

Modernização da infraestrutura de rede Switching e WiFi DPCP2025CP32

Anexo I ao Caderno de Encargos Especificações Técnicas

Conteúdo

Introdução	4
Objeto.....	4
Enquadramento.....	4
Âmbito do procedimento	5
Diagrama da rede pretendida	6
1 - Características técnicas - Switchs	7
Tipo 1 – Switch Core + Agregação	7
Tipo 2 – Switch de 48 portas RJ45 MultiGigabit (Firewall)	9
Tipo 3 – Switch de 48 portas RJ45 Gigabit (Servidores, Desenvolvimento e WAN)	11
Tipo 4 – Switch Multigigabit 48 portas RJ45 PoE (Edifício A e L - 1)	14
Tipo 5– Switch Multigigabit de 24 portas RJ45 POE (Lisboa (Edifício D, Edifício L-2, Portaria e Palacete) e restantes 12 Localizações Remotas)	16
2 - Características técnicas – Access Points (APs).....	18
3 - Características técnicas “Controladoras” e Plataforma de Gestão.....	20
Controladora de rede sem fios (WLC)	20
Network Access Control (NAC)	24
Plataforma Gestão (Switchs/APs)	28
Tipo de implementação das controladoras.....	30
4 - Características técnicas – Cablagem e bastidores	32
Quadro de característica base para cablagem e bastidores.....	33
5 - Mapas de quantidades	34
Mapa de quantidades de equipamentos ativos a fornecer	34
Mapa de mínimas quantidades de controladoras/plataformas a fornecer	34

Mapa de quantidades e distribuição de Switchs por bastidor	35
Mapa de quantidades de stack a implementar por bastidor	36
Mapa de previsão de quantidades de Access Points por local de instalação e piso.	37
Mapa de previsão de quantidades de Access Points por bastidor	38
Mapa de previsão de quantidades de cablagem.....	38
Mapa de quantidades de Patch cords e transceivers/SFPs	39
Bastidores e acessórios	39
6 – Prazos, locais de entrega, serviços e garantia	40
Prazos	40
Serviços de instalação	40
Garantia.....	41
Serviços de suporte	41
Serviços de apoio à exploração	41
7 – Plantas dos locais.....	42
Lisboa – Edifício A - Piso -1	42
Lisboa – Edifício A - Piso 0	43
Lisboa – Edifício A - Piso 1	44
Lisboa – Edifício A - Piso 2	45
Lisboa – Edifício A - Piso 3	46
Lisboa – Edifício D.....	47
Lisboa – Edifício L – Piso 0	48
Lisboa – Edifício L – Piso 1	49
Lisboa – Palacete – Piso 0.....	50
Lisboa – Palacete – Piso 1.....	51
Lisboa – Palacete – Sotão	52
Lisboa – Campus.....	53
Porto – Piso 0	54
Porto – Piso 1	55
Coimbra – Piso 1.....	56
Coimbra – Piso 4.....	57
Viana do Castelo.....	58
Braga.....	59
Bragança	60
Viseu	61
Aveiro	62



Guarda.....	63
Covilhã.....	64
Leiria.....	65
Évora.....	66
Faro.....	67

Introdução

Objeto

Modernização da infraestrutura de rede (Switches de core, switches de acesso, Access Points, Plataformas de gestão...) do IAPMEI, I.P. - Agência para a Competitividade e Inovação (IAPMEI), de acordo com as especificações e características mínimas que constam neste documento.

Com este procedimento pretende-se a aquisição de todos os equipamentos, acessórios, licenciamentos e serviços para a implementação do projeto.

Enquadramento

O IAPMEI, têm presença em vários locais de Portugal continental, localizando-se o seu Data Center em Lisboa. Em Lisboa os serviços encontram-se no mesmo campus, embora distribuídos por vários edifícios. Existem instalações no Porto e Coimbra, com uma dimensão superior às restantes, que se distribuem ainda por Viana do Castelo, Braga, Bragança, Viseu, Guarda, Covilhã, Aveiro, Leiria, Évora e Faro.

No Data Center da arquitetura é:

- Stack Core;
- Stack Firewall;
- Stack Servidores;
- Stack Desenvolvimento;
- Stack Operador

Localização dos bastidores de rede é:

- Lisboa
 - Edifício A (2 Stack)
 - Edifício D
 - Edifício L Bastidor 1 (1 Stack)
 - Edifício L Bastidor 2 (1 Stack)
 - Palacete
 - Portaria
- Porto
 - Bastidor 1 (2 Stack)
 - Bastidor 2
- Todos os outros locais apenas com um bastidor, sem stack.

Em Lisboa, as ligações entre os vários bastidores são asseguradas por fibras óticas. O mesmo acontece na ligação entre os dois bastidores do Porto.

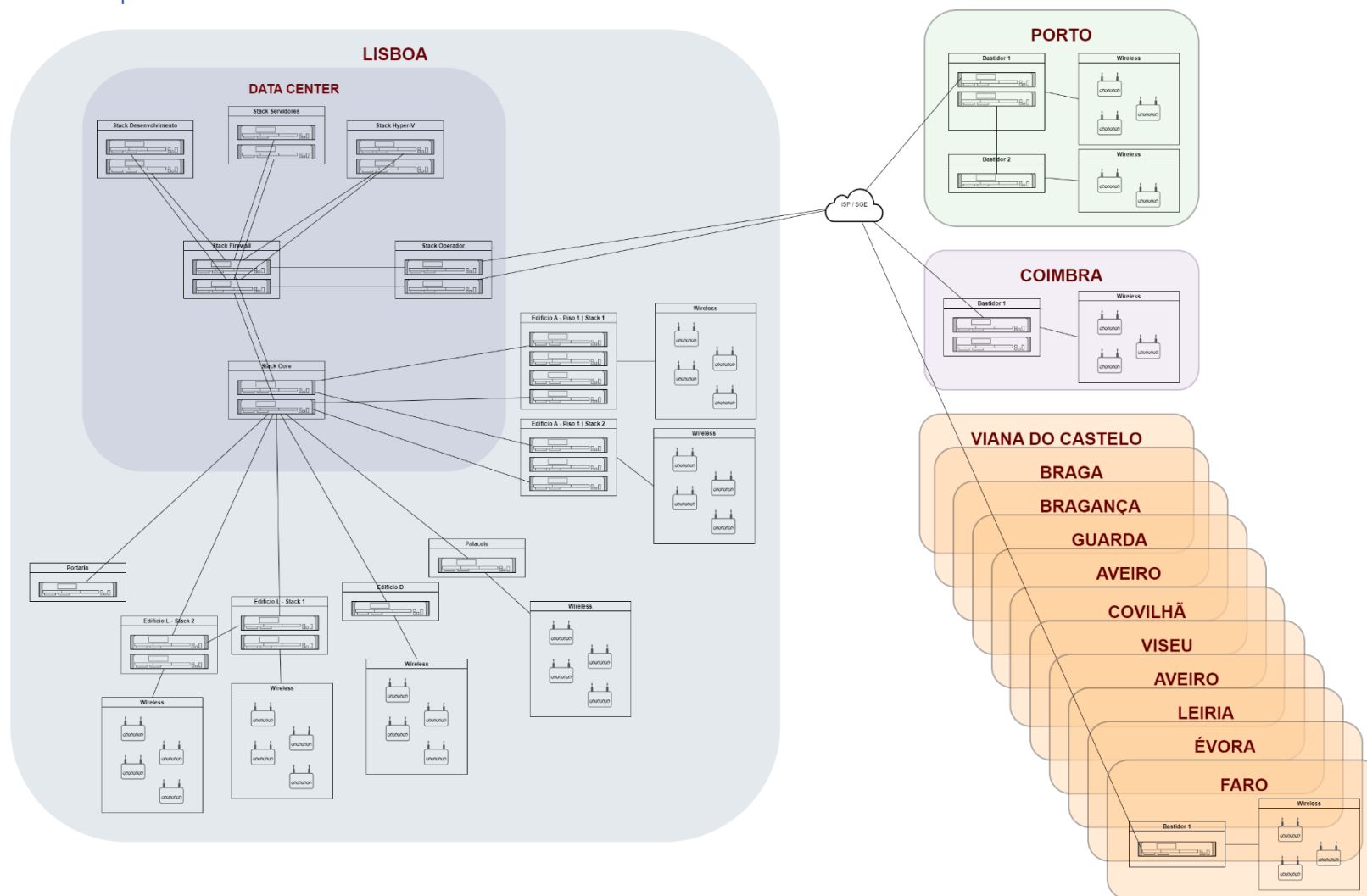
Âmbito do procedimento

É objetivo com este procedimento a substituição dos equipamentos ativos (Switchs e controladoras), e a instalação de uma rede solução wi-fi, com a duas redes (rede corporativa e rede Guest) em todo os locais do IAPMEI. Este projeto incluirá a troca/substituição das fibras óticas existentes em Lisboa e Porto e a passagem de cablagem para ligação dos APs a instalar em cada um dos locais.

Assim, este procedimento, engloba a aquisição de serviços e equipamentos (ativos e passivos) e inclui:

- Aquisição dos equipamentos Switchs, Access Points, solução de gestão dos Acess Points, Solução de Network Access Control (NAC), Solução de Gestão (Switchs/APs) de um único fornecedor, incluindo todos os licenciamentos, conforme o descrito nos pontos 1, 2, 3, 4 e 5 deste documento;
- Aquisição de 2 bastidores, e componentes para bastidores de forma a dar cumprimento ao descrito no ponto 6 deste documento;
- Aquisição de cablagem cabo S/FTP Cat.6A ou superior e cabo de fibra ótica de 8 fibras, conforme o descrito no ponto 7 deste documento;
- Em cada um dos locais, a passagem dos cabos entre os pontos de colocação dos APs e respetivo bastidor, com todos os equipamentos e acessórios necessários (tomada, patch panel, patch coord, ...), garantindo a sua ligação e certificação, conforme o descrito nos pontos 6 e 7 deste documento;
- Em cada um dos locais, a Instalação dos Switchs nos bastidores e a instalação dos APs, conforme o descrito no ponto 8 deste documento;
- Instalação/configuração das plataformas de gestão;
- Serviço de suporte com duração de 36 meses;
- Garantia;
- Deve ser incluído uma bolsa de 75 horas para apoio à exploração da solução com uma validade de 36 meses.

Diagrama da rede pretendida



1- Características técnicas- Switchs

Tipo 1 – Switch Core + Agregação

1.	Características Físicas
1.1	Deve possuir as dimensões 1RU e EIA standard 19 in.
1.2	Deve possuir fontes de alimentação redundantes incluídas;
1.3	Deve possuir fontes de alimentação amovíveis;
1.4	Deve permitir que as fontes de alimentação sejam substituídas no local sem interromper o funcionamento do equipamento;
1.5	Deve possuir pelo menos 24 portas 1GE/10GE (SFP/SFP+) e 2 portas 40GE/100GE (QSFP+/QSFP28) line rate de uplink, seja através de módulo ou diretamente no equipamento;
1.6	Caso seja necessário um modulo de portas 10GE/25GE (SFP+/SFP28), o mesmo deve vir de base com o equipamento;
1.7	Deve suportar auto negociação da velocidade das portas e duplex;
2.	Escalabilidade e Performance
2.1	Deve ter a capacidade de switching de pelo menos 850 Gbps;
2.2	Deve ter a capacidade de forwarding de pelo menos 700 Mpps;
2.3	Deve suportar pelo menos 4000 VLAN IDs;
2.4	Deve suportar pelo menos 32000 endereços MAC;
2.5	Deve suportar pelo menos 24000 rotas IPv4;
2.6	Deve suportar pelo menos 12000 rotas IPv6;
2.7	Deve suportar pelo menos 3500 entradas ACL;
3.	Características de Stack / Grupo de Equipamentos
3.1	O equipamento deve ter a capacidade de suporte de stacking ou tecnologia que garanta a redundância entre vários equipamentos de um grupo;
3.2	O stack/grupo de equipamentos deverá ter a capacidade de crescer até aos 8 elementos;
3.3	Todos os elementos do stack/grupo de equipamentos devem ser geridos como se se tratasse de um único elemento;
3.4	O stack/grupo de equipamentos deve ser gerido através de um endereço único de gestão;
3.5	A ligação do stack/grupo de equipamentos deve ser estabelecido por meio das interfaces Ethernet regulares ou de interfaces dedicadas;
3.6	A ligação entre os vários equipamentos de stack / grupo de equipamentos deve suportar 200 Gbps de largura de banda;
3.7	Todos os elementos do stack / grupo de equipamentos tem de ser do mesmo modelo.
3.8	Os stacks de switchs devem ser implementados com ligações físicas entre os vários equipamentos do grupo, não sendo necessário nenhum outro equipamento para o seu funcionamento.
3.9	Um dos Switchs deve assumir o papel de master e em caso de avaria, um outro switch do stack assuma esse papel, garantindo assim a operacionalidade do stack
4.	Acesso ao equipamento
4.1	Deve permitir o acesso via CLI (Telnet/SSH);
4.2	Deve permitir o acesso Web GUI (HTTP/HTTPS);
4.3	Deve permitir desabilitar o acesso por Telnet;
4.4	Deve permitir desabilitar o acesso por HTTP e HTTPS;

5. Características gerais

5.1	Deve suportar Layer 2 e Layer 3;
5.2	Deve suportar IPv4, IPv6 e Dual Stack;
5.3	Deve suportar ACL (IPv4 e IPv6);
5.4	Deve suportar QoS (IPv4 e IPv6);
5.5	Deve suportar a definição de interfaces de Loopback;
5.6	Deve suportar Inter-VLAN Routing;
5.7	Deve suportar routing estático (IPv4 e IPv6);
5.8	Deve suportar o protocolo de routing RIP (IPv4 e IPv6);
5.9	Deve suportar o protocolo de routing OSPF (IPv4 e IPv6);
5.10	Deve suportar VRRP;
5.11	Deve suportar CDP ou LLDP (802.1ab);
5.12	Deve suportar a configuração de VLAN (802.1Q);
5.13	Deve suportar a seleção de VLAN com base em ACL;
5.14	Deve suportar a seleção de VLAN com base em endereço MAC;
5.15	Deve suportar a seleção de VLAN com base em endereço IP;
5.16	Deve suportar a seleção de VLAN com base em 802.1X;
5.17	Deve suportar private VLAN;
5.18	Deve suportar Jumbo Frames;
5.19	Deve suportar LACP (802.3ad);
5.20	Deve suportar STP (802.1D), MSTP (802.1s), RSTP (802.1w), PSVT+ e RPVST+;
5.21	Deve suportar Portfast, BPDU Guard, BPDU Filtering e Root Guard ou equivalente
5.22	Deve suportar BFD;
5.23	Deve suportar UDLD;
5.24	Deve suportar NTP;
5.25	Deve suportar SNMP v2c e v3
5.26	Deve suportar Syslog;
5.27	Deve suportar Port Mirroring;
5.28	Deve suportar SPAN e ERSPAN;
5.29	Deve suportar Netflow ou sFlow;
5.30	Deve suportar FTP cliente;
5.31	Deve suportar TFTP cliente e servidor;
5.32	Deve suportar IGMP;
5.33	Deve suportar IGMP snooping;
5.34	Deve suportar MLD;
5.35	Deve suportar MLD snooping;

6. Características de segurança

6.1	Deve suportar TACACS+ e RADIUS;
6.2	Deve suportar 802.1x com autenticação baseada na porta
6.3	Deve suportar 802.1x com autenticação baseada no endereço MAC
6.4	Deve suportar 802.1x Guest VLAN
6.5	Deve suportar 802.1x MAC Authentication Bypass (MAB)
6.6	Deve suportar 802.1x Dynamic VLAN Assignment

7. Integração com plataformas externas

- | | |
|-----|--|
| 7.1 | Deverá suportar mecanismos de integração com plataformas externas recorrendo a protocolos de configuração, linguagens de modelação dos dados ou interfaces de programação de aplicações (API) abertas para, por exemplo, permitir a automação e execução de ações e telemetria |
|-----|--|

Tipo 2 – Switch de 48 portas RJ45 MultiGigabit (Firewall)

1. Características Físicas

- | | |
|-----|--|
| 1.1 | Deve possuir as dimensões 1RU e EIA standard 19 in. |
| 1.2 | Deve possuir fontes de alimentação redundantes incluídas; |
| 1.3 | Deve possuir fontes de alimentação amovíveis; |
| 1.4 | Deve permitir que as fontes de alimentação sejam substituídas no local sem interromper o funcionamento do equipamento; |
| 1.5 | Deve possuir 48 portas RJ45 e 6 portas 10GE/25GE (SFP+/SFP28) line rate de uplink, seja através de módulo ou diretamente no equipamento. Das 48 portas RJ45 pelo menos 24 têm de suportar pelo menos 5 GE e as restantes podem suportar apenas 1 GE; |
| 1.6 | Caso seja necessário um módulo de portas 10GE/25GE (SFP+/SFP28), o mesmo deve vir de base com o equipamento; |
| 1.7 | Deve suportar auto negociação da velocidade das portas e duplex |

2. Escalabilidade e Performance

- | | |
|-----|---|
| 2.1 | Deve ter a capacidade de switching de pelo menos 700 Gbps; |
| 2.2 | Deve ter a capacidade de forwarding de pelo menos 800 Mpps; |
| 2.3 | Deve suportar pelo menos 4000 VLAN IDs; |
| 2.4 | Deve suportar pelo menos 32000 endereços MAC; |
| 2.5 | Deve suportar pelo menos 16000 rotas IPv4; |
| 2.6 | Deve suportar pelo menos 8000 rotas IPv6; |
| 2.7 | Deve suportar pelo menos 5000 entradas ACL; |

3. Características de Stack / Grupo de Equipamentos

- | | |
|-----|---|
| 3.1 | O equipamento deve ter a capacidade de suporte de stacking ou tecnologia que garanta a redundância entre vários equipamentos de um grupo; |
| 3.2 | O stack/grupo de equipamentos deverá ter a capacidade de crescer até aos 8 elementos; |
| 3.3 | Todos os elementos do stack/grupo de equipamentos devem ser geridos como se se tratasse de um único elemento; |
| 3.4 | O stack/grupo de equipamentos deve ser gerido através de um endereço único de gestão; |
| 3.5 | A ligação do stack/grupo de equipamentos deve ser estabelecido por meio das interfaces Ethernet regulares ou de interfaces dedicadas; |
| 3.6 | A ligação entre os vários equipamentos de stack / grupo de equipamentos deve suportar 40 Gbps de largura de banda; |
| 3.7 | Todos os elementos do stack / grupo de equipamentos tem de ser do mesmo modelo. |
| 3.8 | Os stacks de switches devem ser implementados com ligações físicas entre os vários equipamentos do grupo, não sendo necessário nenhum outro equipamento para o seu funcionamento. |
| 3.9 | Um dos Switchs deve assumir o papel de master e em caso de avaria, um outro switch do stack assuma esse papel, garantindo assim a operacionalidade do stack |

4. Acesso ao equipamento

- | | |
|-----|--|
| 4.1 | Deve permitir o acesso via CLI (Telnet/SSH); |
|-----|--|

- 4.2 Deve permitir o acesso Web GUI (HTTP/HTTPS);
- 4.3 Deve permitir desabilitar o acesso por Telnet;
- 4.4 Deve permitir desabilitar o acesso por HTTP e HTTPS;

