prevenir que apareçam problemas na rede, e se ele aparecerem, sejam logo solucionados.



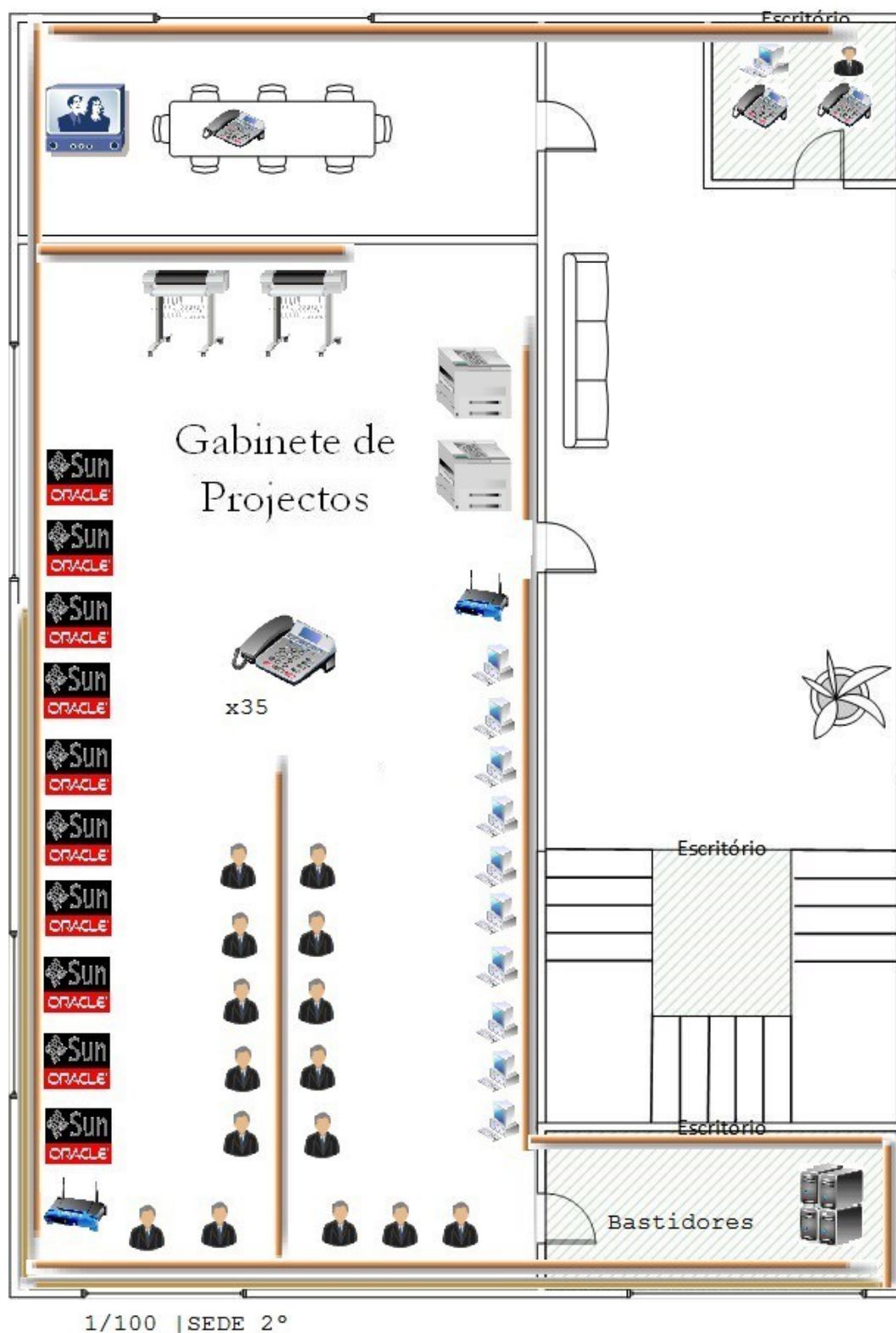
- Desenho Físico da rede

