Entitat Pública Empresarial Local
Parc Tecnocampus Mataró

PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGIRAN LA CONTRACTACIÓ DEL PROJECTE DE RENOVACIÓ, IMPLANTACIÓ I SERVEI DE MANTENIMENT DE BASE DE LA INFRAESTRUCTURA DE XARXA, SEGURETAT I SERVEIS ASSOCIATS DEL TECNOCAMPUS MATARÓ-MARESME

Exp. Número ES_LA0011123_2026_EXP_34

1. Objecte del contracte 5

2. Abast del Contracte 5

2.1 Termini, recepció i inici del servei 5

3. Situació actual 6

3.1 Pla Tecnològic 7

3.2 Pla de securització 7

3.3 Pla de transformació 8

3.4 Servei de manteniment de base 8

4. Pla Tecnològic 9

4.1 Plataforma actual 9

4.1.1 Llistat d'equipament actual 11

4.1.2 Cablejat existent 12

4.2 Plataforma proposada 12

4.2.1 Equipament Core 12

4.2.2 Equipament d'accés/LAN 13

4.2.3 Servei de NAC 14

4.2.3.3 Servei de Radius 15

4.2.4 Servei de DDI + NTP 17

4.2.4.6 Proposta del DDI+NTP 19

4.3 Experiència d'usuari 20

4.4 Plataforma de gestió tecnològica 21

4.4.1 Gestió 21

4.4.2 Seguretat de la Xarxa 21

4.4.3 Analítica de Xarxa 22

5. Pla de Securització 23

5.1 Estat actual 23

5.2 Proposta 25

5.2.1 Arquitectura 25

5.2.2 Seguretat LAN 25

5.2.3 Seguretat WAN 26

5.2.4 Funcionalitats de la plataforma 26
5.2.5 Polítiques i altres serveis 26
5.2.6 Gestió de la configuració dels equips: 27
5.2.7 Monitorització del trànsit a temps real 27
5.2.8 Monitoratge i operació 27
5.2.9 Seguretat 27
5.3 Funcionalitats plataforma – Servei VPN 28
5.4 Integració plataforma SOC TecnoCampus 29
6. Servei de manteniment de base 30
6.1 Monitorització 31
6.1.1 Eina de Monitorització TecnoCampus 31
6.2 Casos d'us 32
6.3 Paràmetres de gestió de la qualitat de servei 32
6.4 Pla de devolució del servei 33
6.4.1 Fase de captura i planificació 33
6.4.2 Fase de traspàs. 34
7. Transferència de coneixements 34
8. Pla de qualitat 35
8.1 Exigències transversals de qualitat 35
8.2 Exigències mediambientals 35
9. Memòria 36
9.1 Proposta detallada d'equipament i serveis 37

1. OBJECTE DEL CONTRACTE

L'objecte del contracte és renovar, implantar, migrar, posar en producció i prestar el servei de manteniment de base sobre la infraestructura, seguretat i serveis associats del TecnoCampus, incloent connectivitat LAN/Core, seguretat perimetral i interna, control d'accés, NAC, DDI/NTP, plataformes de gestió, monitorització i servei de manteniment de base associat, d'acord amb el que estableix el PPT.

El servei de manteniment de base inclourà l'operació ordinària de la infraestructura, el manteniment preventiu i correctiu, la coordinació amb la monitorització corporativa, la gestió d'incidències, el reporting, la documentació operativa i les accions ordinàries de millora contínua. Restaran fora d'aquest servei les actuacions evolutives, ampliacions, nous serveis, canvis majors de disseny i actuacions no recurrents que excedeixin l'operació ordinària definida al PPT.

Queda exclòs el desplegament de nova infraestructura passiva de xarxa (cablejat estructurat, canalitzacions, suports o racks), que serà responsabilitat del TecnoCampus. Resten incloses les tasques de desconnexió, neteja, pentinat, etiquetatge, embridat, reconnexió i retirada del cablejat innecessari als racks afectats.

L'adjudicatari executarà les actuacions d'acord amb els procediments del TecnoCampus i l'oferta adjudicada.

2. ABAST DEL CONTRACTE

L'execució del contracte s'estructurarà en quatre blocs funcionals: pla tecnològic, pla de securització, pla de transformació i servei de manteniment de base. Aquests blocs hauran d'estar coordinats entre si i reflectir les dependències tècniques, operatives i temporals necessàries per garantir una implantació ordenada, segura i amb mínima afectació al servei.

2.1 Termini, recepció i inici del servei

El termini total del contracte serà de cinc (5) anys des de la formalització, sense possibilitat de pròrroga. La fase de provisió, implantació, migració, proves i posada en producció haurà de completar-se en un màxim de quatre (4) mesos. La recepció global es formalitzarà mitjançant acta de conformitat un cop superades les proves d'acceptació i lliurada la documentació requerida. Des d'aquesta data s'iniciaran el servei de manteniment de base, els ANS i la seva facturació, fins a la finalització del contracte

3. SITUACIÓ ACTUAL

L'Entitat Pública Empresarial Local Parc TecnoCampus Mataró (EPEL TecnoCampus) gestiona les infraestructures i serveis del Parc TecnoCampus, ubicat a l'Av. Ernest Lluch, 32 de Mataró

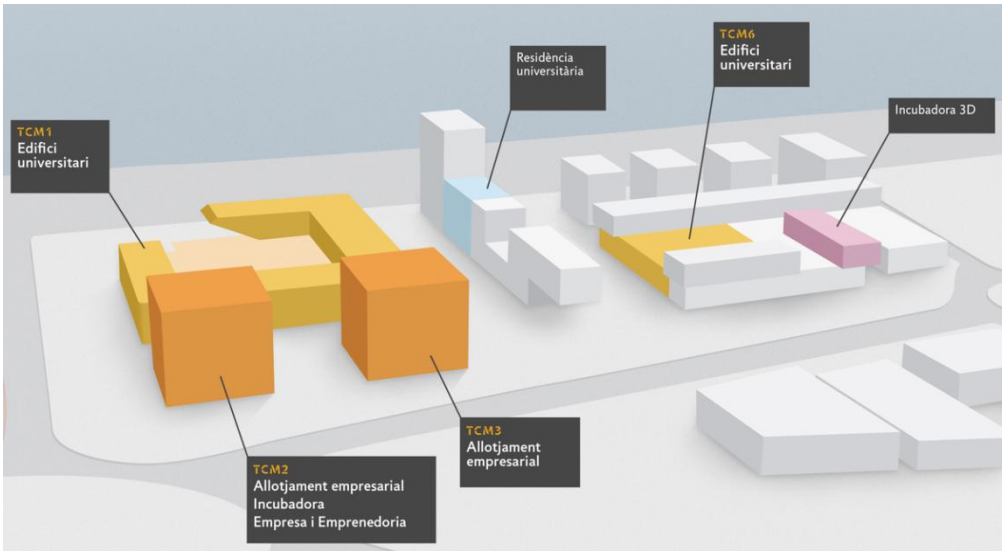


Figura 1 – Esquema ubicacions TecnoCampus

Disposa d'un campus universitari, parc empresarial i diversos edificis interconnectats mitjançant infraestructura LAN, WAN i serveis de seguretat que donen suport a l'activitat universitària, corporativa i empresarial.

L'equipament actual presenta limitacions de suport, gestió, seguretat i capacitat d'evolució. La nova solució haurà de substituir-lo minimitzant afectacions i garantint la continuïtat dels serveis. Les millores necessàries per poder donar un alt nivell d'excel·lència als serveis tecnològics resulten inviables amb l'equipament actual i per tant no permeten adaptar-se a les necessitats de servei actuals.

A continuació i de manera paral·lela a les tasques d'instal·lació de l'equipament es desplega el pla de transformació dels serveis actuals cap al nou equipament, incorporant totes les funcionalitats, millores, migracions i transformacions requerides per donar compliment al projecte adjudicatari, així com la seva completa documentació física i lògica, minimitzant d'igual manera qualsevol afectació al servei.

Es considera un pla de securització de tot l'entorn, on queda reflectit tot el procés d'implementació i transformació dels serveis de seguretat perimetral i d'accés a la xarxa del sistema de Firewall i NAC proposat.

El darrer pla és el de gestió del servei, on l'adjudicatari gestionarà de manera reactiva i proactiva tota la plataforma, reduint al mínim la càrrega operativa ordinària del TecnoCampus, sense perjudici de les funcions de govern, supervisió, validació i actuacions bàsiques de control que aquest pugui exercir.

A continuació es descriu amb més nivell de detall els requeriments de cada pla, així com les seves sinèrgies i afectacions.

3.1 Pla Tecnològic

El pla tecnològic haurà de descriure l'arquitectura proposada, equipament físic o virtual, ubicacions, connectivitat, plataformes de gestió, integracions i compliment dels requeriments tècnics mínims.

Tot el hardware proposat haurà de complir els mínims requerits a aquest document, tant a nivell hardware com de servei, i haurà de ser completament compatible amb tot l'equipament existent i que romandrà a la xarxa després del període de transformació.

El licitador haurà d'acreditar aquest extrem mitjançant documentació oficial del fabricant o declaració responsable del fabricant o del canal autoritzat corresponent, i qualsevol ampliació serà avaluada com a millora.

Cal estructurar aquesta proposta a mida de les infraestructures i equipament actual, com queda indicat al llarg d'aquest document per cada entorn i plataforma. Totes les propostes presentades han de seguir de manera estricta en format, estructura i volum segons queda definit a continuació.

La solució haurà de garantir gestió i observabilitat integrada, amb visibilitat consolidada, traçabilitat i gestió per rols i haurà de separar funcionalment les polítiques i dominis de seguretat LAN i WAN, i justificar l'arquitectura aportada per assolir els objectius de rendiment, segmentació, continuïtat i seguretat exigits.

3.2 Pla de securització

El pla de securització haurà de definir l'arquitectura de seguretat proposada per a la nova infraestructura del TecnoCampus, tant a nivell perimetral com intern, i haurà de garantir la correcta segmentació dels diferents entorns LAN i WAN, la protecció dels serveis corporatius i la integració amb la resta de plataformes incloses al contracte.

La proposta haurà de partir de l'arquitectura i polítiques actuals i definir el model objectiu, identificant clarament els equips i serveis implicats, les zones de seguretat, els fluxos principals de comunicació, les polítiques d'accés, els mecanismes d'inspecció i protecció i les dependències amb els serveis de xarxa, NAC, DDI/NTP i gestió.

El pla haurà de contemplar, com a mínim:

- Arquitectura de seguretat LAN i WAN proposada;
- Definició de zones, segmentació i criteris de separació entre entorns;
- Polítiques de seguretat, control d'accés, inspecció i filtratge;
- Mecanismes d'alta disponibilitat, redundància i continuïtat del servei;
- Integració amb els serveis corporatius d'identitat, NAC i DDI/NTP;
- Integració amb la plataforma SOC/XDR corporativa del TecnoCampus;
- Gestió centralitzada, logging, monitorització i traçabilitat dels esdeveniments;
- Procediment de migració de les polítiques i serveis actuals cap a la nova plataforma;
- Proves de validació, criteris d'acceptació i mecanismes de rollback;
- Documentació final de l'arquitectura, configuracions, polítiques i procediments operatius.

El pla de securització haurà d'estar coordinat amb el pla tecnològic i el pla de transformació, de manera que la implantació de les mesures de seguretat es realitzi de forma ordenada, minimitzant qualsevol afectació sobre els serveis productius.

La proposta haurà d'identificar especialment els canvis que puguin tenir afectació sobre la connectivitat, autenticació, accés dels usuaris, serveis publicats, VPN, trànsit entre zones o integracions amb altres plataformes, indicant per a cada cas les dependències, afectacions previstes, proves i procediment de posada en producció.

Així mateix, el licitador haurà de descriure els mecanismes de coordinació amb el servei SOC/XDR del TecnoCampus, incloent els fluxos d'informació, generació i enviament d'esdeveniments, procediments d'escalat, tractament d'alertes i possibles actuacions de resposta sobre els elements de xarxa i seguretat.

El resultat final haurà de proporcionar una arquitectura de seguretat integrada, resilient i gestionable, que permeti mantenir una separació clara entre els diferents dominis de seguretat, millorar la visibilitat dels esdeveniments i facilitar la seva operació dins del servei de manteniment de base.

3.3 Pla de transformació

El pla de transformació haurà de descriure les fases de migració de cada servei, dependències, calendari, afectacions, proves, criteris d'acceptació, rollback, documentació final i pas al servei de manteniment de base. Descriurà, per cada plataforma, la situació inicial i final, metodologia, calendari, dependències, riscos, actuacions, proves, criteris d'acceptació, rollback i documentació. El calendari global haurà de respectar el termini màxim establert al punt 2.1 i incloure auditoria inicial, migració, posada en producció i recepció global.

3.4 Servei de manteniment de base

El servei inclourà l'operació ordinària de la infraestructura, manteniment preventiu i correctiu, assegurament del servei, millora contínua, reporting, documentació i transferència de coneixement al TecnoCampus cap als gestors del servei del TecnoCampus.

El servei de manteniment de base s'operarà de manera continuada a partir dels mínims establerts en aquest plec, que inclourà les actuacions ordinàries de manteniment preventiu, manteniment correctiu, coordinació operativa, seguiment del servei i atenció d'incidències dins l'abast contractual.

Restaran fora del servei els evolutius, ampliacions, nous serveis, canvis majors de disseny i actuacions no recurrents que excedeixin l'operació ordinària definida al catàleg de servei. El manteniment preventiu i correctiu necessari per complir els ANS quedarà inclòs al servei de manteniment de base, excepte quan comporti ampliacions, redissenys o actuacions no previstes a l'abast inicial i clarament fora del seu abast.

Els recursos tècnics del servei hauran de disposar de coneixement actualitzat de l'entorn, accés a la documentació operativa i experiència en serveis comparables.

La monitorització corporativa serà prestada per TecnoCampus mitjançant la seva eina Centreon. L'adjudicatari haurà d'integrar-hi els equips i serveis objecte del contracte, mantenir aquesta integració i atendre els escalats conforme als ANS.

El model de responsabilitat del servei quedarà estructurat en tres capes:

1) Monitorització corporativa, responsabilitat del TecnoCampus mitjançant Centreon.
2) Integració i manteniment de la monitorització, responsabilitat de l'adjudicatari.

3) Atenció d'escalats i incidències, responsabilitat del servei de manteniment de base prestat per l'adjudicatari, d'acord amb els ANS aplicables.

Es podran proposar millores d'automatització, responsabilitats de monitorització, reporting, traçabilitat i escalat, sempre que no alterin l'abast mínim.

Durant tota la vigència contractual, inclòs el desplegament, l'adjudicatari adscriurà un Service Manager. Addicionalment, durant la fase de subministrament, desplegament i implantació adscriurà un Cap de Projecte amb un mínim de 5 anys d'experiència i participació com a responsable en almenys 3 projectes comparables, responsable de planificació, coordinació, riscos, fites i posada en producció.

L'inici i durada del servei de manteniment de base es regiran pel punt 2.1 d'aquest PPT.

4. PLA TECNOLÒGIC

Aquest apartat defineix la plataforma actual i els requeriments tècnics mínims de la nova arquitectura Core, LAN/Accés, NAC, DDI/NTP i gestió tecnològica. La proposta haurà d'acreditar el compliment dels requeriments mínims de cada domini, el dimensionament de l'equipament, la integració entre plataformes i la coherència amb l'estructura de memòria tècnica definida al punt 9 d'aquest document.

4.1 Plataforma actual

La xarxa actual es divideix en entorns de veu/dades i clima/CCTV, amb equipament de xarxa, seguretat i comunicacions associat. El dimensionament futur té en compte la reducció d'ús de ports cablejats i l'increment de serveis WiFi i enllaços d'alta capacitat.

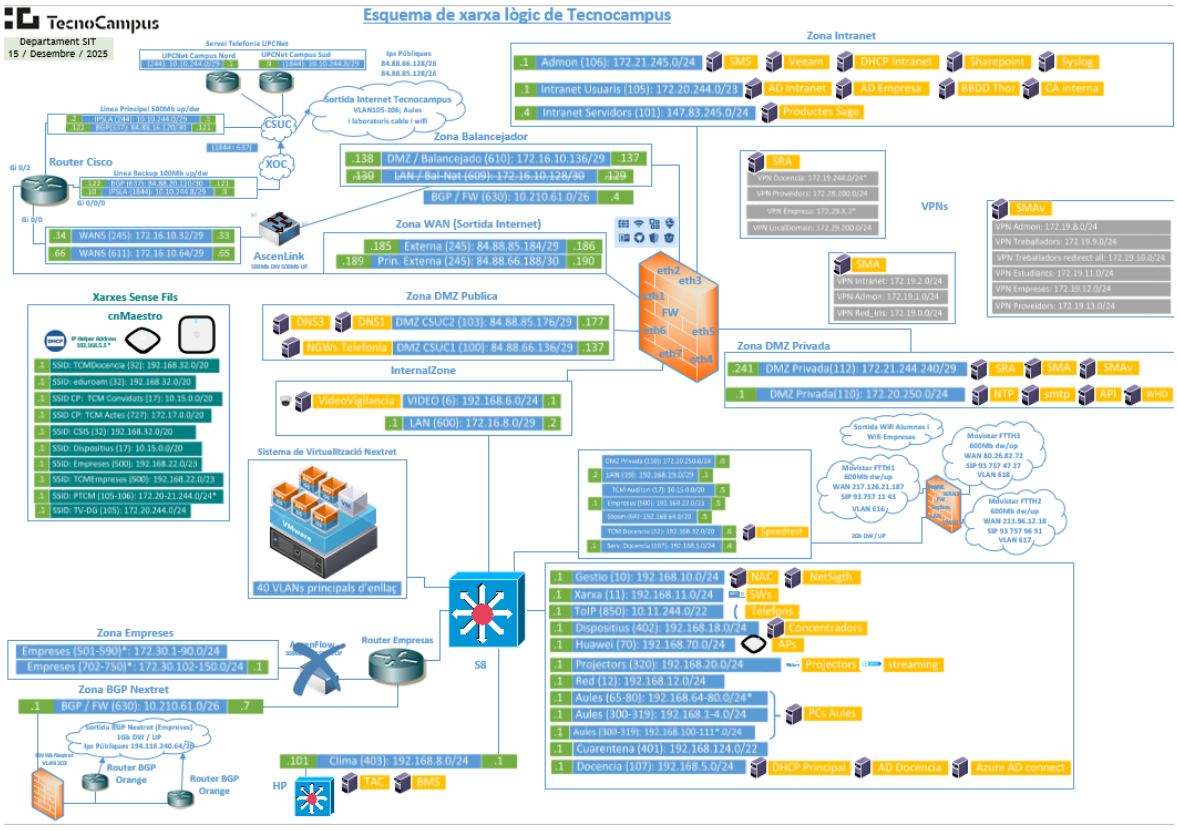


Figura 2 - Esquema lògic

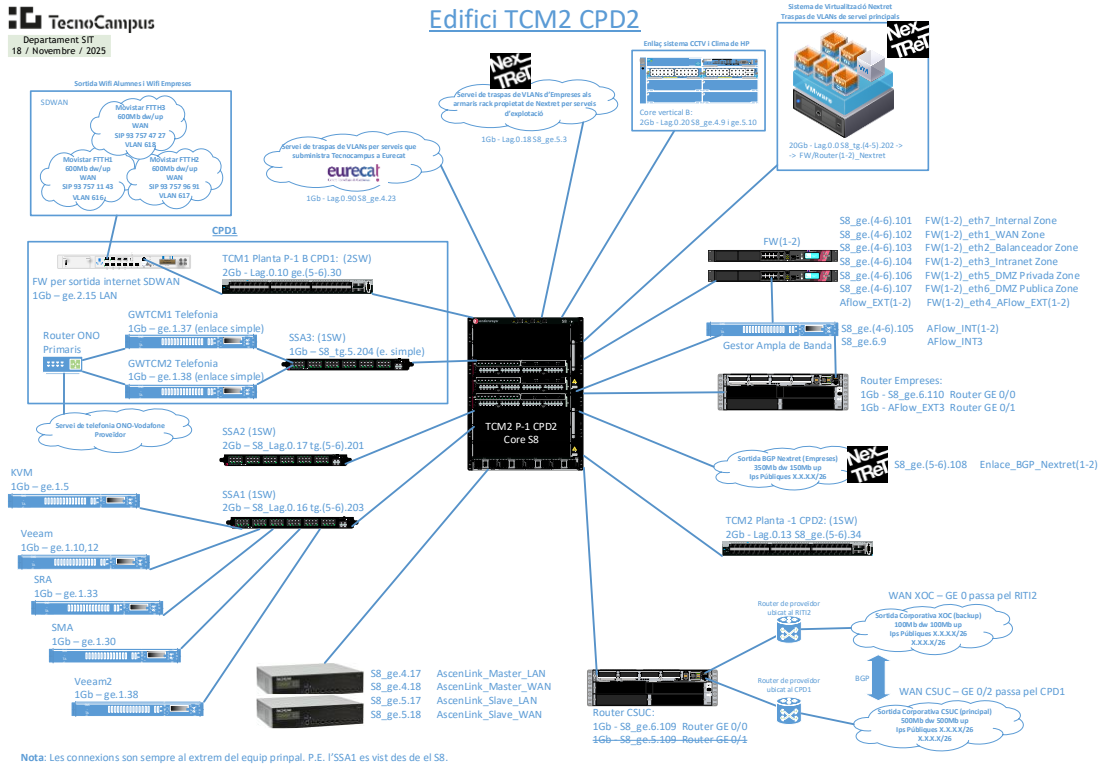


Figura 3 - Esquema físic

Les ubicacions actuals es mantindran. L'adjudicatari haurà d'instal·lar el nou equipament, retirar l'obsolet i ordenar, etiquetar i reconnectar el cablejat afectat d'acord amb l'auditoria i el pla de transformació, considerant l'estat actual de les ubicacions documentades, documentat gràficament a la documentació adjunta a aquest contracte

4.1.1 Llistat d'equipament actual

L'equipament de xarxa esta dividit en dos àmbits: Veu i dades (el més important i rellevant) i el de clima i CCTV amb menors requeriments de throughput.

4.1.1.1 Equipament actual - Xarxa de veu i dades

- 80x B5G124-48P2
- 1x S8
    - 3 Mòduls del S8 model SG1201-0848-F6
    - 3 Fonts del S8 model SOT1206-0112
    - 3 Fonts del S8 model SOK1208-0104
- 2 SSA Model SSA-T4068-0252
- 1 5420F-48P-4XE-EXOS
- 1 Appliance virtual Netsigth en versió 6.2.0.211
- 2 Appliance virtual NAC en la seva versió 6.2.0.211

4.1.1.2 Equipament actual - Xarxa de clima i CCTV

- 3 HP ProCurve E2910al-48G-PoE
- 5 HP ProCurve 2910al-24G-PoE
- 2 Aruba 2920
- 2 Aruba 2530 48G
- 1 HP ProCurve E5406z
    - 1 Mòdul del HP ProCurve E5406z model J8706A
    - 1 Mòdul del HP ProCurve E5406z model J8702A
    - 1 Mòdul del HP ProCurve E5406z model J9534A

4.1.1.3 Equipament actual - Seguretat i comunicacions

El llistat d'equipament que actualment tenim a nivell de seguretat i Routing.

- Router CISCO3925-CHASSIS (revisió 1.0) C3900-SPE100/K9
- Router CISCO3925-CHASSIS (revisin 1.0) C3900-SPE100/K9
- 2 Firewall Sophos XGS136 (SFOS 19.5.1 MR-1-Build278)
- 2 Firewall CheckPoint 5900 v. R80.40 Kernel 3.10.0-957.21.3cpx86_64
- 2 Balancejador AscenLink V6.3-B3638-M5050-F0-P17
- Control de Quotes AscenFlow M3050-V3.5-B20110607-F0-P9-INTL

4.1.2 Cablejat existent

El cablejat existent queda fora de l'abast de renovació, excepte les tasques de desconnexió, reconnexió, ordenació i etiquetatge vinculades a la substitució d'equipament.

Tots els edificis del campus resten units per enllaços de fibra òptica de característiques adequades a la distància en format semi estrella finalitzant contra les sales CPD on es disposa dels equips de CORE.

4.2 Plataforma proposada

El dimensionament mínim previst és de 2.688 ports en 37 ubicacions, distribuïts segons la taula següent documentada al document específic d'aquesta licitació "Annex Plataforma bàsica TecnoCampus". El licitador haurà de validar-lo en auditoria i justificar qualsevol ajust proposat. Les dades indicades a l'annex representen una avaluació inicial mínima, pero poden ser modificats en el sentit que el licitador consideri per fer-la més eficient i funcional.

Durant tota la vigència del contracte, l'adjudicatari haurà de garantir suport del fabricant, dret a actualitzacions, substitució d'equipament defectuós i servei de recanvi NBD o equivalent justificat, sense sobrecostos no previstos per a les funcionalitats incloses a l'oferta adjudicada.

4.2.1 Equipament Core

Els equips Core hauran de disposar, com a mínim, d'una capacitat de commutació igual o superior a 1,4 Tbps —1.400 Gbps— i d'una taxa de forwarding igual o superior a 1.000 Mpps per equip, segons fitxa tècnica oficial del fabricant. Així mateix, hauran d'incloure un mínim de 24 ports SFP28 i 8 QSFP28 40/100G, suport per a 4.094 VLANs, agregació d'enllaços 802.3ad, mecanismes d'alta disponibilitat, aprovisionament zero-touch, control d'accés basat en rols i autenticació multifactor —RBAC/MFA—, diagnosi remota i gestió centralitzada.

La plataforma de gestió ha de permetre actualitzacions programades, automatitzades i supervisades. Els equips hauran d'oferir mecanismes de redundància, agregació i escalabilitat que permetin assolir la disponibilitat i capacitat requerides, ja sigui mitjançant stacking físic, virtual chassis, MLAG, fabric, VSF o tecnologia equivalent suportada pel fabricant.

L'equipament de CORE haurà de disposar d'intel·ligència distribuïda i capacitat d'operació autònoma, de manera que les funcions pròpies de commutació, encaminament, autenticació, seguretat, alta disponibilitat i gestió continuïn disponibles independentment de l'estat de les plataformes centralitzades de gestió o orquestració.

La pèrdua de connectivitat, reinici, actualització o indisponibilitat de qualsevol plataforma centralitzada de gestió o control no haurà d'afectar el funcionament dels equips de CORE ja desplegats ni impedir-ne l'administració local mitjançant interfície de línia d'ordres (CLI) i accés segur per SSH.

Pel que fa a capacitats Ethernet (capa 2) es requereixen les següents funcionalitats i/o capacitats:

La solució ha de suportar la qualitat de servei 802.1p, assegurant una gestió eficient del trànsit de xarxa. A més, ha de proporcionar suport de VLAN i trunking per a fins a 4,094 VLANs, amb 1000 VLANs actives amb STP habilitat, oferint una segmentació robusta i flexible.

La solució ha de permetre una instància única del protocol MSTP 802.1s, interoperable amb RSTP, STP, PVST, i RPVST, garantint una compatibilitat completa amb diferents protocols de spanning tree.

La solució haurà de proporcionar capacitats de visibilitat i anàlisi de trànsit, incloent classificació d'aplicacions quan sigui aplicable, mitjançant els components de xarxa, seguretat, telemetria o gestió inclosos a l'oferta, sense costos addicionals no previstos.

El control de tempestes de broadcast és un altre aspecte crucial, assegurant que la xarxa no es vegi afectada per trànsit excessiu.

L'agregació d'enllaços 802.3ad amb fins a 8 ports per agregat, i agregats multichasis suportats en switches apilats, és essencial per oferir una major capacitat i redundància. La solució ha de permetre el port mirroring, facilitant la monitorització del trànsit de xarxa.

El snooping IGMP per a filtratge multicast és també un requeriment important, assegurant una gestió eficient del trànsit multicast. Finalment, la solució ha de permetre fins a 32K adreces de reenviament MAC, oferint una capacitat robusta per a la gestió de dispositius de xarxa.