5. Características gerais

- 5.1 Deve suportar Layer 2 e Layer 3;
- 5.2 Deve suportar IPv4, IPv6 e Dual Stack;
- 5.3 Deve suportar ACL (IPv4 e IPv6);
- 5.4 Deve suportar QoS (IPv4 e IPv6);
- 5.5 Deve suportar a definição de interfaces de Loopback;
- 5.6 Deve suportar Inter-VLAN Routing;
- 5.7 Deve suportar routing estático (IPv4 e IPv6);
- 5.8 Deve suportar o protocolo de routing RIP (IPv4 e IPv6);
- 5.9 Deve suportar o protocolo de routing OSPF (IPv4 e IPv6);
- 5.10 Deve suportar VRRP;
- 5.11 Deve suportar CDP ou LLDP (802.1ab);
- 5.12 Deve suportar a configuração de VLAN (802.1Q);
- 5.13 Deve suportar a seleção de VLAN com base em ACL;
- 5.14 Deve suportar a seleção de VLAN com base em endereço MAC;
- 5.15 Deve suportar a seleção de VLAN com base em endereço IP;
- 5.16 Deve suportar a seleção de VLAN com base em 802.1X;
- 5.17 Deve suportar private VLAN;
- 5.18 Deve suportar Jumbo Frames;
- 5.19 Deve suportar LACP (802.3ad);
- 5.20 Deve suportar STP (802.1D), MSTP (802.1s), RSTP (802.1w), PSVT+ e RPVST+;
- 5.21 Deve suportar Portfast, BPDU Guard, BPDU Filtering e Root Guard
- 5.22 Deve suportar BFD;
- 5.23 Deve suportar UDLD;
- 5.24 Deve suportar NTP;
- 5.25 Deve suportar SNMP v2c e v3
- 5.26 Deve suportar Syslog;
- 5.27 Deve suportar Port Mirroring;
- 5.28 Deve suportar SPAN e ERSPAN;
- 5.29 Deve suportar Netflow ou sFlow;
- 5.30 Deve suportar FTP cliente;
- 5.31 Deve suportar TFTP cliente e servidor;
- 5.32 Deve suportar IGMP;
- 5.33 Deve suportar IGMP snooping;
- 5.34 Deve suportar MLD;
- 5.35 Deve suportar MLD snooping;

6. Características de segurança

- | | |
|-----|---|
| 6.1 | Deve suportar TACACS+ e RADIUS; |
| 6.2 | Deve suportar 802.1x com autenticação baseada na porta |
| 6.3 | Deve suportar 802.1x com autenticação baseada no endereço MAC |
| 6.4 | Deve suportar 802.1x Guest VLAN |
| 6.5 | Deve suportar 802.1x MAC Authentication Bypass (MAB) |
| 6.6 | Deve suportar 802.1x Dynamic VLAN Assignment |

7. Integração com plataformas externas

- | | |
|-----|--|
| 7.1 | Deverá suportar mecanismos de integração com plataformas externas recorrendo a protocolos de configuração, linguagens de modelação dos dados ou interfaces de programação de aplicações (API) abertas para, por exemplo, permitir a automação e execução de ações e telemetria |
|-----|--|

Tipo 3 – Switch de 48 portas RJ45 Gigabit (Servidores, Desenvolvimento e WAN)

1. Características Físicas

- | | |
|-----|---|
| 1.1 | Deve possuir as dimensões 1RU e EIA standard 19 in. |
| 1.2 | Deve possuir fontes de alimentação redundantes incluídas; |
| 1.4 | Deve possuir pelo menos 48 portas 1GE (RJ-45) e 4 portas 10GE (SFP+) line rate de uplink, seja através de módulo ou diretamente no equipamento; |
| 1.5 | Caso seja necessário um módulo de portas 10GE (SFP+), o mesmo deve vir de base com o equipamento; |
| 1.6 | Deve suportar auto negociação da velocidade das portas e duplex |

2. Escalabilidade e Performance

- | | |
|-----|---|
| 2.1 | Deve ter a capacidade de switching de pelo menos 170 Gbps; |
| 2.2 | Deve ter a capacidade de forwarding de pelo menos 130 Mpps; |
| 2.3 | Deve suportar pelo menos 1000 VLAN IDs; |
| 2.4 | Deve suportar pelo menos 30000 endereços MAC; |
| 2.5 | Deve suportar pelo menos 16000 rotas IPv4; |
| 2.6 | Deve suportar pelo menos 6000 rotas IPv6; |
| 2.7 | Deve suportar pelo menos 1000 entradas ACL; |

3. Características de Stack / Grupo de Equipamentos

- | | |
|-----|--|
| 3.1 | O equipamento deve ter a capacidade de suporte de stacking ou tecnologia que garanta a redundância entre vários equipamentos de um grupo; |
| 3.2 | O stack/grupo de equipamentos deverá ter a capacidade de crescer até aos 8 elementos; |
| 3.3 | Todos os elementos do stack/grupo de equipamentos devem ser geridos como se se tratasse de um único elemento; |
| 3.4 | O stack/grupo de equipamentos deve ser gerido através de um endereço único de gestão; |
| 3.5 | A ligação do stack/grupo de equipamentos deve ser estabelecido por meio das interfaces Ethernet regulares ou de interfaces dedicadas; |
| 3.6 | A ligação entre os vários equipamentos de stack / grupo de equipamentos deve suportar 20 Gbps de largura de banda; |
| 3.7 | Todos os elementos do stack / grupo de equipamentos tem de ser do mesmo modelo. |
| 3.8 | Os stacks de switchs devem ser implementados com ligações físicas entre os vários equipamentos do grupo, não sendo necessário nenhum outro equipamento para o seu funcionamento. |

- 3.9 Um dos Switchs deve assumir o papel de master e em caso de avaria, um outro switch do stack assumo esse papel, garantindo assim a operacionalidade do stack

4. Acesso ao equipamento

- 4.1 Deve permitir o acesso via CLI (Telnet/SSH);
- 4.2 Deve permitir o acesso Web GUI (HTTP/HTTPS);
- 4.3 Deve permitir desabilitar o acesso por Telnet;
- 4.4 Deve permitir desabilitar o acesso por HTTP e HTTPS;

5. Características gerais

- 5.1 Deve suportar Layer 2 e Layer 3;
- 5.2 Deve suportar IPv4, IPv6 e Dual Stack;
- 5.3 Deve suportar ACL (IPv4 e IPv6);
- 5.4 Deve suportar QoS (IPv4 e IPv6);
- 5.5 Deve suportar a definição de interfaces de Loopback;
- 5.6 Deve suportar Inter-VLAN Routing;
- 5.7 Deve suportar routing estático (IPv4 e IPv6);
- 5.8 Deve suportar o protocolo de routing RIP (IPv4 e IPv6);
- 5.9 Deve suportar o protocolo de routing OSPF (IPv4 e IPv6);
- 5.10 Deve suportar VRRP;
- 5.11 Deve suportar CDP ou LLDP (802.1ab);
- 5.12 Deve suportar a configuração de VLAN (802.1Q);
- 5.13 Deve suportar a seleção de VLAN com base em ACL;
- 5.14 Deve suportar a seleção de VLAN com base em endereço MAC;
- 5.15 Deve suportar a seleção de VLAN com base em endereço IP;
- 5.16 Deve suportar a seleção de VLAN com base em 802.1X;
- 5.17 Deve suportar private VLAN;
- 5.18 Deve suportar Jumbo Frames;
- 5.19 Deve suportar LACP (802.3ad);
- 5.20 Deve suportar STP (802.1D), MSTP (802.1s), RSTP (802.1w), PSVT+ e RPVST+;
- 5.21 Deve suportar Portfast, BPDU Guard, BPDU Filtering e Root Guard
- 5.22 Deve suportar BFD;
- 5.23 Deve suportar UDLD;
- 5.24 Deve suportar NTP;
- 5.25 Deve suportar SNMP v2c e v3
- 5.26 Deve suportar Syslog;
- 5.27 Deve suportar Port Mirroring;
- 5.28 Deve suportar SPAN e ERSPAN;
- 5.29 Deve suportar Netflow ou sFlow;
- 5.30 Deve suportar FTP cliente;
- 5.31 Deve suportar TFTP cliente e servidor;
- 5.32 Deve suportar IGMP;
- 5.33 Deve suportar IGMP snooping;
- 5.34 Deve suportar MLD;
- 5.35 Deve suportar MLD snooping;

6. Características de segurança

- | | |
|-----|---|
| 6.1 | Deve suportar TACACS+ e RADIUS; |
| 6.2 | Deve suportar 802.1x com autenticação baseada na porta |
| 6.3 | Deve suportar 802.1x com autenticação baseada no endereço MAC |
| 6.4 | Deve suportar 802.1x Guest VLAN |
| 6.5 | Deve suportar 802.1x MAC Authentication Bypass (MAB) |
| 6.6 | Deve suportar 802.1x Dynamic VLAN Assignment |

7. Integração com plataformas externas

- | | |
|-----|--|
| 7.1 | Deverá suportar mecanismos de integração com plataformas externas recorrendo a protocolos de configuração, linguagens de modelação dos dados ou interfaces de programação de aplicações (API) abertas para, por exemplo, permitir a automação e execução de ações e telemetria |
|-----|--|

Tipo 4 – Switch Multigigabit 48 portas RJ45 PoE (Edifício A e L- 1)

1. Características Físicas

1.1	Deve possuir as dimensões 1RU e EIA standard 19 in.
1.2	Deve possuir fontes de alimentação redundantes incluídas;
1.3	Deve possuir fontes de alimentação amovíveis;
1.4	Deve permitir que as fontes de alimentação sejam substituídas no local sem interromper o funcionamento do equipamento;
1.5	Deve possuir pelo menos 48 portas 1GE (RJ-45), sendo que pelo menos 24 das portas têm de ser mGig e suportar pelo menos 2.5GE, e 4 portas 10GE (SFP+) line rate de uplink, seja através de módulo ou diretamente no equipamento;
1.6	Caso seja necessário um modulo de portas 10GE (SFP+), o mesmo deve vir de base com o equipamento;
1.7	Deve garantir POE+ 30 W (IEEE 802.3at Type 2) em todas as 48 portas 1GE (RJ-45) ou POE++ 60 W (IEEE 802.3bt Type 3) em pelo menos 24 das portas 1GE (RJ-45);
1.8	Deve suportar auto negociação da velocidade das portas e duplex

2. Escalabilidade e Performance

2.1	Deve ter a capacidade de switching de pelo menos 500 Gbps;
2.2	Deve ter a capacidade de forwarding de pelo menos 450 Mpps;
2.3	Deve suportar pelo menos 4000 VLAN IDs;
2.4	Deve suportar pelo menos 16000 endereços MAC;
2.5	Deve suportar pelo menos 3000 rotas IPv4;
2.6	Deve suportar pelo menos 1500 rotas IPv6;
2.7	Deve suportar pelo menos 1500 entradas ACL;

3. Características de Stack / Grupo de Equipamentos

3.1	O equipamento deve ter a capacidade de suporte de stacking ou tecnologia que garanta a redundância entre vários equipamentos de um grupo;
3.2	O stack/grupo de equipamentos deverá ter a capacidade de crescer até aos 8 elementos;
3.3	Todos os elementos do stack/grupo de equipamentos devem ser geridos como se se tratasse de um único elemento;
3.4	O stack/grupo de equipamentos deve ser gerido através de um endereço único de gestão;
3.5	A ligação do stack/grupo de equipamentos deve ser estabelecido por meio das interfaces Ethernet regulares ou de interfaces dedicadas;
3.6	A ligação entre os vários equipamentos de stack / grupo de equipamentos deve suportar 20 Gbps de largura de banda;
3.7	Todos os elementos do stack / grupo de equipamentos tem de ser do mesmo modelo.
3.8	Os stacks de switchs devem ser implementados com ligações físicas entre os vários equipamentos do grupo, não sendo necessário nenhum outro equipamento para o seu funcionamento.
3.9	Um dos Switchs deve assumir o papel de master e em caso de avaria, um outro switch do stack assuma esse papel, garantindo assim a operacionalidade do stack

4. Acesso ao equipamento

4.1	Deve permitir o acesso via CLI (Telnet/SSH);
4.2	Deve permitir o acesso Web GUI (HTTP/HTTPS);
4.3	Deve permitir desabilitar o acesso por Telnet;
4.4	Deve permitir desabilitar o acesso por HTTP e HTTPS;

5. Características gerais

5.1	Deve suportar Layer 2 e Layer 3;
5.2	Deve suportar IPv4, IPv6 e Dual Stack;
5.3	Deve suportar ACL (IPv4 e IPv6);
5.4	Deve suportar QoS (IPv4 e IPv6);
5.5	Deve suportar a definição de interfaces de Loopback;
5.6	Deve suportar Inter-VLAN Routing;
5.7	Deve suportar routing estático (IPv4 e IPv6);
5.8	Deve suportar o protocolo de routing RIP (IPv4 e IPv6);
5.9	Deve suportar o protocolo de routing OSPF (IPv4 e IPv6);
5.10	Deve suportar VRRP;
5.11	Deve suportar CDP ou LLDP (802.1ab);
5.12	Deve suportar a configuração de VLAN (802.1Q);
5.13	Deve suportar a seleção de VLAN com base em ACL;
5.14	Deve suportar a seleção de VLAN com base em endereço MAC;
5.15	Deve suportar a seleção de VLAN com base em endereço IP;
5.16	Deve suportar a seleção de VLAN com base em 802.1X;
5.17	Deve suportar private VLAN;
5.18	Deve suportar Jumbo Frames;
5.19	Deve suportar LACP (802.3ad);
5.20	Deve suportar STP (802.1D), MSTP (802.1s), RSTP (802.1w), PSVT+ e RPVST+;
5.21	Deve suportar Portfast, BPDU Guard, BPDU Filtering e Root Guard
5.22	Deve suportar BFD;
5.23	Deve suportar UDLD;
5.24	Deve suportar NTP;
5.25	Deve suportar SNMP v2c e v3
5.26	Deve suportar Syslog;
5.27	Deve suportar Port Mirroring;
5.28	Deve suportar SPAN e ERSPAN;
5.29	Deve suportar Netflow ou sFlow;
5.30	Deve suportar FTP cliente;
5.31	Deve suportar TFTP cliente e servidor;
5.32	Deve suportar IGMP;
5.33	Deve suportar IGMP snooping;
5.34	Deve suportar MLD;
5.35	Deve suportar MLD snooping;

6. Características de segurança

6.1	Deve suportar TACACS+ e RADIUS;
6.2	Deve suportar 802.1x com autenticação baseada na porta
6.3	Deve suportar 802.1x com autenticação baseada no endereço MAC
6.4	Deve suportar 802.1x Guest VLAN
6.5	Deve suportar 802.1x MAC Authentication Bypass (MAB)

6.6 Deve suportar 802.1x Dynamic VLAN Assignment

7. Integração com plataformas externas

7.1 Deverá suportar mecanismos de integração com plataformas externas recorrendo a protocolos de configuração, linguagens de modelação dos dados ou interfaces de programação de aplicações (API) abertas para, por exemplo, permitir a automação e execução de ações e telemetria

Tipo 5– Switch Multigigabit de 24 portas RJ45 POE (Lisboa (Edifício D, Edifício L-2, Portaria e Palacete) e restantes 12 Localizações Remotas)

1. Características Físicas

- 1.1 Deve possuir as dimensões 1RU e EIA standard 19 in.
- 1.2 Deve possuir fontes de alimentação redundantes incluídas;
- 1.3 Deve possuir pelo menos 24 portas 1GE (RJ-45), sendo que 8 das portas têm de ser mGig e suportar pelo menos 2.5GE, e 4 portas 10GE (SFP+) line rate de uplink, seja através de módulo ou diretamente no equipamento;
- 1.4 Caso seja necessário um módulo de portas 10GE (SFP+), o mesmo deve vir de base com o equipamento;
- 1.5 Deve garantir POE+ 30 W (IEEE 802.3at Type 2) em todas as 24 portas 1GE (RJ-45) ou POE++ 60 W (IEEE 802.3bt Type 3) em pelo menos 12 das portas 1GE (RJ-45);
- 1.6 Deve suportar auto negociação da velocidade das portas e duplex

2. Escalabilidade e Performance

- 2.1 Deve ter a capacidade de switching de pelo menos 170 Gbps;
- 2.2 Deve ter a capacidade de forwarding de pelo menos 200 Mpps;
- 2.3 Deve suportar pelo menos 4000 VLAN IDs;
- 2.4 Deve suportar pelo menos 16000 endereços MAC;
- 2.5 Deve suportar pelo menos 1000 rotas IPv4;
- 2.6 Deve suportar pelo menos 500 rotas IPv6;
- 2.7 Deve suportar pelo menos 1000 entradas ACL;

3. Características de Stack / Grupo de Equipamentos

- 3.1 O equipamento deve ter a capacidade de suporte de stacking ou tecnologia que garanta a redundância entre vários equipamentos de um grupo;
- 3.2 O stack/grupo de equipamentos deverá ter a capacidade de crescer até aos 8 elementos;
- 3.3 Todos os elementos do stack/grupo de equipamentos devem ser geridos como se se tratasse de um único elemento;
- 3.4 O stack/grupo de equipamentos deve ser gerido através de um endereço único de gestão;
- 3.5 A ligação do stack/grupo de equipamentos deve ser estabelecido por meio das interfaces Ethernet regulares ou de interfaces dedicadas;
- 3.6 A ligação entre os vários equipamentos de stack / grupo de equipamentos deve suportar 20 Gbps de largura de banda;
- 3.7 Todos os elementos do stack / grupo de equipamentos tem de ser do mesmo modelo.
- 3.8 Os stacks de switches devem ser implementados com ligações físicas entre os vários equipamentos do grupo, não recorrendo a nenhum outro equipamento para o seu funcionamento.
- 3.9 Um dos Switchs deve assumir o papel de master e em caso de avaria, um outro switch do stack assuma esse papel, garantindo assim a operacionalidade do stack

4. Acesso ao equipamento

- | | |
|-----|--|
| 4.1 | Deve permitir o acesso via CLI (Telnet/SSH); |
| 4.2 | Deve permitir o acesso Web GUI (HTTP/HTTPS); |
| 4.3 | Deve permitir desabilitar o acesso por Telnet; |
| 4.4 | Deve permitir desabilitar o acesso por HTTP e HTTPS; |

5. Características gerais

- | | |
|------|---|
| 5.1 | Deve suportar Layer 2 e Layer 3; |
| 5.2 | Deve suportar IPv4, IPv6 e Dual Stack; |
| 5.3 | Deve suportar ACL (IPv4 e IPv6); |
| 5.4 | Deve suportar QoS (IPv4 e IPv6); |
| 5.5 | Deve suportar a definição de interfaces de Loopback; |
| 5.6 | Deve suportar Inter-VLAN Routing; |
| 5.7 | Deve suportar routing estático (IPv4 e IPv6); |
| 5.8 | Deve suportar o protocolo de routing RIP (IPv4 e IPv6); |
| 5.9 | Deve suportar o protocolo de routing OSPF (IPv4 e IPv6); |
| 5.10 | Deve suportar VRRP; |
| 5.11 | Deve suportar CDP ou LLDP (802.1ab); |
| 5.12 | Deve suportar a configuração de VLAN (802.1Q); |
| 5.13 | Deve suportar a seleção de VLAN com base em ACL; |
| 5.14 | Deve suportar a seleção de VLAN com base em endereço MAC; |
| 5.15 | Deve suportar a seleção de VLAN com base em endereço IP; |
| 5.16 | Deve suportar a seleção de VLAN com base em 802.1X; |
| 5.17 | Deve suportar private VLAN; |
| 5.18 | Deve suportar Jumbo Frames; |
| 5.19 | Deve suportar LACP (802.3ad); |
| 5.20 | Deve suportar STP (802.1D), MSTP (802.1s), RSTP (802.1w), PSVT+ e RPVST+; |
| 5.21 | Deve suportar Portfast, BPDU Guard, BPDU Filtering e Root Guard |
| 5.22 | Deve suportar BFD; |
| 5.23 | Deve suportar UDLD; |
| 5.24 | Deve suportar NTP; |
| 5.25 | Deve suportar SNMP v2c e v3 |
| 5.26 | Deve suportar Syslog; |
| 5.27 | Deve suportar Port Mirroring; |
| 5.28 | Deve suportar SPAN e ERSPAN; |
| 5.29 | Deve suportar Netflow ou sFlow; |
| 5.30 | Deve suportar FTP cliente; |
| 5.31 | Deve suportar TFTP cliente e servidor; |
| 5.32 | Deve suportar IGMP; |
| 5.33 | Deve suportar IGMP snooping; |
| 5.34 | Deve suportar MLD; |
| 5.35 | Deve suportar MLD snooping; |