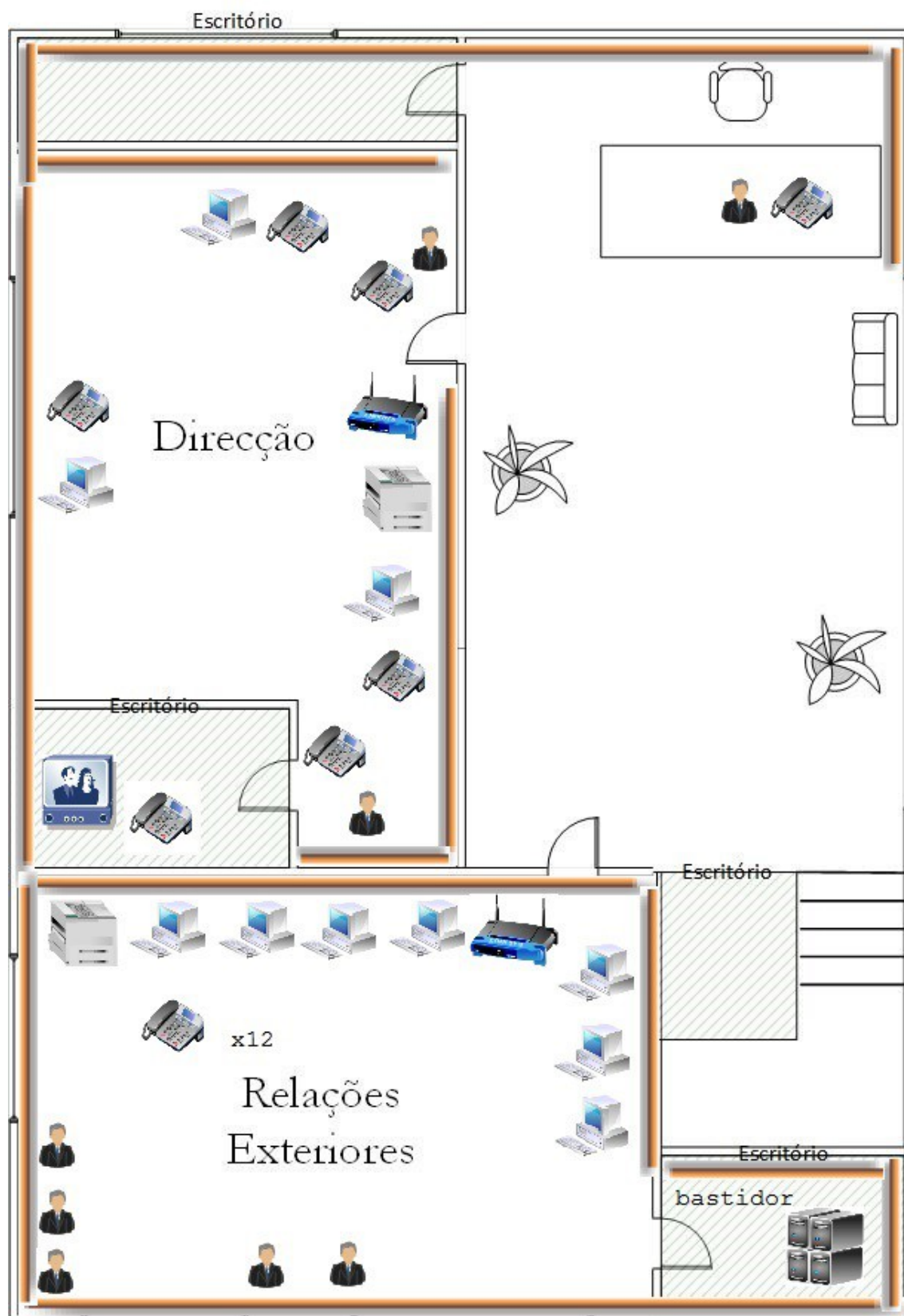






INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP
DELEGAÇÃO REGIONAL DO ALENTEJO
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL

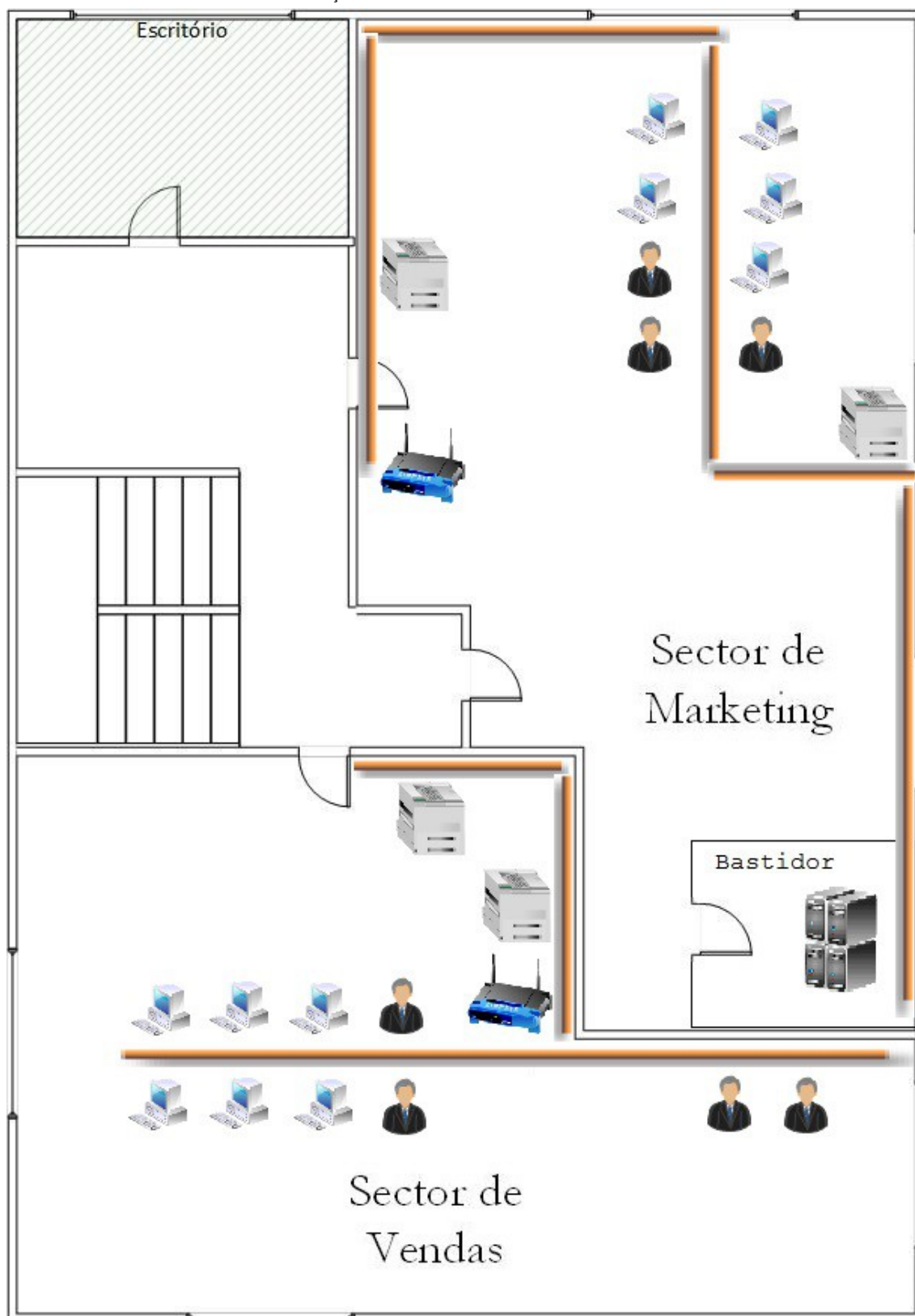




1/100 - LPPB 2



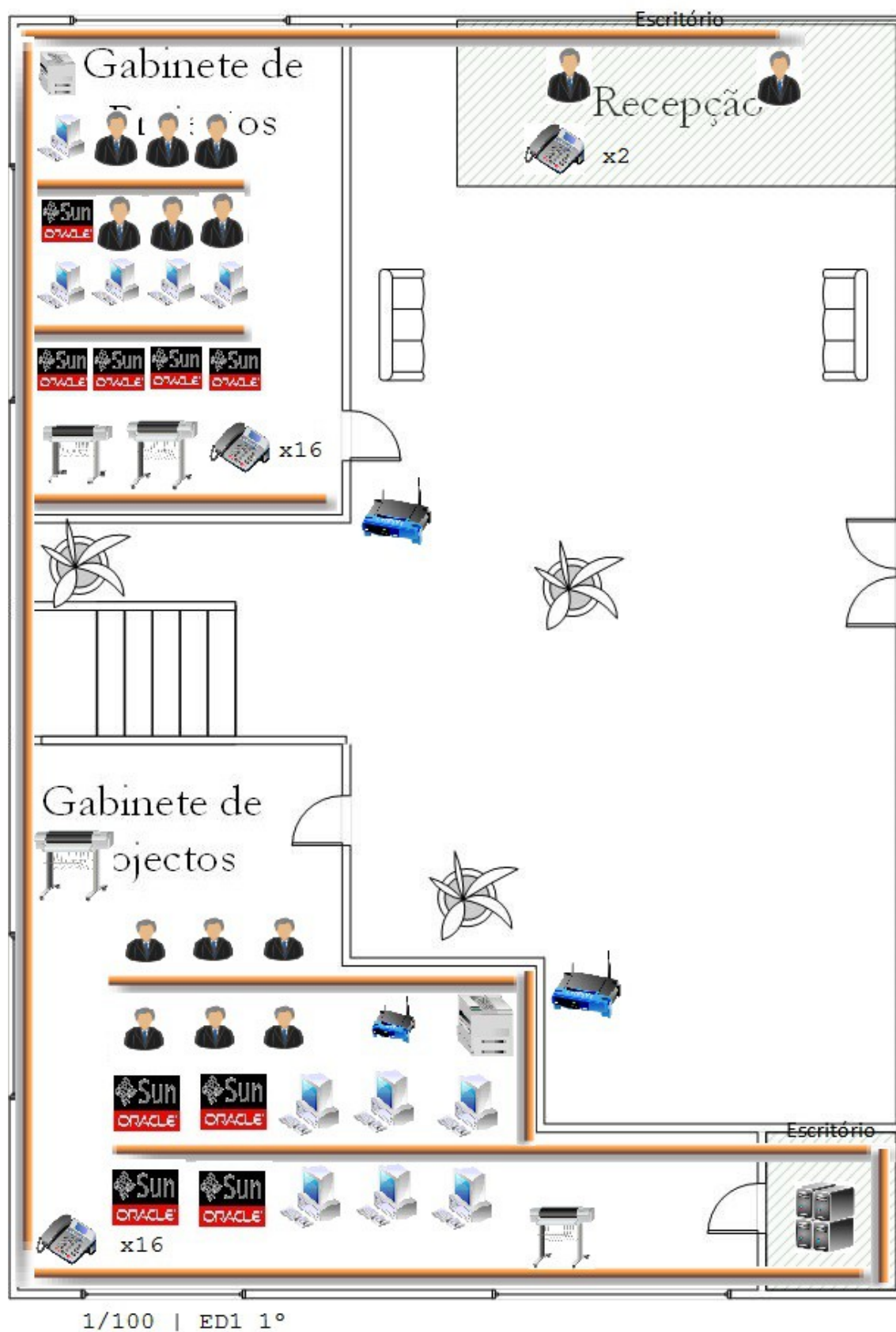
INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP
DELEGAÇÃO REGIONAL DO ALENTEJO
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL



1/100 | ED1 R/C

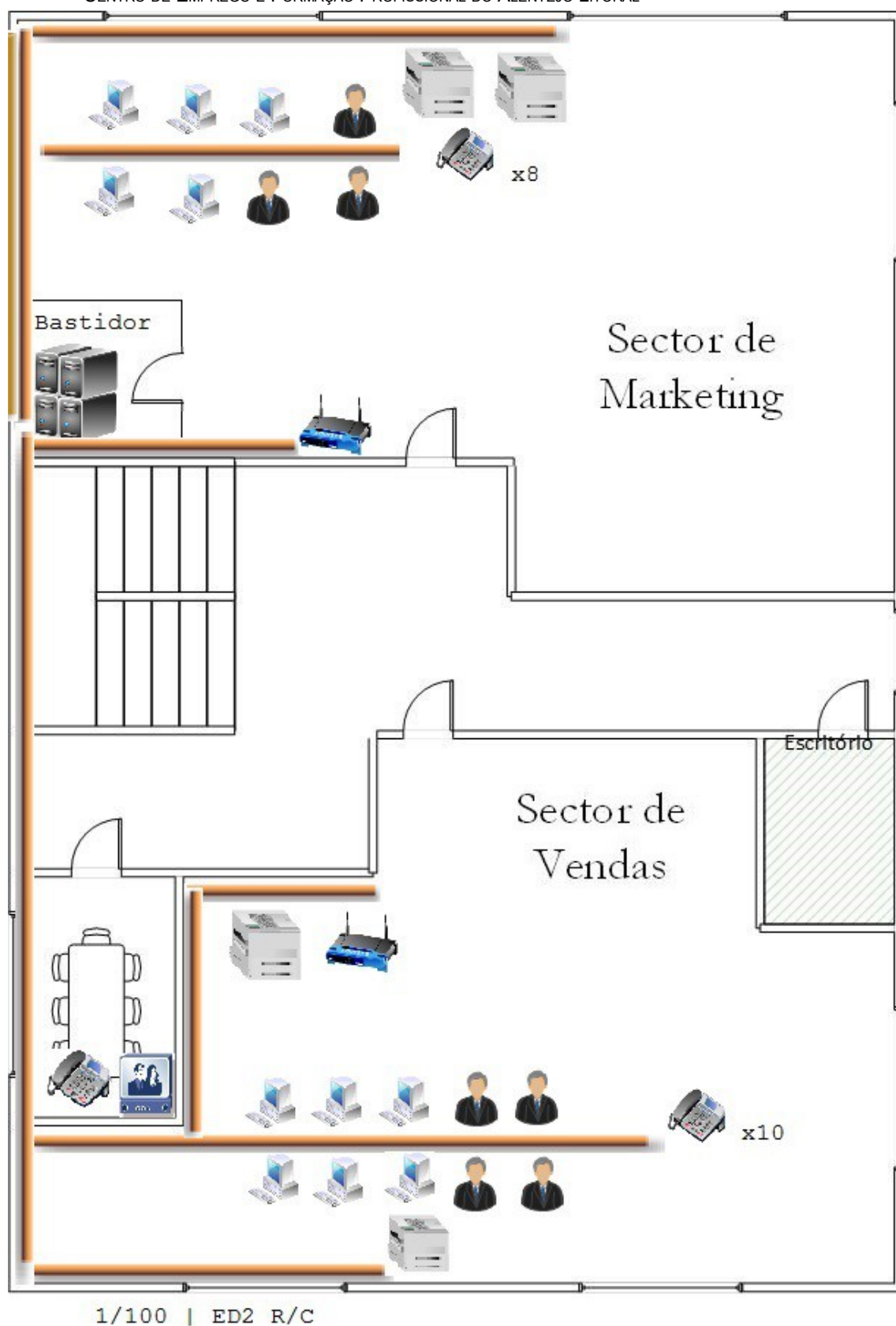


INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP
DELEGAÇÃO REGIONAL DO ALENTEJO
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL



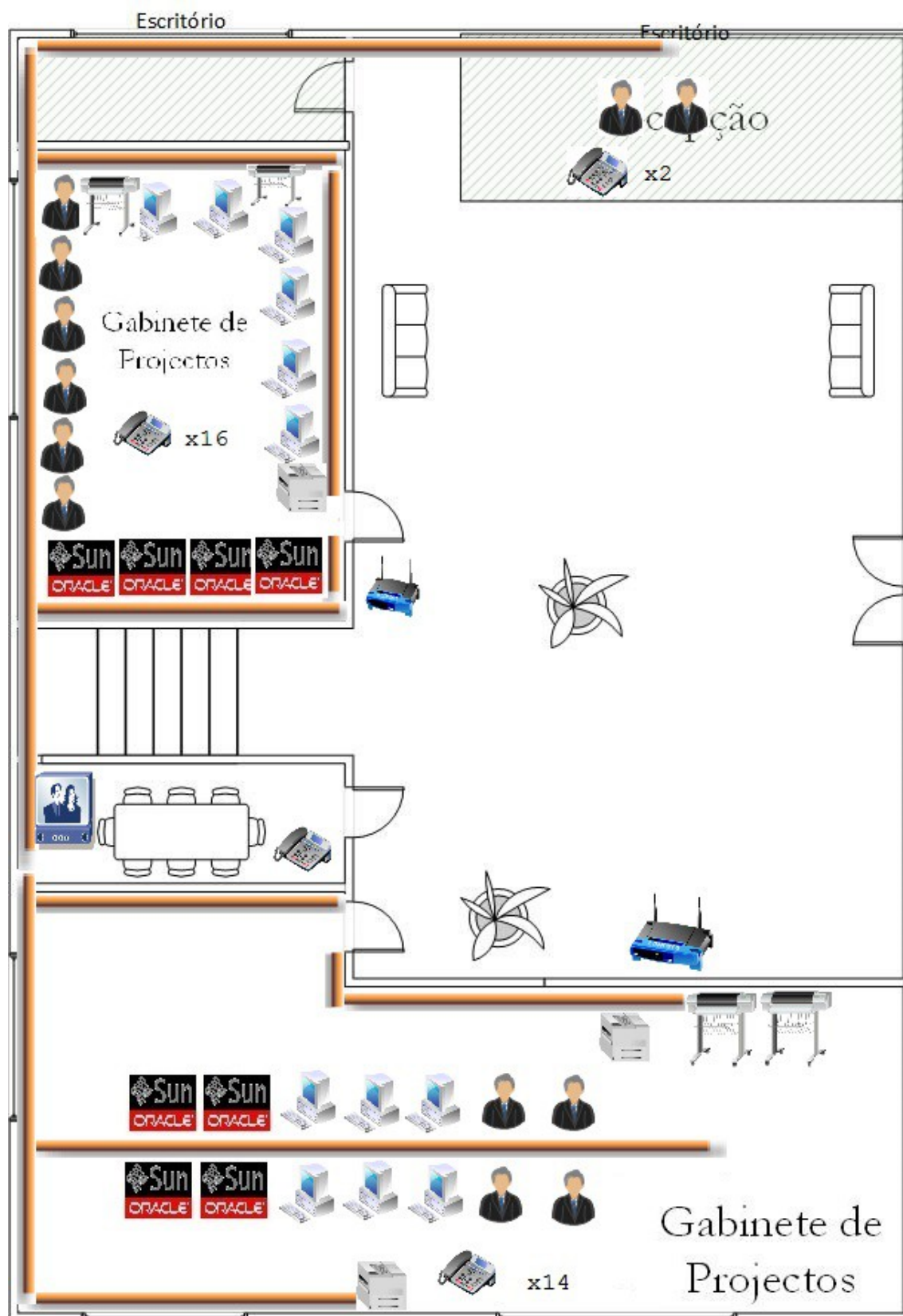


INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP
DELEGAÇÃO REGIONAL DO ALENTEJO
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL





INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP
DELEGAÇÃO REGIONAL DO ALENTEJO
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL





• Servidores

Descrição de todos os servidores de rede, as suas características e serviços prestados

Temos então nos servidores de rede o DELL POWER EDGE R530 como servidor de cada um dos serviços. O DELL, montado em rack 2U, tem como principais características:

- CPU INTEL XEON E5-2600
- CHIPSET INTEL C610
- 32GB DDR4 (comprado separadamente)
- SUPORTE A HYPERVISOR (VIRTUALIZAÇÃO)
- SUPORTE A DISCOS SSD E SAS com controlador RAID (comprado separadamente)
- PSU 750W
- VGA MATROX g200 Integrada
- 4 x 1 GB ETHERNET
- SUPORTE até 5 PCIe SLOTS

Visto então as características principais do servidor, vamos aos serviços de cada um

SERVIDOR AD (Active Directory)

- SOFTWARE WINDOWS SERVER 2012
 - Configuração de domínio Cefpal.pt
 - Configuração de postos de trabalho
 - Administração da rede
 - Análise de logs e registos de rede

SERVIDOR WEB (DMZ)

- SOFTWARE LINUX RED HAT ENTERPRISE
- SOFTWARE APACHE WEB SERVER
 - Alojamento de páginas com suporte a php e ligação a mysql
- SOFTWARE vsftpd (Embutido no RED HAT) FTP
 - Alojamento de ficheiros disponíveis ao público e internamente

SERVIDOR MAIL (DMZ)

- SOFTWARE LINUX RED HAT ENTERPRISE



INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP
DELEGAÇÃO REGIONAL DO ALENTEJO
CENTRO DE EMPREGO E FORMAÇÃO PROFISSIONAL DO ALENTEJO LITORAL

- POSTFIX (SMTP) Embutido
- DOVECOT (POP3) Instalado posteriormente

SERVIDOR DE FICHEIROS (LIGADO AO DATACENTER)

- SOFTWARE LINUX RED HAT ENTERPRISE
- VAFTPD (FTP)
- SAMBA (PARTILHA FICHEIROS)
- CIFS (PARTILHA FICHEIROS)

SERVIDOR BD (BASE DADOS)

- SOFTWARE ORACLE ENTERPRISE LINUX
- MYSQL (Instalado posteriormente)

DATACENTER

- SOFTWARE APACHE HADOOP
- 2 SERVIDORES
 - 1*8 TB SSD – Para data mais acedida
 - 1*48 TB HDD – Para data armazenada



• Descrição das políticas de segurança e salvaguarda da informação a adotar

Em relação à políticas de segurança e backup a adotar temos que rever certos pontos. São Eles:

- Confidencialidade: limitar o acesso à informação às entidades legítimas, quer isto dizer, a quem é autorizado pelo proprietário
- Integridade: garantir que toda a informação mantenha as características definidas pelo proprietário durante o seu ciclo de vida (criação, manutenção, destruição)
- Disponibilidade: garantir que a informação esteja sempre disponível para uso legítimo
- Autenticidade: garantir que a informação não foi alterada por outros

Para o uso destas políticas deve-se ter em conta

- Riscos associados à falta de segurança
- Benefícios
- Custos de implementação dos mecanismos

Níveis de segurança

Temos os níveis de segurança de acesso físico e lógico.