Pel que fa a capacitats de routing (capa 3) es requereixen les següents funcionalitats i/o capacitats mínimes:

- Static routing, OSPFv2.
- Multicast routing (PIM-SM i PIM-SSM).
- Warm Spare (VRRP).
- DHCP Relay.

Pel que fa a capacitats específiques de seguretat, es requereix les següents funcionalitats i/o capacitats mínimes:

- IEEE 802.1X RADIUS i MAB, autenticació híbirda i RADIUS server testing.
- Autenticació Single-Host/Multi-Domain/Multi-Host/Multi.
- Seguretat per ports: Sticky MAC, llista de MACs permeses.
- DHCP snooping, detecció i bloqueig, inspecció dinàmica ARP.
- ACLs per a IPv4 i IPv6.

4.2.2 Equipament d'accés/LAN

Els equips d'accés hauran de complir, com a mínim: 208 Gbps de switching, 154 Mpps, models de 24/48 ports GbE PoE+, 2 ports SFP+ 10GE, 12 ports MultiGigabit, valorables amb capacitat POE++ en els equips requerits, 4.094 VLANs, agregació, alta disponibilitat, zero-touch, RBAC/MFA, diagnosi remota i gestió centralitzada. Les velocitats mínimes suportades pels ports MultiGigabit RJ45, requerint com a mínim suport per 1 Gbps, 2,5 Gbps i 5 Gbps

La plataforma de gestió ha de permetre actualitzacions programades, automatitzades i supervisades. Els equips hauran d'oferir mecanismes de redundància, agregació i escalabilitat que permetin assolir la disponibilitat i capacitat requerides, ja sigui mitjançant stacking físic, virtual chassis, MLAG, fabric, VSF o tecnologia equivalent suportada pel fabricant.

Els commutadors d'accés hauran de permetre l'operació coordinada de fins a 8 unitats mitjançant stacking o tecnologia equivalent suportada pel fabricant, proporcionant gestió unificada, alta disponibilitat i simplificació operativa. La solució haurà de permetre que els equips apilats es comportin com un únic dispositiu lògic, disposant d'una única configuració, una única adreça IP de gestió i un únic pla de control i administració unificat. Aquesta capacitat simplifica significativament les tasques de desplegament, operació, manteniment, actualització de firmware i resolució d'incidències.

Així mateix, es considerarà una capacitat tècnica favorable quan contribueixi a l'optimització del dimensionament, dins dels aspectes de qualitat previstos per al criteri LAN.

Les capacitats L2, L3 i de seguretat dels equips d'accés hauran de ser equivalents a les indicades per al Core, adaptades al seu rol d'accés, incloent QoS, VLAN, STP/RSTP/MSTP, LACP, mirroring, IGMP, routing bàsic, DHCP Relay, 802.1X/MAB, seguretat per port, DHCP snooping, inspecció ARP i ACL IPv4/IPv6.

La solució haurà de proporcionar visibilitat dels dispositius connectats, informació LLDP, capacitat d'aïllament de ports, APIs documentades i telemetria suficient per a l'operació i automatització del servei, sense costos addicionals no previstos.

L'oferta haurà d'incloure, durant tota la vigència contractual, suport 24x7, substitució NBD o equivalent justificat, actualitzacions i suport del fabricant, sense costos addicionals per al TecnoCampus respecte de les funcionalitats incloses.

Els equips d'ACCÉS hauran disposar d'intel·ligència distribuïda i capacitat d'operació autònoma, de manera que les funcions pròpies de commutació, encaminament, autenticació, seguretat, alimentació PoE, alta disponibilitat i gestió continuïn disponibles independentment de l'estat de les plataformes centralitzades de gestió, control o orquestració.

4.2.3 Servei de NAC

4.2.3.1 Entorn actual

El NAC actual permet assignació de VLANs i serveis en funció de regles, però no opera en mode plenament restrictiu.

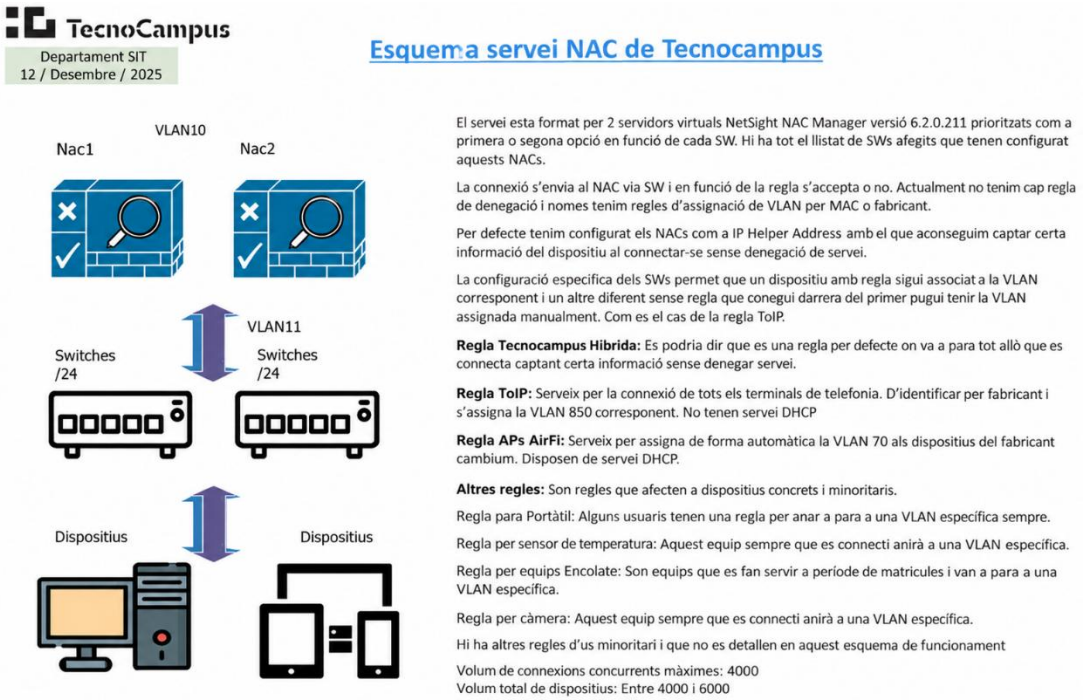


Figura 4 - Esquema servei NAC TecnoCampus

4.2.3.2 Proposta requerida

La solució NAC haurà de proporcionar control d'accés cablejat i sense fils, autenticació 802.1X/MAB/RADIUS, integració amb directoris corporatius, alta disponibilitat, portals de convidats, perfilat de dispositius, registre d'accessos, polítiques per rols i operació en entorns multifabricant.

El compliment de les funcionalitats requerides haurà d'acreditar-se mitjançant documentació oficial del fabricant o evidències tècniques equivalents.

La solució haurà de registrar intents de connexió, ubicació física, MAC/IP, usuari, dispositiu, sistema operatiu i estat d'autenticació, permetent polítiques per horari, localització, grups de directori, mètode d'autenticació, llistes blanques/negres i ha de comptar amb fingerprints de DHCP per a la caracterització del sistema operatiu del dispositiu client.

Els portals de convidats i usuaris hauran de permetre autoregistre, validació, credencials temporals, traçabilitat, accés amb credencials corporatives, gestió delegada i consulta d'estadístiques, logs i alarmes..

La plataforma haurà de proporcionar una experiència de gestió unificada per a l'administració de la infraestructura de xarxa i del control d'accés, facilitant una visió centralitzada dels dispositius, usuaris, polítiques i esdeveniments de seguretat.

Es valorarà especialment que la plataforma de gestió de xarxa i la solució NAC comparteixin de forma nativa l'inventari de dispositius, la telemetria, les alarmes, els esdeveniments, les polítiques i els mecanismes d'automatització, evitant la necessitat d'integracions externes entre productes independents.

La solució haurà de permetre integració amb MDM/UEM mitjançant connectors, APIs o mecanismes equivalents, incorporant l'estat del dispositiu a les decisions d'accés.

La solució haurà de notificar esdeveniments via correu, syslog, SNMP o APIs, integrar-se amb SIEM/SOC i permetre accions de resposta sobre dispositius o accessos compromesos.

Es valoraran funcionalitats avançades de classificació automàtica, postura sense agent, resposta automatitzada, integració amb intel·ligència de seguretat i aplicació de polítiques zero trust, sempre que aportin millora operativa demostrable..

La solució NAC haurà d'integrar-se amb la solució DDI proposada, de manera que la solució NAC actualitzi a la solució amb informació de classes a través de trucades a API o amb integració directa.

4.2.3.3 Servei de Radius

Actualment TecnoCampus disposa de 3 servidors Radius (Intranet, Docència i Empresa), serveis que cal integrar al nou sistema de Radius per donar un valor afegit al servei de gestió.

Principalment els serveis que es nodreixen dels servidors radius son les wifis amb autenticació 802.1x que validen amb credencials personalitzades.

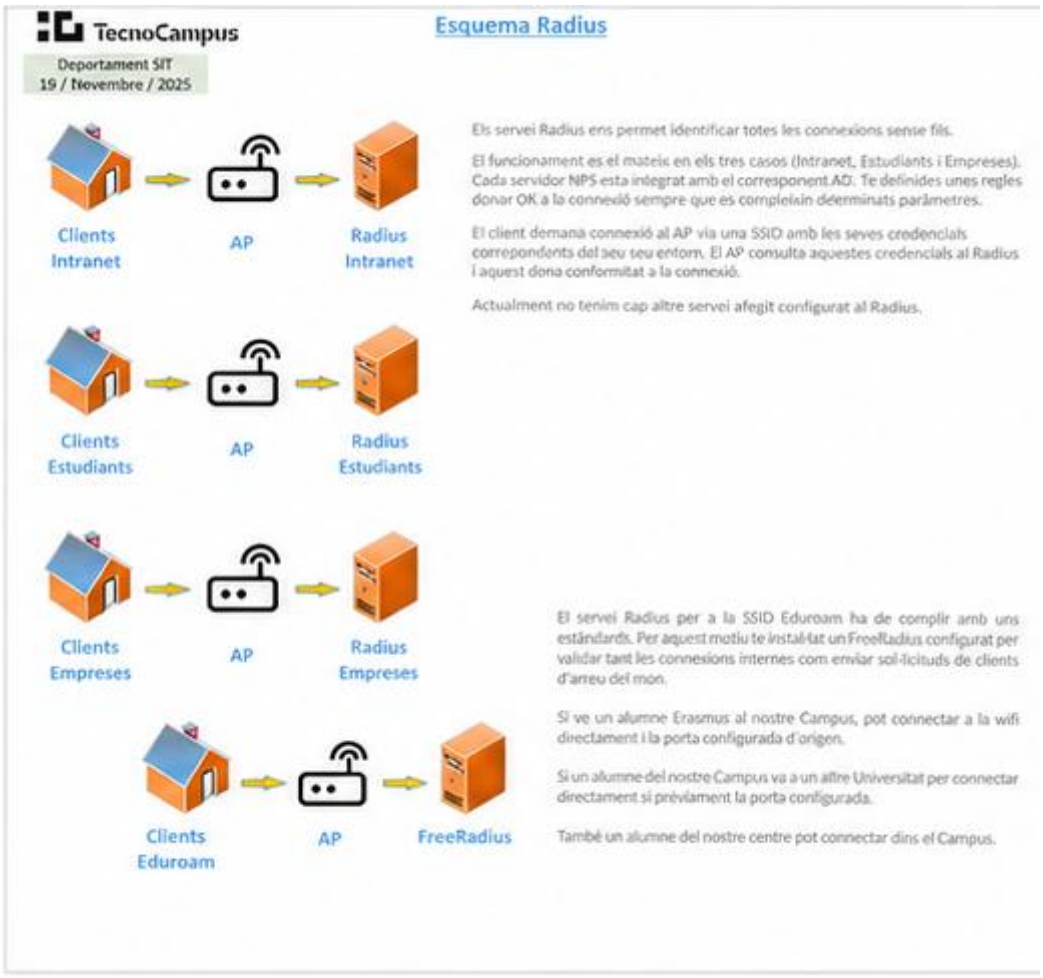


Figura 5 – Esquema Radius actual

Per tant s'ha de proposar la implementació d'aquest servei a l'entorn de NAC per obtenir les màximes sinèrgies i valor afegit a aquest entorn, conforme aquests paràmetres:

- Configuració com a servidor Radius o com a servidor intermediari Radius
- Atributs Radius a enviar completament personalitzables en funció de cada perfil dús i de la infraestructura client.

Per tant, la configuració de NAC haurà de contemplar 4 necessitats bàsiques per a TecnoCampus:

- Configuració de NAC com RADIUS (seguint les configuracions del servidors actuals).
- Configuracions d'autenticacions 802.1X per accés d'usuaris a la xarxa amb credencials d'usuari segons el directoris actius.
- Evitar que equips no desitjats (no corporatius) tinguin accés a la xarxa. Restricció de ports LAN.
- Perfilat d'equips que accedeixin a la xarxa.

La implantació RADIUS/NAC haurà d'incloure preparació, desplegament, integració amb directoris, polítiques d'accés, proves, suport a canvis i pas a producció.

FASE 1: Preparació i implementació inicial de la nova plataforma NAC

- Definició de requeriments i maquinari, desplegament i configuració inicial.
- Integració amb directori actiu.

- Creació de servidor RADIUS: Configuració de servidor RADIUS i vincular-lo als directoris actius corporatiu del TecnoCampus . S'haurà de configurar en base als servidors RADIUS existents.
- Configuració inicial de polítiques d'accés a la xarxa.

FASE 2: Control sobre aplicació de canvis en switches, creació de perfils i generació de les polítiques d'accés

FASE 3: Configuració de certificats en equips corporatius, polítiques de compliment i configuració d'agents en equips finals necessaris

4.2.4 **Servei de DDI + NTP**

4.2.4.1 Entorn actual

Per tal de facilitar la comprensió i propostes d'implementació dels diferents entorns referits a aquest punt es donen les dades bàsiques de configuració, dimensionament i operativa actual dins l'entorn del TecnoCampus.

4.2.4.2 Servei DNS

L'entorn DNS actual esta format per quatre grups de clients: Empreses, Estudiants, Corporatiu i resta del mon.

- **Empreses**: es el més simple. No hi ha serveis interns i per aquest motiu es consulten directament els DNS públics.
- **Estudiants**: Els clients consulten directament els DNS del Directori Actiu. En cas de no tenir resposta es consulta la cara interna dels nostres dominis principals com TecnoCampus.cat.
- **Corporatiu**: Els clients consultes directament els DNS del Directori Actiu. Per qüestions docents, també poden consultar una replica del AD d'Estudiants. En cas de no tenir resposta es consulta la cara interna dels nostres dominis principals com TecnoCampus.cat.
- **Resta del Mon**: La resta del mon consulta directament la cara publica a AWS dels nostres dominis públics principals.

Els clients configuren el seus DNS a traves dels serveis DHCP en el 90% dels casos. Els servidors ho fan en la seva totalitat de forma manual i en funció del servei. Hi ha que tenen els interns d'intranet, interns docents, públics cara interna, públics o no tenen.

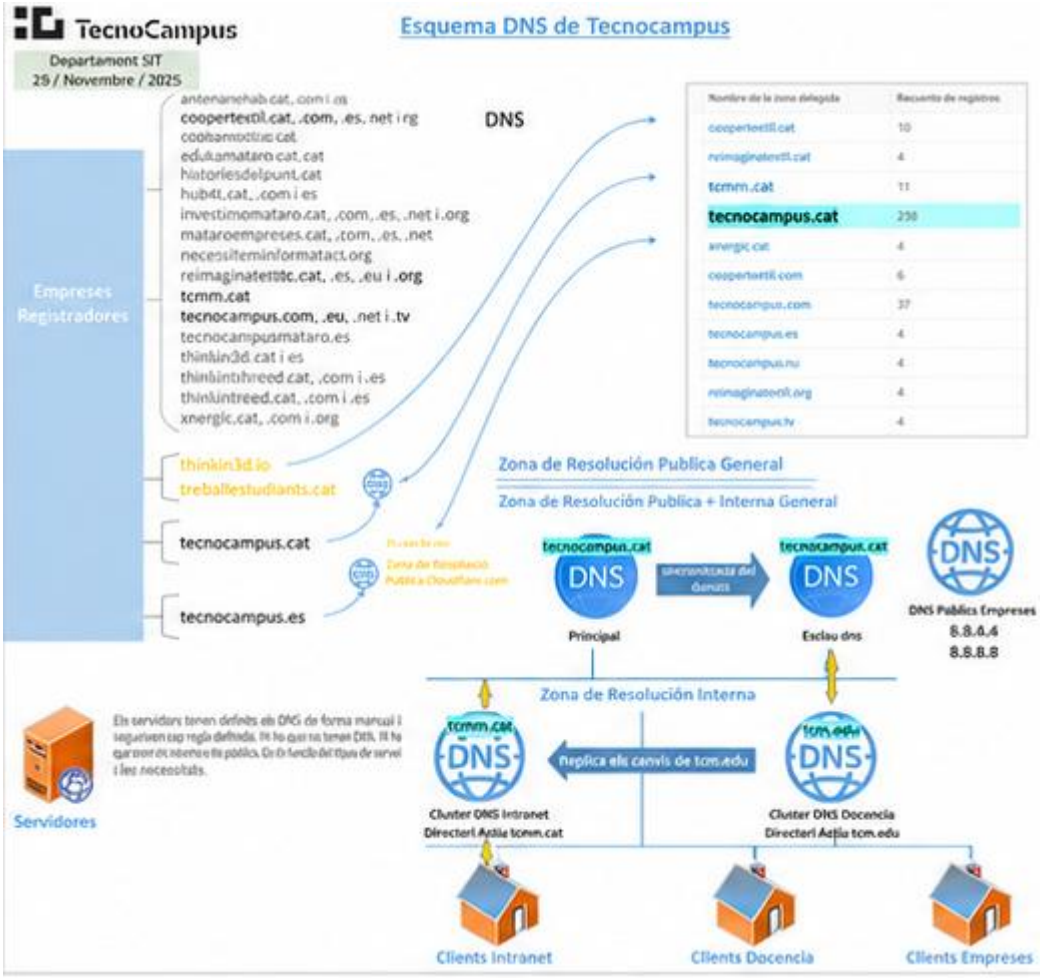


Figura 6 – Esquema DNS TecnoCampus

4.2.4.3 Servei DHCP

L'entorn DHCP esta format per 2 servidors (corporatiu i resta de serveis). La majoria de clients utilitzen el servei DHCP. Algunes excepcions son: equips de telefonia, projectors o càmeres de videovigilància que actualment tenen assignacions manuals de adreçament IP.

Els àmbits no segueixen cap estàndard. En funció de les necessitats del servei destí, es configura el pool d'adreces, el temps de renovació, dns, etc... dels clients.

- **Corporatiu**: El servei DHCP corporatiu facilitat adreçament als perfils corporatius de Intranet i Admon. Queda separat del resta de àmbits per qüestions de seguretat.
- **Resta de serveis**: Aquest servidor facilitat un total de 190 àmbits. Més de 100 estan destinats a empresa i encara que hi ha empreses que no el fan servir, es un servei que tenim ofert com a base.

La resta son àmbits que ens permeten major segmentació en funció de la tipologia de servei: wifi empreses, wifi alumnes, aules, laboratoris, aps, dispositius, etc...

4.2.4.4 Servei NTP

El servidor sincronitza amb servidors de temps públics i dona servei NTP a tot aquell dispositiu o servidor intern que ho necessiti: SWs, APs, CCTV, servidors standalone, etc...

4.2.4.5 Servei IPAM

El servidor s'integra amb els diferents directoris actius, servidors DNS i àmbits DHCP. Escaneja periòdicament tots els àmbits, obtenint certa informació del dispositiu enllaçant la informació amb les diferents integracions.

També permet la inserció i reserva manual.

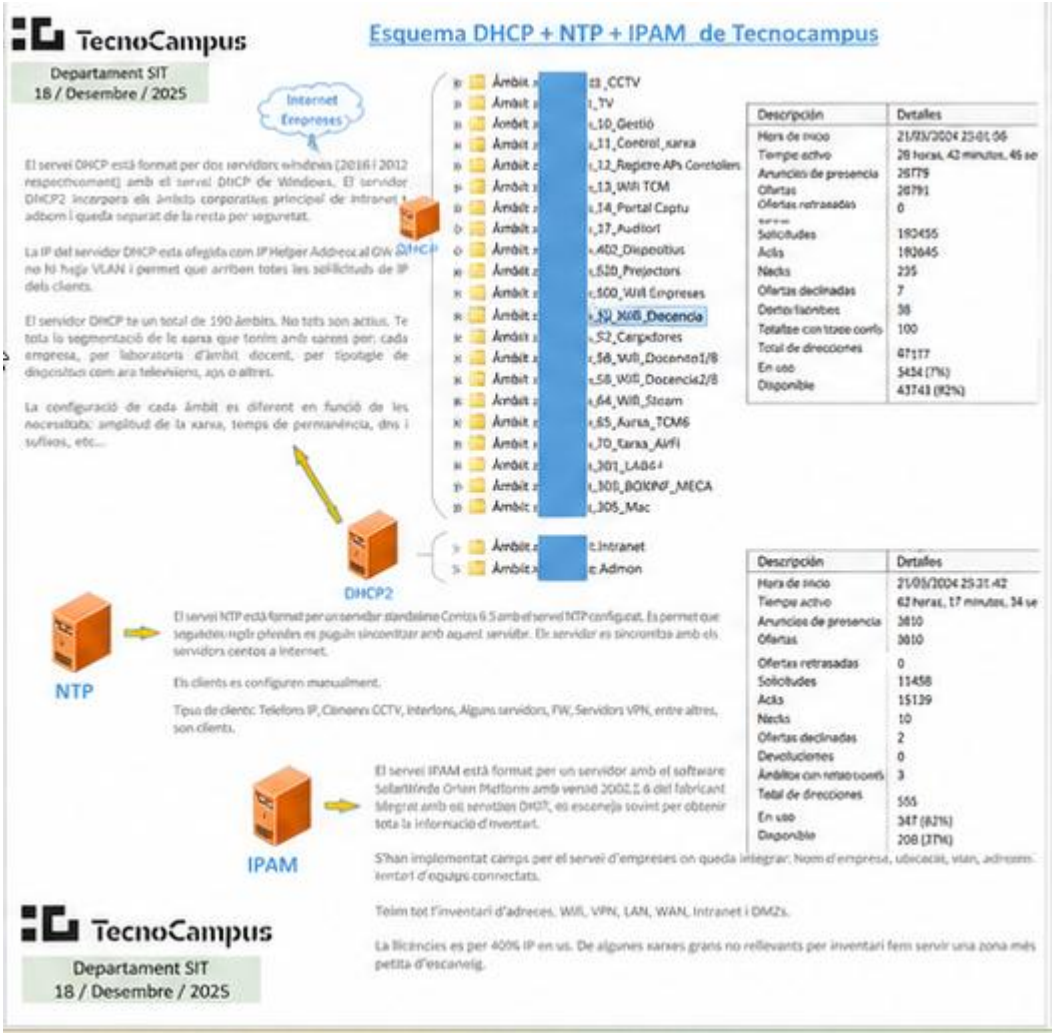


Figura 7 – Esquema DHCP, NTP i IPAM TecnoCampus

4.2.4.6 Proposta del DDI+NTP

La solució DDI/NTP haurà d'oferir arquitectura en alta disponibilitat per a DNS, DHCP, IPAM i NTP, amb el dimensionament mínim indicat a la taula següent.

Entorn	Concepte	Rendiment per equip
Gestió centralitzada e IPAM	IPAM	10.000 IPs
	Servidors DNS i DHCP Gestionats	50
Servei DNS RECURSIU PRIVAT	Peticions DNS per segon	33.750
Servei DHCP	Cessions DHCP per segon	225
Descobriment de Cloud	Instàncies a descobrir	100
Gestió d'inventari	Objectes de xarxa	100
Correlació entre usuaris de domini de Microsoft e IPAM	Usuaris per Domini	1500

La solució ha de comptar amb un sistema operatiu de propòsit específic, desenvolupat pel fabricant específicament per a funcions DDI (DNS, DHCP i IPAM). Les llicències necessàries per a la prestació dels serveis DNS, DHCP, IPAM i NTP inclosos a l'abast hauran d'estar incloses en l'oferta.

La solució DDI/NTP haurà de proporcionar serveis DNS, DHCP, IPAM i NTP en alta disponibilitat, amb suport IPv4/IPv6, DNSSEC, integració amb directoris corporatius, APIs documentades, logs, control d'accés administratiu, traçabilitat de canvis, còpies de seguretat, actualitzacions controlades i recuperació davant incidències, així com permetre integracions específiques assimilables per l'entorn del TecnoCampus.

4.2.4.7 Sistema

La plataforma haurà de disposar de gestió centralitzada, base de dades consistent, interfície web segura, delegació de permisos, auditoria, metadades o etiquetes operatives, importació/exportació i eines de cerca i informes.

El servei DHCP haurà de funcionar en alta disponibilitat, suportar DHCPv4/v6, opcions avançades, historial de cessions, identificació de dispositius, estadístiques i protecció davant abusos o denegació de servei dins l'abast ofert.

El servei DNS haurà de suportar rendiment mínim indicat, vistes DNS, DNSSEC, IPv6, TSIG, RRL, protecció DNS, alta disponibilitat, estadístiques, integració amb sistemes de seguretat i recuperació davant desastre.

Es valoraran funcionalitats avançades de descobriment cloud, inventari, delegació avançada, integració amb eines d'orquestració, automatització i routing dinàmic, sempre que siguin aplicables a l'entorn del TecnoCampus.

Es valorarà, quan sigui aplicable a l'arquitectura proposada, el suport d'Anycast i routing dinàmic, inclosa la capacitat d'exportar i aprendre rutes mitjançant BGP

4.3 Experiència d'usuari

La solució haurà de preveure la incorporació futura de monitoratge d'experiència d'usuari. El licitador haurà de descriure arquitectura, integració, casos d'ús i model d'operació, sense que la implantació inicial sigui obligatòria.

El licitador podrà descriure les capacitats disponibles o previstes. Aquesta informació tindrà caràcter descriptiu i no serà objecte de puntuació específica, excepte quan estigui vinculada als aspectes expressament valorats a la plataforma de gestió de proves sintètiques, monitoratge WiFi/cablejat/web,

detecció proactiva, històrics, llindars, alertes, seguretat de dades i exportació de mètriques a eines corporatives.

La solució haurà de garantir la protecció integral de la infraestructura de xarxa, amb mecanismes que assegurin la confidencialitat, integritat i disponibilitat de les dades. Els requisits mínims inclouran un xifratge robust de dades en trànsit i en repòs, un hashing i restriccions de credencials d'accés i la disponibilitat d'auditories independents de seguretat

El monitoratge d'experiència d'usuari no forma part del desplegament mínim. La proposta podrà descriure capacitats de proves sintètiques, telemetria, anàlisi de rendiment, diagnosi i captura remota, indicant-ne cobertura, integració i llicenciament. Aquestes capacitats es valoraran dins dels criteris de plataforma de gestió i observabilitat quan correspongui.

4.4 Plataforma de gestió tecnològica

La solució haurà de proporcionar una plataforma de gestió i observabilitat, en model cloud, híbrid o integrat funcionalment, que permeti operar els dominis inclosos al contracte amb visibilitat consolidada, gestió centralitzada, control d'accés per rols, auditoria, inventari, topologia, reporting, actualitzacions i diagnosi remota.

La plataforma haurà de permetre la coexistència i transició progressiva entre entorns de gestió on-premises i cloud, sense interrupció del servei ni pèrdua de funcionalitats operatives. La proposta haurà de justificar el model de desplegament, la residència i tractament de dades, la disponibilitat, la seguretat i el compliment normatiu aplicable.

La solució haurà de disposar de llicenciament i model operatiu compatibles amb l'evolució entre entorns on-premises i cloud, sense costos addicionals no previstos per mantenir les funcionalitats adjudicades.