6. Características de segurança

- | | |
|-----|---|
| 6.1 | Deve suportar TACACS+ e RADIUS; |
| 6.2 | Deve suportar 802.1x com autenticação baseada na porta |
| 6.3 | Deve suportar 802.1x com autenticação baseada no endereço MAC |
| 6.4 | Deve suportar 802.1x Guest VLAN |
| 6.5 | Deve suportar 802.1x MAC Authentication Bypass (MAB) |
| 6.6 | Deve suportar 802.1x Dynamic VLAN Assignment |

7. Integração com plataformas externas

- | | |
|-----|--|
| 7.1 | Deverá suportar mecanismos de integração com plataformas externas recorrendo a protocolos de configuração, linguagens de modelação dos dados ou interfaces de programação de aplicações (API) abertas para, por exemplo, permitir a automação e execução de ações e telemetria |
|-----|--|

2- Características técnicas – Access Points (APs)

1. Conectividade à LAN

- | | |
|-----|---|
| 1.1 | Deve possuir pelo menos uma porta de ligação à rede 100/1000/2500 Base-T (RJ45); |
| 1.2 | As portas de ligação à rede devem suportar MDI/MDIX; |
| 1.3 | Deve suportar nas suas portas de rede as seguintes especificações IEEE referentes a conectividade: 802.3, 802.3ab, 802.3ad, 802.3bz |
| 1.4 | Deve suportar nas suas portas de rede as seguintes especificações IEEE referentes a PoE : 802.3af, 802.3at, 802.3bt |
| 1.5 | Deve possuir uma interface RJ45 ou USB que desempenhe as funções de consola; |
| 1.6 | Deve possuir uma interface USB para ligação de um dispositivo externo; |

2. Sistema wireless

- | | |
|------|---|
| 2.1 | Deve ser concebido para espaços interiores; |
| 2.2 | Deve possuir antenas internas omnidireccionais em azimute, otimizadas para montagem horizontal em teto; |
| 2.3 | Deve funcionar nas três gamas de frequência 2.4GHz, 5GHz e 6GHz; |
| 2.4 | Deve possuir pelo menos três rádios concorrentes para utilização Wi-Fi nas gamas de frequência 2.4GHz, 5GHz e 6GHz, respetivamente; |
| 2.5 | Os rádios devem suportar 4x4:4 MIMO; |
| 2.6 | Deve suportar as Larguras de Canal 20 MHz nas gamas de frequência 2.4GHz; |
| 2.7 | Deve suportar as Larguras de Canal 20/40/80 MHz nas gamas de frequência 5GHz; |
| 2.8 | Deve suportar as Larguras de Canal 20/40/80/160MHz nas gamas de frequência 6GHz; |
| 2.9 | Deve suportar as modulações BPSK, QPSK, 64-QAM, 256-QAM e 1024-QAM; |
| 2.10 | Deve possuir um rádio Bluetooth Low Energy (BLE); |
| 2.11 | Deve possuir pelo menos um rádio para poder realizar tarefas de scanning na rede wireless; |
| 2.12 | Deve suportar no mínimo 16 SSIDs simultâneos; |

3. Alimentação de energia

- | | |
|-----|---|
| 3.1 | Deve possuir pelo menos uma porta com suporte por defeito de 802.3bt |
| 3.2 | Deve funcionar em pleno, com todas as suas capacidades ativas, apenas com uma porta alimentada por PoE (802.3bt). |
| 3.3 | Deve suportar redundância de PoE. |

4. Segurança

- | | |
|-----|--|
| 4.1 | Deve suportar os seguintes protocolos de autenticação: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP/EAP-MSCHAPv2, PEAP/EAP-GTC, EAP-FAST |
| 4.2 | Deve suportar os seguintes métodos de autenticação: WPA, WPA2 e WPA3 |
| 4.3 | Deve suportar 802.1X |

5. Certificações IEEE

- | | |
|-----|---|
| 5.1 | Deve suportar 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax |
| 5.2 | Deve suportar >=400 clientes por rádio. |

6. Tecnologias wireless

- | | |
|-----|---|
| 6.1 | Deve suportar Uplink Orthogonal Frequency Division Multiple Access (UL OFDMA) |
| 6.2 | Deve suportar Downlink Orthogonal Frequency Division Multiple Access (DL OFDMA) |
| 6.3 | Deve suportar BSS Coloring (Reutilização espacial) |
| 6.4 | Deve suportar Band Steering |
| 6.5 | Deve suportar Beamforming |
| 6.6 | Deve suportar Uplink Multiuser, Multiple Input, Multiple Output (UL MU-MIMO) |
| 6.7 | Deve suportar Downlink Multiuser, Multiple Input, Multiple Output (DL MU-MIMO) |
| 6.8 | Deve suportar Enhanced Target Wake Time (TWT) |

7. Modos de funcionamento do AP

- | | |
|-----|---|
| 7.1 | Deve poder funcionar em modo Tunnel |
| 7.2 | Deve poder funcionar em modo Bridge |
| 7.3 | Deve poder funcionar em modo Site Survey e analisar o espectro rádio |
| 7.4 | Deve poder funcionar em modo Sniffer |
| 7.5 | Deve poder funcionar de forma a detetar e identificar a presença de Rogue APs |
| 7.6 | Deve poder funcionar em modo WIPS/WIDS |
| 7.7 | Deve suportar Seleção Dinamica de Frequências (DFS) |

8. Modos de montagem

- | | |
|-----|---|
| 8.1 | Deve poder ser montado em tecto, calha (T-Rail) e parede em alguns casos excepcionais; |
| 8.2 | Deve ter os acessórios de montagem incluídos; |
| 8.3 | Deve possuir um slot para utilização de um dispositivo do tipo cadeado Kensington para protecção do equipamento contra furto; |

9. Certificação Wi-Fi Alliance

- | | |
|-----|--|
| 9.1 | Deve possuir a certificação Wi-Fi 6 atribuída pela Wi-Fi Alliance (o Wi-Fi 6E faz parte integrante da certificação Wi-Fi 6); |
|-----|--|

3- Características técnicas “Controladoras” e Plataforma de Gestão

Controladora de rede sem fios (WLC)

1	Características gerais da Plataforma
1.1	Deve desempenhar as funções de gestão e controlo centralizado sobre um conjunto de Access Points permitindo que estes sejam aprovisionados, configurados, atualizados e geridos a partir de uma única interface, garantindo a consistência da sua parametrização, o seu funcionamento e a sua manutenção.
1.2	Deve ser centralizada (controlador wireless) para gestão total da rede wireless e dos Access Points que a constituem;
1.3	Deve ser constituída por equipamentos físicos não sendo aceite uma plataforma que se baseie em serviços de cloud;
1.4	Deve ser redundante, formando um cluster, para garantir a resiliência da solução;
1.5	Deve permitir a sua configuração através de CLI (Telnet/SSH);
1.6	Deve permitir a sua configuração através de GUI Web (HTTP/HTTPS);
1.7	Deve permitir desabilitar o acesso por Telnet;
1.8	Deve permitir desabilitar o acesso por HTTP;
1.9	Deve permitir ser totalmente gerida através de um GUI disponibilizado através de um navegador (browser).
2.	Características da Plataforma física
2.1	Deve ser constituída pelo menos por dois equipamentos idênticos;
2.2	Deve possuir a dimensão de 1RU - EIA standard 19 in.;
2.3	Deve ser fornecido com todos os acessórios de montagem em bastidor;
2.4	Deve possuir fontes de alimentação AC internas redundantes;
2.5	Deve ser fornecido com cabos de alimentação com fichas IEC60320-C14 ou CEE 7/4 (Schuko) ou CEE 7/7.
2.6	Deve possuir uma porta de consola (RJ-45 ou USB);
2.7	Deve possuir uma porta de rede dedicada para gestão out-of-band (OOBM);
2.8	Deve possuir uma porta física dedicada, ou dedicada por configuração do software, para redundância Stateful Switchover (SSO);
2.9	Deve possuir duas portas de rede de serviço, com o suporte mínimo 1G/10G Base-T ou 10GE Base-SR, para o tráfego de serviço dos APs, tráfego de gestão in-band e tráfego de utilizadores;
2.10	As portas de serviço, referidas no ponto anterior, devem suportar LACP e poder ser ligadas a dois equipamentos distintos de um cluster de switches;
3.	Redundância e Alta-disponibilidade da plataforma
3.1	Para garantir a resiliência, confiabilidade, disponibilidade e escalabilidade da solução, deve suportar configurações de redundância e alta disponibilidade, para minimizar o tempo de inatividade em caso de falhas de hardware ou manutenção;
3.2	Deve constituir uma solução de alta-disponibilidade, sem pontos únicos de falha que possam colocar em causa o funcionamento do serviço wireless.
3.3	Deve fornecer informação sobre o estado de funcionamento da alta-disponibilidade e estatísticas sobre a mesma;
3.4	Deve suportar pelo menos o modo de funcionamento Single Active/Single Standby (1+1) em alta disponibilidade.
3.5	Deve ter a capacidade de hitless failover de sessões de clientes de dados, voz e vídeo, em caso de falha da controladora em que o dispositivo se encontra registado.
3.6	Deve ter a capacidade de atualização de software do controlador wireless sem interrupção do serviço;

3.7 Deve ter a capacidade de atualização do software dos APs sem interrupção do serviço;

4. Capacidades da plataforma

4.1 Número mínimo de APs geridos: 500;

4.2 Número mínimo de dispositivos terminais distintos geridos: 10 000;

4.3 Taxa de transferência mínima (IMIX): 5 Gbps;

4.5 Número mínimo de WLANs suportadas: 4000

4.6 Número mínimo de VLANs suportadas 4000.

5. Características base da plataforma

5.1 Deve suportar IPv4, IPv6 e Dual Stack;

5.2 Deve permitir a definição das interfaces em modo acesso e em modo trunk;

5.3 Deve permitir a definição de múltiplos interfaces lógicos com configuração IP (IPv4 e IPv6) e atribuição de VLAN;

5.4 Deve permitir a definição de grupos de interfaces lógicos;

5.5 Deve fazer o mapeamento entre VLAN e SSID;

5.6 Deve permitir a definição de perfis de WLAN;

5.7 Deve permitir a mobilidade transparente dos dispositivos clientes entre APs sem que estes tenham de reiniciar o processo de ligação.

5.8 Deve permitir a ligação a um sistema de gestão de políticas de controlo de acesso de utilizadores e dispositivos terminais.

6. Suporte de múltiplas redes e locais

6.1 Deve ter a capacidade de segmentar e controlar várias redes autónomas de Access Points, com múltiplos SSIDs, que podem estar colocalizadas ou geograficamente dispersas.

7. Gestão dos recursos de rádio

7.1 Deve incluir as funcionalidades necessárias para avaliar e otimizar os recursos de radiofrequência (RF), podendo ajustá-los dinamicamente, tais como potência de transmissão, atribuição de canais e outras configurações de RF, para atenuar a interferência e otimizar o desempenho.

8. Mobilidade e Roaming

8.1 Deve garantir a mobilidade e roaming contínuos dos dispositivos terminais, garantindo que estes se possam mover entre diferentes APs e áreas sem sofrer interrupções ou quebras de ligação, o que é crucial para manter uma experiência de utilizador consistente durante a transição entre as áreas de cobertura.

9. Relógio da plataforma

9.1 Deve suportar a configuração de data/hora através do protocolo NTP;

9.2 Deve suportar a configuração de zona horária;

9.3 Deve suportar a configuração da mudança automática de hora (hora de verão/hora de inverno);

10. Gestão de utilizadores

10.1 Deve permitir a definição de utilizadores locais e a sua autenticação para executar tarefas de administração;

10.2 Os utilizadores locais devem poder ser autenticados localmente ou através de um servidor de autenticação, autorização e auditoria (AAA);

10.3 Deve permitir a definição de uma ou mais plataformas centralizadas RADIUS ou TACACS+, para autenticação, autorização e auditoria (AAA) de utilizadores, podendo estas funções estar separadas.

10.4 Deve permitir a ligação a uma plataforma centralizada LDAP ou Active Directory para autenticação de utilizadores;

10.5 Deve permitir a definição de vários perfis de utilizadores;

11. Modos de funcionamento da plataforma

- 11.1 Deve suportar o funcionamento de APs em modo Tunnel (CAPWAP);
- 11.2 Deve suportar o funcionamento de APs em modo Bridge (Local-Breakout);
- 11.3 Deve ter a capacidade de suportar o funcionamento de APs em modo Mesh ponto-a-ponto e ponto-multiponto;
- 11.4 Deve suportar em simultâneo os vários modos de funcionamento;
- 11.5 Deve suportar a configuração de SSIDs com split-tunneling.

12. Gestão

- 12.1 Deve permitir a configuração e gestão centralizada dos APs;
- 12.2 Deve permitir a actualização centralizada do firmware/software dos Aps;
- 12.3 Deve suportar a monitorização e alarmística através de uma plataforma de gestão;
- 12.4 Deve ter a capacidade de envio de logs para uma plataforma de gestão;

13. Certificações IEEE

- 13.1 Deve suportar 802.11a, 802.11b, 802.11d, 802.11e (WMM), 802.11g, 802.11h, 802.11k, 802.11n, 802.11r, 802.11w, 802.11ac (Wave1 e Wave2), 802.11ax
- 13.2 Deve suportar 802.1Q (VLAN tagging)
- 13.3 Deve suportar 802.1AX (Link Aggregation)

14. Wireless

- 14.1 Deve suportar múltiplos perfis de WLANs;
- 14.2 Deve suportar múltiplos SSIDs;
- 14.3 Deve suportar em simultâneo vários grupos de APs;
- 14.4 Deve suportar grupos de APs em locais geograficamente dispersos;
- 14.5 Deve suportar diferentes modos de funcionamento associados a vários SSIDs no mesmo grupo de APs;
- 14.6 Deve ter a capacidade de deteção, identificação, classificação e mitigação de Rogue APs
- 14.7 Deve ter a capacidade de detecção de intrusões wireless
- 14.8 Deve suportar Beamforming
- 14.9 Deve suportar Band Steering
- 14.10 Deve suportar DFS
- 14.11 Deve suportar QoS na rede wireless

15. Protocolos

- 15.1 Deve suportar CDP ou LLDP
- 15.2 Deve suportar NTP
- 15.3 Deve suportar SNMP v2c e v3
- 15.4 Deve suportar USM (User-Based Security Model) para SNMPv3
- 15.5 Deve suportar SNMP MIB e MIB II
- 15.6 Deve suportar Syslog

16. Segurança

- 16.1 Deve suportar WPA Personal e WPA Enterprise
- 16.2 Deve suportar WPA2 Personal e WPA2 Enterprise

16.3	Deve suportar WPA3 Personal, WPA3 Enterprise
16.4	Deve suportar Management Frame Protection (MFP)
16.5	Deve suportar Simultaneous Authentication of Equals (SAE)
16.6	Deve suportar Enhanced Open
16.7	Deve suportar Passpoint
16.8	Deve suportar 802.1X
16.9	Deve suportar TKIP
16.10	Deve suportar AES e suas variantes
16.11	Deve suportar DES / 3DES e suas variantes
16.12	Deve suportar TLS
16.13	Deve suportar DTLS
16.14	Deve suportar um Captive Portal interno customizável;
16.15	Deve permitir a integração com plataforma que implemente um Captive Portal externo customizável;
16.16	Deve permitir a integração com plataforma de Network Access Control (NAC);
16.17	Deve ter a capacidade de restrição da gestão do controlador wireless através da rede WiFi que é gerida pelo próprio controlador;
17. Monitorização disponibilizada pela plataforma	
17.1	Listar todos os APs geridos/configurados na plataforma
17.2	Listar todos os APs ativos na plataforma
17.3	Listar os APs que estão a operar em cada uma das gamas de frequências, indicando o seu estado, frequência, canal, endereço MAC, endereço IP, utilização
17.4	Listar os clientes, indicando a força do sinal, SNR, nome de utilizador, endereço IP, tipo de dispositivo
17.5	Mostrar gráficos gerais de desempenho;
17.6	Mostrar gráficos individualizados de desempenho;
18. Análise e monitorização integrada	
18.1	Deve proporcionar visibilidade sobre o desempenho e uso da rede wireless através de ferramentas de monitorização, análise e apresentação de relatórios, permitindo obter informações sobre o comportamento dos clientes, integridade da rede e padrões de uso para que seja possível tomar decisões informadas e otimizar os recursos da rede.
19. Detecção e identificação de problemas (troubleshooting)	
19.1	Deve permitir a verificação do estado de funcionamento dos Aps;
19.2	Deve permitir controlar os LEDs dos APs;
19.3	Deve permitir a configuração de APs a funcionar em modo de Sensor;
19.4	Deve permitir a configuração de APs a funcionar em modo de Sniffer;
19.5	Deve permitir a captura de tráfego e criação de um ficheiro PCAP (Packet Capture);
20. Integração com plataformas externas	
20.1	Deverá suportar mecanismos de integração com plataformas externas recorrendo a protocolos de configuração, linguagens de modelação de dados ou interfaces de programação de aplicações (API) abertas para, por exemplo, permitir a automação e execução de ações e telemetria

Network Access Control (NAC)

1	Características gerais da Plataforma
1.1	Deve garantir que apenas os dispositivos terminais e utilizadores autorizados têm permissão para se ligar à rede, impondo políticas que determinam quem pode aceder, como pode, se o dispositivo terminal está qualificado para aceder e quais os recursos a pode aceder após estar ligado.
1.2	Deve ser centralizada para gestão total do acesso à rede wired e wireless que constituem a rede da organização;
1.3	Deve ser constituída por equipamentos físicos, não sendo aceite uma plataforma que se baseie em serviços de cloud;
1.4	Deve ser redundante, formando um cluster, para garantir a resiliência da solução;
1.5	Deve possuir uma arquitetura escalável por adição de mais elementos à solução;
1.6	Deve permitir a sua configuração inicial básica através de consola ou CLI (Telnet ou SSH);
1.7	Deve permitir ser configurada e gerida através de um GUI Web, acedido por HTTPS através de um navegador (browser);
1.8	Deve permitir configurar e gerir os serviços de autenticação e autorização;
1.9	Deve suportar IPv4, IPv6 e Dual Stack;
1.10	Deve ter licenciamento deve permitir o mínimo de 2500 dispositivos em simultâneo.
2.	Características da Plataforma física
2.1	Deve ser constituída pelo menos por dois equipamentos idênticos e dedicados. Não é permitido que esta plataforma coexista nos mesmos equipamentos das outras plataformas;
2.2	Deve ser implementada em bastidor (EIA standard 19 in.);
2.3	Deve ser fornecida com todos os acessórios de montagem em bastidor;
2.4	Deve possuir fontes de alimentação AC internas redundantes;
2.5	Deve ser fornecido com cabos de alimentação com fichas IEC60320-C14 ou CEE 7/4 (Schuko) ou CEE 7/7.
2.6	Deve possuir uma porta de consola (RJ-45 ou USB);
2.7	Deve possuir uma porta de rede dedicada para gestão out-of-band (OOBM);
2.9	Deve possuir duas portas de rede de serviço, com o suporte mínimo 1G/10G Base-T ou 10GE Base-SR , para o tráfego de serviço e tráfego de gestão;
2.10	As portas de serviço, referidas no ponto anterior, devem garantir a redundância de ligações fisicamente ligadas, em simultâneo, a dois equipamentos distintos de um cluster de Switches, garantindo que a solução não é afetada pela falha ou colocação fora de serviço de uma porta física (do sistema de NAC ou do Switch) ou da ligação;
3.	Alta-disponibilidade da plataforma
3.1	Deve constituir uma solução redundante, com alta-disponibilidade, sem pontos únicos de falha que possam colocar em causa o funcionamento do serviço.
3.3	Deve possuir redundância dos seus vários elementos, para garantir que a solução mantém o serviço sem impactar os utilizadores, em caso de falha de um deles.
3.4	Deve ter a capacidade não impactar o serviço aos utilizadores em caso de falha de um dos seus elementos.
3.5	Deve ter a capacidade de actualização de software sem interrupção do serviço;
4.	Escalabilidade
4.1	Deve possuir uma arquitetura expansível, permitindo o seu crescimento através da adição de mais elementos e licenças;
4.2	Deve permitir uma implementação geograficamente dispersa;
4.3	Deve poder cobrir áreas específicas da rede ou áreas geográficas específicas;
4.3	O seu funcionamento não se deve basear na replicação de tráfego na rede;