Controlo de acesso físico



- Portas / Trancas / Leitores de Cartões / Biometria / Paredes / Blindagem / Seguranças

Controlo de acesso logico

Temos neste campo a acesso lógico, à informação, ou seja através de software. Como mecanismos de segurança temos:

- Mecanismos de cifração ou encriptação – Permite a transformação da informação de certo modo a que não seja “visível” com encriptação na origem e desencriptação no destino através de tecnologia de encriptação com chave secreta. Por exemplo RSA e Kerberos
- Assinatura Digital – Dados criptografados que necessitam de certificado associado (SSL)
- Garantia da integridade da informação – Verificação do HASH para confirmar se os dados não estão corromptos (Temos o exemplo do MD5)
- Controlo de acesso – Passwords, biometria, firewalls, cartões inteligentes, dispositivos de acesso como pen que bloqueia e desbloqueia o software
- Certificação – Verificar a validade de um documento
- Integridade – Verificar se um serviço/informação está protegido contra acesso indesejado
- Protocolos seguros – Uso das medidas de segurança acima mencionadas

Ameaças à segurança

- Perda de confidencialidade – Quando há uma perda de sigilo de certa informação (password de utilizador ou adm por exemplo), permitindo o acesso desta a terceiros
- Perda de integridade – Quando a informação é alterada por terceiros sem aprovação
- Perda de disponibilidade – Quando a informação deixa de estar acessível a quem necessita

As ameaças à rede podem vir de um agente malicioso, tal como um cracker. A informação exposta pode ser usada para diversos fins, assim como a notoriedade, auto-estima, espionagem industrial, vingança e dinheiro. Temos o famoso caso que estourou recentemente devido às revelações de um antigo analista de segurança da NSA, do programa PRISM, que espionava governos, instituições e pessoas de outros países. Estalou a nova guerra fria.

Para prevenir o acima descrito devemos implementar as seguintes políticas de segurança:

- Os utilizadores devem memorizar passwords, não fornecer passwords, alterar password com frequência, terminar sessão quando não estão perto do computador, não permitir que terceiros tenham acesso aos postos de trabalho, terem formação para casos de engenharia social, não aceder a ficheiros ou paginas de fontes desconhecidas, encriptação de dados trocados



- Os administradores devem proceder à encriptação de informação (Discos neste caso), dar formação e informação constante aos utilizadores sobre medidas de segurança, manter os sistemas actualizados, implementar políticas de passwords, fazer o controlo de activos, impor restrições de acesso, implementar acessos (se possível) através da biometria / cartões de acesso, verificar logs e manter as firewall atualizadas e com o mínimo de excepções, implementar políticas de backup constante, para além de administrar a rede e servidores

Pontos de controlo de segurança a ter em conta (Segundo Bluephoenix (2008))

- Políticas de segurança da informação
- Organização de segurança da informação
- Gestão e controlo de activos
- Segurança recursos humanos
- Segurança física e do ambiente
- Gestão das operações e comunicações
- Controlo de acessos
- Aquisição. Desenvolvimento e Manutenção de Sistemas de Informação
- Gestão da continuidade do negócio
- Conformidade Legal

Quanto a políticas de backup devemos ter em atenção:

- Dados a serem salvaguardados
- Ciclo temporal de backups
- Tamanho dos dados a serem salvaguardados

Em termos de estratégias de backup temos o backup parcial, completo, ou diferencial. Temos que ter em atenção os suportes de armazenamento, nos quais deveremos usar sistemas redundantes (RAID e MIRRORING), e também para backups de longa data usar sistemas de armazenamento como TAPE.

Os backups serão feitos de forma regular (diário para ficheiros alterados e mensal para o sistema completo) ou antes de ser feita alguma atualização aos sistemas como já foi descrito acima.



- **Funcionamento do helpdesk e comunicação de avarias pelos clientes**

Cada funcionário terá um número mecanográfico, que será o seu número de identificação na comunicação de erros ao helpdesk. Será pedido o nome completo e o número mecanográfica, que estará depois na base de dados a sua conta no AD. Após a identificação será resolvido o problema remotamente, através de serviços remotos do AD ou a deslocação ao local de um funcionário do departamento da informática caso o problema não seja possível de resolver remotamente.

- **Forma de implementação de sistemas de comunicação por voz e vídeo**

A implementação de comunicação por voz será feita através de VOIP, com um servidor PBX. Os telefones terão uma extensão interna para comunicação dentro da empresa, e o PBX permitirá também a ligação ao exterior através de conversão IP ISDN. O vídeo funcionará também com ligação ao PBX.