Durant la fase de transició, la plataforma haurà de permetre visibilitat i gestió operativa dels elements existents que siguin tècnicament integrables, incloent entorns multivendor quan sigui possible mitjançant protocols, APIs, connectors o mecanismes equivalents suportats..

4.4.1 Gestió

La plataforma haurà de permetre gestió centralitzada, alta d'equips, plantilles, actualitzacions programades, diagnosi remota, topologia, informes, APIs, automatització i, si escau, capacitats AIOps de suport a l'operació, i la pèrdua temporal de connexió amb la plataforma cloud no haurà d'afectar la continuïtat de la xarxa. Les funcions exclusivament cloud hauran de disposar de degradació controlada o recuperació automàtica.

4.4.2 Seguretat de la Xarxa

La plataforma haurà de permetre l'aplicació centralitzada i coherent de polítiques de seguretat i accés en els dominis inclosos, integrant identitat, rols, segmentació, dispositius i sistemes corporatius.

La solució haurà d'integrar-se amb serveis d'identitat corporatius o cloud, incloent, com a mínim, mecanismes compatibles amb directoris corporatius, autenticació multifactor, control d'accés per rols i assignació de privilegis en funció del perfil d'usuari, dispositiu o servei.

La plataforma haurà de proporcionar mecanismes de classificació i identificació de dispositius, incloent dispositius corporatius, IoT i mòbils, mitjançant fingerprints, telemetria, integració amb NAC, inventari, client d'usuari o mecanismes equivalents.

Les plataformes cloud o SaaS utilitzades hauran de complir els requisits de seguretat, privacitat i protecció de dades aplicables, incloent xifratge en trànsit i en repòs, control d'accés, traçabilitat, auditoria i certificacions o evidències equivalents de seguretat, com ISO 27001, ISO 27017, ISO 27018, CSA, CIS o equivalents.

4.4.3 Analítica de Xarxa

La solució haurà de mostrar el rendiment de les aplicacions i de la xarxa mitjançant eines de telemetria i inspecció profunda de paquets (DPI). Per a això, combinarà tecnologies basades en fluxos amb un ampli conjunt de tècniques d'identificació i empremta digital d'aplicacions.

La plataforma haurà de permetre diferenciar clarament si una incidència està relacionada amb la infraestructura de xarxa o amb l'aplicació, facilitant la identificació ràpida de la causa arrel dels problemes de rendiment.

Per aconseguir-ho, haurà de correlacionar el rendiment de les aplicacions amb serveis centrals de la infraestructura com DNS, RADIUS, Active Directory i altres serveis crítics, permetent determinar de forma ràpida si l'origen d'una incidència es troba a la xarxa o a l'aplicació.

La solució haurà de proporcionar visibilitat i anàlisi del trànsit de xarxa en temps real a través de múltiples capes, tant en entorns cablejats com sense fils, així com sobre aplicacions i serveis desplegats en entorns híbrids i multi-cloud.

La plataforma haurà de generar alertes automàtiques quan la qualitat de l'experiència d'una aplicació monitoritzada experimenti degradacions significatives respecte al seu comportament habitual.

Així mateix, haurà de permetre la captura remota de paquets des d'una consola centralitzada sobre qualsevol port de qualsevol commutador de la infraestructura de xarxa de la Universitat, facilitant tasques de diagnòstic, resolució d'incidències i anàlisi forense de seguretat.

Les funcionalitats d'analítica hauran d'estar disponibles i suportades sobre la totalitat dels commutadors inclosos en la solució proposada i integrada en la mateixa interface de la plataforma de gestió

5. PLA DE SECURITZACIÓ

5.1 Estat actual

La proposta haurà de prendre com a base l'arquitectura actual descrita als esquemes adjunts i transformar-la cap al model objectiu definit en aquest plec, garantint continuïtat, segmentació i integració amb els serveis corporatius.

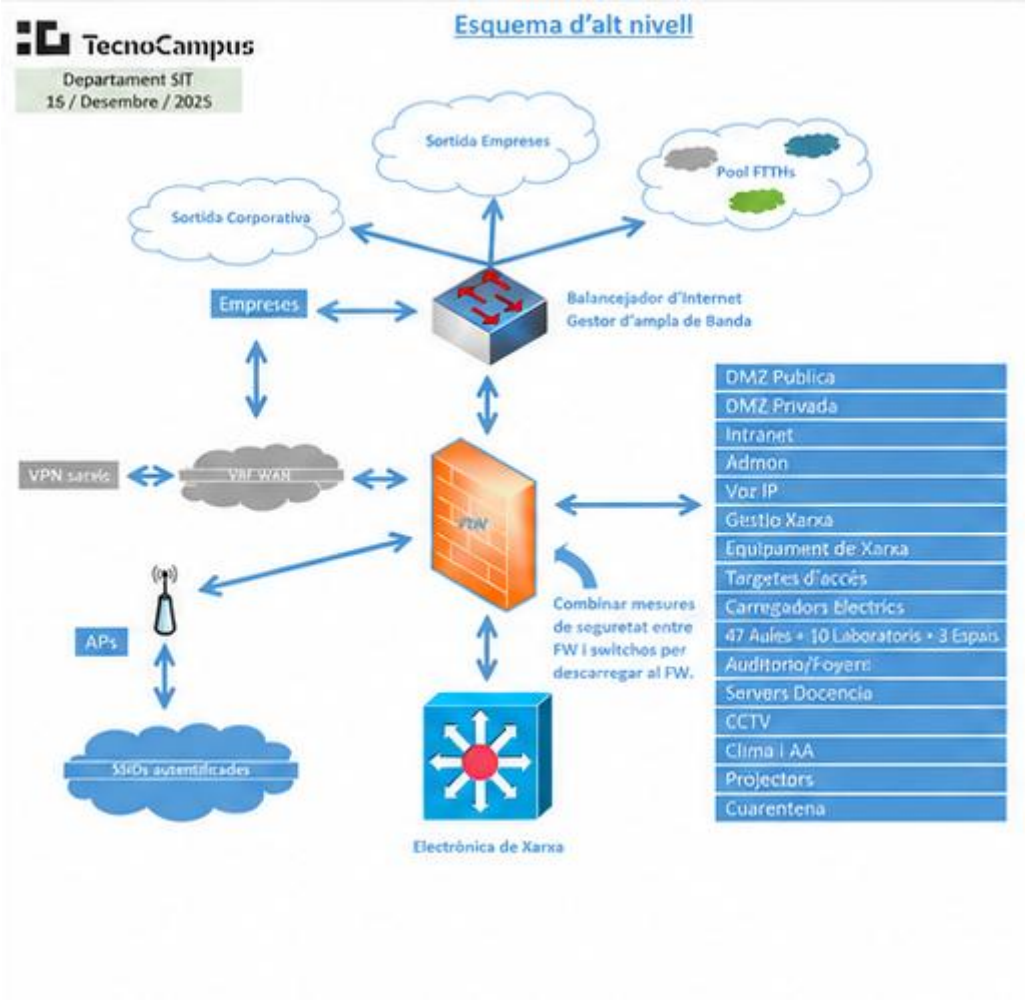


Figura 8 – Esquema d'alt nivell xarxa TecnoCampus

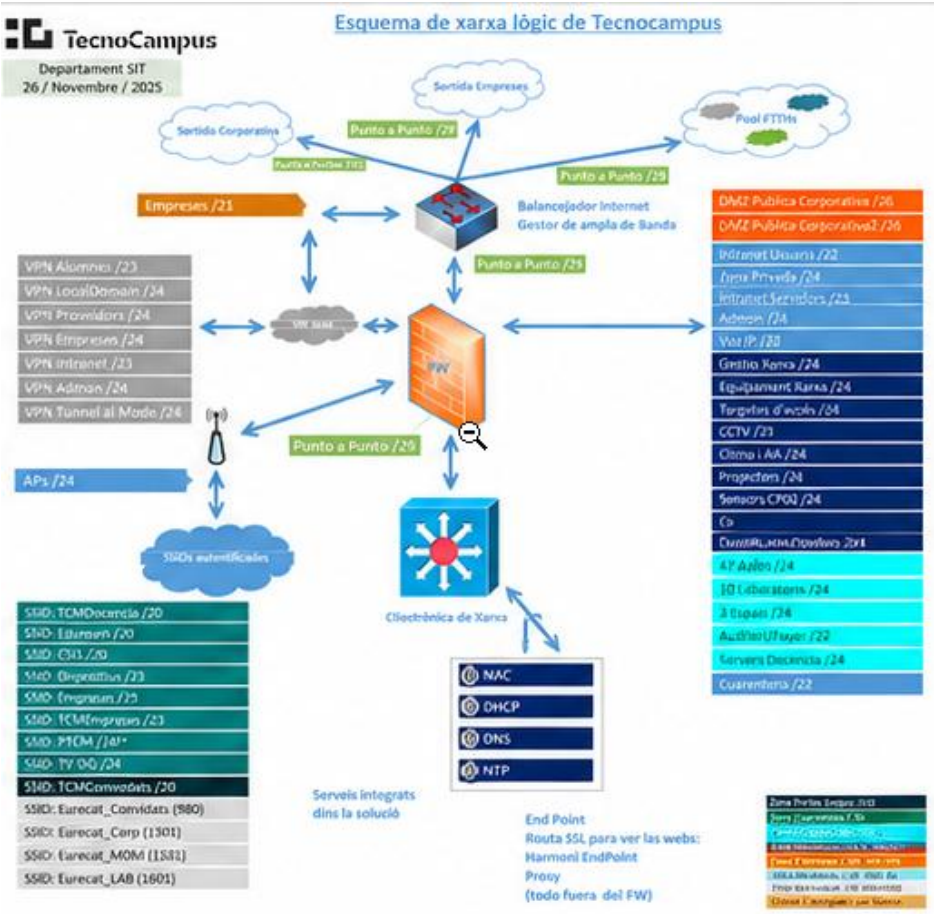


Figura 9 – Esquema de xarxa lògica TecnoCampus

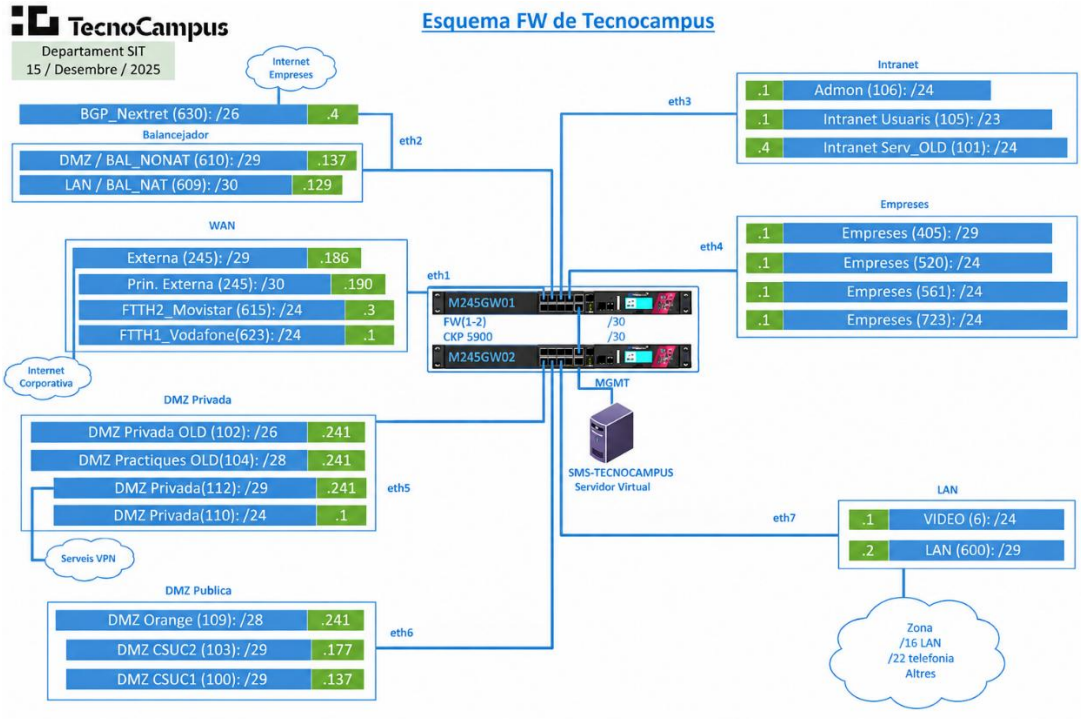


Figura 10 – Esquema servei de FW TecnoCampus

5.2 Proposta

La nova solució haurà de transformar l'entorn actual de seguretat garantint continuïtat, segmentació, integració amb serveis corporatius i migració controlada dels serveis existents, i haurà de definir zones, regles, polítiques, canvis, manteniment i monitoratge de seguretat, partint del model mínim indicat i permetent millores justificades.

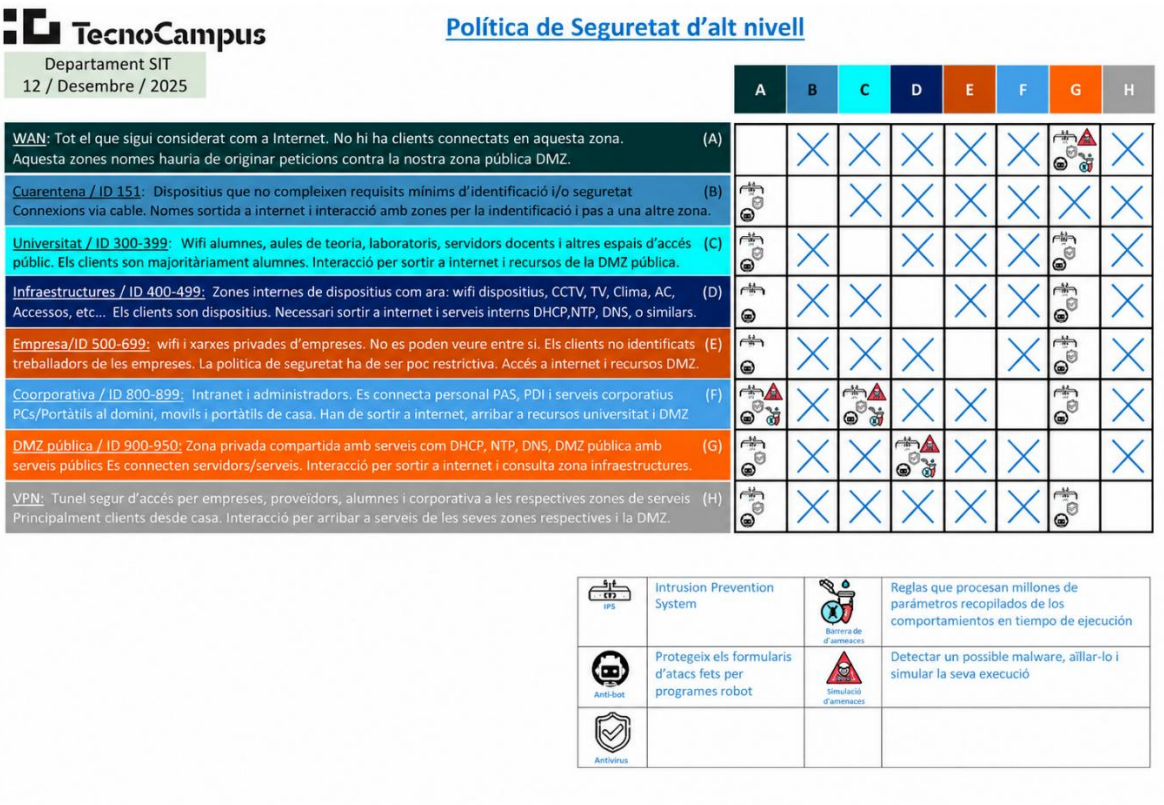


Figura 11 – Quadre de proposta inicial de política de seguretat d'alt nivell

5.2.1 Arquitectura

La solució de seguretat haurà d'oferir alta disponibilitat, rendiment acreditat, segmentació LAN/WAN, suport de polítiques avançades, logging, gestió centralitzada, integració SOC/XDR i continuïtat operativa.

5.2.2 Seguretat LAN

La seguretat LAN haurà de protegir el trànsit intern entre zones i segments del campus, aplicant polítiques específiques per a comunicacions est-oest i integrant-se amb la resta de components de seguretat.

La seguretat LAN haurà d'acreditar, com a mínim, 30 Gbps de throughput de firewalling i 24 Gbps d'inspecció IPS, amb latència i impacte operatiu compatibles amb les necessitats del servei.

El licitador haurà d'acreditar el rendiment requerit amb les funcionalitats de seguretat activades, independentment de l'arquitectura interna utilitzada.

5.2.3 Seguretat WAN

La seguretat WAN haurà de protegir el trànsit entrant i sortint, amb filtratge L4-L7, VPN, web filtering, priorització i capacitats SD-WAN o equivalents per garantir continuïtat i control del trànsit.

Haurà d'acreditar, com a mínim, 6 Gbps de throughput de firewalling amb les funcionalitats de seguretat requerides activades i ha de disposar de les interfícies necessàries per cobrir WAN, LAN, redundància i creixement previst, i haurà de suportar com a mínim 1.500 dispositius.

La solució WAN haurà d'incloure gestió centralitzada, failover, balanceig, VPN site-to-site, IPv6, polítiques de priorització, IDS/IPS, filtratge web/contingut, alta disponibilitat i separació de dominis o contextos de seguretat, i haurà de generar alertes operatives i de seguretat exportables als sistemes corporatius de monitorització i SOC.

5.2.4 Funcionalitats de la plataforma

La plataforma haurà de suportar, com a mínim, routing, NAT, VLAN, agregació, multicast, DHCP relay, IPv6, SNMP, QoS, traffic shaping, VPN, inspecció de seguretat, protecció antimalware i gestió/reporting centralitzat.

- Rendiment mínim: 36 Gbps en firewalling, 28 Gbps en inspecció IPS i 6 milions de sessions concurrents.
- Capacitat mínima: 240.000 noves connexions per segon i 16 Gbps de rendiment VPN IPsec.
- Suport mode firewall, mode IDS/IPS i mecanismes de clustering o escalabilitat equivalent.

Ha d'incloure la capacitat d'interfícies necessària per a la segmentació, connexions WAN/LAN, redundància i creixement previstos, mitjançant ports natius o mòduls suportats, així com l'actualització automàtica de signatures, intel·ligència d'amenaces, inspecció IPS i protecció antimalware.

5.2.5 Polítiques i altres serveis

La solució haurà de permetre polítiques per zona, origen, destinació, usuari, grup, aplicació, servei, URL, país i reputació, integrades amb directoris actius corporatius i bases de dades de seguretat actualitzades.

Control d'aplicacions. Polítiques i regles de gestió per a aplicacions.

La solució ha de permetre indicar quin trànsit s'analitzarà a nivell 4 i quin a nivell 7, oferint una flexibilitat completa en la gestió de la seguretat.

L'equip s'ha de poder integrar amb solució d'anàlisi de comportament de les mostres sospitoses via emulació en entorn aïllat (Sandboxing) , i la prevenció d'entrada de codi maliciós de dia zero de forma dinàmica, abans que es generi una signatura que el pugui reconèixer.

La solució ha de tenir la capacitat de bloquejar o no els fitxers amb valoració desconeguda, oferint flexibilitat en la gestió de la seguretat. L'anàlisi al núvol ha de complir amb els requeriments legals derivats de la LOPD i del RGPD, garantint la conformitat legal.

La solució haurà de permetre definir polítiques sobre fitxers desconeguts i garantir el compliment normatiu aplicable en l'anàlisi de mostres.

El sistema ha de ser utilitzable per a altres solucions de seguretat, incloent-hi connexió sniffer PCAP i integració via JSON API.

La solució ha de permetre compartir els hash dels fitxers analitzats per evitar validar fitxers ja coneguts en temps real.

La solució haurà de permetre balanceig i selecció de camí WAN segons disponibilitat, qualitat de línia, destinació, usuari, trànsit i ample de banda.

La solució haurà de permetre traffic shaping i protecció davant atacs de denegació de servei.

5.2.6 Gestió de la configuració dels equips:

La plataforma haurà de permetre gestió centralitzada de polítiques, objectes i dispositius, administració per rols, traçabilitat de canvis, visualització de topologia, identificació de regles sense ús i escalabilitat operativa.

La plataforma haurà de registrar connexions autoritzades i denegades, logs L4/L7, aplicacions, amenaces i polítiques, i permetre consultes, filtres i informes programats o a demanda.

5.2.7 Monitorització del trànsit a temps real

La solució haurà de proporcionar visibilitat en temps real del trànsit i esdeveniments de seguretat, amb dashboards, alertes, logs consolidats, exportació a sistemes externs i retenció/rotació de logs.

5.2.8 Monitoratge i operació

La solució haurà de suportar polítiques SD-WAN o equivalents i automatització de túnels IPsec per topologies hub/spoke o similars.

Els equips hauran de disposar d'APIs documentades per automatització, gestió i actualitzacions massives controlades.

5.2.9 Seguretat

La solució haurà d'incloure control d'aplicacions L7, filtratge URL/contingut, IPS, protecció antimalware, logs en temps real, suport de protocols amb fluxos múltiples, autodiagnosi de configuració i actualització automàtica de signatures i motors de seguretat.

5.2.9.1 Condicions mínimes de seguretat

Els components NGFW/IPS hauran d'estar inclosos i vigents al CPSTIC del CCN com a producte qualificat per a ENS Alt, o aportar certificació/evidència equivalent acceptada pel CCN quan correspongui.

5.3 Funcionalitats plataforma – Servei VPN

La plataforma haurà de permetre la migració i operació dels serveis VPN actuals, integrant-los en el servei de manteniment de base i garantint continuïtat, seguretat i evolució posterior.

L'esquema següent llista la configuració actual dels diferents serveis i perfilats VPN dels que disposa el TecnoCampus, servei a redefinir per a la seva optimització i configuració dins de la nova plataforma.

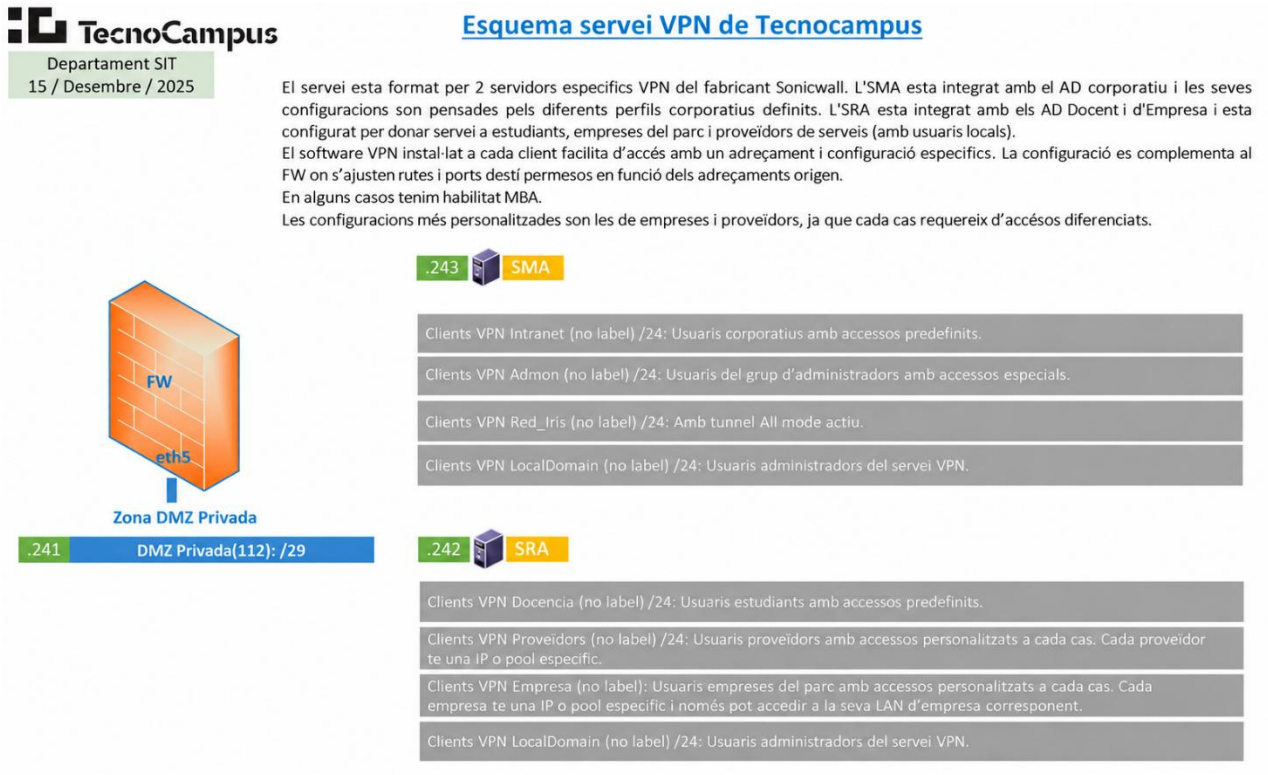


Figura 12 – Esquema del servei actual de VPN

La solució haurà de suportar VPN site-to-site, accés remot, túnels HTTPS, accés web sense agent, túnel complet amb agent, IPsec/GRE i agregació o balanceig de túnels.

5.4 Integració plataforma SOC TecnoCampus

La proposta haurà de garantir la integració funcional amb el SOC/XDR corporatiu del TecnoCampus, descrivint fluxos d'informació, casos d'ús, responsabilitats i procediments d'escalat.

La proposta haurà de garantir la integració funcional amb la plataforma SOC/XDR corporativa vigent, actualment Trend Micro Vision One, o la plataforma SOC/XDR corporativa vigent que el TecnoCampus determini durant la vigència contractual, mitjançant mecanismes suportats, APIs, connectors o procediments equivalents.

Es valoraran les propostes que aprofitin dades del SOC/XDR per enriquir polítiques, detectar comportaments anòmals, prioritzar riscos i activar respostes operatives.

Els productes llicenciats a la plataforma corporativa són:

- VisionOne Endpoint Security Essentials
- VisionOne Endpoint Security Pro
- VisionOne Email & Collaboration Security Dual
- XDR for Email
- VisionOne Sandboxing
- TrendMicro Internet Security
- TrendMicro Managed XDR
- CyberRisk Exposure Management Essentials

La compatibilitat amb el SOC/XDR corporatiu haurà d'estar acreditada mitjançant documentació del fabricant, connectors suportats, APIs, referències o evidències equivalents

6. SERVEI DE MANTENIMENT DE BASE

El servei haurà de garantir l'operació ordinària, el suport, el manteniment de base, el reporting, la documentació i la millora contínua de les plataformes incloses.

Aquest servei serà reactiu a les incidències reportades per TecnoCampus i proactiu envers la planificació de totes les intervencions programades o requerides de manteniment preventiu i normatiu de les infraestructures i serveis del contracte. Aquesta planificació ha de ser presentada a inici del servei i de manera trimestral al TecnoCampus.

El servei disposarà d'una bossa econòmica per a material, components o recanvis necessaris per a manteniment correctiu, restitució del servei o substitució d'elements no coberts per garantia o suport de fabricant. No es podrà destinar a ampliacions, nous projectes, nous serveis ni evolutius. El consum requerirà autorització prèvia i només es facturarà el material efectivament subministrat i recepcionat.

Les intervencions del servei de gestió de base quedaran definides de la següent manera:

Servei de manteniment (Servei de Base):

Assumirà totes les tasques pròpies d'un servei correctiu i preventiu que asseguri en tot moment un servei òptim de les infraestructures incloses en aquest projecte. Totes aquestes intervencions quedaran dins del servei definit com a manteniment de base, incloent:

- **Manteniment Correctiu**: Servei reactiu assumit pels recursos de l'adjudicatari per solucionar qualsevol incidència reportada pel TecnoCampus, donant compliment als SLAs indicats aquest contracte.
- **Manteniment Preventiu i de millora continua**: Servei proactiu, que inclou totes les tasques recomanades per mantenir l'entorn físic i lògic en perfecte funcionament, actualitzat i optimitzat per treballar de la manera més eficient i segura en tot cas.