5. Tipo de dispositivos suportados

- | | |
|-------|---|
| 5.1 | Deve ser integrada com os dispositivos de rede e os dispositivos de segurança existentes, assim como os que serão incluídos na nova arquitectura; |
| 5.2 | Os tipos de equipamentos existentes são: |
| 5.2.1 | - Switches de acesso, agregação e core |
| 5.2.2 | - Pontos de Acesso Wireless |
| 5.2.3 | - Controladores Wireless |
| 5.2.4 | - Firewalls |
| 5.2.5 | - Routers |

6. Características gerais da solução

- | | |
|--------|---|
| 6.1 | Deve ser agnóstica aos fabricantes dos equipamentos que disponibilizam o meio de acesso à rede, seja com fios, sem fios ou VPN, e, portanto, válida em redes heterogéneas multi-fabricante; |
| 6.2 | Deve ser baseada em standards da indústria, de modo a assegurar compatibilidade com diferentes tipos de equipamentos de acesso (switches, routers, firewalls, controladoras WLAN, terminadores de VPN, etc.); |
| 6.3 | Deve garantir a flexibilidade e a capacidade de permitir a escolha do modo como é implementada a segurança no acesso à rede, para proteger os serviços disponibilizados e a integridade da informação; |
| 6.4 | Deve garantir uma aproximação automatizada para descobrir, estabelecer o perfil, autenticar e autorizar utilizadores e dispositivos terminais de confiança no acesso à infraestrutura de rede, independentemente do meio utilizado. |
| 6.5 | Deve garantir o controlo do acesso de utilizadores e dispositivos terminais à rede, através de ligações com cabo (wired), sem fios (wireless) e VPN; |
| 6.6 | Deve poder funcionar tanto com agentes instalados nos dispositivos terminais, como sem agentes; |
| 6.7 | Deve proporcionar visibilidade abrangente e controlo sobre os utilizadores e dispositivos terminais que se ligam à rede; |
| 6.8 | Deve monitorar continuamente e verificar o nível de confiabilidade do utilizador e do dispositivo terminal e ajustar automaticamente as políticas de acesso; |
| 6.9 | Através do GUI único, deve permitir definir, configurar e gerir perfis e postura de utilizadores e dispositivos; |
| 6.10 | Através do GUI único, deve permitir configurar e gerir os serviços de autenticação e autorização; |
| 6.11 | Através do GUI único, deve permitir configurar e gerir os acessos de utilizadores externos e convidados (guest); |
| 6.12 | Deve integrar com múltiplos repositórios externos de identidade, entre os quais Microsoft Active Directory (On-Prem ou Microsoft Entra ID), Lightweight Directory Access Protocol (LDAP), RADIUS, TACACS+, Open Database Connectivity (ODBC) e SAML; |
| 6.13 | Deve gerir identidades de utilizadores e atributos dos dispositivos terminais, permitindo conceder ou negar o acesso à rede com base em políticas de controlo de acesso baseado na sua função (Role-Based Access Control - RBAC). |
| 6.14 | Deve suportar vários métodos de autenticação, tais como 802.1X, portal cativo, autenticação MAC, MAB (MAC Authentication Bypass) e outros. |
| 6.15 | Deve incluir os seguintes blocos funcionais: |
| 6.15.1 | - Visibilidade da rede e perfilagem dos dispositivos conectados ; |
| 6.15.2 | - Automação do processo de aprovisionamento da rede, dependendo do tipo de dispositivo que está a ser ligado; |
| 6.15.3 | - OnBoarding de novos dispositivos, simples, versátil e potente. |
| 6.15.4 | - Conformidade de dispositivos terminais, permitindo à organização implementar políticas associadas a diferentes grupos de utilizadores, verificar a conformidade e notificar desvios, permitindo configurar diferentes protocolos de remediação, desde ações imediatas de isolamento a simples notificações e ações diferidas. |
| 6.15.5 | - Identificação de Ameaças, através da integração com outros elementos, e execução de ações de remediação de acordo com o evento. |

- 6.15.6 - Gestão de convidados e utilizadores externos: Fácil e rápido, sem a necessidade de envolver o pessoal de TI no registo de novos utilizadores externos.

7. Definição e aplicação de políticas

- 7.1 Deve aplicar as políticas de acesso à rede, controlando e adaptando dinamicamente o acesso à mesma, com base na função do utilizador, tipo de dispositivo terminal, localização, hora do dia e outros atributos contextuais verificados em tempo real.
- 7.2 As políticas a aplicar ao controlo de acesso de dispositivos terminais e utilizadores, devem poder integrar pelo menos os seguintes elementos de contexto:
- 7.2.1 - Identidade do utilizador, onde se incluem também outros atributos da base de dados de utilizador para além das credenciais, tais como organização, departamento, contactos, grupo de segurança, etc.;
 - 7.2.2 - Identificação única (fingerprinting) do dispositivo terminal utilizado no acesso:
 - 7.2.2.1 - Tipo (PC, smartphone, tablet, consola);
 - 7.2.2.2 - Família de produto (MAC, Windows, Linux);
 - 7.2.2.3 - Sistema Operativo;
 - 7.2.2.4 - Identificador organizacionalmente exclusivo (OUI);
 - 7.2.3 - Integridade do dispositivo terminal;
 - 7.2.4 - Método e tipo de autenticação;
 - 7.2.5 - Localização do acesso;
 - 7.2.6 - Dispositivo de rede a partir do qual é efectado o acesso (NAD);
 - 7.2.7 - Data e hora de acesso;
- 7.3 Deve disponibilizar ferramentas de criação e teste de políticas, tais como:
- 7.3.1 - Templates pré-configurados;
 - 7.3.2 - Guia de configuração de políticas;
 - 7.3.3 - Navegador de LDAP para busca rápida de atributos da AD a integrar nas políticas;
 - 7.3.4 - Simulador integrado para testar as políticas criadas;
- 7.4 Deve garantir que os utilizadores e os dispositivos terminais têm acesso aos recursos de que necessitam, cumprindo os requisitos de segurança e conformidade;
- 7.5 Deve poder isolar numa zona restrita da rede os dispositivos terminais que não estejam conformes ou que se encontrem comprometidos e executar ações de correção para os colocar em conformidade;

8. Dispositivos terminais pessoais (Bring Your Own Device – BYOD)

- 8.1 Deve poder integrar e autenticar dispositivos terminais pessoais, ao mesmo tempo que deve aplicar políticas para garantir a sua conformidade e a segurança no acesso à rede.

9. Portal cativo para utilizadores externos (visitantes ou prestadores de serviços)

- 9.1 Deve suportar múltiplos e distintos portais cativos;
- 9.2 Deve permitir a definição de fluxos flexíveis de autenticação e autorização;
- 9.3 Deve ser adaptado à imagem de cada local da organização, permitindo a utilização de logos, imagens de fundo, utilização de cores, organização dos campos do formulário e outros elementos (botões, menus drop-down, check lists, radio buttons), e definição de mensagens;
- 9.4 Deve permitir a definição e adaptação dos campos dos formulários a utilizar;
- 9.5 Deve suportar múltiplas línguas, entre as quais Português (de Portugal) e Inglês;
- 9.6 Deve permitir realizar todas estas definições através de interface GUI e edição HTML ou CSS;
- 9.7 Deve permitir que os utilizadores externos façam o seu auto registo através do portal cativo;
- 9.8 Deve poder ajustar o portal cativo a ecrans de pequenas dimensões através da identificação automática de dispositivos móveis que acedem.
- 9.9 Deve permitir a escolha de acesso como visitante ou como utilizador externo com sponsor (elemento interno à organização responsável pela aprovação do acesso);

9.10	Deve suportar múltiplos sponsors;
9.11	Deve suportar a definição de fluxos de aprovação pelos sponsors;
9.12	Deve permitir que o sponsor autorize e estabeleça o período de utilização do utilizador externo;
9.13	Deve permitir a atribuição de códigos de acesso gerados previamente;
9.14	Deve permitir a atribuição de códigos de acesso gerados automaticamente no processo de registo;
9.15	Deve permitir a disponibilização de códigos de acesso através de SMS e e-mail;
9.16	Deve permitir que o e-mail seja enviado a partir de um endereço no-reply da organização;
9.17	Deve suportar Multi Factor Authentication (MFA);
9.18	Deve obrigar os utilizadores a aceitar os termos de utilização;
9.19	Deve limitar o tempo de acesso do utilizador visitante ao período fixo definido;
9.20	Deve limitar o tempo de acesso com sponsor ao período aprovado pelo mesmo;
9.21	Deve implementar MAC caching após a autenticação, com duração customizável, para que não seja necessário o utilizador inserir as credenciais sempre que se liga à rede durante validade do seu período de acesso.
9.22	Deve registar os dados fornecidos pelo utilizador, disponibilizando-os para fins de análise e auditoria;
9.23	Deve proceder à aplicação de políticas de acesso em conformidade para permitir o acesso seguro à rede sem comprometer a segurança;
9.24	Deve permitir a simulação dos fluxos definidos durante a sua criação, antes de entrar em produção;

10. Protocolos

10.1	Deve suportar NTP
10.2	Deve suportar SNMP v2c e v3
10.3	Deve suportar SNMP MIB e MIB II
10.4	Deve suportar Syslog

11. Integração com plataformas externas

11.1	Deve suportar pelo menos a integração com os seguintes tipos de soluções de terceiras:
11.1.1	- Next Generation Firewall (NGFW) - inbound e outbound
11.1.2	- Security information and event management (SIEM) - inbound e outbound
11.1.3	- Multi Factor Authentication (MFA)
11.1.4	- Mobile device management (MDM) e Enterprise Mobility Management (EMM)
11.1.5	- IP Address Management (IPAM)
11.2	Deve suportar pelo menos a integração com as seguintes soluções de Mobile Device Management (MDM):
11.2.1	- Aruba AirWave
11.2.2	- Ivanti MobileIron
11.2.3	- Microsoft Intune
11.2.4	- SOTI Mobicontrol
11.2.5	- VMware Workspace ONE (AirWatch)
11.2.6	- Citrix XenMobile
11.3	Deve suportar pelo menos os seguintes repositórios externos de identidade:
11.3.1	- Microsoft Active Directory (On-Prem ou Microsoft Entra ID)
11.3.2	- Lightweight Directory Access Protocol (LDAP)
11.3.3	- RADIUS
11.3.4	- TACACS+
11.3.5	- Open Database Connectivity (ODBC)

11.3.6 - SAML

11.4	Deverá suportar mecanismos de integração com plataformas externas recorrendo a protocolos de configuração, linguagens de modelação de dados ou interfaces de programação de aplicações (API) abertas para, por exemplo, permitir a automação e execução de ações e telemetria
------	---

12. Relatórios

12.1	Deve possuir um sistema de reporting integrado, com capacidade de gerar relatórios com registos de acessos de dispositivos terminais e autenticações de utilizadores, por calendarização e a pedido;
12.2	Deve poder gerar relatórios em formato PDF e CSV;
12.3	Deve poder gerar relatórios com campos customizados;
12.4	Deve poder exportar os relatórios para repositórios externos;
12.5	Deve poder criar relatórios recorrendo a filtros, para que apenas sejam apresentados os campos pretendidos;
12.6	Os relatórios deverão poder ser enviados por e-mail para endereços previamente configurados;

Plataforma Gestão (Switchs/APs)

1 Características gerais da Plataforma

1.1	Deve garantir a gestão unificada dos vários elementos da rede wired e wireless, tais como configurar, monitorar, manter e analisar o seu comportamento.
1.2	Deve ser constituída por equipamentos físicos, não sendo aceite uma plataforma que se baseie em serviços de cloud;
1.3	Deve ser redundante, formando um cluster, para garantir a resiliência da solução;
1.4	Deve possuir uma arquitetura escalável por adição de licenciamento à solução;
1.5	Deve ser centralizada, não devendo recorrer a sondas dispersas ao longo da rede;
1.6	Deve permitir a sua configuração inicial básica através de consola ou CLI (Telnet ou SSH);
1.7	Deve permitir ser configurada e gerida através de um GUI Web, acedido por HTTPS através de um navegador (browser);
1.8	Deve permitir configurar e gerir os serviços de autenticação e autorização;
1.9	Deve suportar IPv4, IPv6 e Dual Stack;
1.10	A gestão dos switchs e access points poderá ser realizada em plataformas diferenciadas ou na mesma plataforma.

2. Características da Plataforma

2.1	Deve ser constituída pelo menos por dois equipamentos idênticos. Caso a gestão dos switchs e AP seja efetuada numa única plataforma, a mesma deve ser constituída no mínimo por três equipamentos idênticos;
2.2	Deve ser implementada em bastidor (EIA standard 19 in.);
2.3	Deve ser fornecida com todos os acessórios de montagem em bastidor;
2.4	Deve possuir fontes de alimentação AC internas redundantes;
2.5	Deve ser fornecido com cabos de alimentação com fichas CEE 7/4 (Schuko) ou CEE 7/7.
2.6	Deve possuir uma porta de consola (RJ-45 ou USB);
2.7	Deve possuir uma porta de rede dedicada para gestão out-of-band (OOBM);

- | | |
|-----|---|
| 2.8 | Deve possuir duas portas de rede de serviço, com o suporte mínimo 1G/10G Base-T ou 10GE Base-SR , para o tráfego de serviço e tráfego de gestão; |
| 2.9 | As portas de serviço, referidas no ponto anterior, devem suportar LACP e poder ser ligadas a dois equipamentos distintos de um cluster de switches; |

3. Capacidade de elementos geridos

- | | |
|-----|--|
| 3.1 | Deve ter a capacidade para gerir pelo menos 100 switches; |
| 3.2 | Deve ter a capacidade para gerir pelo menos 250 APs e 2500 clientes; |
| 3.3 | Deve ter a capacidade de adicionar e gerir outros tipos de equipamentos, como por exemplo IoT; |

4. Funcionalidades

- | | |
|------|--|
| 4.1 | Deve permitir a definição de utilizadores e organizá-los em perfis e grupos, de acordo com as suas permissões. |
| 4.2 | Deve permitir organizar e representar a rede, recorrendo a uma estrutura de localizações geográficas, locais, edifícios, andares, dispositivos e ligações; |
| 4.3 | Deve permitir a automatização das operações na rede. |
| 4.4 | Deve permitir automatizar o processo de descoberta de dispositivos de rede, a sua inclusão e o seu aprovisionamento, bem como gerir o inventário; |
| 4.5 | Deve permitir definir perfis para enquadrar os equipamentos de rede e consolidar o conjunto de elementos a que têm de corresponder; |
| 4.6 | Deve permitir definir modelos de configuração a aplicar aos dispositivos de rede; |
| 4.7 | Deve disponibilizar fluxos predefinidos que permitam facilitar ou automatizar a realização de tarefas de implementação, configuração e manutenção. |
| 4.8 | Deve possuir os mecanismos necessários à manutenção e atualização do software dos dispositivos de rede garantido a sua conformidade. |
| 4.9 | Deve permitir definir quais as imagens de software aprovadas para cada tipo de dispositivo de rede e classificar essas imagens de acordo com a sua prioridade de utilização; |
| 4.10 | Deve permitir a descoberta de dispositivos terminais e a aplicação de políticas aos dispositivos de rede de acordo com grupos de perfis definidos; |
| 4.11 | Deve proporcionar uma administração baseada em políticas, permitindo que os administradores definam políticas que são traduzidas em configurações e aplicadas a todos os dispositivos de rede. |
| 4.12 | Deve permitir o uso de políticas para automatizar e acelerar a implementação de serviços; |
| 4.13 | Deve permitir a configuração dos equipamentos de rede, mas ao mesmo tempo permitir a configuração direta dos mesmos através de CLI, seja remotamente ou por consola. |
| 4.14 | Deve permitir que as configurações realizadas através de CLI sejam refletidas na plataforma de gestão. |
| 4.15 | Deve proporcionar visibilidade completa sobre a integridade e desempenho dos dispositivos de rede que permitam otimizar o seu funcionamento. |
| 4.16 | Deve proporcionar visibilidade completa sobre a integridade e desempenho da rede e o seu impacto nas aplicações e experiência do utilizador. |
| 4.17 | Deve permitir identificar os problemas que podem estar a afetar o desempenho da rede, determinar a sua causa e resolvê-los. |
| 4.18 | Deve monitorar o funcionamento dos dispositivos de rede. |
| 4.19 | Deve monitorar a conformidade das configurações dos dispositivos de rede para que sejam consistentes com as definições estabelecidas. |

4.20	Deve monitorar a conformidade do software nos dispositivos de rede para que as suas atualizações sejam realizadas atempadamente e de acordo com as políticas corporativas.
4.21	Deve apresentar eventos de acordo com uma classificação definida e com um conjunto de elementos relevantes.
4.22	Deve facilitar as atividades de identificação e resolução de problemas para que qualquer incidente possa ser resolvido rapidamente;
4.23	Deve possuir um conjunto amplo de relatórios predefinidos.
4.24	Deve permitir a adaptação dos relatórios predefinidos e a criação de novos relatórios.
4.25	Deve permitir a criação de relatórios a pedido e por agendamento prévio.
4.26	Deve permitir o agendamento periódico da criação e envio de relatórios por e-mail ou através da disponibilização de uma ligação para acesso através de um navegador (browser).
4.27	Deve suportar a disponibilização dos relatórios pelo menos em PDF e CSV.
4.28	Deve ter disponível um amplo conjunto de ferramentas para realizar tarefas necessárias às atividades de gestão da rede.
4.29	Deve ter disponível um amplo conjunto de ferramentas para planejar e executar alterações à rede.
4.30	Deve possuir uma extensa livreria de fluxos de tarefas predefinidos para realizar tarefas necessárias às atividades de gestão da rede.
4.31	Deve possuir mecanismos que permitam a identificação proativa de potenciais problemas.
4.32	Deve produzir e manter registos das atividades realizadas pelos utilizadores.
4.33	Deve permitir a integração com aplicações de terceiras partes para a automação de outros processos de TI.
4.34	Deve suportar APIs para permitir customizar e automatizar a integração com outras aplicações.

5. Licenciamento

- | | |
|-----|---|
| 5.1 | Deve ser apresentado o modelo completo de licenciamento aplicável à solução proposta. |
|-----|---|

Tipo de implementação das controladoras

A implantação das controladoras pode ser através de appliances físicas ou virtuais. No caso de a opção ser através de uma appliance virtual é da responsabilidade do proponente o fornecimento da solução chave na mão, ou seja, o fornecimento do hardware, do sistema de virtualização, do sistema operativo, do software da controladora e de qualquer outro componente de hardware ou software necessários ao funcionamento da solução, assim como de todos os licenciamentos aplicáveis, e o suporte e a manutenção dos mesmos, de acordo com os SLAs indicados no neste documento.

No caso de uma solução virtual, a redundância deverá ser considerada nos vários níveis, ou seja, hardware e sistema de virtualização.

As plataformas de Gestão de rede sem fios (WLC) e de gestão de (Switchs/APs) podem partilhar a mesma infraestrutura (física e/ou virtual). A plataforma de segurança (NAC) deve estar em infraestrutura completamente isolada das restantes plataformas.

4- Características técnicas – Cablagem e bastidores

No âmbito do procedimento deverão ser fornecidos, e instalados 2 bastidores, patch panel de fibra, Patch panel de cobre com um mínimo de 24 portas, cabo fibra ótica, cabo Ethernet e todos os outros componentes e acessórios considerados necessários pelo proponente para a execução do projecto na integra.

Na generalidade dos locais a intervenção nos bastidores incluirá a instalação de um patch panel para as novas ligações por cobre e a substituição do switch.

Os equipamentos ativos substituídos deverão ser agrupados e entregues ao IAPMEI em local a indicar.