- **Análise de custos de toda a solução apresentada**

EQUIPAMENTO ACTIVO REDE			
Designação	Unidades	Preço Unitário	Preço Total
1U Rack PDU Protector 8 Power Strip HAMSWAN	12	3 7,30 €	4 47,6 €
APC Smart-UPS SUA2200RM2U 2200VA USB and Serial 2U Rackmount UPS	4	72 7,93 €	2.9 11,7 €
APC Smart-UPS 1500VA USB and Serial 2U Rackmount UPS	8	59 4,24 €	4.7 53,9 €
Switch CISCO Catalyst 3560G-48PS (PoE) 48 Ports	16	3.55 7,78 €	56.9 24,5 €
Switch CISCO Catalyst 3560G-24TS (PoE) 24 Ports	6	2.65 2,41 €	15.9 14,5 €
ASA 5545-X IPS Edition - 3DES/AES Encryption	2	20.59 8,70 €	41.1 97,4 €
Cisco Meraki MX400	2	21.83 3,50 €	43.6 67,0 €
DELL PowerEdge R530 Rack Server	7	2.45 5,87 €	17.1 91,1 €
Samsung 1TB EVO 850 Series 2.5 SATA III SSD - MZ-75E1T0B	10	38 3,00 €	3.8 30,0 €
Western Digital Red 6TB SATA III 64MB (WD60EFRX)	12	29 3,90 €	3.5 26,8 €
Monitor Rack 15inch LCDR6U15-01-DVI	2	593,267	1.1 86,5 €
SFP Tranceiver Module 1000BASE-ZX Fiber	24	13 5,58 €	3.2 53,9 €
EQUIPAMENTO PASSIVO			
Designação	Unidades	Preço Unitário	Preço Total
Cabo CAT6 UTP multifilar CCA - condutor 100% cobre	9357	0,31 €	2.8 67,9 €
FICHAS RJ45 CAT6	504	0,28 €	1 43,3 €
Cablexpert Cabo de Rede cat6 c/ Fichas RJ45 - 1.5m	504	2,50 €	1.2 60,0 €
Adaptador Q45 para calhas tampa L60/L75 - Efapel	20		



10986ABR		1,50 €	30,0 €
Calha Parede 90x50mm L75 branca - Efapel 10180RBR	570	4,91 €	2.7 98,7 €
Adaptador duplo Q45 para calhas tampa L75 - Efapel 10952ABR	184	2,30 €	4 23,2 €
Ângulo interior variável para calha 90x50mm branco - Efapel 10182RBR	40	2,65 €	1 06,0 €
Ângulo exterior variável para calha 90x50mm branco - Efapel 10186RBR	20	3,65 €	73,0 €
Topo para calha 90x50mm branco - Efapel 10185RBR	10	1,36 €	13,6 €
Junta para calha 90x50mm branca - Efapel 10184RBR	20	1,23 €	24,6 €
Tomada RJ45 Cat.6 dupla de parede	233	6,58 €	1.5 33,1 €
TOMADA RJ45 CAT6 UTP SÉRIE MEC21 - EFAPEL	38	4,50 €	1 71,0 €
Calha de chão 75x17mm cinzenta - Efapel 10120CCZ	114	3,48 €	3 96,7 €
Caixa saliente serie APOLO 5000 para calhas de chão - Efapel 10997ACZ	60	1,25 €	75,0 €
Patch Panel 24P	2	2,48 €	3 65,0 €
Patch Panel 48P 2U	16	3,04 €	5 8 48,6 €
Armário de Chão 30 Unidades Fonestar FRA-30U	11	9,90 €	51 5.7 18,9 €
Linux REDHAT ENTERPRISE SERVER	3	7,03 €	72 2.1 81,1 €
Windows SERVER 2012 Standard	1	802,548	8 02,5 €
Windows Server 2012 5-Device Client Access License	30	1,98 €	17 5.1 59,3 €
CABLEMATIC Fibra óptica multimodo 62.5/125 4 fibras exteriores	2500	2,06 €	5.1 50,0 €
ST Stainless alloy ferrule 3mm boot MM	24	2,57 €	61,6 €
Registo DOMINIO CEFPAL.PT - 5 Anos	1	65,00 €	65,0 €
INSTALAÇÃO			
Colocação calha, cablagem e obras de construção civil - 15 dias			
1 Meste Obra	15	5,00 €	7 1.12 5,00 €
3 Serventes	15	5,00 €	3 52 5,00 €
3 Técnicos Especialistas	15	10	1.57



		5,00 €	5,00 €
Certificação e testes dos pontos de red cat6 e fibra optica	1	20.00 0,00 €	20.00 0,00 €
Obras - Montagem compartimentos bastidores	1	3.00 0,00 €	3.00 0,00 €
TOTAL			250.99 7,98 €