Els recursos del servei estaran definits per:

- **Equip de suport tècnic**: servei proper al client que es compon per un equip tècnic multidisciplinari de suport que gestiona tots els assumptes relacionats amb el dia a dia del servei de TecnoCampus quan aquest ho requereixi. El licitador ha d'assegurar que els recursos tenen en tot moment un coneixement adequat de l'entorn del TecnoCampus i que disposen de tota la documentació per assumir les intervencions de primer nivell i escalar i gestionar la intervenció dels equips especialitzats en cas requerit.
  En cas necessari també seran responsables d'elevar consulta de segon o tercer nivell/fabricant per atendre les incidències escalades en cas necessari, o bé per peticions o projectes. De la mateixa manera l'adjudicatari del servei vetllarà per a que el coneixement del servei i accés a documentació específica sigui continuada, ràpida i eficient en tot cas.
- **Service Manager**: La funció de la gestió de servei és desenvolupada pel Service Manager responsable operatiu dels serveis contractats, en conjunt, amb background tècnic important en la solució implantada a TecnoCampus. Una de les seves funcions principals és liderar el servei del client assegurant la màxima disponibilitat dels serveis i màxima satisfacció del client. Dins de les seves múltiples funcions, cal destacar l'elaboració i la presentació dels informes següents:

- Informe de Servei: Document mitjançant el qual es fa constatar el compliment contractual de la qualitat de servei, mesurant la consecució dels objectius de cadascun dels KPIs.
- Informe d'incidències complert

Per altra banda serà també el responsable i interlocutor amb els responsables del contracte per definir totes les tasques i projectes proposades pel TecnoCampus per millorar el servei, projectes de baix o alt impacte requerits per solucionar de manera definitiva incidències resoltes en primer nivell. Aquest seguiment serà evident des de la validació de la proposta al seu pas a producció i monitorització a l'eina específica del TecnoCampus (Centreon, veure punt 6.1.1))

6.1 Monitorització

Tota l'equipament i serveis de la solució implantada estarà monitoritzada a l'eina corporativa del TecnoCampus, conforme indicat al punt 6.1.1.

Dins del procés de transformació cal implementar els nivells de monitorització adequats per que els serveis del TecnoCampus puguin tenir visibilitat 24x7 de tot l'equipament instal·lat, serveis desplegats i tota la informació que es consideri necessària per poder monitoritzar adequadament el servei i elevar les incidències al servei de manteniment de base de l'adjudicatari amb la criticitat adequada.

Els ajustos ordinaris derivats de l'operació del servei s'inclouran en el servei base. Les ampliacions, evolutius o canvis substancials es tramitaran mitjançant el mecanisme previst per a actuacions evolutives

Queda doncs dins de les responsabilitats de l'adjudicatari del servei presentar i implementar una proposta de monitorització de cadascun dels equipaments i serveis desplegats de manera específica, definint variables a monitoritzar i els nivells d'alarma (OK / Warning / Critical) de cada valor monitoritzat. Els valors monitoritzats podran ser modificats, eliminats o ampliats durant la vigència del contracte

6.1.1 Eina de Monitorització TecnoCampus

Tecnocampus disposa d'un entorn de monitorització propi gestionat per un servei extern que rep i fa seguiment de les alarmes rebudes, així com l'escalat als serveis que corresponguin en cada cas segons procediment acordat i nivells de criticitat. Aquesta plataforma és Centreon v25.10.10

TecnoCampus opera la plataforma corporativa Centreon. L'adjudicatari haurà d'integrar-hi i mantenir monitoritzats tots els equips i serveis objecte del contracte, definir variables i llindars, atendre els escalats segons ANS i documentar les incidències. La coordinació es realitzarà amb el proveïdor de Centreon que el TecnoCampus determini en cada moment.

Es requereix que el licitador presenti i implementi una proposta de monitorització de tots els elements i serveis inclosos a aquest projecte complerta i en compliment dels requeriments de fabricant i experiència pròpia, prioritzant la via SNMP i via API en cas necessari. Aquesta integració requerirà treballar conjuntament amb el mantenidor actual de la plataforma Centreon, l'empresa Ithink UPC a

data d'adjudicació d'aquest contracte o bé amb el proveïdor que determini el TecnoCampus durant el temps de contracte, esdevenint una part de projecte claus en ma.

TecnoCampus opera Centreon; l'adjudicatari integra, manté la integració, atén escalats i documenta incidències.

6.2 Casos d'us

Es plantegen diferents situacions operatives sobre les quals el licitador haurà de descriure el procediment complet d'actuació, incloent detecció, diagnosi, priorització, escalat, execució, comunicació al TecnoCampus, temps estimats de resposta i resolució, documentació posterior i incorporació a la millora contínua. Els temps proposats hauran de ser coherents amb els ANS del servei.

- **Situació 1**: Recepció d'una alarma o notificació d'avaria d'un switch de planta no apilat. El licitador haurà de descriure el procediment de diagnosi, confirmació d'impacte, comunicació, substitució o recuperació del servei, verificació posterior i actualització documental.
- **Situació 2**: Sol·licitud de creació d'un nou servei que requereixi una VLAN interna, etiquetatge, dimensionament, extensió a punts concrets, polítiques de control i condicions de sortida a Internet. El licitador haurà d'indicar si aquesta actuació es considera canvi ordinari, actuació evolutiva o projecte específic, i descriure el procediment d'anàlisi, aprovació, execució, proves i documentació.
- **Situació 3**: Ens arriba la creació d'una nova zona de seguretat amb detall de com ha de comportar-se amb la resta de zones en producció.
- **Situació 4:** Ens arriba un problema de lentitud a una de les SSIDs publicades. Procediment d'interacció/coordinació amb el servei de manteniment vigent de la xarxa sense fils i elements a verificar dins el servei.
- **Situació 5**: Es detecta un adreçament incorrecte no inventariat dins els nostres sistemes. Els clients que el tenen no poden sortir ni a la LAN, ni a la WAN. Procediment i elements a verificar dins el servei.

6.3 Paràmetres de gestió de la qualitat de servei

Els següents aspectes i indicadors seran un referent per avaluar la correcta gestió de la qualitat del servei i seran revisats de forma mensual pel TecnoCampus. Es considera aquesta avaluació de manera específica dins del servei de gestió, ja que serà el servei del que dependrà qualsevol interacció amb la infraestructura inclosa a aquest contracte, i per tant la qualitat de servei.

Es considera adient limitar aquests paràmetres a la gestió de les incidències amb afectació al servei, i per tant es classificaran els diferents tipus d'incidències segons la seva criticitat:

- **Urgent.** Seran les incidències que provoquin una afectació global, que impedeixin la realització de les activitats i afecti a una majoria dels usuaris, sobre tot en l'àmbit docent. L'objectiu és continuar amb l'activitat docent o empresarial de forma immediata i poder donar-les amb les màximes garanties de qualitat.
- **Alta**. Seran les incidències amb un afectació parcial, que impedeixi el correcte funcionament i que afectin a un nombre reduït de clients.
- **Normal**. Seran les incidències, que no impedeixin la continuïtat dels serveis i permetin continuar amb la activitat normal

Temps de resposta i temps de resolució

Es defineix com a **temps de resposta** el període màxim entre la recepció de la incidència pel servei de gestió o bé la notificació per part dels responsables del contracte del TecnoCampus i l'inici del procediment d'anàlisi i resolució de la mateixa.

Es defineix com a **temps de resolució** el període màxim entre la recepció de la incidència pel servei de gestió o bé la notificació per part dels responsables del contracte del TecnoCampus i la completa resolució de la mateixa i documentació a l'eina de ticketing o seguiment del servei, així com la seva notificació als responsables del contracte del TecnoCampus.

Quadre de compliment de nivells de servei Tipus incidència	Temps resposta	Temps resolució
Urgent	<15'	<1h
Alta	<30'	<4h
Normal	<60'	NBD

Els acords de servei aquí indicats hauran de ser d'obligat compliment per l'adjudicatari.

6.4 Pla de devolució del servei

Amb una antelació mínima de 30 dies abans de la finalització del període contractual s'ha de programar un traspàs dels serveis cap al nou licitador si correspon. Aquest traspàs s'ha de realitzar de forma que en tot moment el funcionament del servei quedi garantit. Cap cost derivat d'aquesta devolució del servei serà facturat a TecnoCampus per part de l'adjudicatari (sortint).

El procés de devolució es desenvoluparà en dues fases.

6.4.1 Fase de captura i planificació.

Aquesta fase es realitzarà dins dels quinze dies anteriors a la finalització del contracte. Durant aquesta fase, l'adjudicatari sortint serà el responsable del servei i de la seva facturació. L'adjudicatari actual del contracte haurà de recollir i aportar en aquesta fase tota la documentació relacionada amb el servei, plans de manteniment, desenvolupaments, millora i/o implementacions efectuades, per tal que el nou adjudicatari pugui planificar i posar en marxa el servei sense problemes. Per a facilitar aquesta transició, l'adjudicatari actual proporcionarà un pla de formació especialment dissenyat per traspassar el coneixement del servei al nou adjudicatari. Aquesta formació ha de quedar estructurada seguint els àmbits inclosos a aquest contracte i ha de ser validada pel TecnoCampus abans de la seva execució. En cas de canvi de plataforma de gestió caldrà col·laborar amb el nou adjudicatari a fi de facilitar la correcta implantació de l'entorn al nou sistema de gestió, facilitat tota la informació necessària

Com a mínim la planificació contindrà aquestes sessions (3h) de formació per àmbit on quedi definida tant la seva estructura com components, així com un històric de les incidències més representatives, millores implementades i canvis representatius.

6.4.2 Fase de traspàs.

S'iniciarà un cop finalitzada la fase anterior. El nou adjudicatari facturarà els serveis i té la responsabilitat del compliment dels nivells de servei oferts per a la seva fase d'execució de la transició, que com a mínim han de ser iguals als actuals, sota la supervisió de l'empresa sortint.

El licitador haurà de preveure el cost d'aquesta fase i estarà inclòs en l'oferta presentada per aquest.

Tot el període de devolució, no superarà el termini d'un mes.

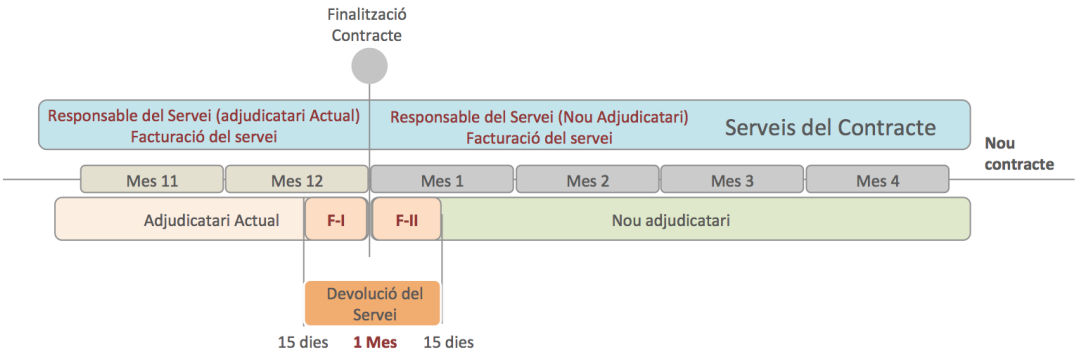


Figura 13 – Esquema de retorn del servei

7. TRANSFERÈNCIA DE CONEIXEMENTS

El licitador presentarà un calendari de formació genèrica i específica per servei, amb sessions per àmbit tecnològic, documentació, materials de suport i resolució de dubtes. Les sessions pràctiques o de refresc addicionals que s'ofereixin s'identificaran a la propostaLa transferència de coneixement haurà d'incloure sessions estructurades per àmbit tecnològic, documentació associada, materials de suport i resolució de dubtes. L'objectiu és que l'equip tècnic del TecnoCampus disposi del coneixement necessari per governar el servei, interpretar la documentació, supervisar l'operació i executar tasques bàsiques de control sobre la nova infraestructura i les eines associades. Es requerirà un refresc d'aquesta formació en una jornada complerta de manera semestral per assegurar que el coneixement continua del tot actualitzat o a petició justificada per part del TecnoCampus.

8. PLA DE QUALITAT

L'adjudicatari haurà d'acreditar sistemes de gestió, certificacions o mecanismes equivalents de qualitat, seguretat, continuïtat i sostenibilitat directament relacionats amb l'objecte del contracte.

- ISO 9001, 14001 i 20000-1
- Certificat ENS Alt
- Relació certificada de partnership amb el fabricant dels productes presentats

8.1 Exigències transversals de qualitat

El fabricant declararà sota responsabilitat que no es troba sotmès a restriccions, llistes o sancions que impedeixin el subministrament d'equips, microprogramari i actualitzacions durant la vigència del contracte; i que disposa de cadena de subministrament i magatzem/logística a la UE per garantir recanvis NBD

Per tal de garantir la solvència tècnica, maduresa i continuïtat tecnològica de les solucions proposades, es requereix que el fabricant hagi figurat com a "Leader" almenys en dues de les tres darreres publicacions dels informes de referència de Gartner corresponents al seu àmbit.

Per a l'equipament CORE/LAN, es prendrà com a referència l'informe *Enterprise Wired and Wireless LAN Infrastructure*; i per a Firewall, els informes SD-WAN i Network Firewalls / Hybrid Mesh Firewall, considerant la continuïtat o evolució de la categoria Gartner.

La plataforma SaaS de gestió i telemetria de tots els equips (LAN/CORE/NAC/Firewall/DDI) haurà d'operar únicament en centres de dades ubicats a la UE, sota entitat jurídica UE, complint ENS Alt ISO/IEC 27001 i amb xifratge end-to-end.

No s'admetran transferències internacionals de dades d'operació/telemetria a països sense decisió d'adequació del RGPD ni sotmeses a legislacions extracomunitàries que permetin accés governamental sense garanties equivalents."

8.2 Exigències mediambientals

Els equips i components subministrats hauran de complir la normativa ambiental aplicable a la comercialització d'aparells elèctrics i electrònics a la Unió Europea i incorporar criteris d'eficiència energètica, durabilitat i reducció de l'impacte ambiental durant el seu cicle de vida.

L'adjudicatari haurà de garantir una correcta gestió dels equips, components i materials retirats durant l'execució del contracte, prioritzant-ne, quan sigui possible, la reutilització i, en la resta de casos, la seva gestió com a residus d'aparells elèctrics i electrònics (RAEE) mitjançant els canals i gestors autoritzats corresponents, aportant al TecnoCampus la documentació acreditativa de la seva correcta gestió.

Així mateix, es requerirà minimitzar els embalatges i materials d'un sol ús, prioritzar materials reutilitzables o reciclables i retirar adequadament els residus generats durant les actuacions d'instal·lació i manteniment.

Els equips proposats hauran de disposar de funcionalitats o mecanismes d'optimització del consum energètic quan aquests siguin aplicables a la seva tipologia i funcionalitat, i el licitador haurà d'aportar, quan estigui disponible, informació del fabricant relativa al consum i eficiència energètica dels equips

9. MEMÒRIA

Els licitadors hauran de presentar una memòria tècnica estructurada segons aquest apartat, orientada a acreditar comprensió de l'entorn, adequació de la solució, pla d'implantació, servei de manteniment de base i compliment dels requisits mínims.

- **Proposta pla tecnològic**

La memòria haurà d'acreditar l'adequació de l'equipament i serveis proposats, el dimensionament, la integració i el compliment dels requeriments mínims per a Core, LAN, FW, NAC, DDI/NTP i plataforma de gestió considerats als punts específics d'aquest document.

- **Procediment de transformació i pas a producció**

Cal presentar una proposta on es faci referència al procediment complert de transformació de cadascun dels serveis, entorn o plataformes que formen part de l'ecosistema actual del TecnoCampus i que queden inclosos a aquesta contractació

La memòria haurà d'incloure, per cada entorn, metodologia, calendari, dependències, pla d'actuació, proves, pas a producció, rollback, documentació i pas al servei de manteniment de base.

- **Servei de manteniment de base**

La memòria haurà de descriure recursos, rols, model operatiu, procediments, monitorització, reporting, millora contínua, escalats, qualitat del servei i devolució.

Com a documentació específica cal considerar:

- Resolució dels casos d'us i/o incidències definides part del servei de gestió indicats al punt 6.2 d'aquest document resolució al nivell de detall adequat dels diferents casos d'us llistats al punt específic. S'ha de procedimentar des de l'event monitoritzat a la completa resolució, informació al TecnoCampus, documentació del cas d'us i ves de consideració per considerar-lo dins del procés de millora contínua del servei per evitar i/o automatitzar casos similars reduint qualsevol afectació al servei.

- **Pla de formació als responsables del contracte per part del TecnoCampus**

Cal proposar segons indicat al punt 7 d'aquest document un calendari de formació genèrica i específica per servei, incloent tota la documentació generada durant el procés d'auditoria inicial, procés de transformació i pas a producció de cada servei i entorn o plataforma. Aquesta formació serà la necessària per que els responsables del servei puguin fer un seguiment del servei adequat, o arribat el cas, fer propostes de canvis o millores del servei, així com els fonaments necessaris per proposar nous serveis o requeriments.

TecnoCampus podrà demanar de manera unilateral i justificada formacions específiques incloses al contracte durant el període de servei a fi d'optimitzar els seus coneixements envers canvis a la plataforma.

- **Pla de devolució del servei**

Cal proposar un pla de compliment del pla de devolució dels servei segons indicat a punt 6.4, cercant la màxima eficiència, assignació de recursos adients de manera justificada i gestió documental adequada.

- **Document de compliment del pla de Qualitat**

Es requereix la presentació de la documentació oficial adient per evidenciar el compliment de totes les certificacions, nivells i exigències llistades al punt 8 i 8.1 d'aquest document. Es considera necessari per assegurar tant la correcta gestió del projecte com la de les dades i informació del mateix, així com el compliment d'estàndards i recomanacions envers la protecció de la dada i dels usuaris

9.1 Proposta detallada d'equipament i serveis

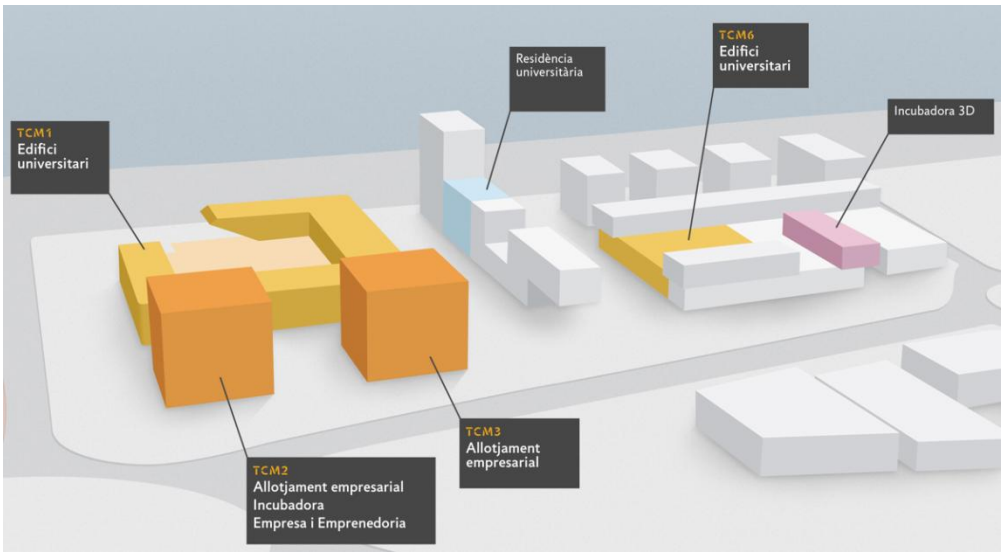
El licitador haurà d'emplenar la proposta detallada d'equipament i serveis per cada entorn d'aquest contracte (CORE, LAN, NAC, DDI, FW) incorporant fitxes, dimensionament, llicenciament, suport i integracions.

- Descripció general centrada en el projecte TecnoCampus.
- Volumetria d'equips justificada proposats seguint els mínims i proposats al punt específic
- Documentació gràfica que justifiqui la proposta (equipament, tipologia d'equips i ports i ubicacions).

ANNEX DE DOCUMENTACIÓ GRÀFICA DEL PROJECTE DE RENOVACIÓ, IMPLANTACIÓ I SERVEI DE MANTENIMENT DE BASE DE LA INFRAESTRUCTURA DE XARXA, SEGURETAT I SERVEIS ASSOCIATS DEL TECNOCAMPUS MATARÓ-MARESME

Exp. Número ES_LA0011122_2026_EXP_277

TecnoCampus es una Fundació Publica ubicada a la av. d'Ernest Lluch 32 de Mataró.



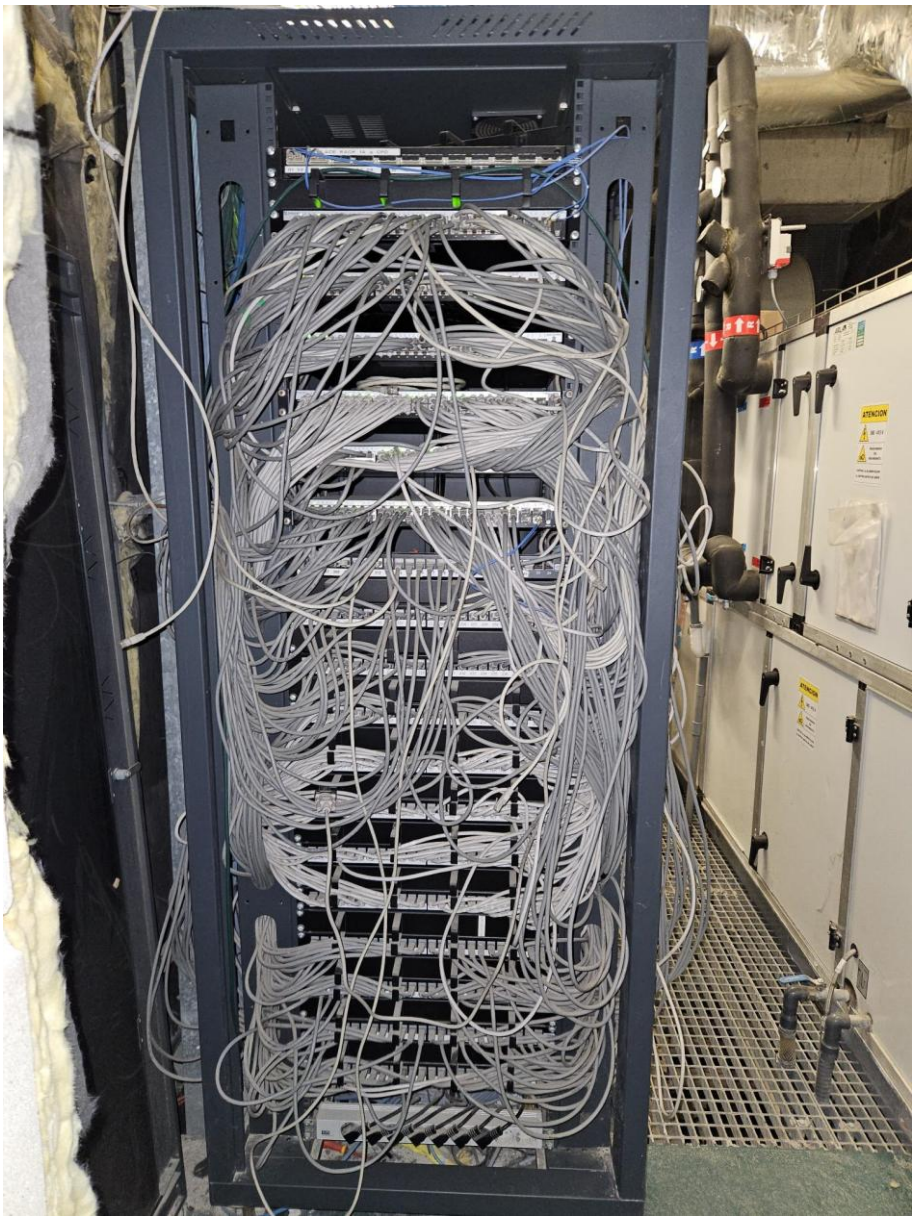
Esquema ubicacions TecnoCampus

A continuació es llisten les fotografies de l'estat actual dels racks a les diferents ubicacions. Qualsevol dubte que generi aquesta documentació s'ha de consultar per les vies definides a aquest procediment.