Em Lisboa será instalado um novo bastidor (a fornecer neste projeto), no piso 1 do edifício A, tem como objeto a instalação dos novos switches e os patch panel de FO e cobre para as ligações ao novos APs.

Em Coimbra o bastidor existente será substituído por um novo (a fornecer neste projeto), sendo de considerar a instalação de patch panel de cobre (retirados de outro bastidor) e o fornecimento de um patch panel novo onde terminarão os cabos a passar para os novos APs, e ainda cabos a retirar de um outro patch panel (retirados de outro bastidor). Serão aqui instalados os novos equipamentos ativos.

Nas intervenções nos bastidores devem ser incluídos todos os acessórios considerados necessários (incluindo os de outros tipos não referenciado neste documento) para a ligação dos equipamentos e a melhor organização dos bastidores. Estes acessórios deverão garantir a melhor performance dos equipamentos.

Os bastidores existentes são de 19in.

Os cabos de cobre a instalar para a ligação entre os bastidores e os access points deverão terminar numa tomada.

Em Lisboa, já estão instalados alguns Access Points, que serão para remover no âmbito deste procedimento. A sua localização poderá ser mantida caso seja considerada a mais adequada para a nova solução. Mesmo nestes casos pretende-se a troca da cablagem existente.

Embora a quantidade de access points a adquirir seja de 205, e que já exista uma previsão da distribuição de access points a instalar por cada local, deve ser prevista a realização de site survey de modo a identificar os melhores locais para a instalação dos equipamentos.

A instalação dos cabos e as intervenções nos armários bastidores podem ser iniciadas logo após a celebração do contrato. O horário laboral para as intervenções deve ser considerado nos dias úteis das 9h00 às 17h30. As atividades inerentes à implementação que sejam considerados críticos às atividades do IAPMEI, por remoção/instalação de ativos ou por criação/alteração de ligações, deverão ser efetuadas em horário pós-laboral, previamente acordado com o IAPMEI. Devem ser considerados trabalhos com impacto na atividade aqueles que: Impliquem paragens no Datacenter e no Campus de Lisboa.

Na instalação dos cabos devem, sempre que possível utilizados os caminhos de cabos já existentes. Quando não for possível, devem ser sempre presentes a não degradação do aspeto estético das paredes, optando por soluções com mínimo impacto visual e prevendo a utilização de esteira armada ou calha técnica para a passagem dos cabos.

A instalação dos cabos deve ser feita por técnicos especializados, utilizando ferramentas adequadas e respeitadas todas as boas práticas da instalação dos cabos, como por exemplo: respeitar os afastamentos aos cabos de energia, respeitar o raio de curvatura mínimo, cuidados na fixação, marcações dos cabos.

Em Lisboa, o IAPMEI utiliza vários edifícios do campus, sendo necessário a passagem de novas/substituição fibras óticas entre os vários bastidores. No Porto também será necessário a passagem de novas/substituição da fibra ótica entre os dois bastidores.

Após a instalação das redes em cada um dos vários locais, deve ser feita uma certificação segundo a Cat.6A, todas as certificações deverão ser apresentadas em formato digital. Deverão ser também entregues plantas, com as marcações dos pontos terminais e os caminhos de cabos. Deverá ser entregue um certificado de garantia da rede de dados.

Quadro de característica base para cablagem e bastidores

1.	Cabo ethernet
1.1	Cabo Categoria 6A ou superior S/FTP
1.2	Revestimento com classificação LSZH
1.3	Resistência ao fogo de acordo com as normas IEC 60332-3-22 respeitando a norma EN50575 CPR – Dca
1.4	Resistente a interferências eletromagnéticas externas
1.5	Suportar 10GBase-T
1.6	Suportar Power Over Ethernet (PoE), Power Over Ethernet Plus (PoE+) e Power Over Ethernet Plus Plus(PoE++).
2.	Cabo de fibra ótica
2.1	Cabo com 8 fibras
2.2	Monomodo (OS2)
2.3	Força de tração $\geq 1500N$
2.4	Revestimento com classificação LSZH
2.5	Resistência a roedores (glass-yarns ou blindagem a aço)
2.6	Alta resistência a tensão
2.7	Resistência à água e humidade
3.	Bastidores
3.1	Tipo: Pavimento
3.2	Dimensões: 19in, 800x800
3.3	Porta frontal e meias portas na traseira perfuradas
3.4	1 (uma) prateleira de fixação frontal e posterior
3.5	Organizador de cabos vertical
3.6	Paneis laterais removíveis
3.7	2 réguas de 8 tomadas SCHUKO, Interruptor e proteção contra sobretensão
3.8	2 ventiladores com capacidade de ventilação $\geq 50 \text{ m}^3/\text{hora}$.
4.	Pacth panel de fibra ótica
4.1	Altura: 1U
4.2	Fixação: 19in

4.3 Tipo de conector: LC

5. Pacht panel de cobre

5.1 Altura: 1U

5.2 Fixação: 19in

5.3 Categoria 6A ou superior

5.4 Mínimo 24 portas RJ45

6. Pacht cord de cobre RJ45

6.1 Categoria 6A ou superior

6.2 Revestimento com classificação LSZH

7. Pacht cord de fibra ótica

7.1 Revestimento com classificação LSZH

8. Ensaio e Certificação

8.1 Após a instalação da infraestrutura de cablagem estruturada, este deverá ser etiquetada, ensaiada e certificada conforme Cat.6A;

8.2 Devem ser entregues plantas com o caminho dos cabos e a localização dos access points

9. Requisitos para serviços de instalação e montagem

9.1 A instalação de caminhos de cabo, cablagem, tomadas e repartidores deverá ser feita de acordo com as normas e as boas práticas de instalação;

9.2 O lixo gerado durante a intervenção deve ser retirado ao final do dia de trabalho

9.3 Toda a cablagem substituída deve ser removida em toda a sua extensão;

5- Mapas de quantidades

Mapa de quantidades de equipamentos ativos a fornecer

Tipo 1	Tipo 2	Tipo 3	Tipo 4	Tipo 5	Access Point
2	2	6	7	23	205

Mapa de mínimas quantidades de controladoras/plataformas a fornecer

Plataforma de gestão Switch / AP	NAC	WLC
2	2	2

No caso da plataforma de gestão e controladora WLC sejam suportadas pelo mesmo hardware (servidor) devem ser considerados 3 equipamentos. Esta condição não se aplica caso sejam propostas *appliances* físicas.

Mapa de quantidades e distribuição de Switchs por bastidor

Local	Rede	Tipo 1	Tipo 2	Tipo 3	Tipo 4	Tipo 5
Lisboa - Data Center	Core	2				
	Firewall		2			
	Servidores			2		
	Desenvolvimento			2		
	WAN – Operador			2		
Lisboa - Rede	Edifício A				5	
	Edifício L1				2	
	Edifício L2					2
	Edifício D					1
	Palacete					1
	Portaria					1
Porto	Bastidor 1					3
	Bastidor 2					2
Coimbra	Bastidor 1					3
Viana do Castelo	Bastidor 1					1
Braga	Bastidor 1					1
Bragança	Bastidor 1					1
Viseu	Bastidor 1					1
Aveiro	Bastidor 1					1
Guarda	Bastidor 1					1
Covilhã	Bastidor 1					1
Leiria	Bastidor 1					1
Évora	Bastidor 1					1
Faro	Bastidor 1					1
TOTAL		2	2	6	7	23

Mapa de quantidades de stack a implementar por bastidor

Sempre que exista mais que um s

Local	Rede	Nº de Stacks
Lisboa - Data Center	Core	1
	Firewall	1
	Servidores	1
	Desenvolvimento	1
	WAN – Operador	1
Lisboa - Rede	Edifício A	2
	Edifício L1	1
	Edifício L2	1
	Edifício D	
	Palacete	
Porto	Portaria	
Porto	Bastidor 1	1
	Bastidor 2	1
Coimbra	Bastidor 1	1
Viana do Castelo	Bastidor 1	
Braga	Bastidor 1	
Bragança	Bastidor 1	
Viseu	Bastidor 1	
Aveiro	Bastidor 1	
Guarda	Bastidor 1	
Covilhã	Bastidor 1	
Leiria	Bastidor 1	
Évora	Bastidor 1	
Faro	Bastidor 1	

Nota: Em Lisboa – Rede, Edifício A, será 2 stack, um com 2 switchs e outro de 3 switchs.

Mapa de previsão de quantidades de Access Points por local de instalação e piso.

Local	Rede	Número de AP
Lisboa	Edifício A Piso 3	11
	Edifício A Piso 2	15
	Edifício A Piso 1	18
	Edifício A Piso 0	15
	Edifício A Piso -1	3
	Edifício L Piso 1	9
	Edifício L Piso 0	47
	Edifício L Régie	1
	Edifício D	3
	Palacete	4
Porto	Piso 0	10
	Piso 1	8
Coimbra	Piso 1	5
	Piso 4	5
Viana do Castelo		5
Braga		4
Bragança		6
Viseu		3
Aveiro		7
Guarda		6
Covilhã		2
Leiria		6
Évora		6
Faro		6
TOTAL		205

Em sede de projeto, poderá verificar-se a necessidade da quantidade de APs a instalar por local ser diferente sendo possível fazer ajustes de quantidades entre locais. O Número total de APs a fornecer é de 205.

Mapa de previsão de quantidades de Access Points por bastidor

Local	Rede	Número de AP
Lisboa	Edifício A Bastidor	62
	Edifício L Bastidor 1	42
	Edifício L Bastidor 2	15
	Edifício D	3
	Palacete	4
Porto	Bastidor 1	14
	Bastidor 2	4
Coimbra	Bastidor 1	10
Viana do Castelo	Bastidor 1	5
Braga	Bastidor 1	4
Bragança	Bastidor 1	6
Viseu	Bastidor 1	3
Aveiro	Bastidor 1	7
Guarda	Bastidor 1	6
Covilhã	Bastidor 1	2
Leiria	Bastidor 1	6
Évora	Bastidor 1	6
Faro	Bastidor 1	6
TOTAL		205

Mapa de previsão de quantidades de cablagem

Tipo de cabo	Quantidade	Observações
Cabo Ethernet cat 6A	8 000 metros	Ligação entre aps e switchs
Cabo de FO (8 fibras)	4 500 metros	<p>Em Lisboa entre:</p> <ul style="list-style-type: none"> • Datacenter e Bastidor Edifício A • Datacenter e Bastidor1 Edifício L • Datacenter e Bastidor 2 Edifício L (caminho diferente da ligação anterior) • Bastidor 1 e Bastidor 2 do Edifício L • Datacenter e Bastidor Edifício D <p>Porto entre:</p> <ul style="list-style-type: none"> • Bastidor 1 e Bastidor 2 <p>Todas a ligações com 2 cabos?</p>

Mapa de quantidades de Patch cords e transceivers/SFPs

Tipo	Quantidade	Observações
Patch Cord Cobre RJ45 0.5m	220 unidades	Para ligação dos AP's e as tomadas
Patch Cord Cobre RJ45 2m	220 unidades	Para ligação dos AP's nos bastidores ao switchs
Patch Cord Cobre RJ45 5m	40 unidades	Para o DataCenter
Patch Cord Cobre RJ45 10m	40 unidades	Para o DataCenter
Patch Cord FO 2m	40 unidades	Para o DataCenter
Patch Cord FO 10m	8 unidades	Para o DataCenter
Transceivers óticos mono modo de 10 GbE	24 unidades	Para a totalidade das portas dos switchs tipo 1
Transceivers óticos mono modo de 10 GbE	48 unidades	Para a ligação entre bastidores

Todos os patch cord cobre RJ45 deverão ser da mesma cor;

Todos os patch cord de FO devem ser da mesma cor (pode ser diferente da cor dos patch cords de FO)

Exclui-se nestas quantidades os componentes necessários para as construções dos stacks

Bastidores e acessórios

O bastidor a instalar em Coimbra é de 32U, o bastidor a instalar em Lisboa no Edifício A é de 42U.

Todos as fibras óticas a instalar deverão terminar em painel.

Todos os cabos de cobre a instalar deverão terminar em painel no bastidor e em tomada junto ao AP a ligar.

Os bastidores existentes são de 19in.

Além dos painéis e tomadas, devem ser incluídos todos os patch cables (cobre e fibra ótica) e todos os outros acessórios e componentes, de forma a garantir o funcionamento da solução proposta.

6 – Prazos, locais de entrega, serviços e garantia

Prazos

- **Entrega de equipamentos ativos** – para a entrega dos equipamentos ativos o prazo máximo é de 60 dias contínuos (correndo em sábados, domingos e feriados) sendo o local de entrega inicial de todos equipamento ativos nas instalações do IAPMEI em Lisboa.
- **Implementação** - Deverá ser garantida a implementação (instalação e configuração) em todos os locais, de todos os novos componentes da solução nos diversos locais indicados no prazo de 100 dias contínuos (correndo em sábados, domingos e feriados).

Serviços de instalação

Deverão ser contemplados todos os serviços de instalação e configuração de todos os componentes a fornecer, bem como os serviços de migração necessários para a transição da atual solução para a nova. O projeto não deverá exceder 100 dias contínuos (correndo em sábados, domingos e feriados) e deverá contemplar um gestor de projeto.

- **Gestão de Projeto** - Deverá ser nomeado um Gestor com experiência em projetos de natureza similar. O Gestor de Projeto terá a responsabilidade de coordenação e acompanhamento de todo o projeto, garantindo a integração dos seus diversos componentes e a ausência de falhas de comunicações.
- **Configuração e distribuição dos equipamentos ativos** – Todos os equipamentos ativos devem ser configurados e testados nas instalações do IAPMEI em Lisboa. A distribuição dos equipamentos pelos vários locais para instalação é da responsabilidade do proponente.
- **Implementação** - Deverá ser garantida a implementação (instalação e configuração) de todos os novos componentes da solução nos diversos locais indicados no prazo de 100 dias contínuos (correndo em sábados, domingos e feriados). Todas as despesas de deslocação e estadias entre as diversas localizações, ficam ao encargo do proponente. A instalação do equipamentos ativos e entrada em produção em cada um dos locais deve ser calendarizado em sede projeto.
- **Migração** - Deverá ser assegurar o levantamento da infraestrutura e das configurações existentes nos atuais equipamentos (a substituir da marca Avaya/Cisco), assegurando assim a otimização da migração para a nova solução. Todo o processo de migração será previamente avaliado e planeado, em conjunto com o IAPMEI, assegurando-se que, em caso de necessidade de paragem dos sistemas, esta ocorra no menor tempo possível e em horário a definir com o IAPMEI, podendo ser necessário considerar trabalhos em horário pós-laboral.
- **Formação** - Deverá ser assegurada a transmissão de conhecimento através de formação “on-job” relativamente aos equipamentos envolvidos, para a equipa técnica do IAPMEI.
- **Documentação** - Deverá ser disponibilizado um dossier do projeto que incluirá o detalhe da solução implementada, bem como o relatório da instalação, num prazo máximo de 15 dias contíguos após o final da implementação.

Garantia

Os equipamentos ativos devem possuir garantia válida durante todo o seu tempo de vida. O tempo de vida é definido e anunciado pelo fabricante com cinco anos de antecedência.

Em caso de avaria, os equipamentos devem ser substituídos ao abrigo da garantia, sendo o prazo de:

- 1 dia útil para os equipamentos tipo 1, 2, 3 e controladoras;
- 2 dias uteis para os restantes equipamentos.

Serviços de suporte

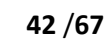
Todos os equipamentos e acessórios fornecidos deverão estar cobertos por um serviço de suporte com as seguintes características mínimas:

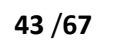
- 3 anos de suporte 7dias x 24horas com 4 horas para início da intervenção;
- O serviço de suporte deve incluir a substituição dos equipamentos em:
 - 1 dia útil para o equipamento do tipo 1, 2, 3 e controladoras
 - 2 dias uteis para os restantes tipos de equipamentos
- O suporte é prestado pelo proponente sendo este o responsável de toda a interação com o fabricante