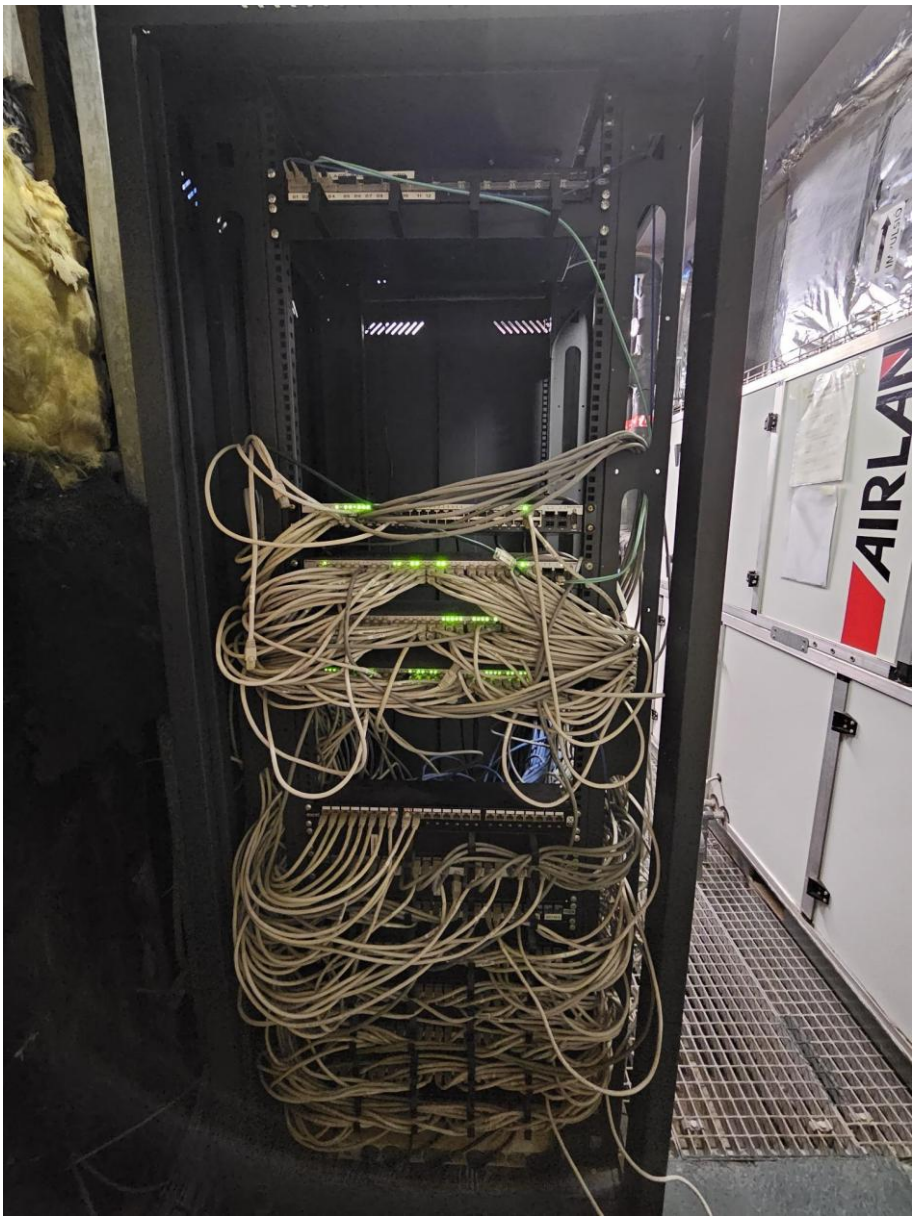
Edifici TCM1

Zona A

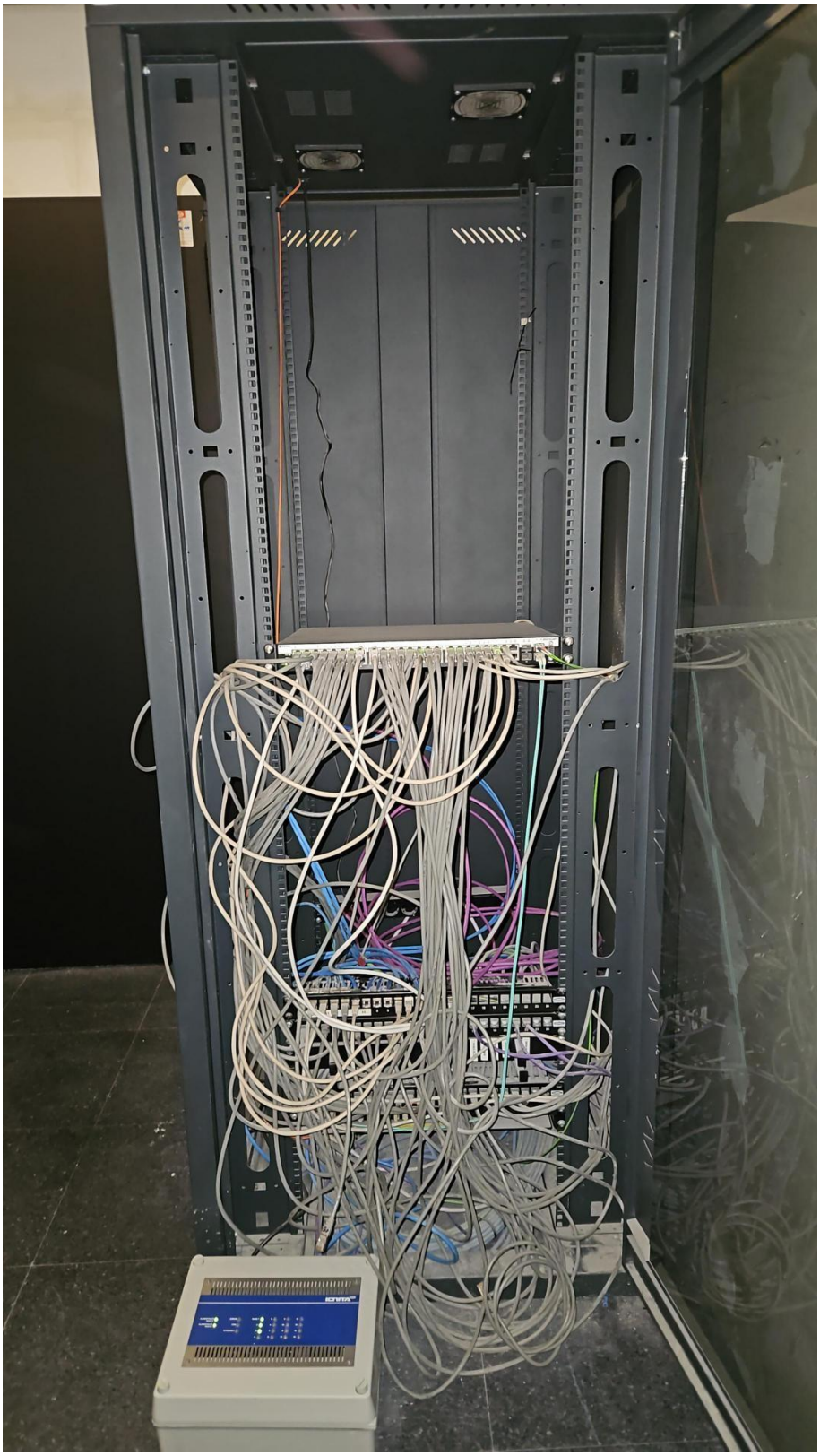
clima_tcm1_pb_a_front



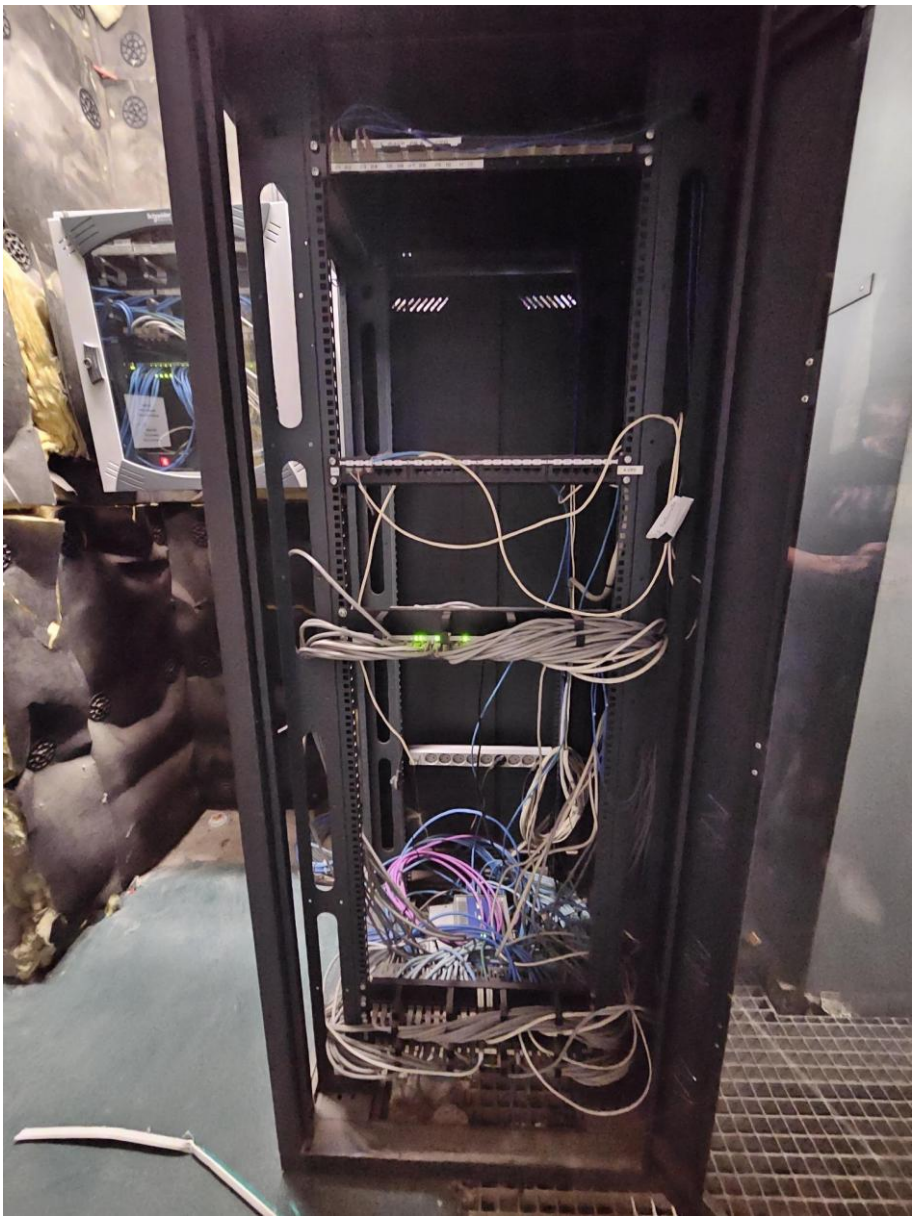
veu_clima_tcm1_p1_a_front



veu_clima_tcm1_p2_a_front

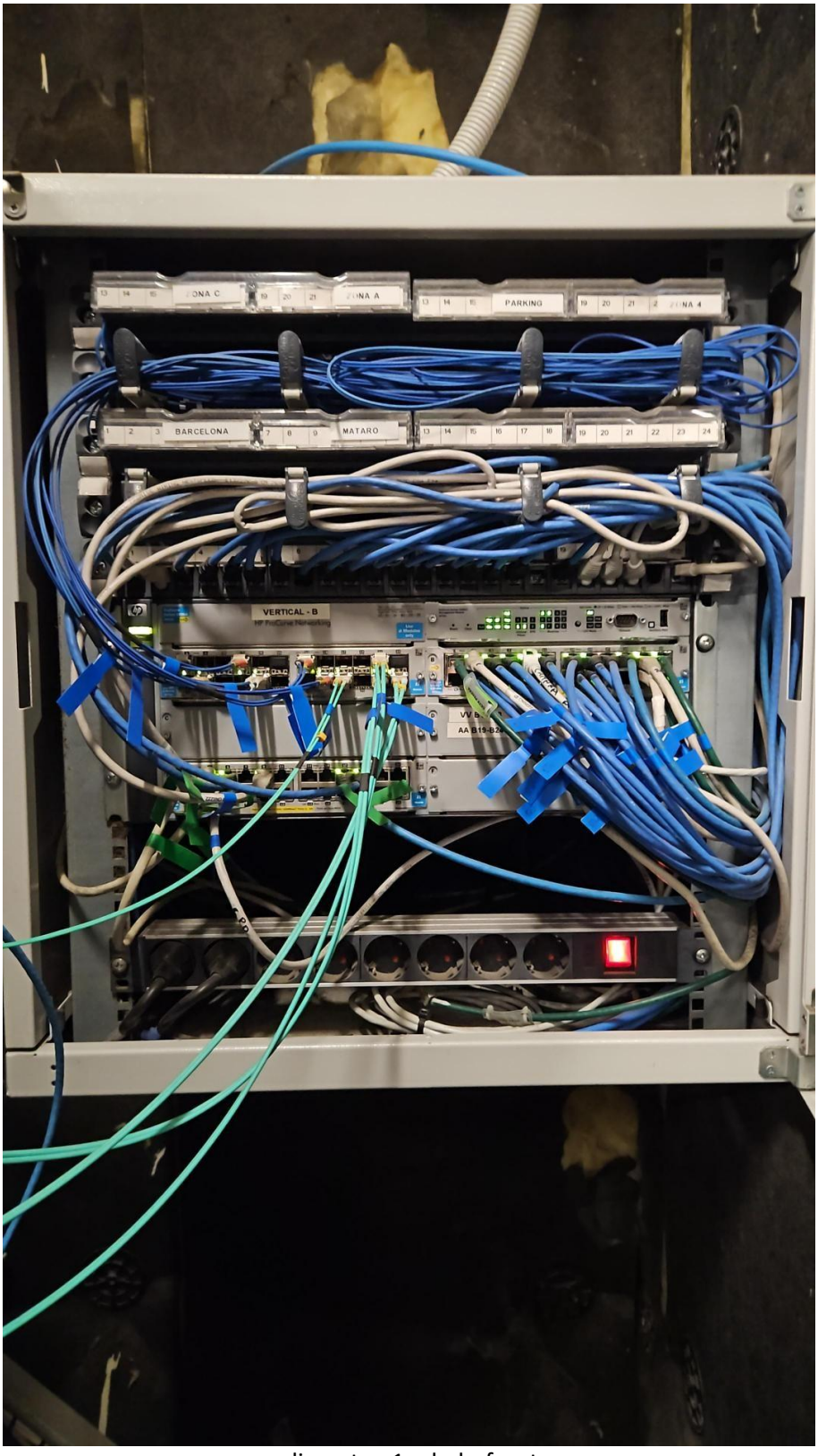


veu_tcm1_p-1_a_front

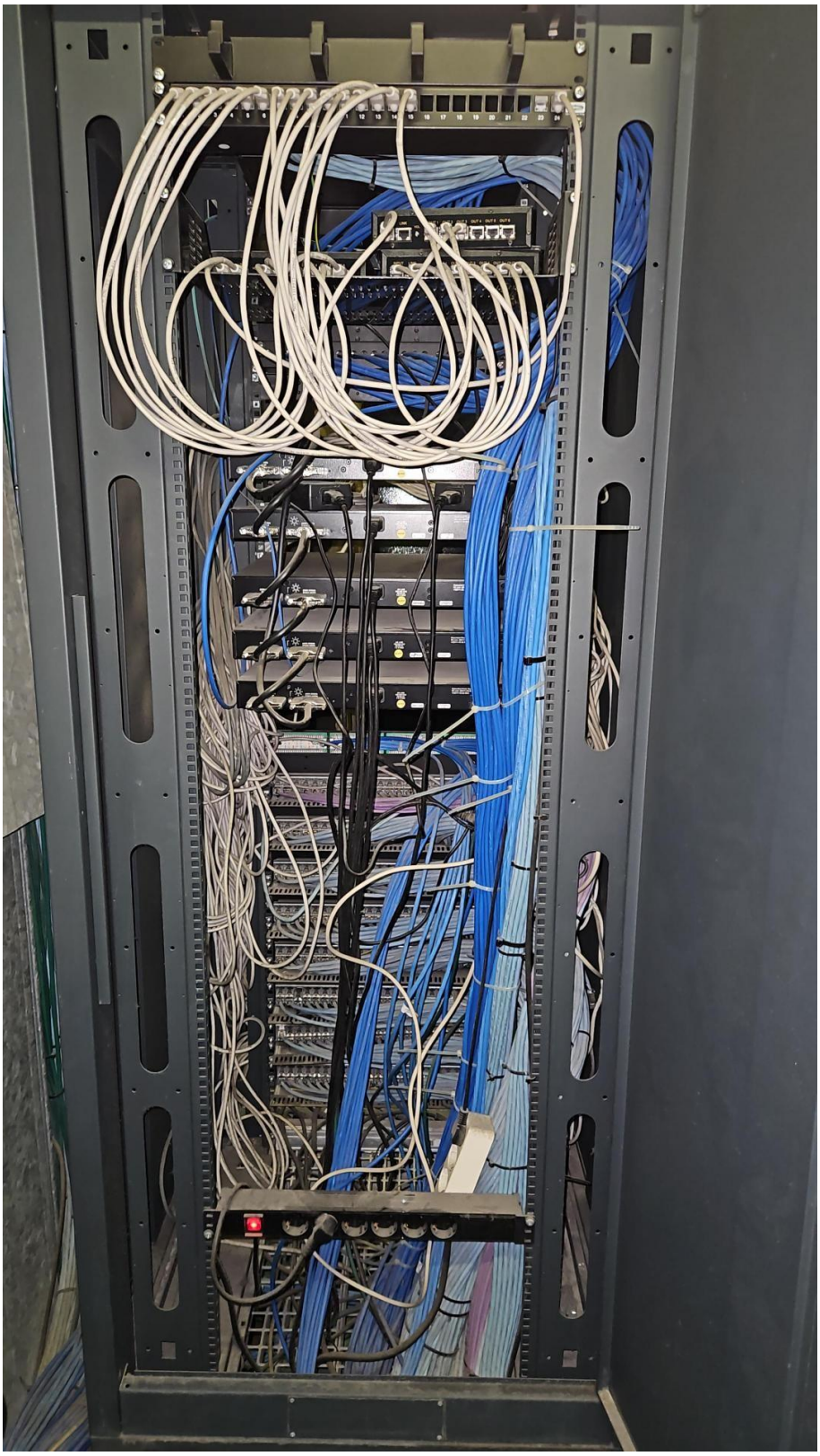


veu_tcm1_pb_a_front

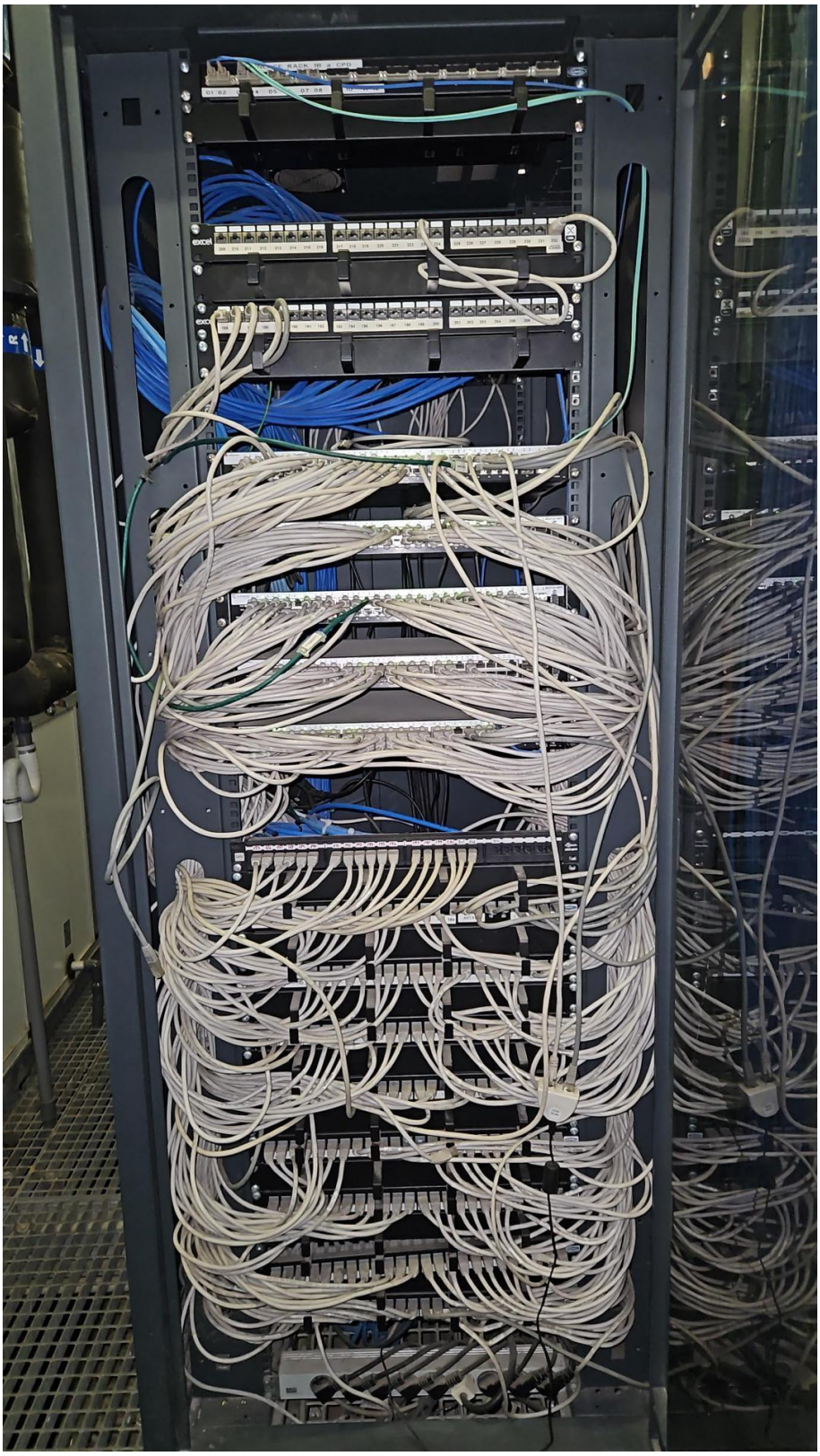
Zona B



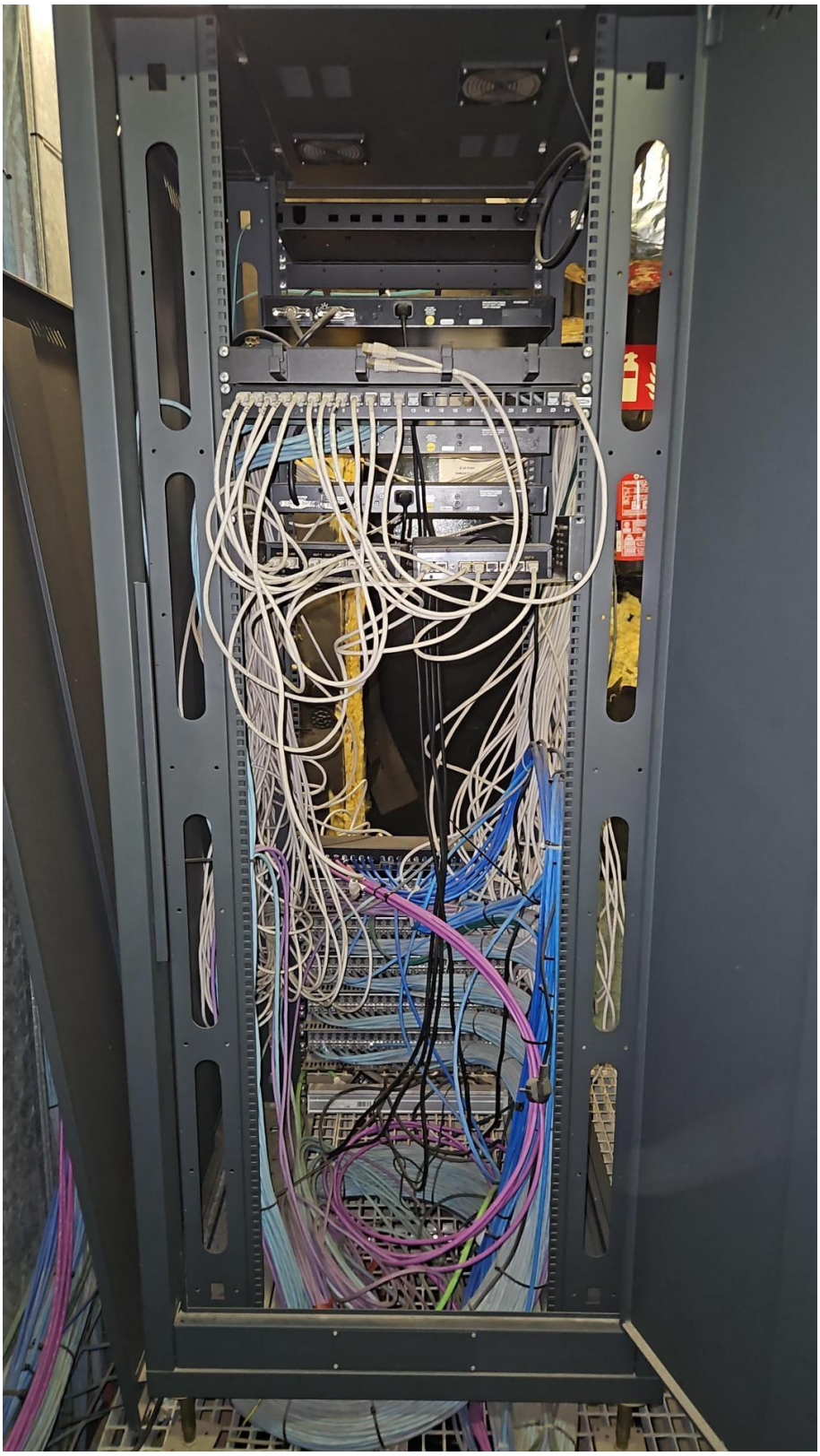
clima_tcm1_pb_b_front



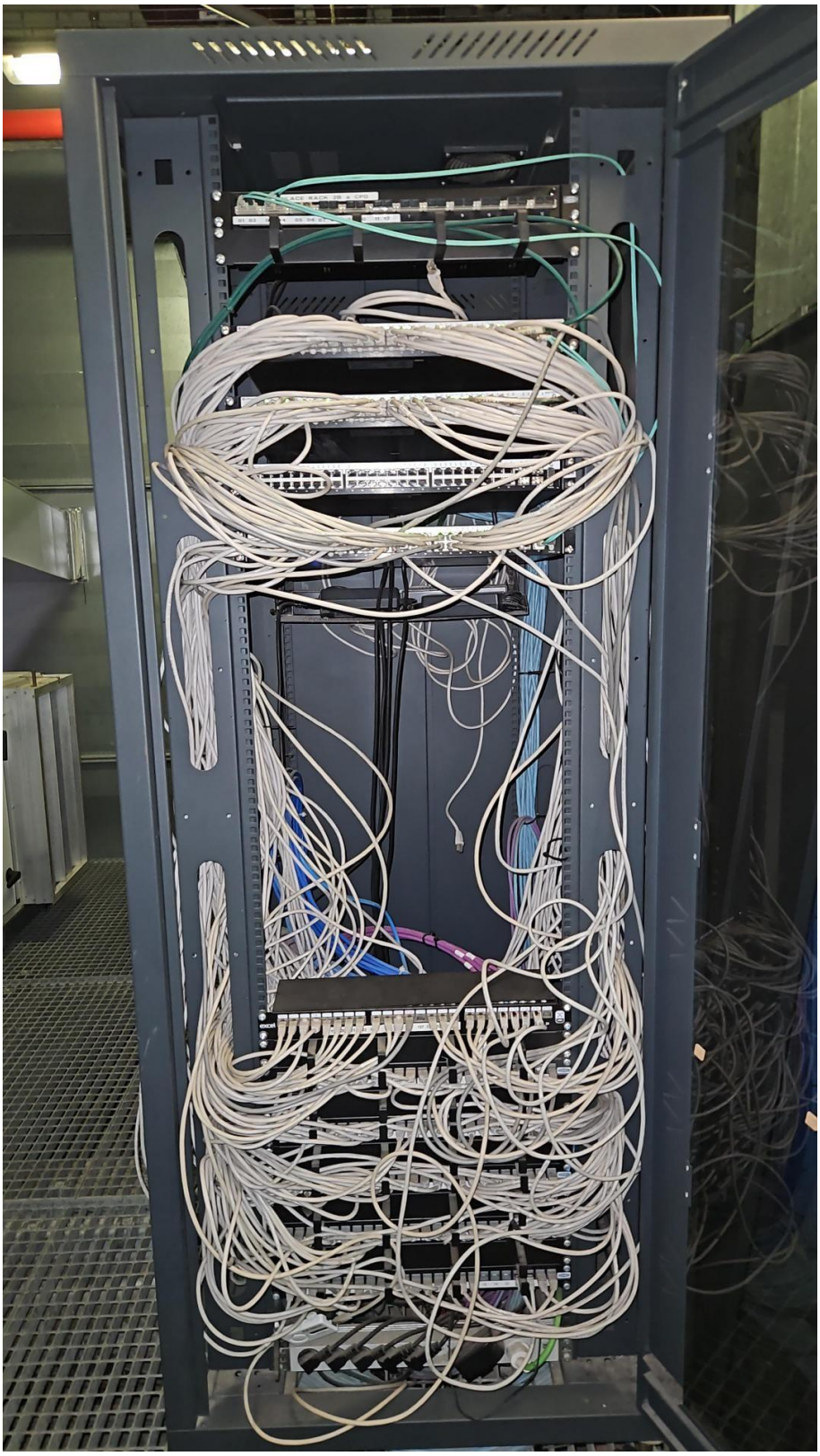
veu_clima_tcm1_p1_b_back



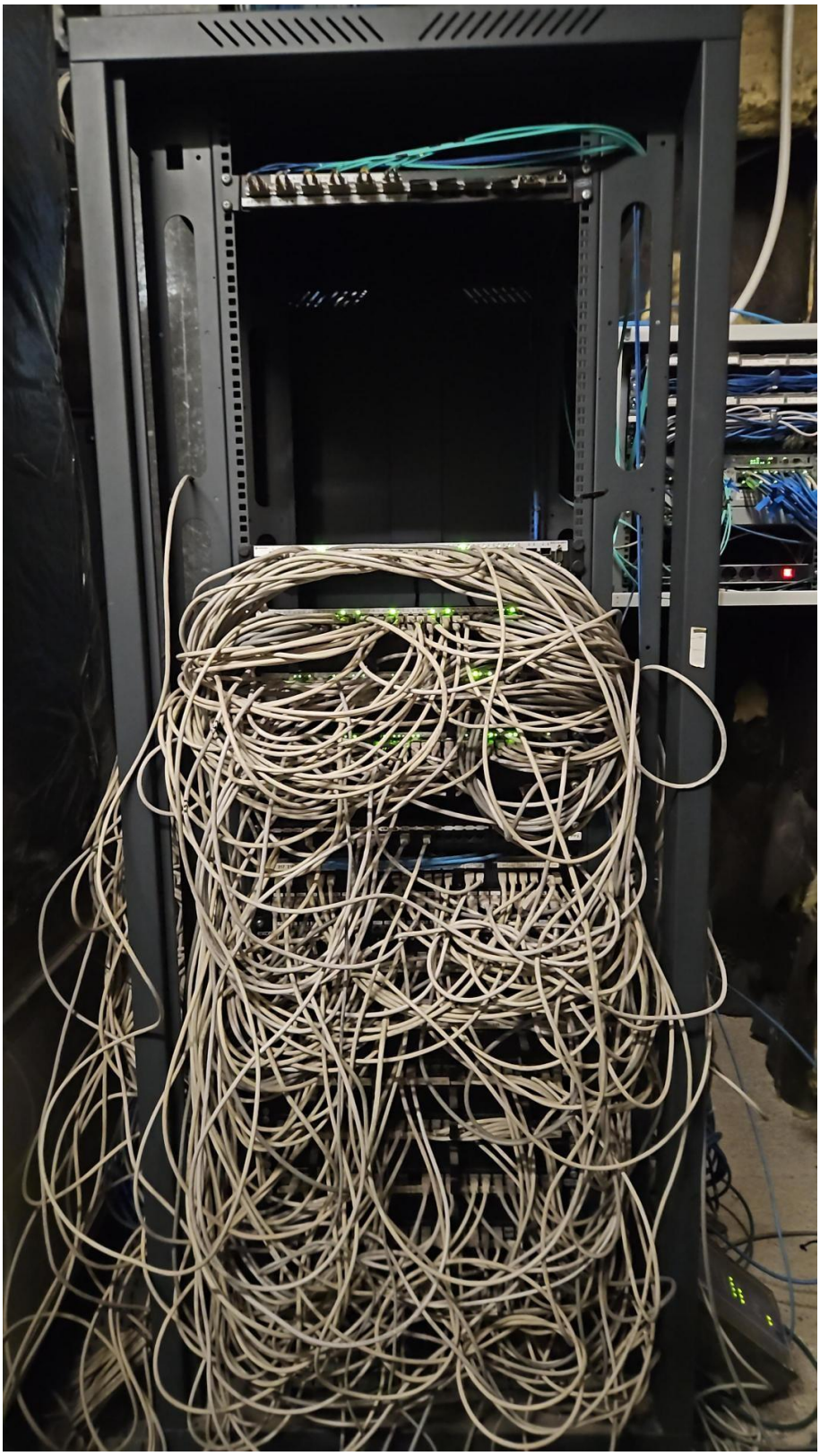
veu_clima_tcm1_p1_b_front



veu_clima_tcm1_p2_b_back

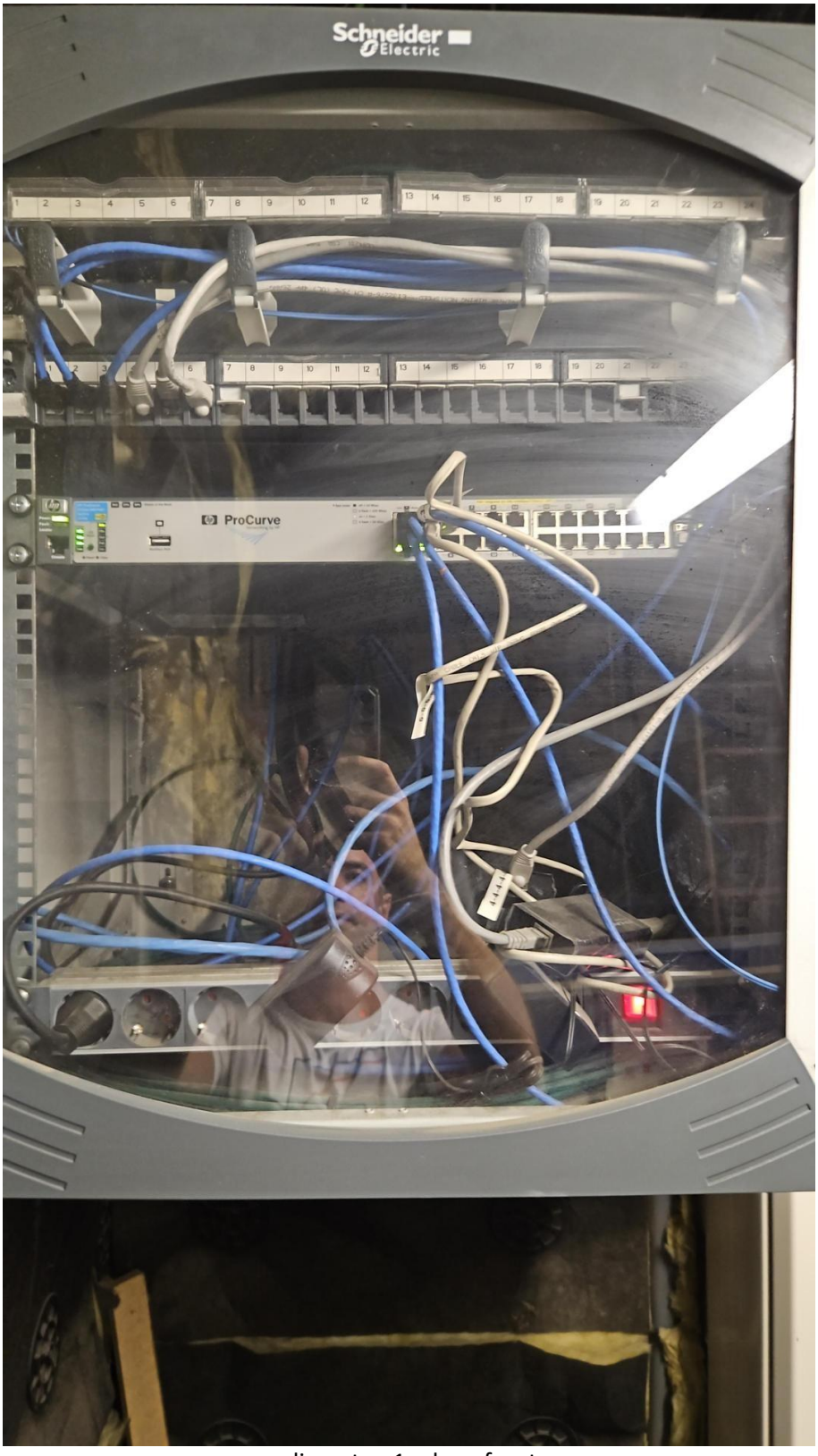


veu_clima_tcm1_p2_b_front

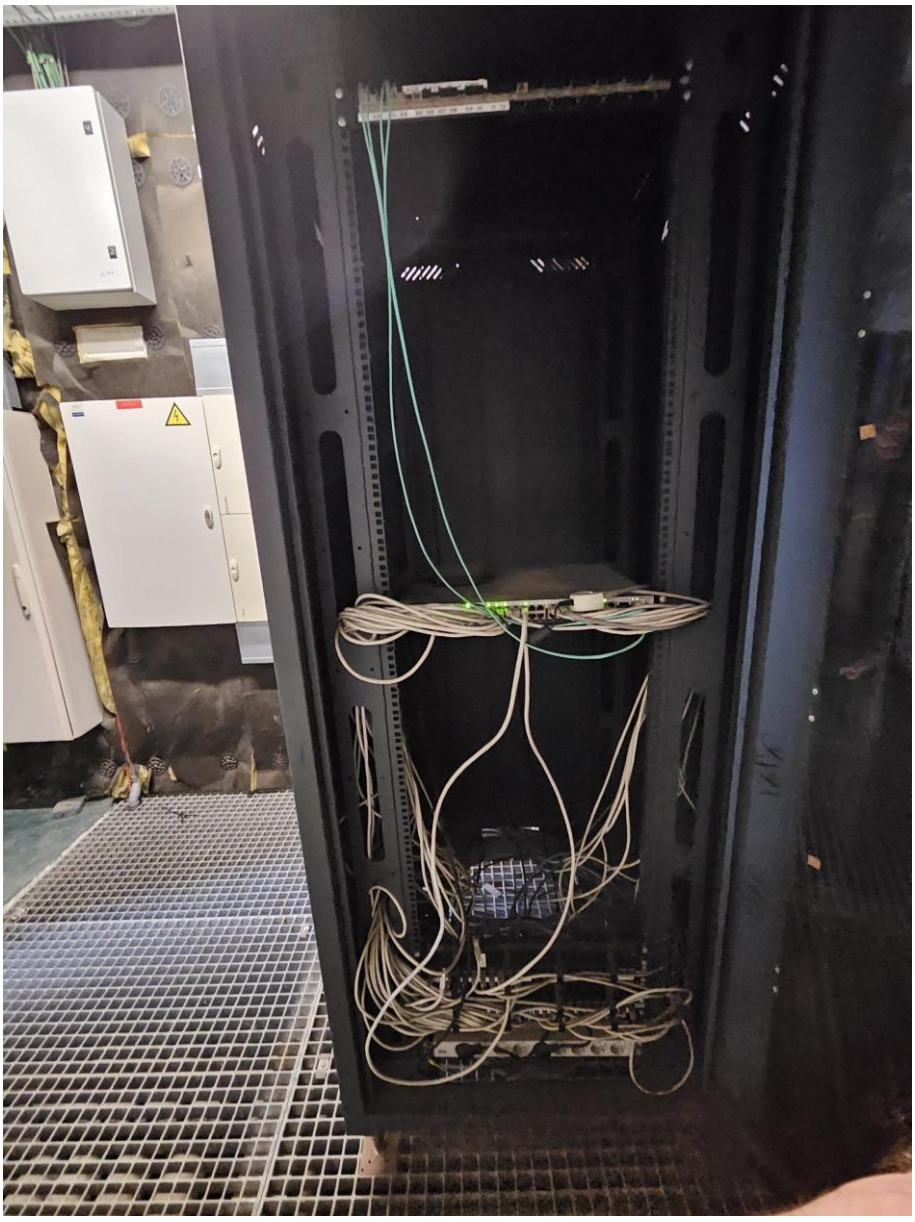


veu_tcm1_pb_b_front

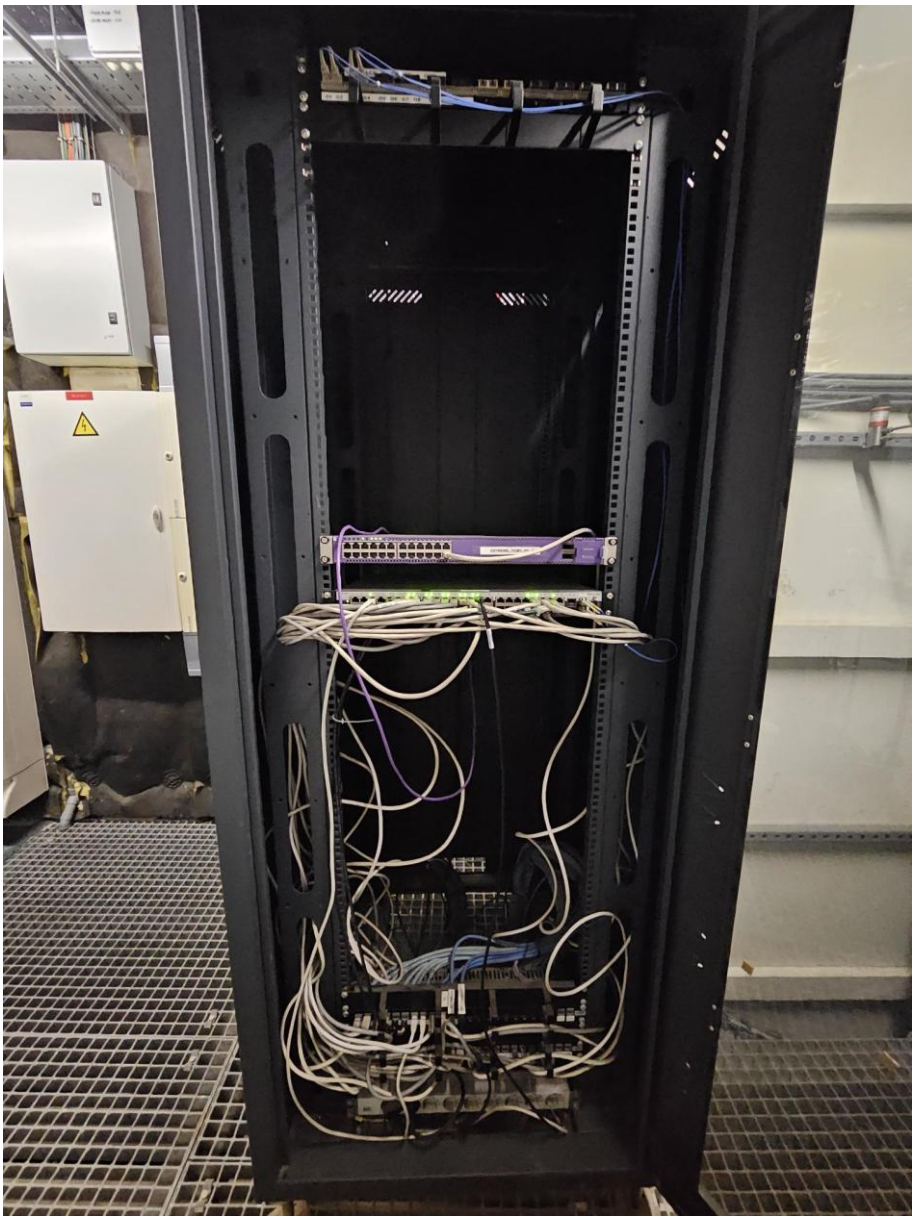
Zona C



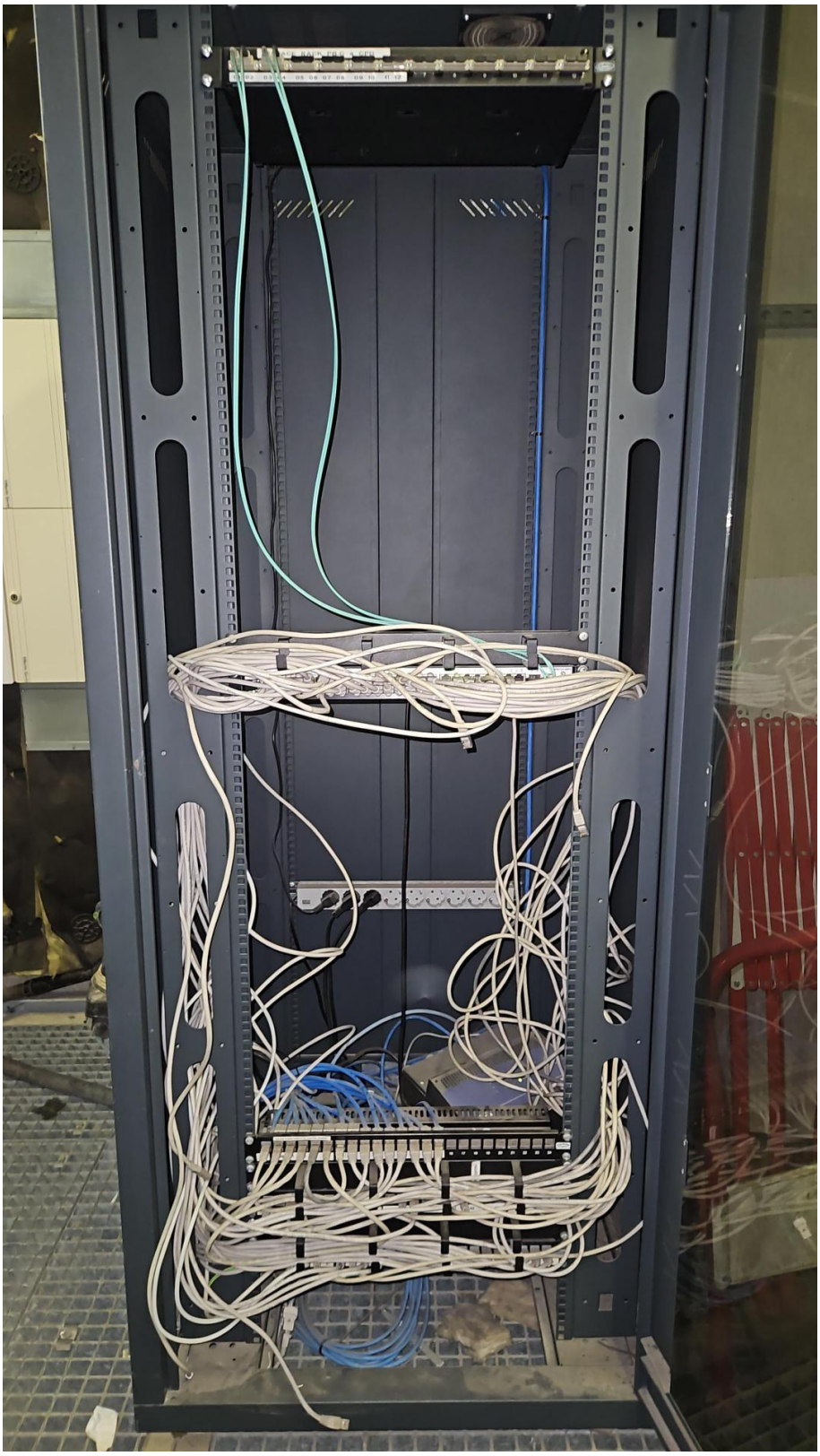
clima_tcm1_pb_c_front



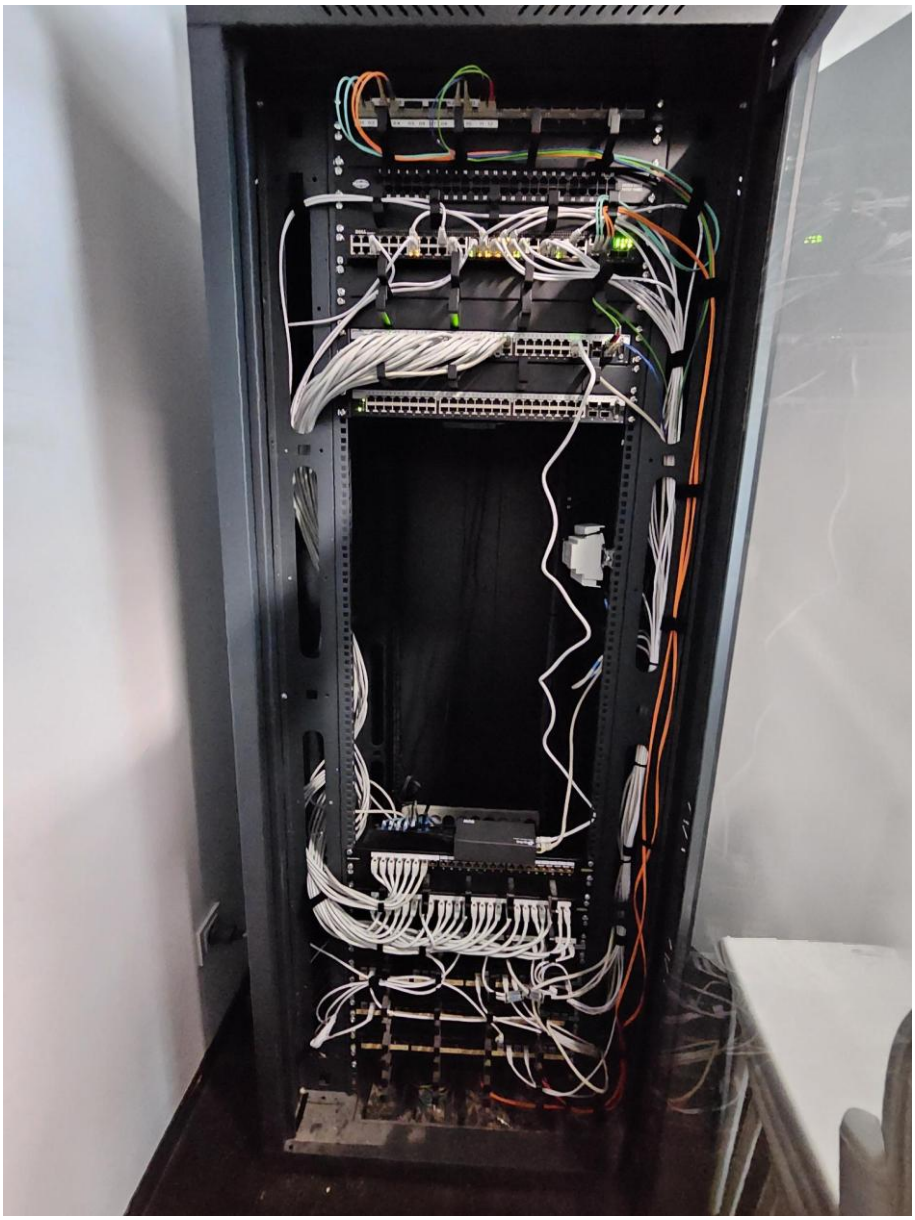
veu_tcm1_p1_c_front



veu_tcm1_p2_c_front

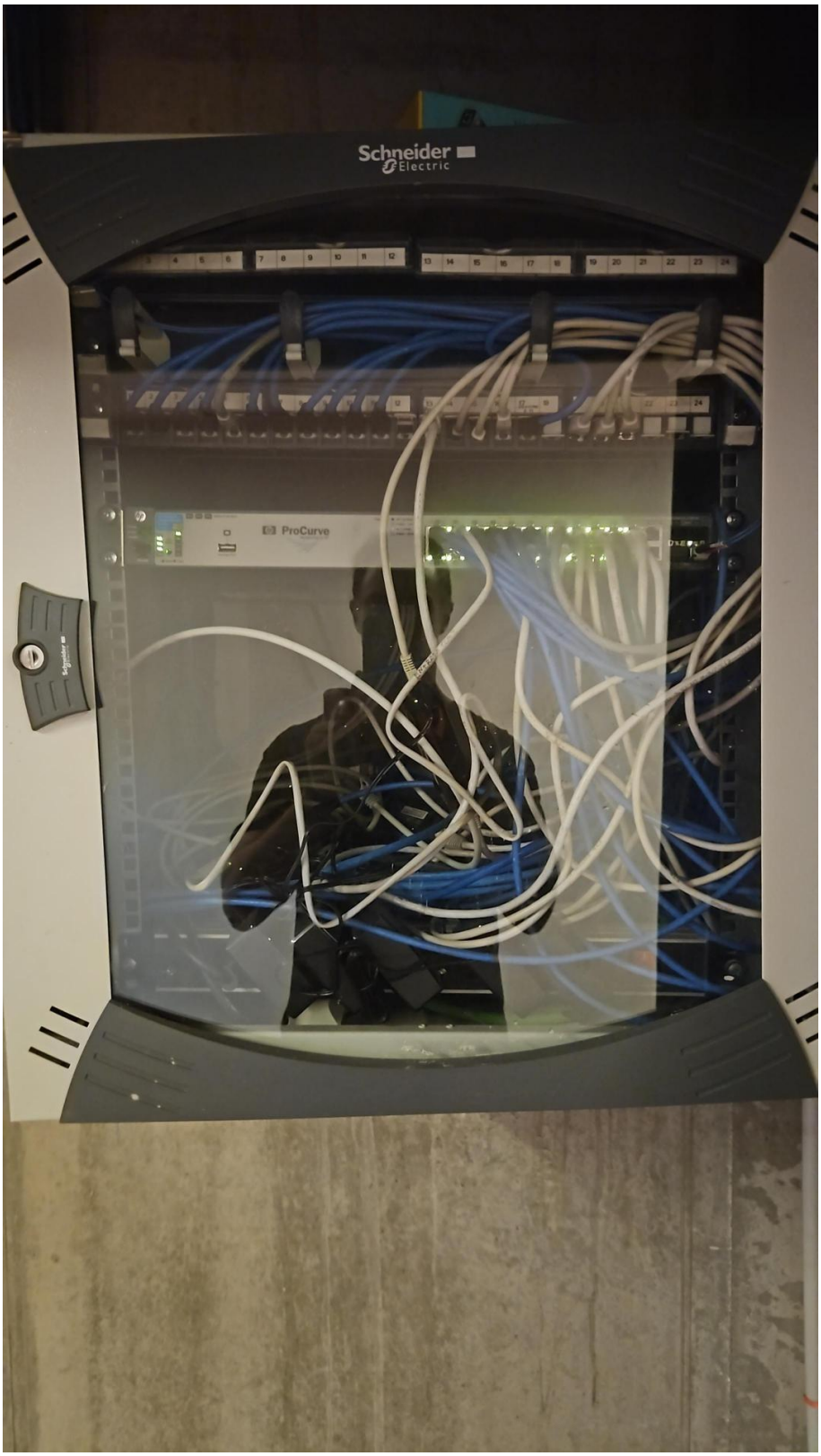


veu_tcm1_pb_c_front

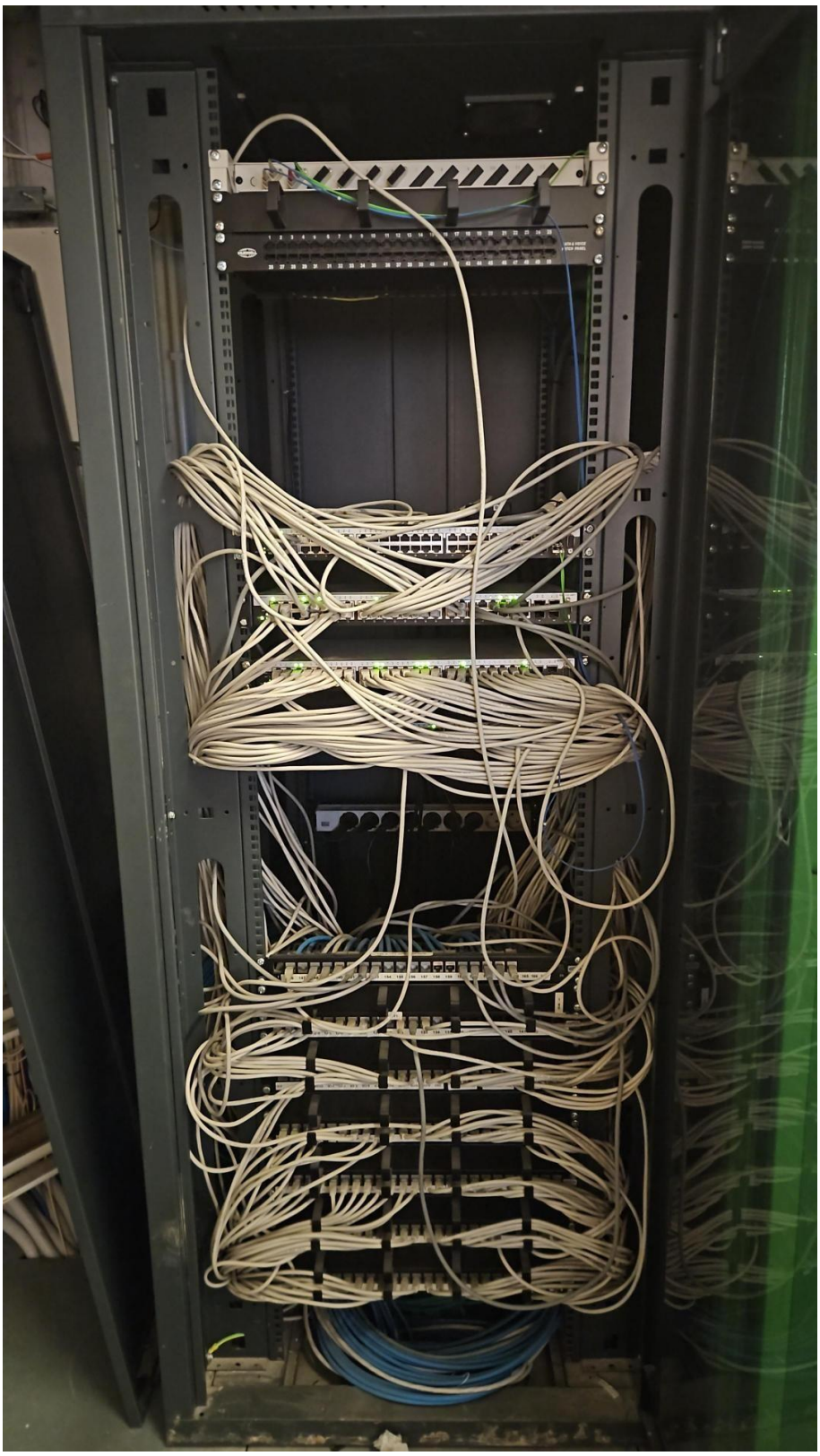


veu_tcm2_p-1_c_front

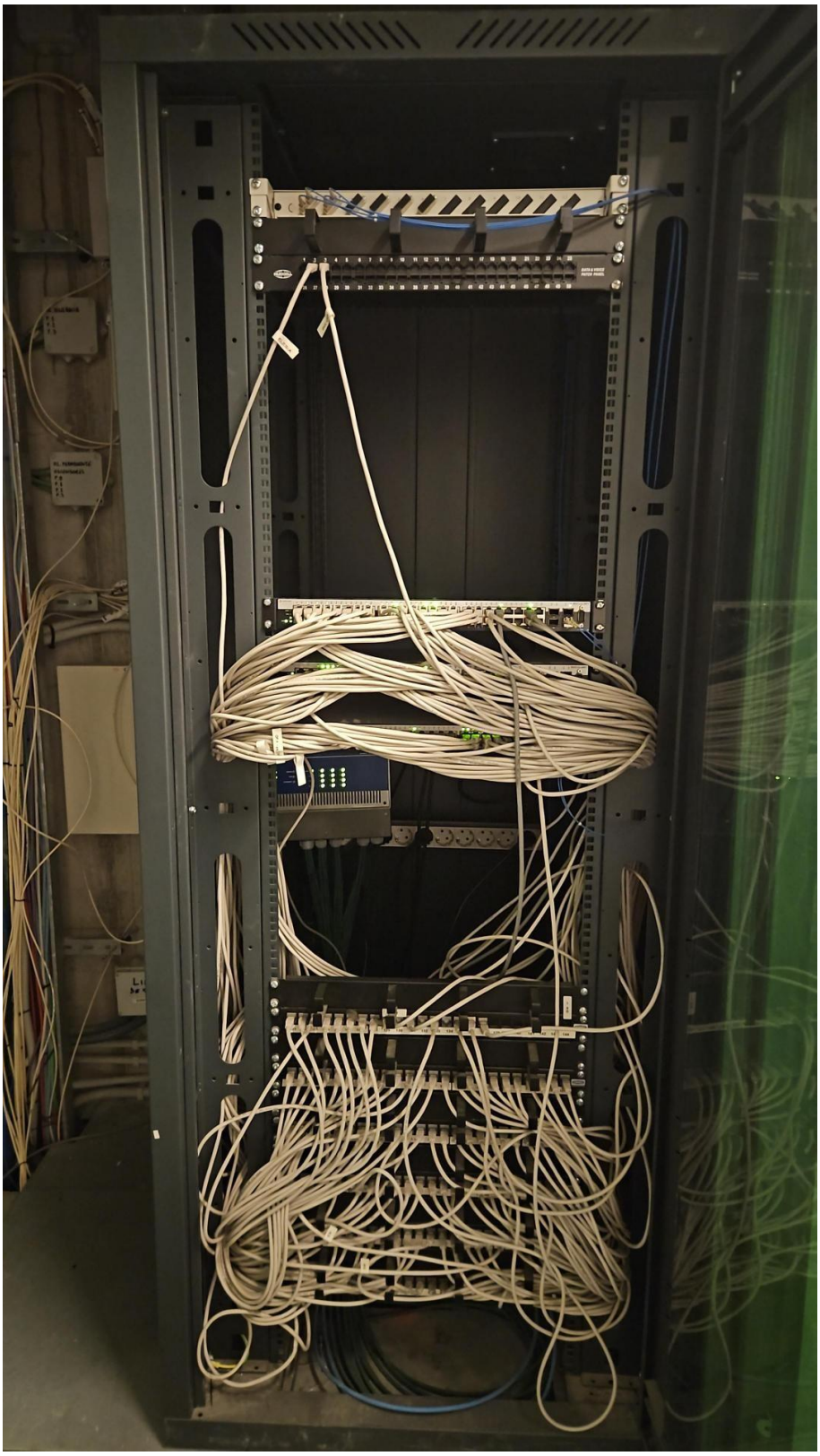