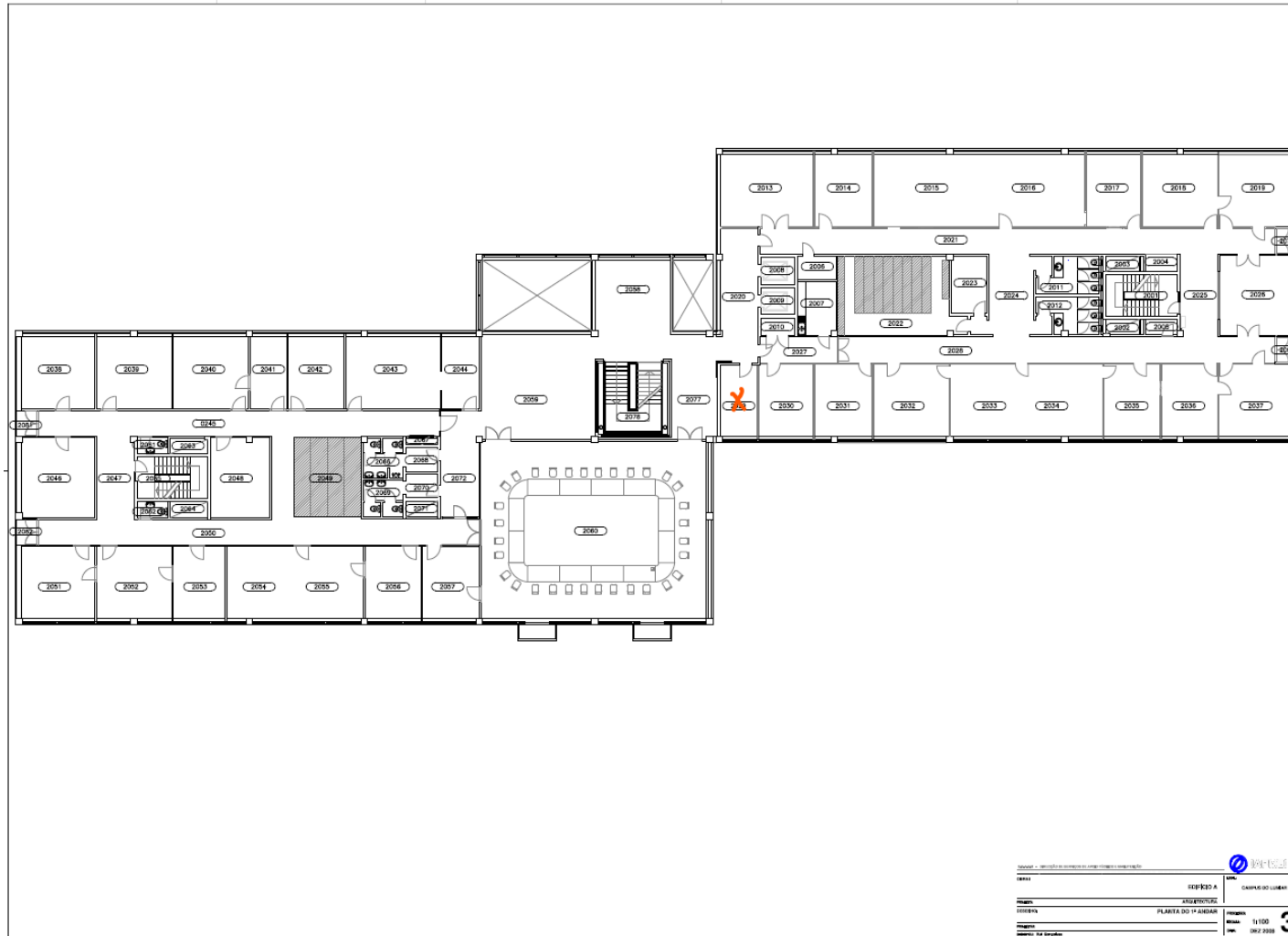
Serviços de apoio à exploração

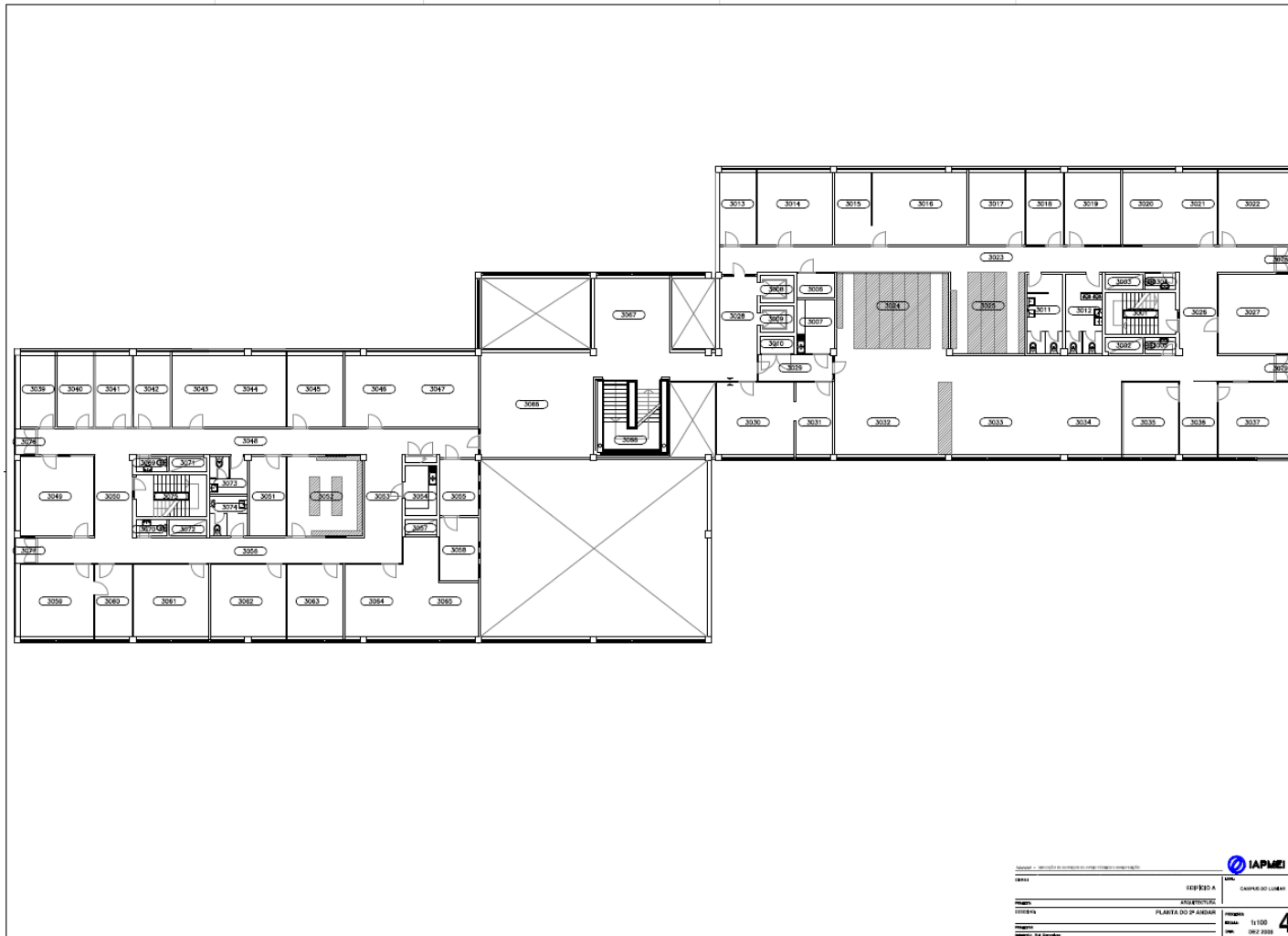
Deve ser incluído uma bolsa de 75 horas para apoio à exploração da solução com uma validade de 36 meses.

.

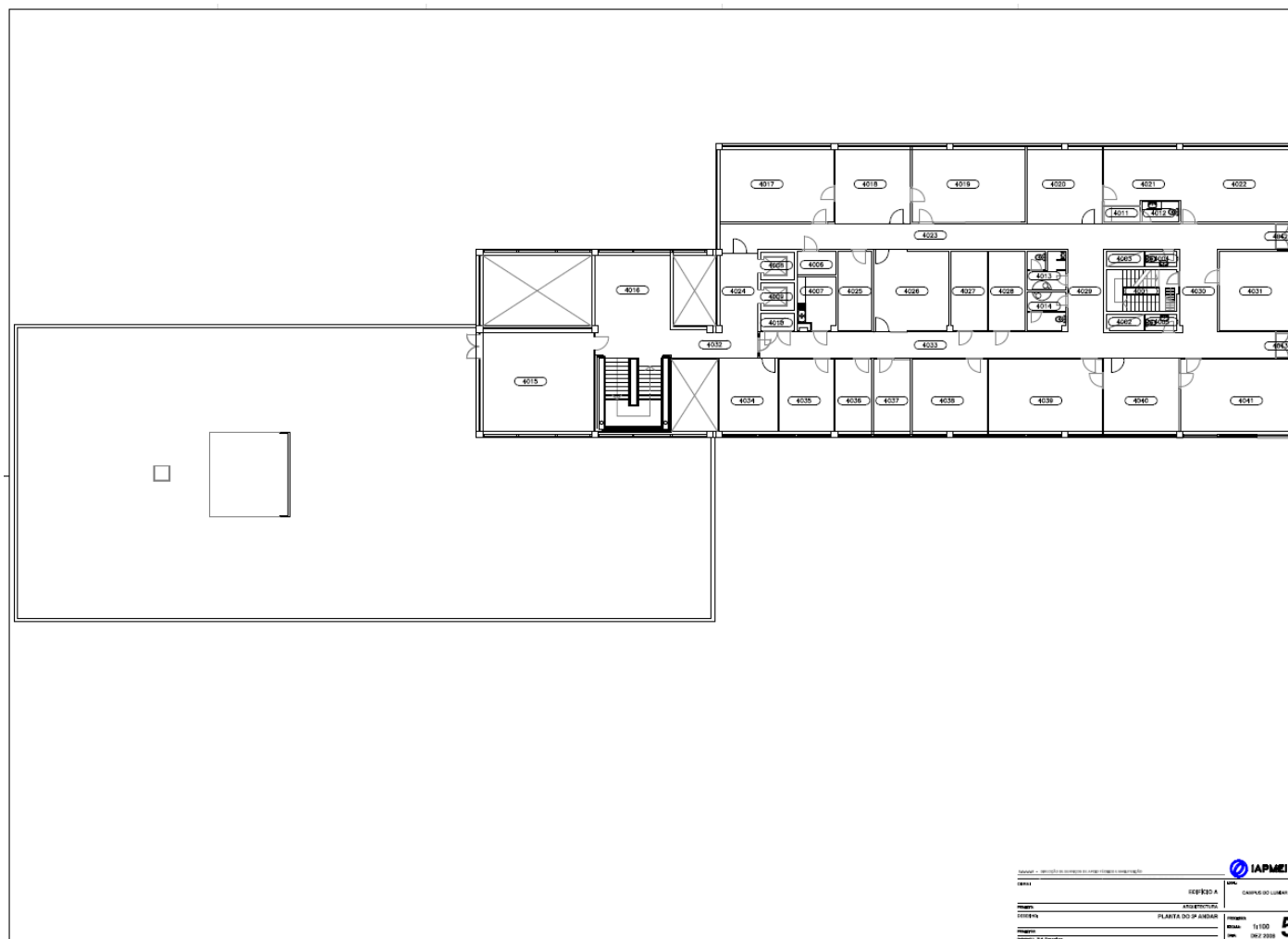


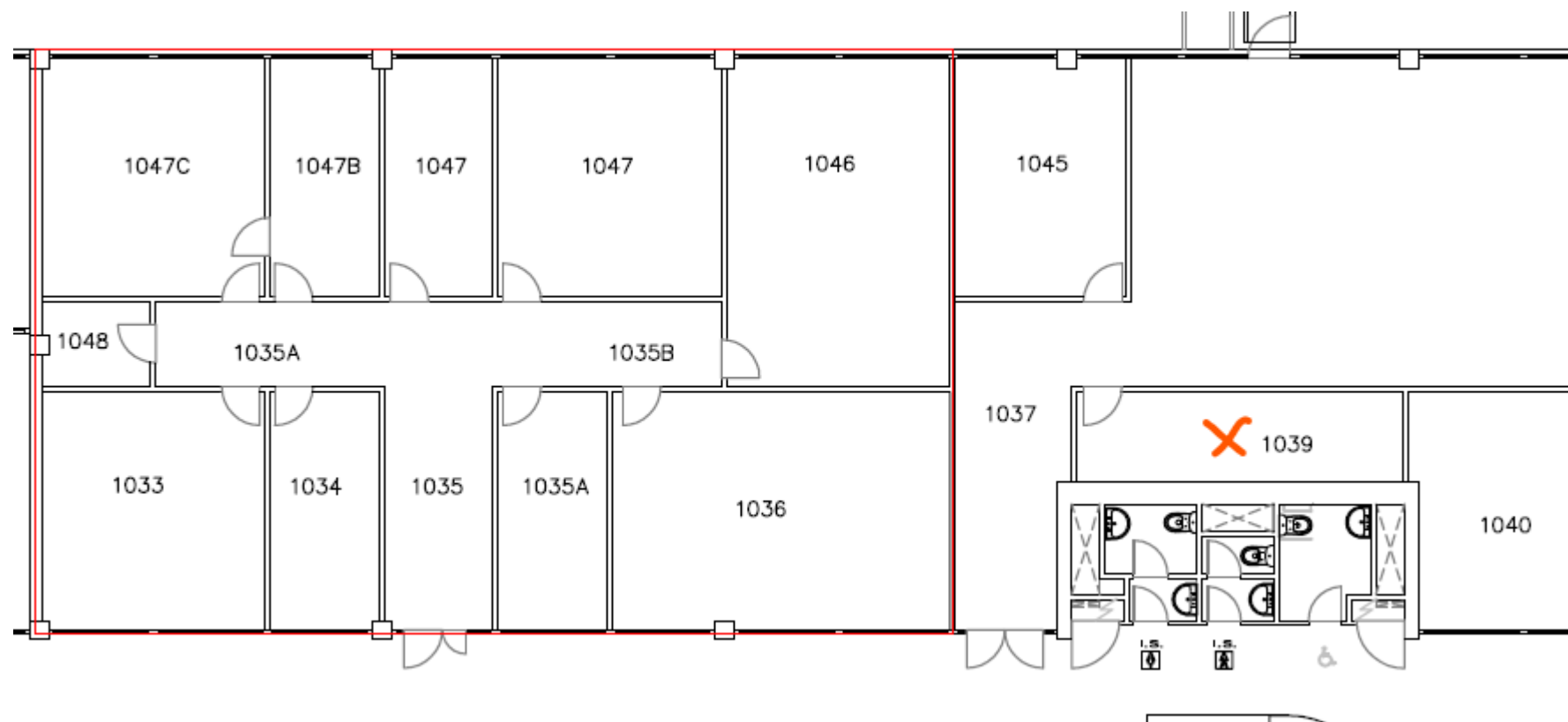


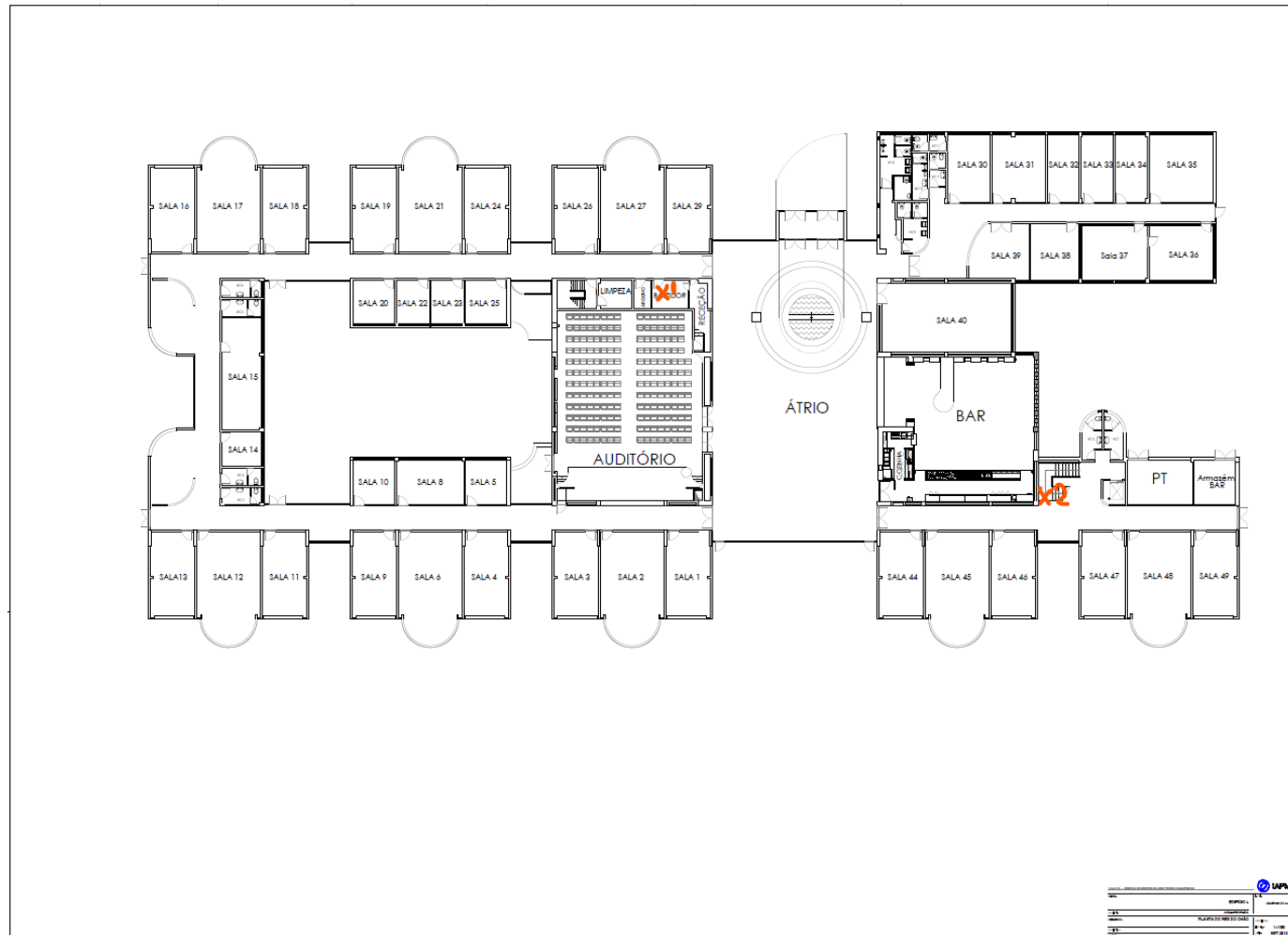


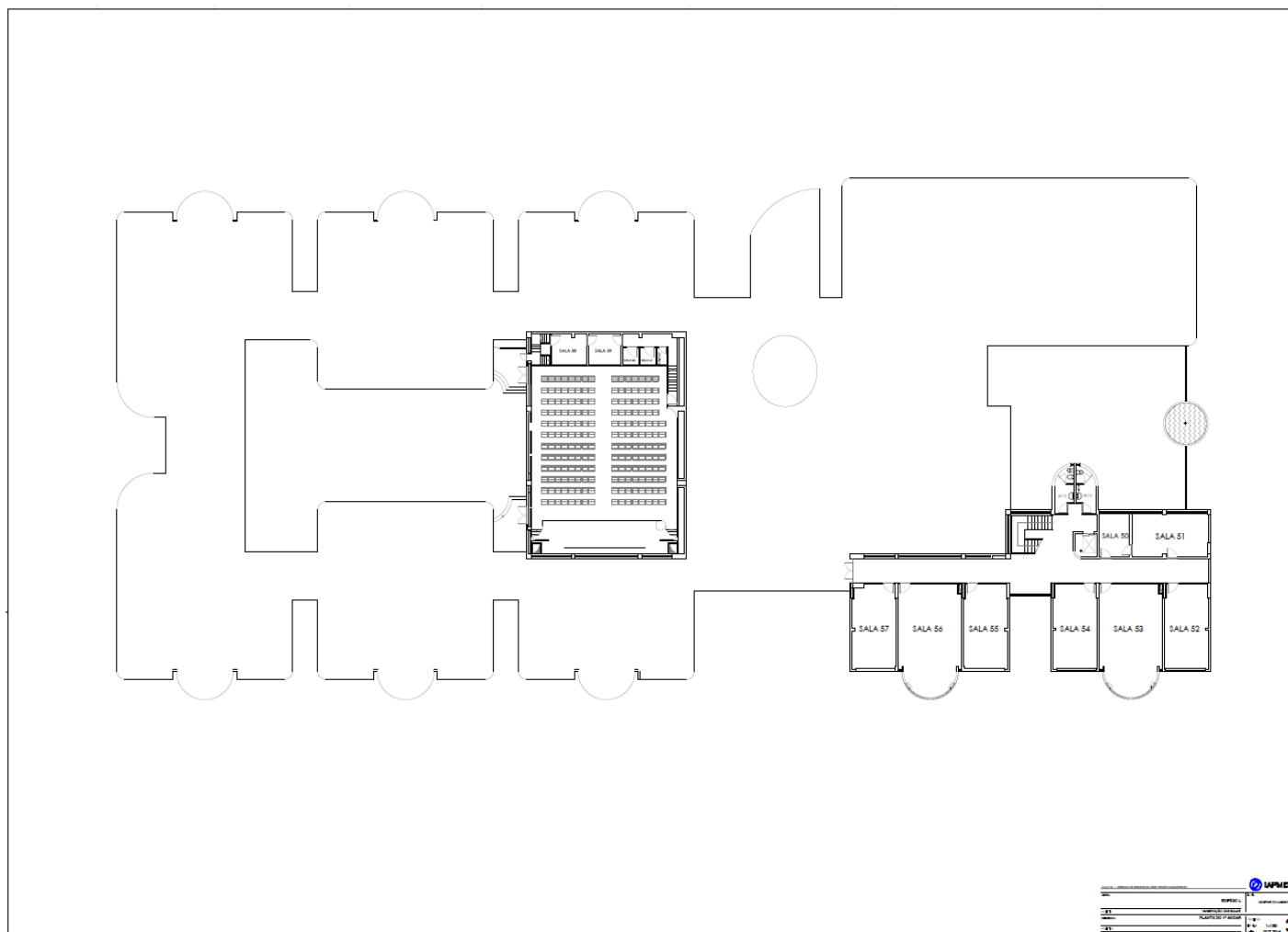


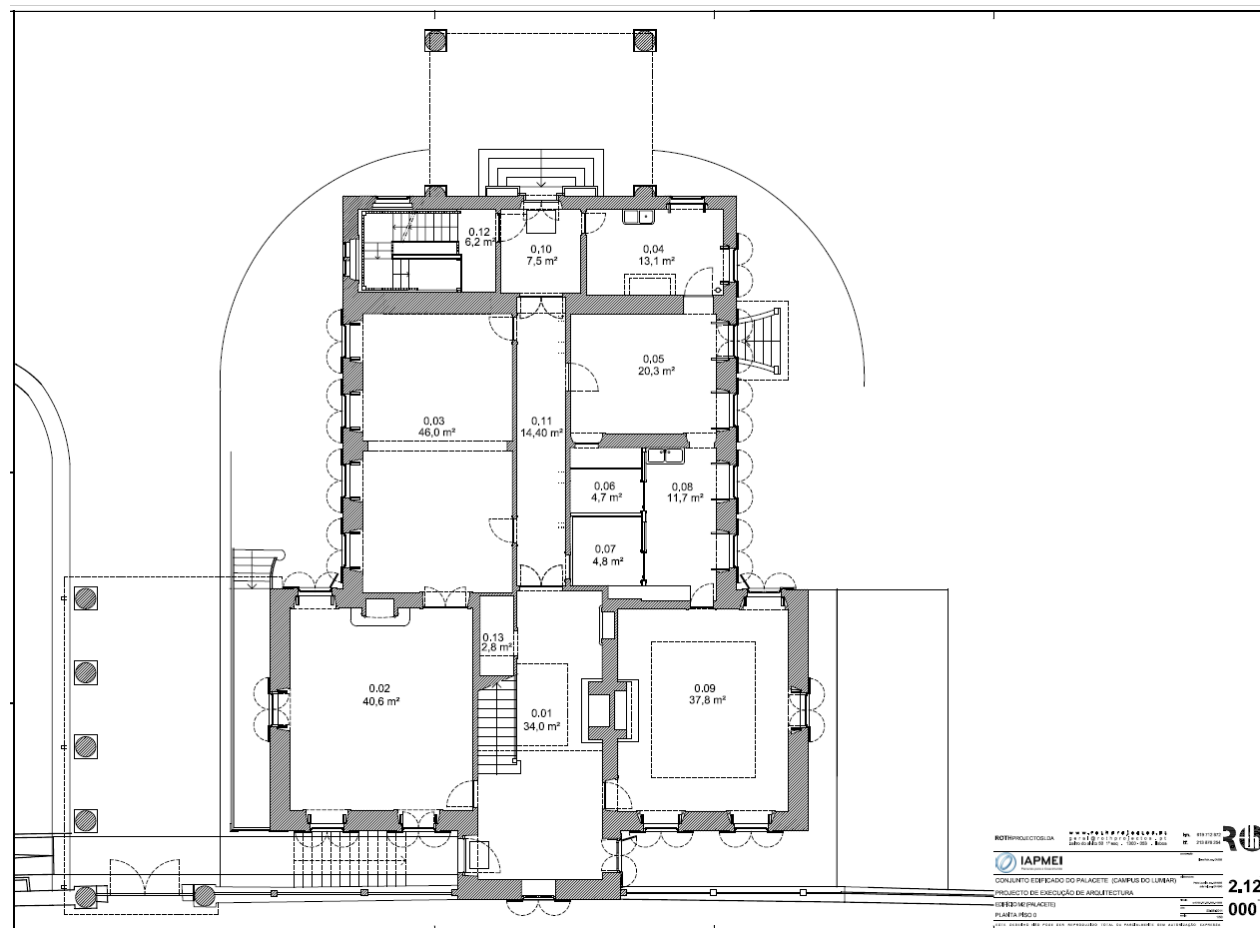
IAPMEI	
EDIFÍCIO A	CAMPUS DE LISBOA
PLANTA DO 2º ANDAR	
PROJEÇÃO	1:100
DATA	09/2008
4	

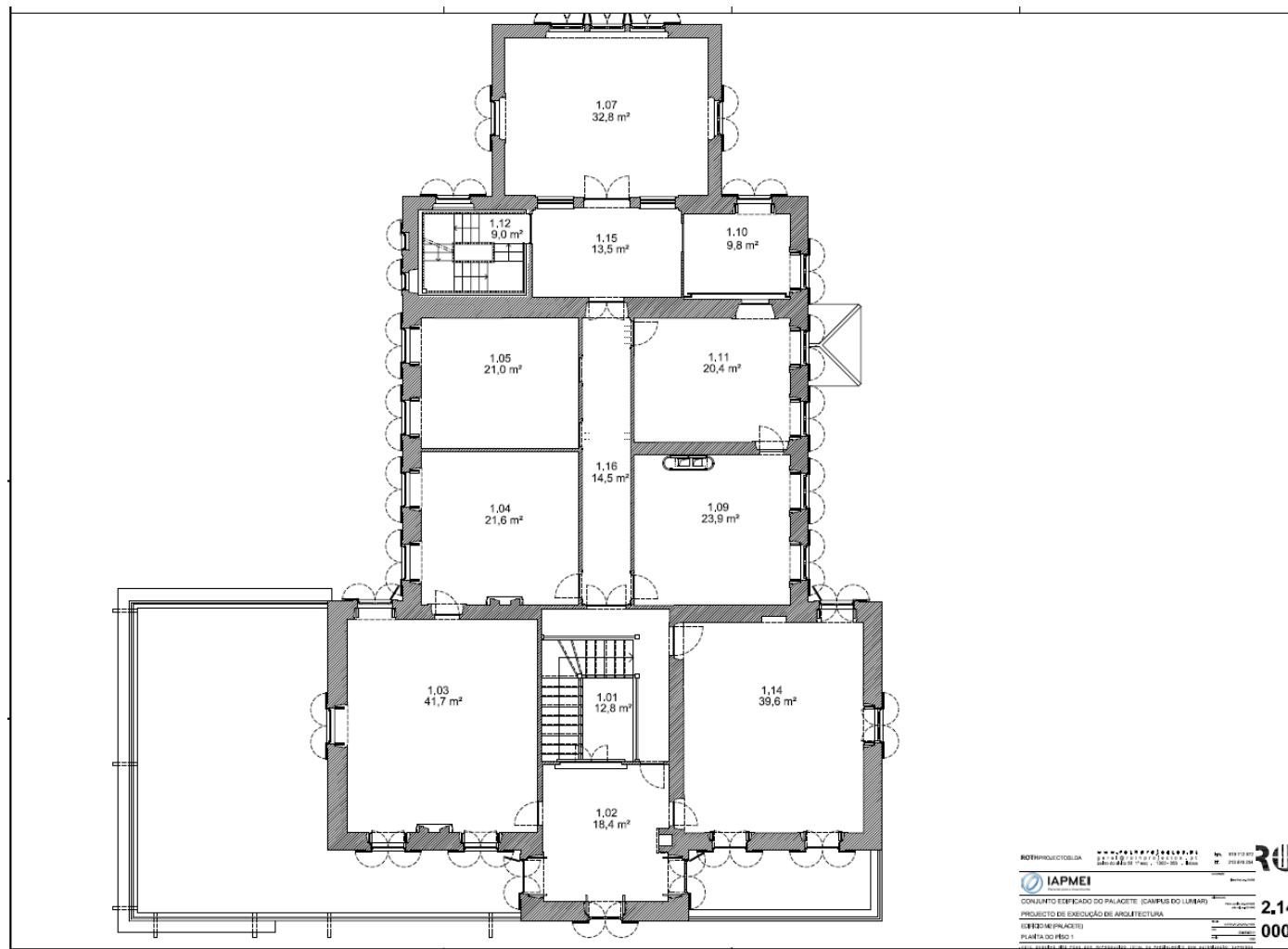






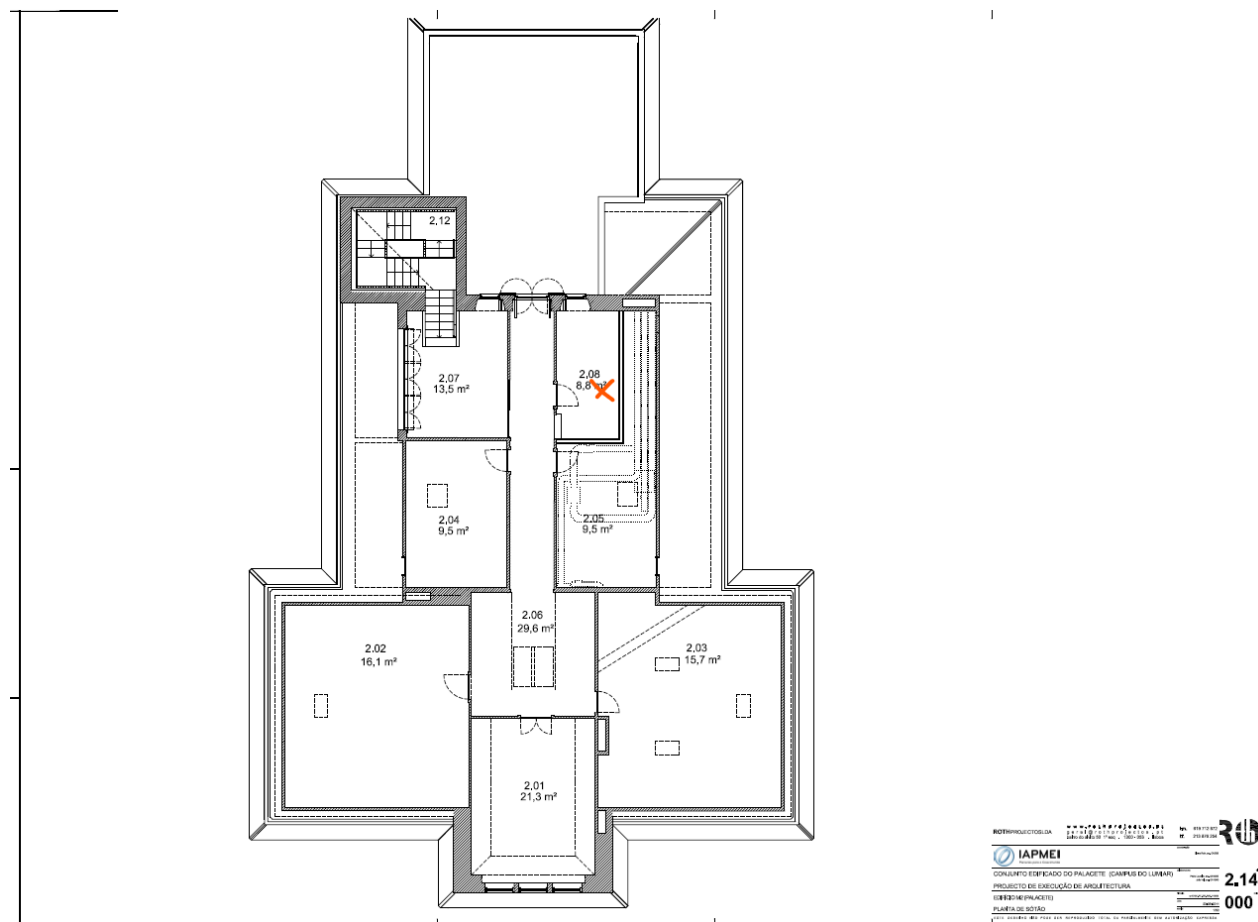


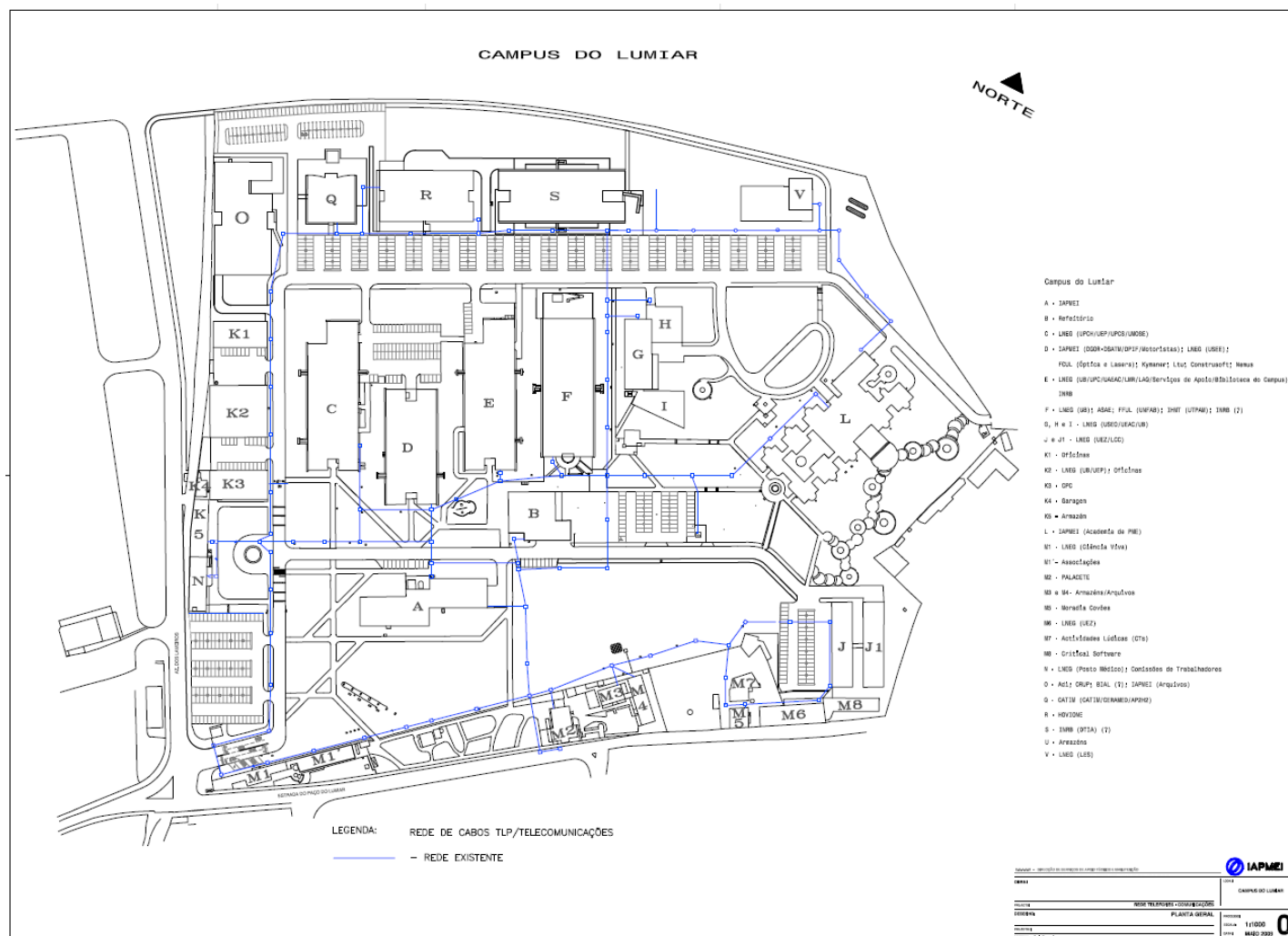




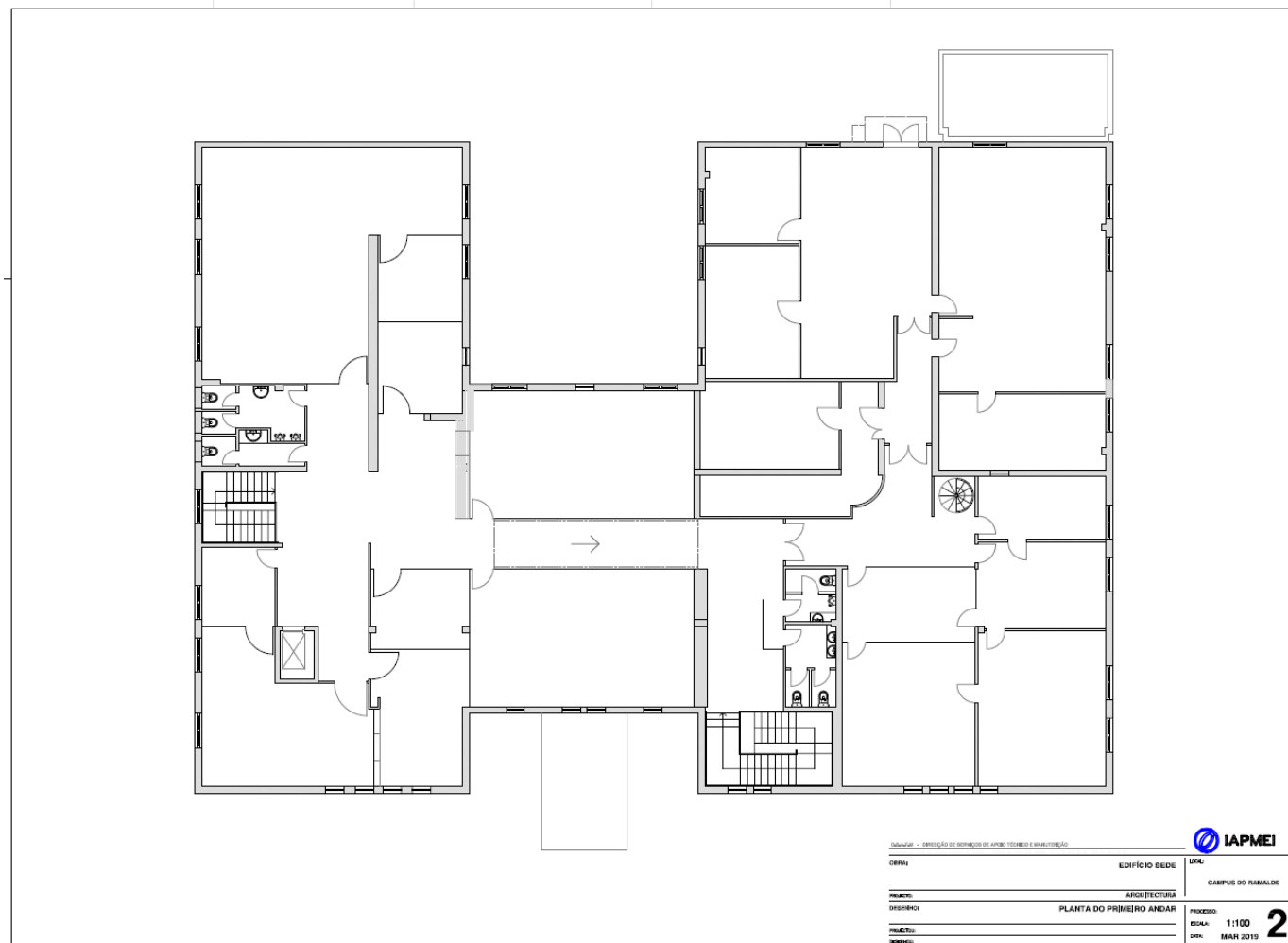
Lisboa – Palacete – Sotão

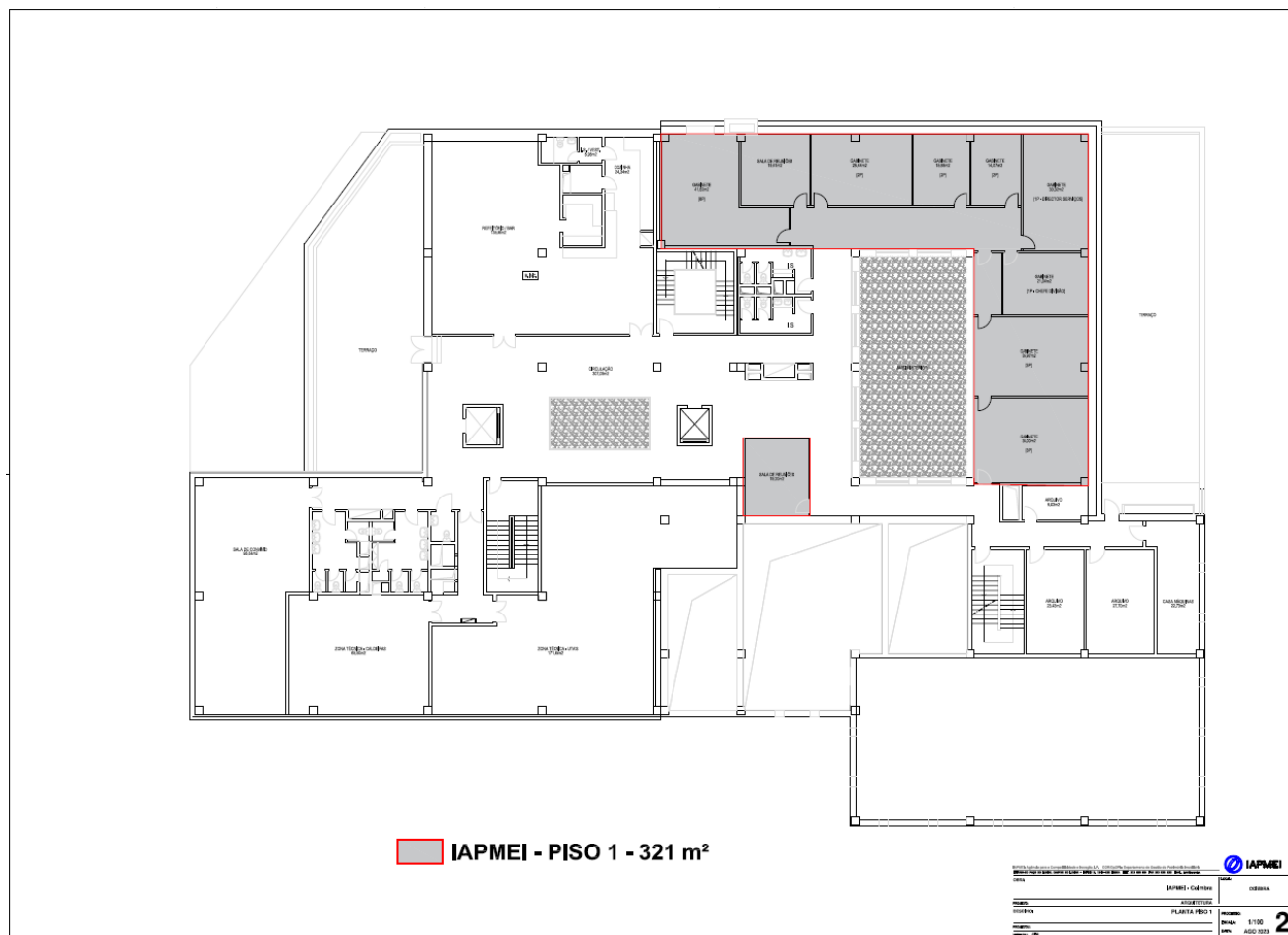
X marca local de bastidor.