Edifici TCM2
ZONA A



clima_tcm2_p-1_front

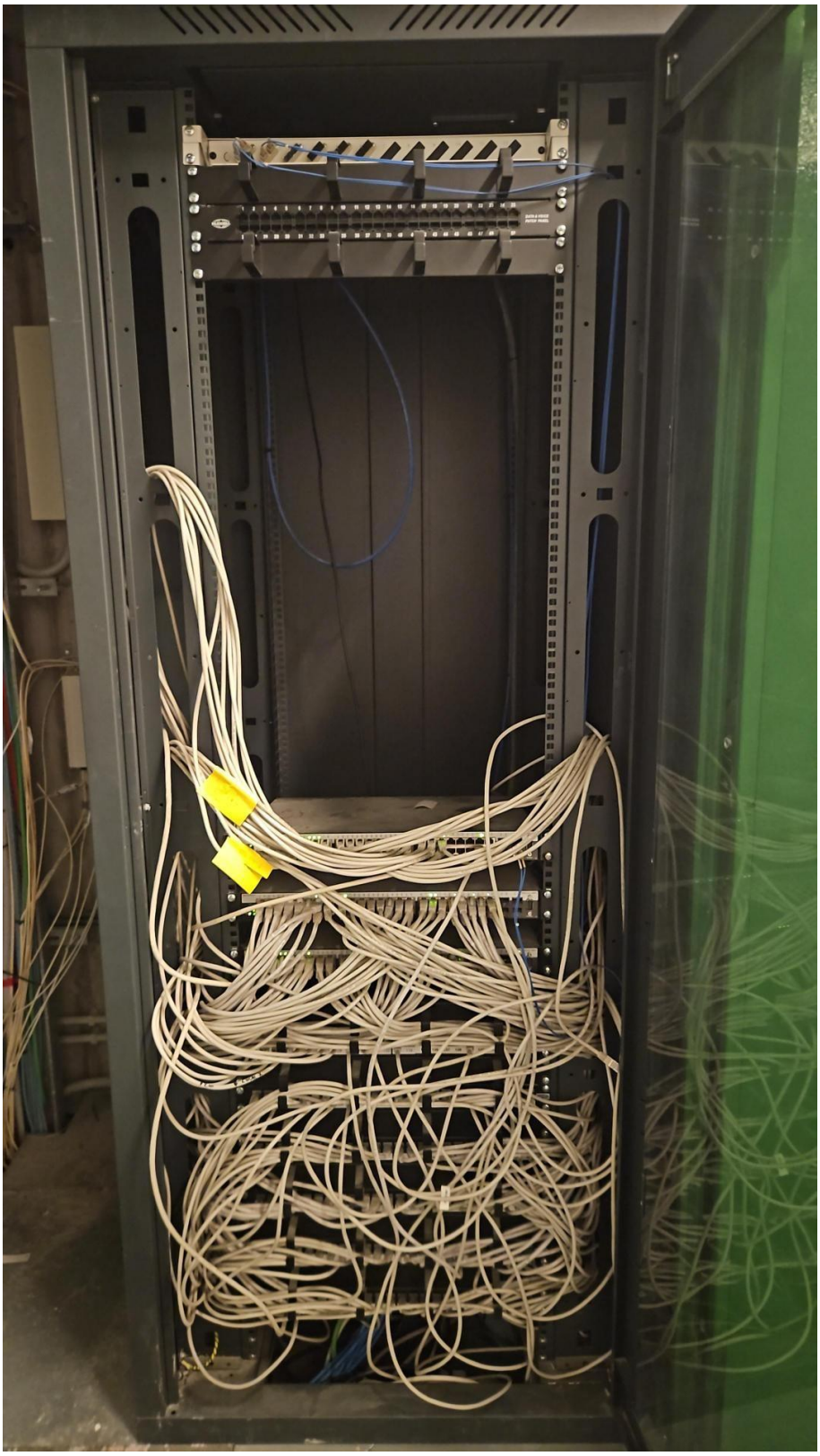


veu_tcm2_p1_front

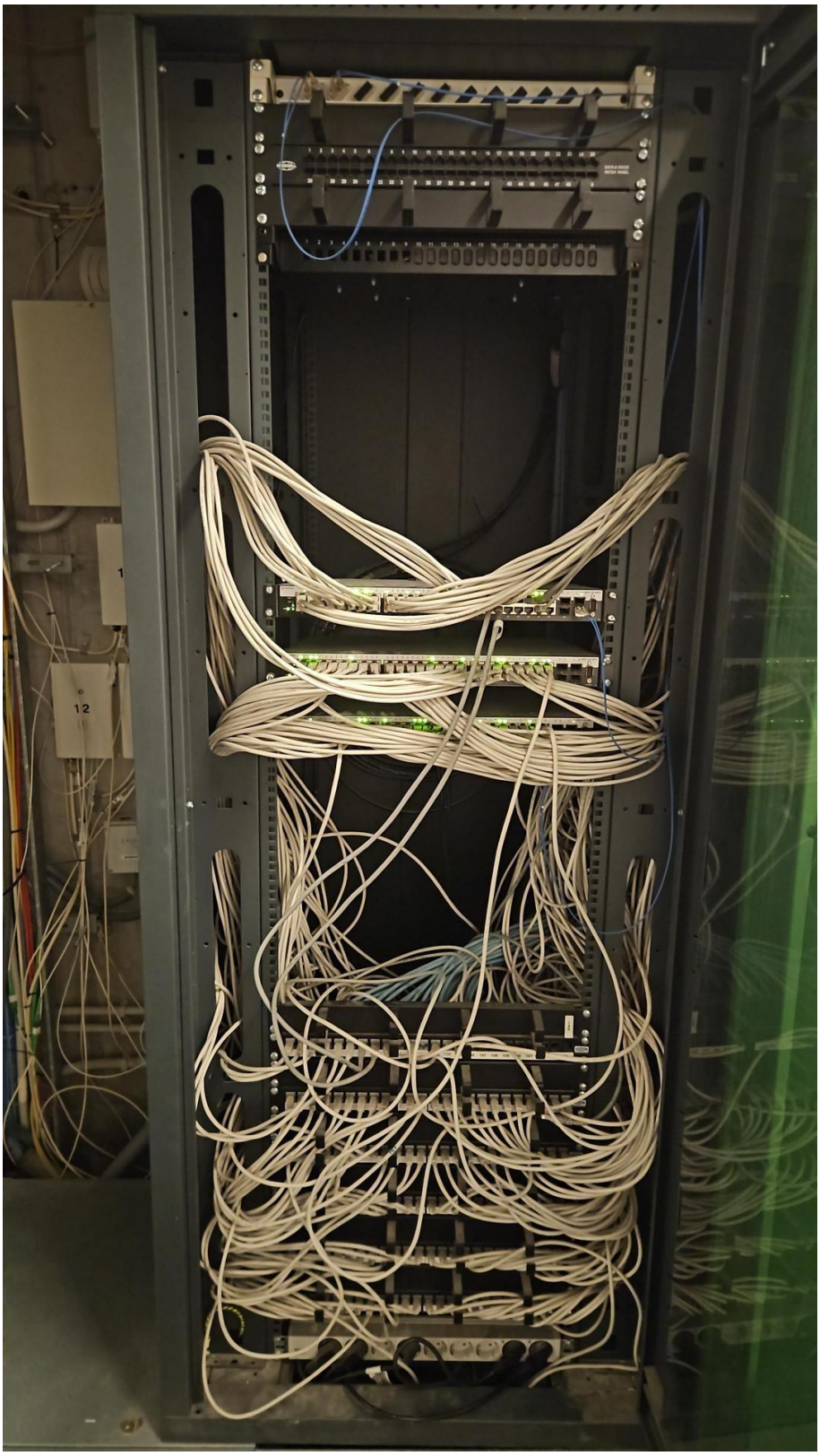


veu_tcm2_p2_front

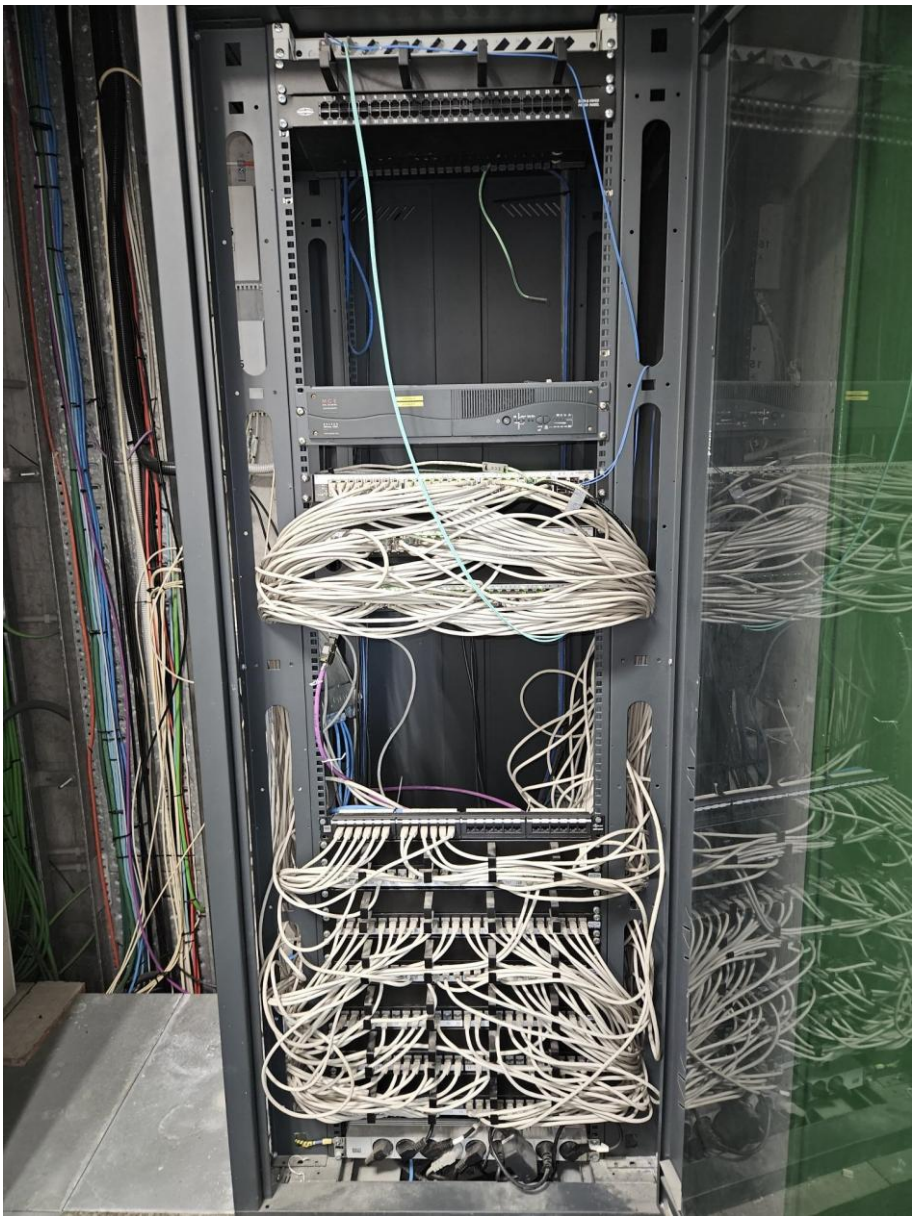
veu_tcm2_p3_front



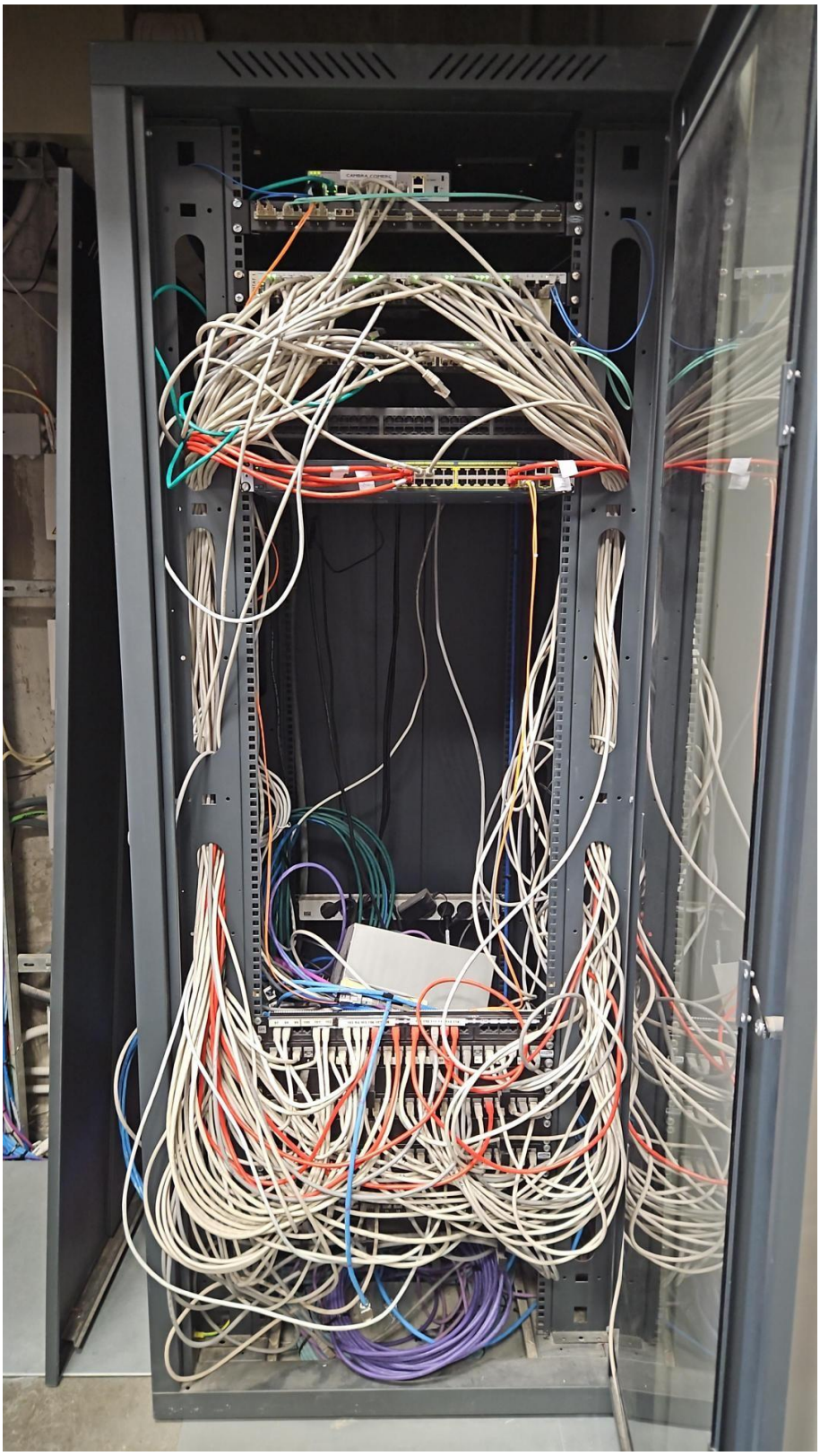
veu_tcm2_p4_front



veu_tcm2_p5_front

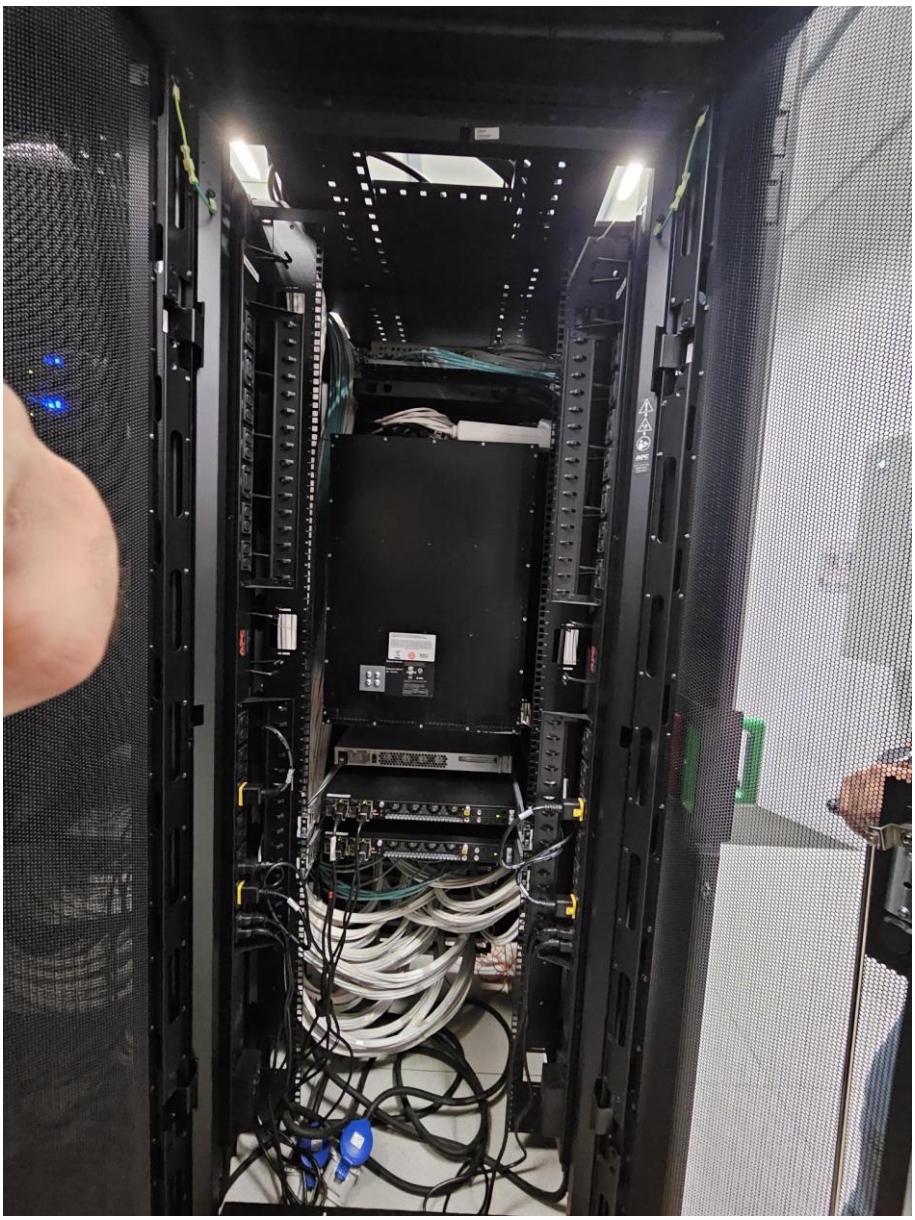


veu_tcm2_p6_front

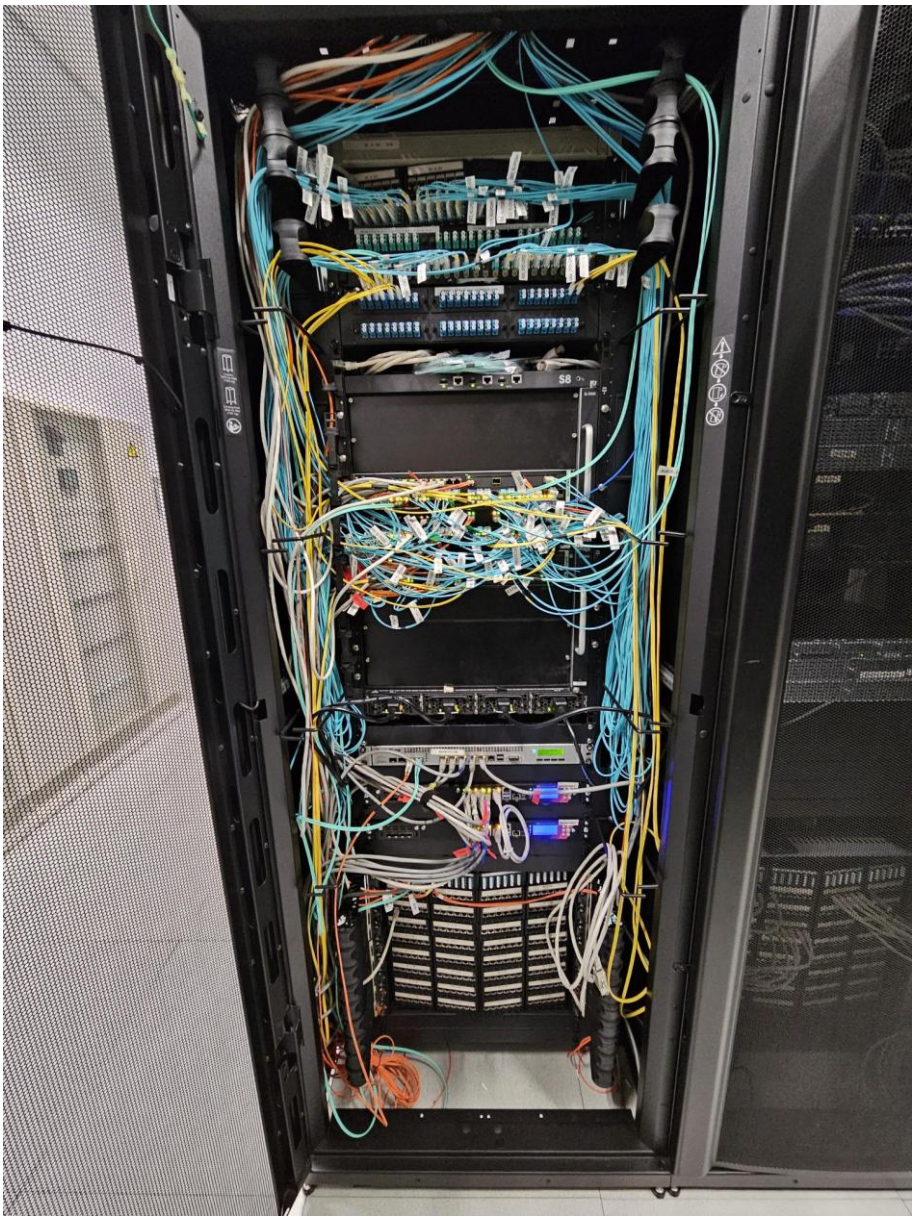


veu_tcm2_pb_front

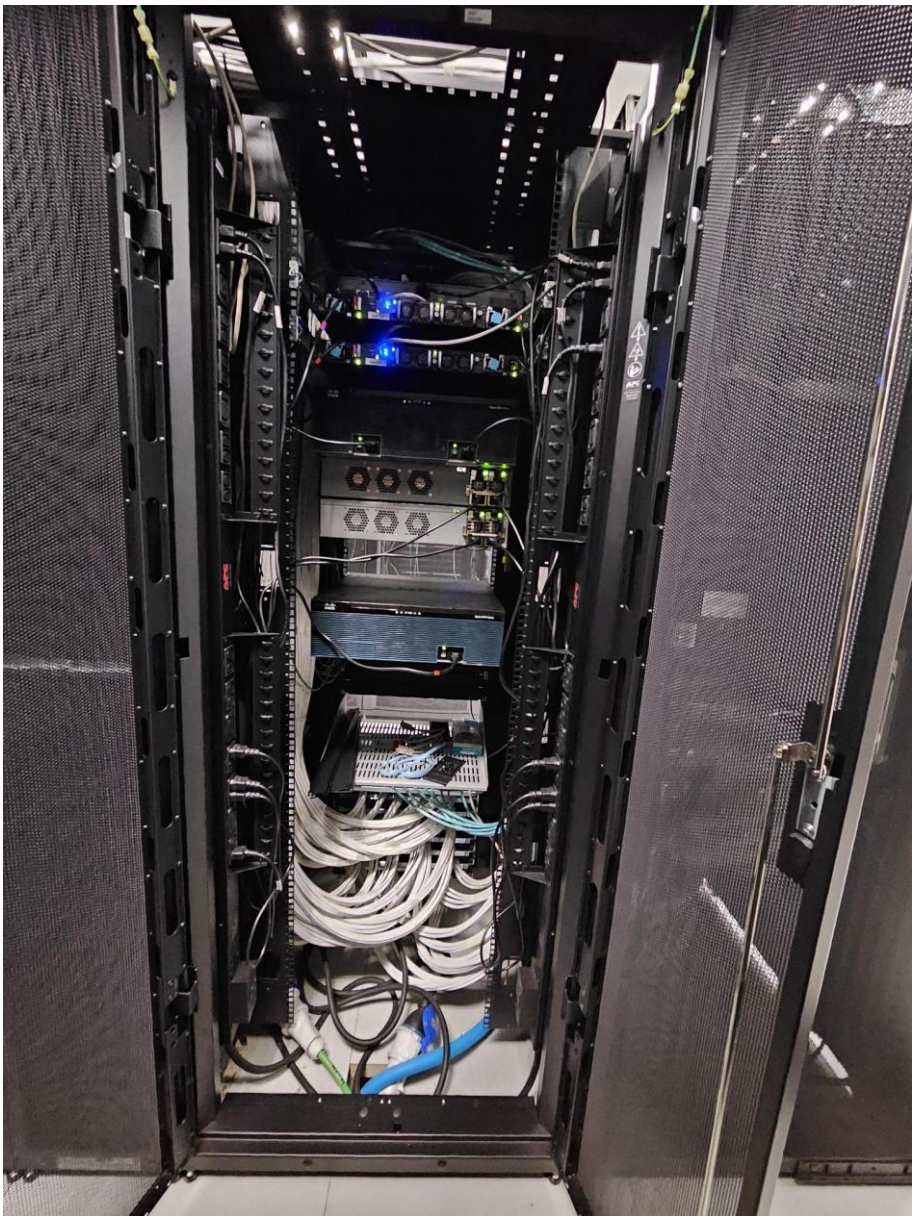
CPD2



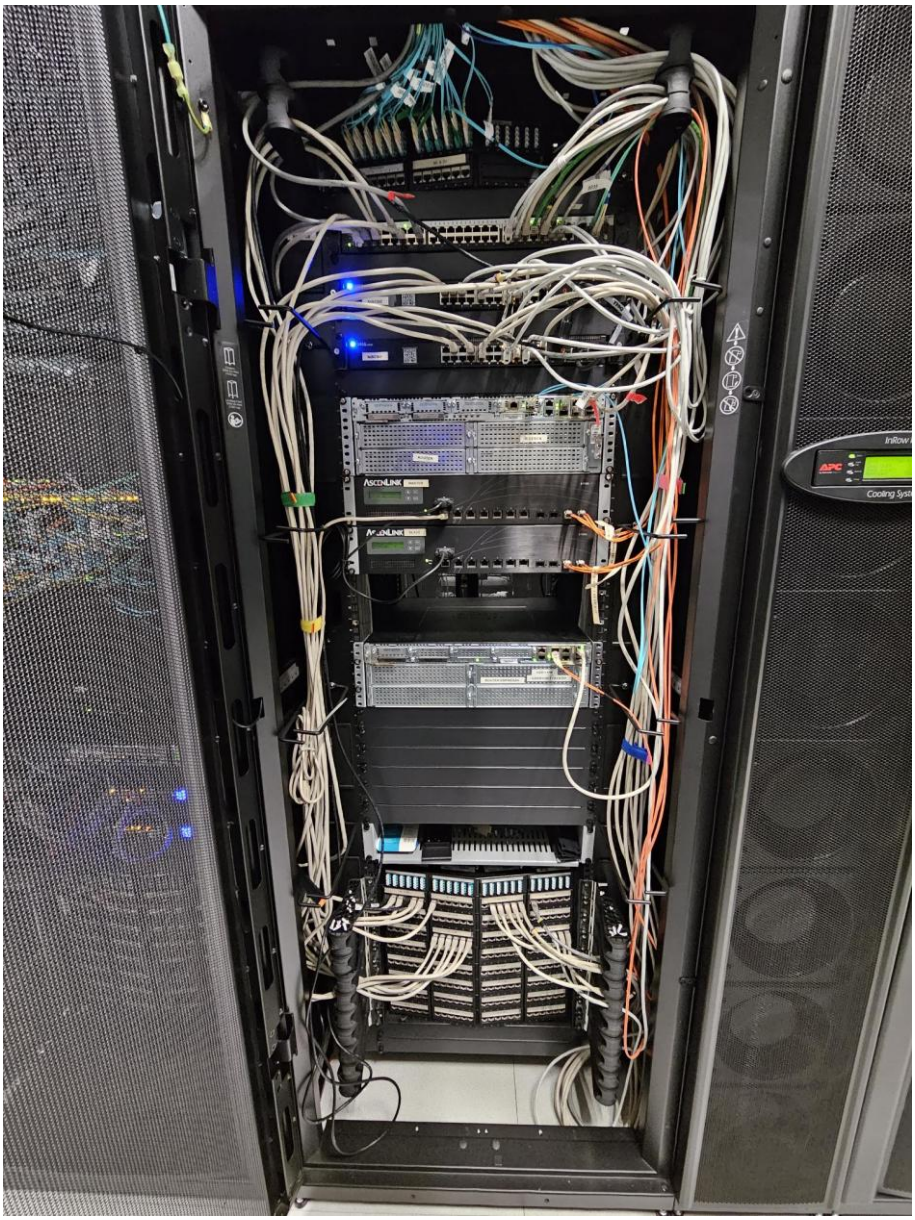
veu_tcm2_p-1_cpd2_racb-01_back