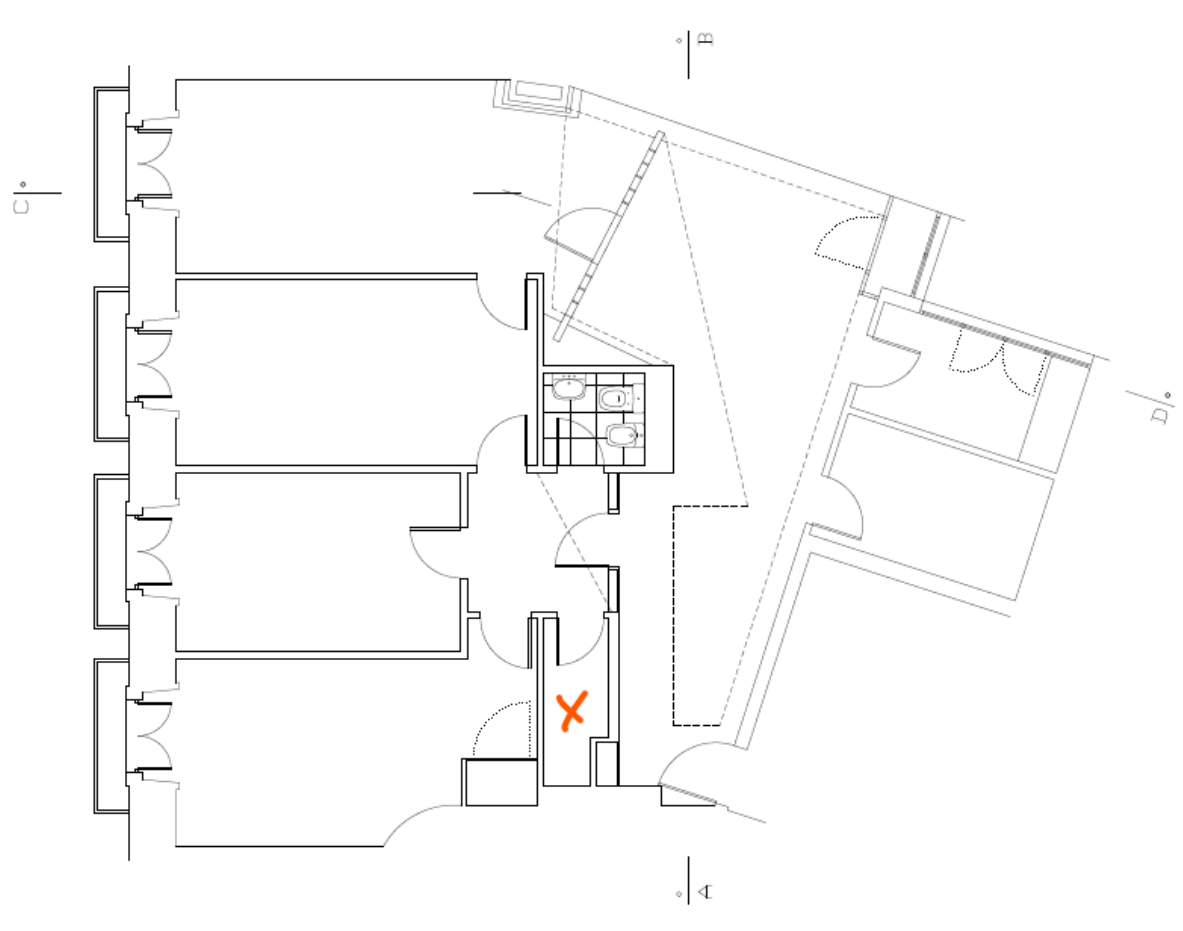




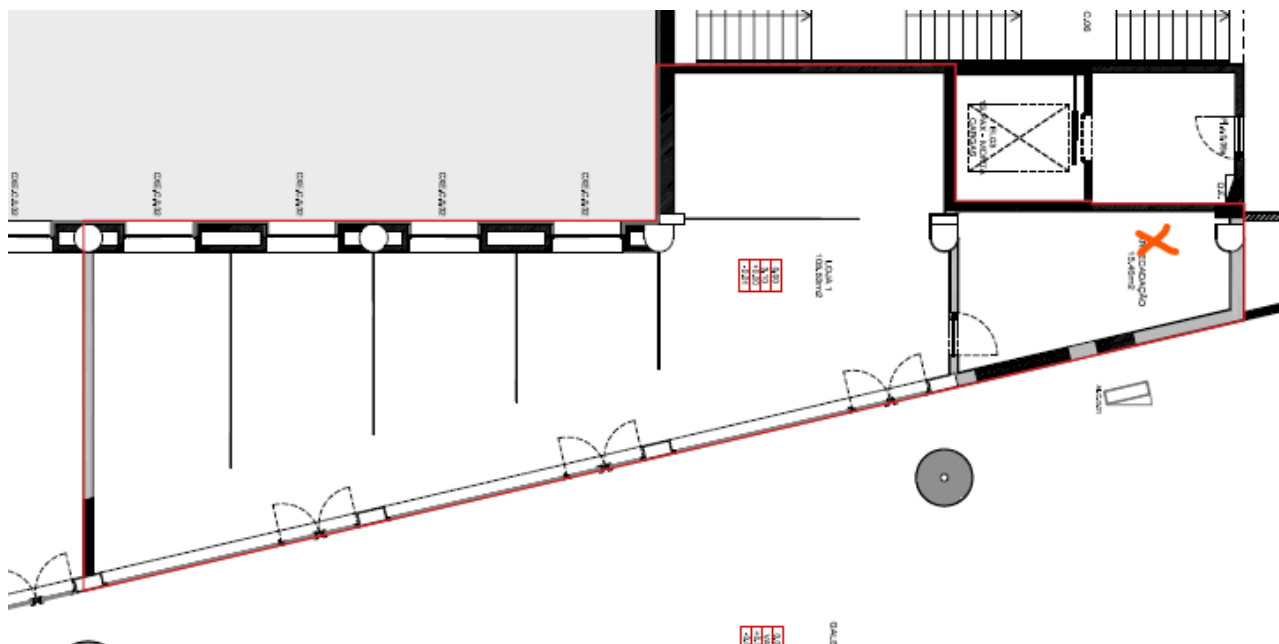


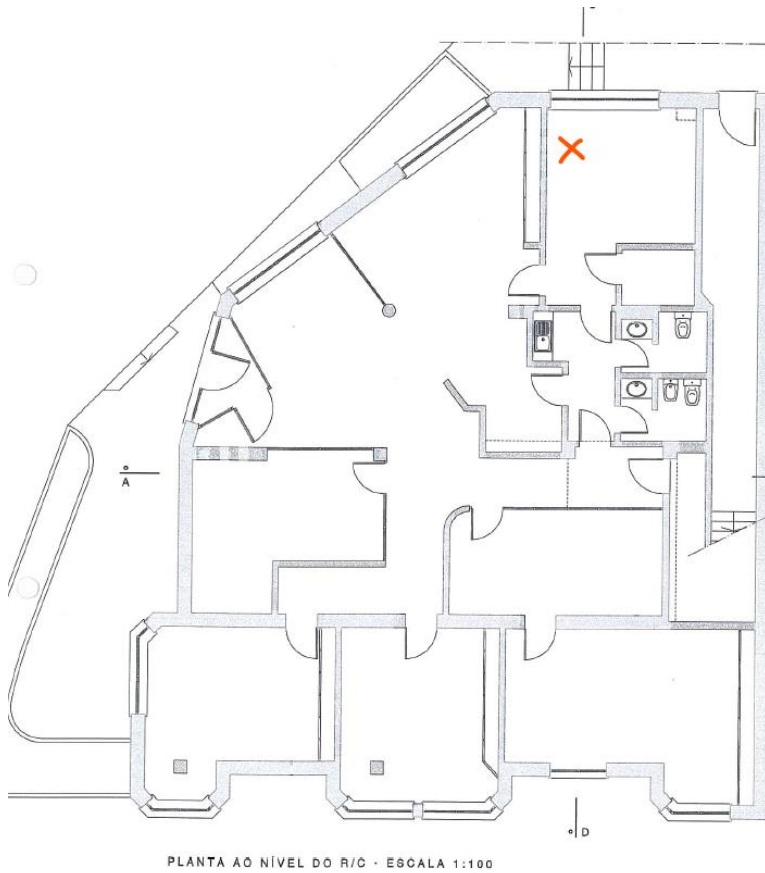
Viana do Castelo

X marca o local do bastidor.



X marca o local do bastidor.





ARQUITECTURA		CONCEIÇÃO MACEDO-DANTE MACEDO-JOSÉ AFONSO	
PROJETO		PROJETO DE RECONSTRUÇÃO DO BARRAQUEAMENTO DA 1.ª BATTALHÃO DA 1.ª DIVISÃO DE BRAGANÇA	
CLIENTE		MINISTÉRIO DA ECOLOGIA	
TÍTULO		- planta ao nível do 2.º andar	
AUTOR		01	
DATA		1.1.2000	

Viseu

X marca o local do bastidor.



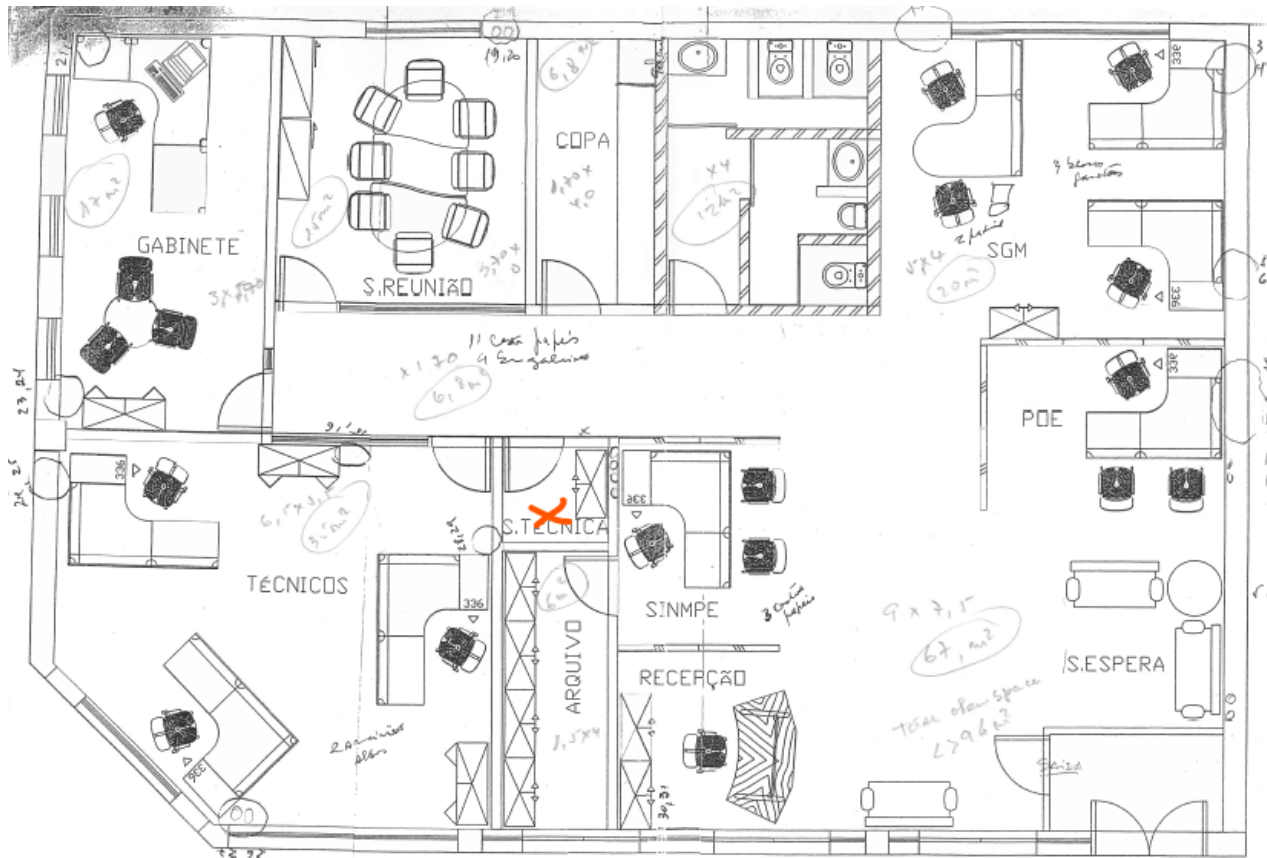
The floor plan shows a building layout with various rooms and corridors. The dimensions are as follows:

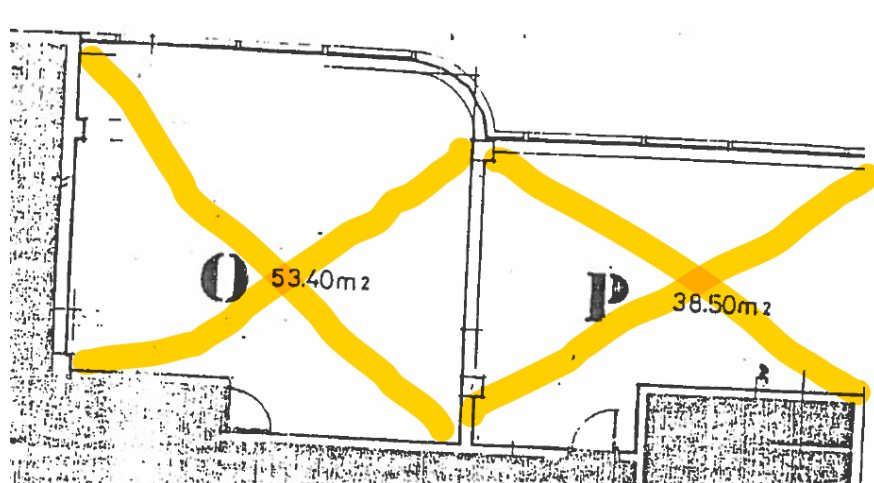
- Top-left room: 11.32 (width) x 5.45 (height)
- Top-right room: 5.45 (width) x 3.40 (height)
- Bottom-left room: 4.32 (width) x 4.30 (height)
- Bottom-right room: 4.20 (width) x 7.05 (height)
- Central corridor: 3.90 (width) x 1.68 (height)
- Small room above corridor: 1.10 (width) x 1.72 (height)
- Small room to the right of corridor: 0.95 (width) x 1.68 (height)

The total area is calculated as 255,60 m², with the label "I.A.P.M.E.I." written in red. An orange 'X' is marked in the bottom-left room.

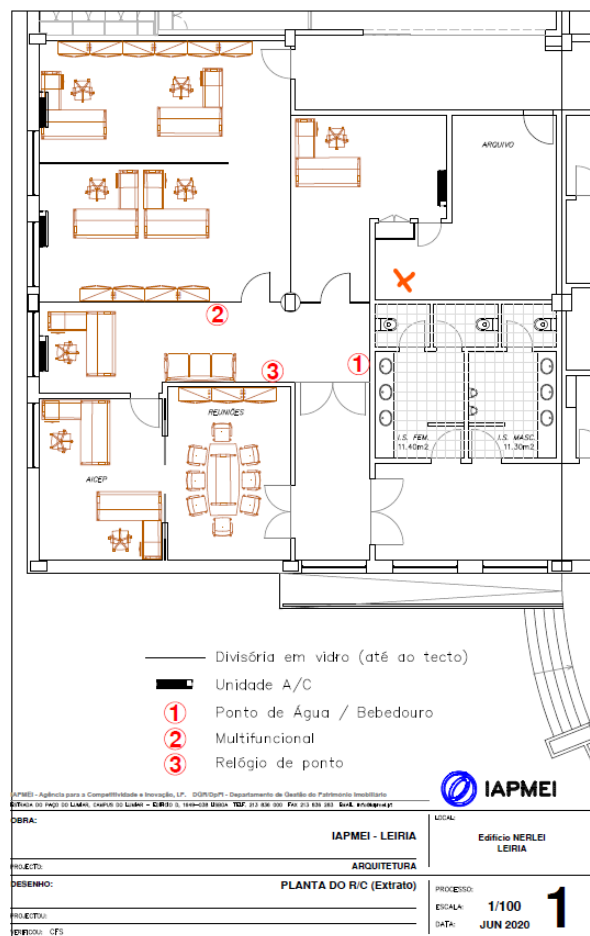
Guarda

X marca o local do bastidor.

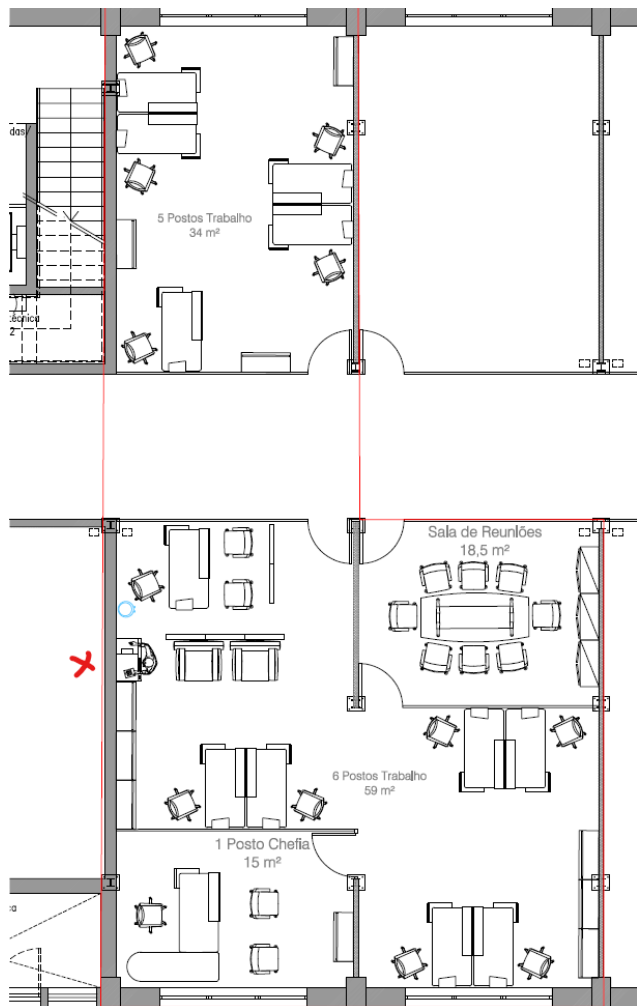




X marca o local do bastidor.



Só salas marcadas a vermelho. X marca o local do bastidor.



Só salas marcadas a vermelho. X marca o local do bastidor.