veu_tcm2_p-1_cpd2_racb-01_front



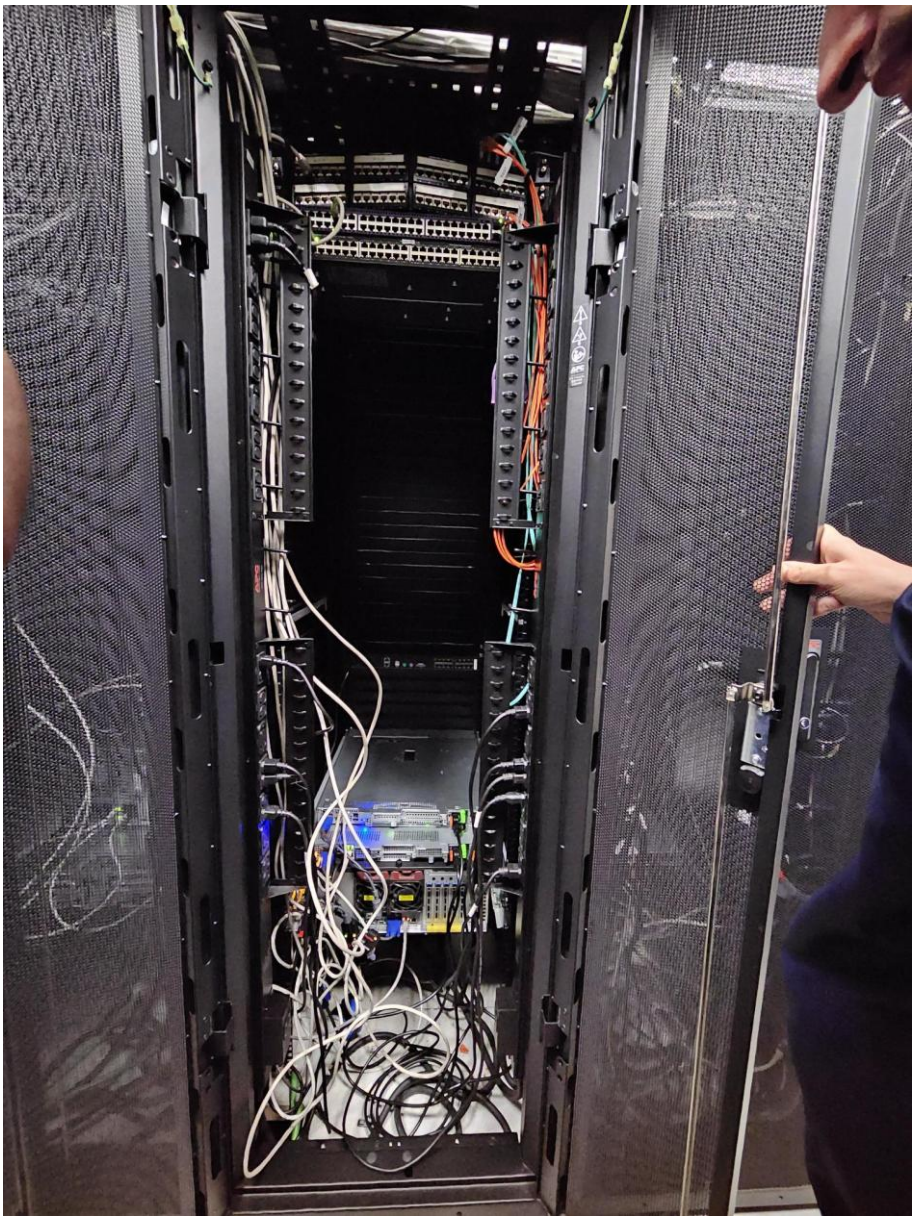
veu_tcm2_p-1_cpd2_racb-02_back



veu_tcm2_p-1_cpd2_racb-02_front

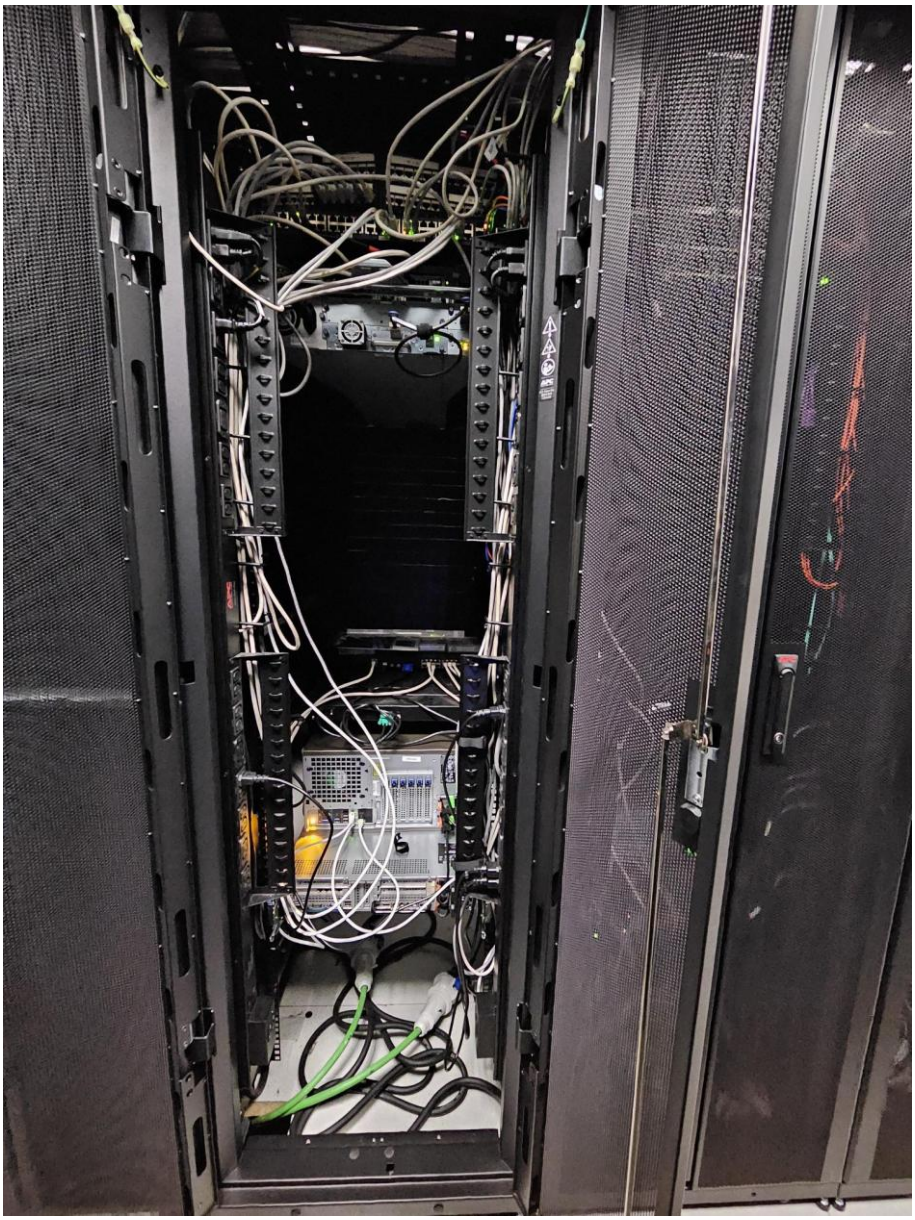
veu_tcm2_p-1_cpd2_racb-03_back

veu_tcm2_p-1_cpd2_racb-03_front



veu_tcm2_p-1_cpd2_racb-04_back

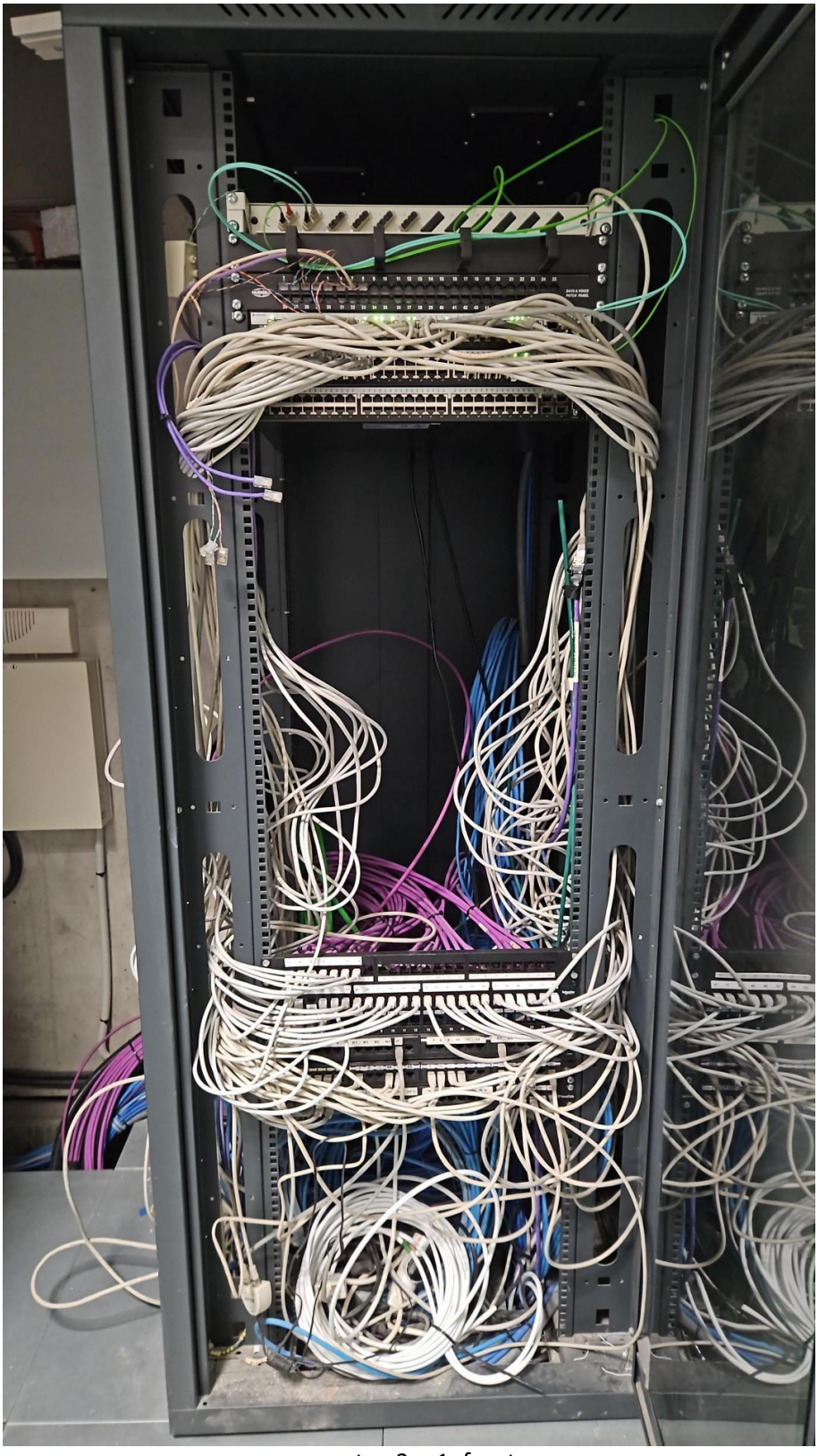
veu_tcm2_p-1_cpd2_racb-04_front



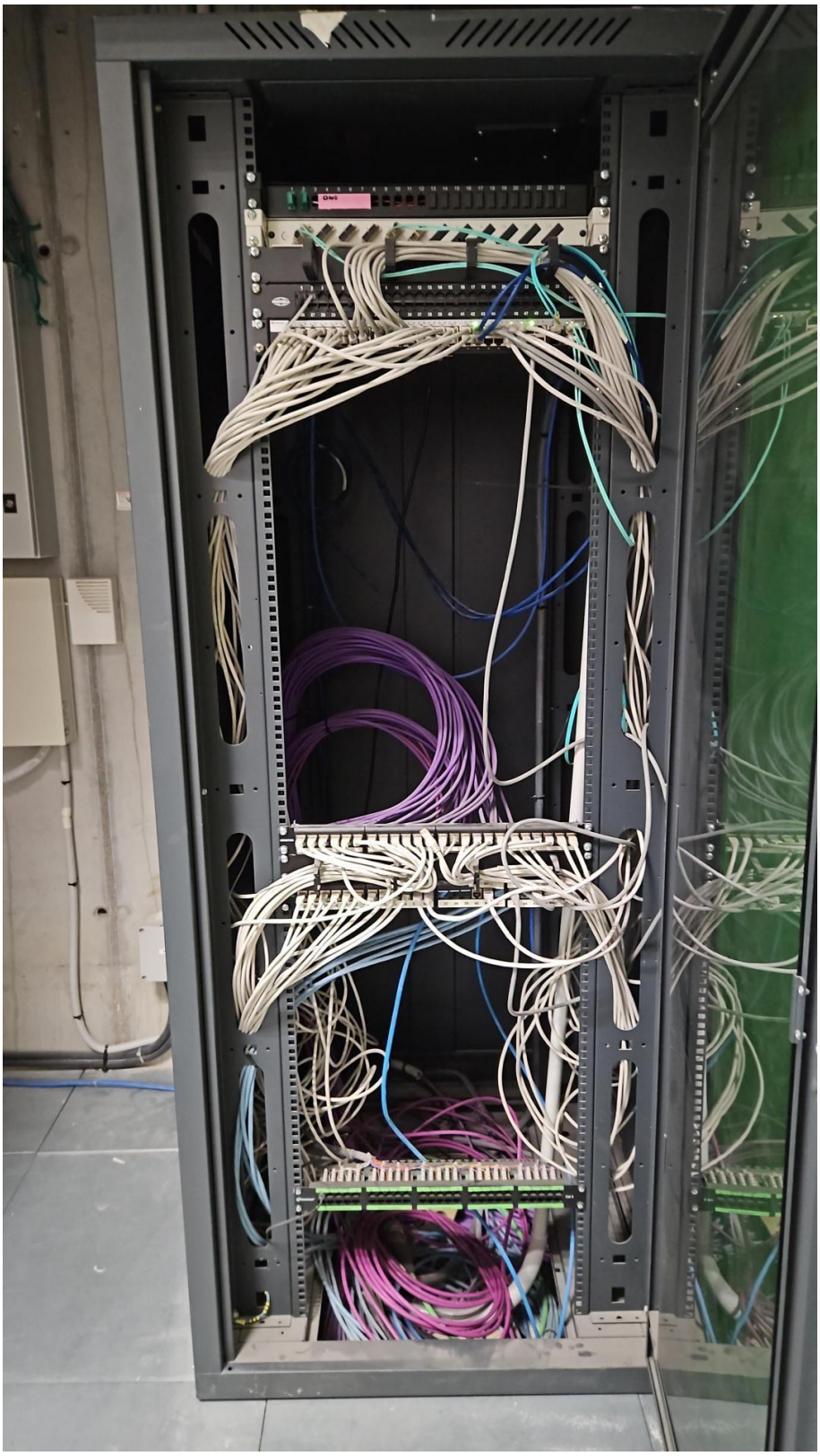
veu_tcm2_p-1_cpd2_racb-05_back

veu_tcm2_p-1_cpd2_racb-05_front

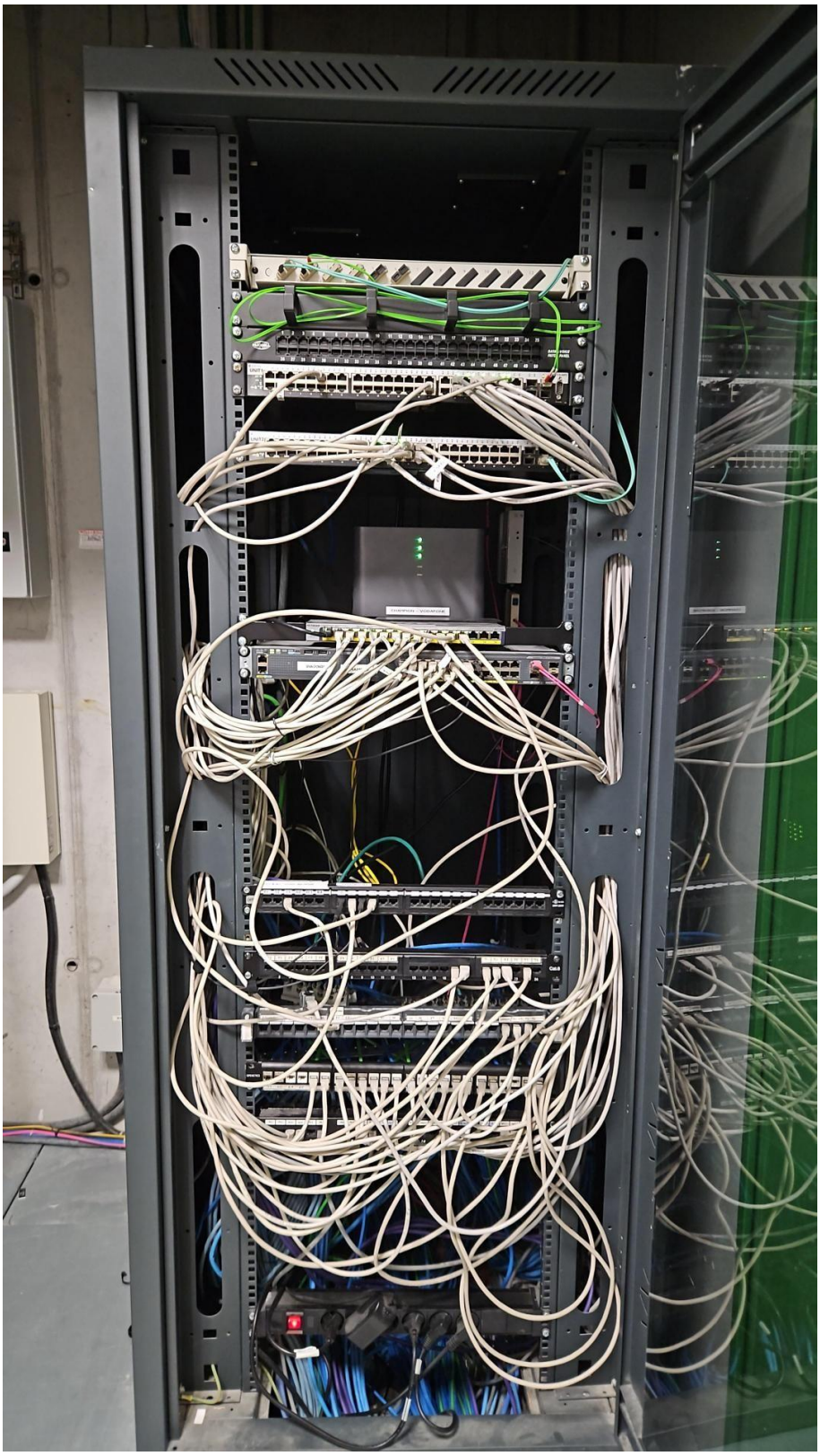
Edifici TCM3



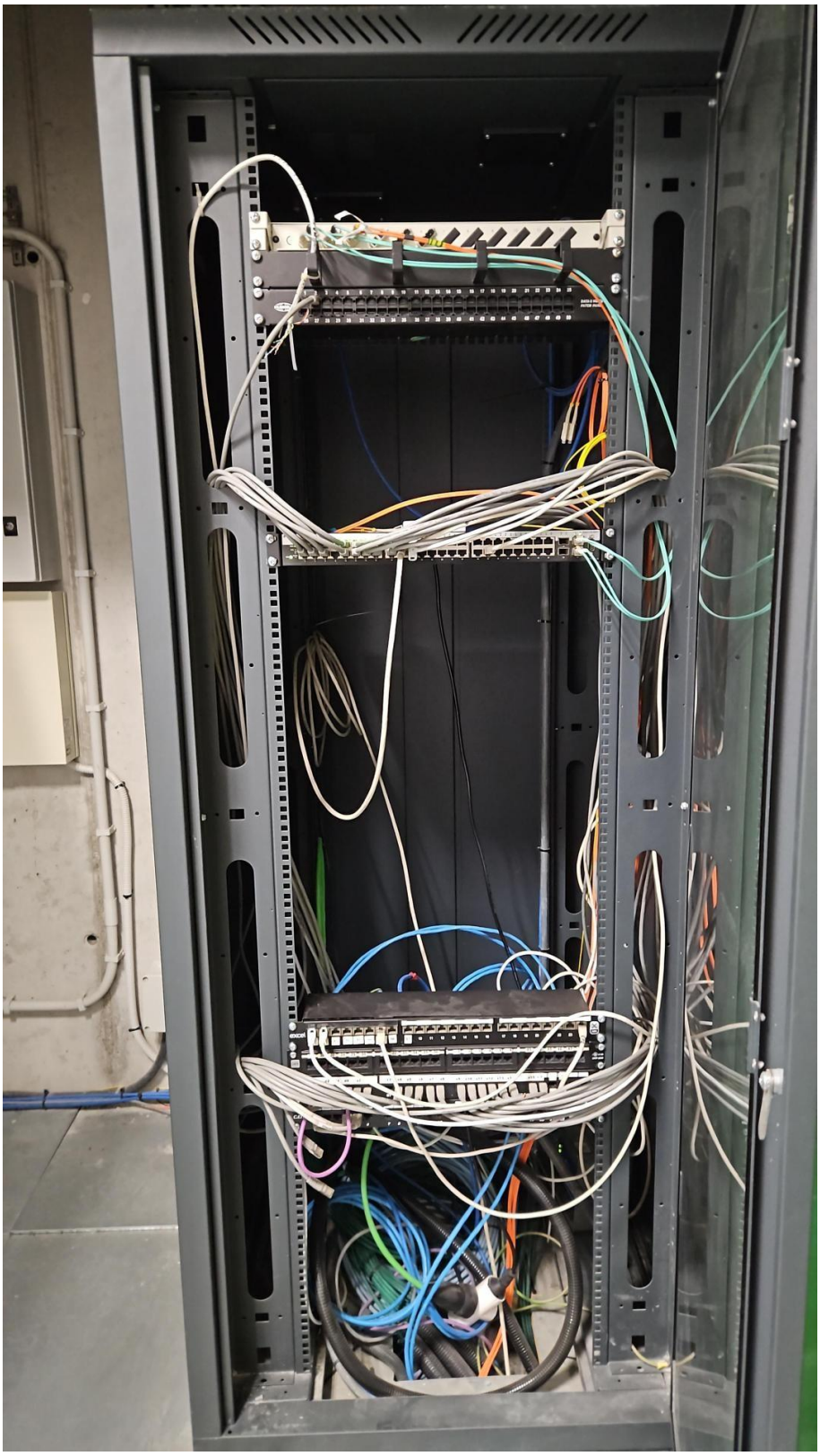
veu_tcm3_p1_front



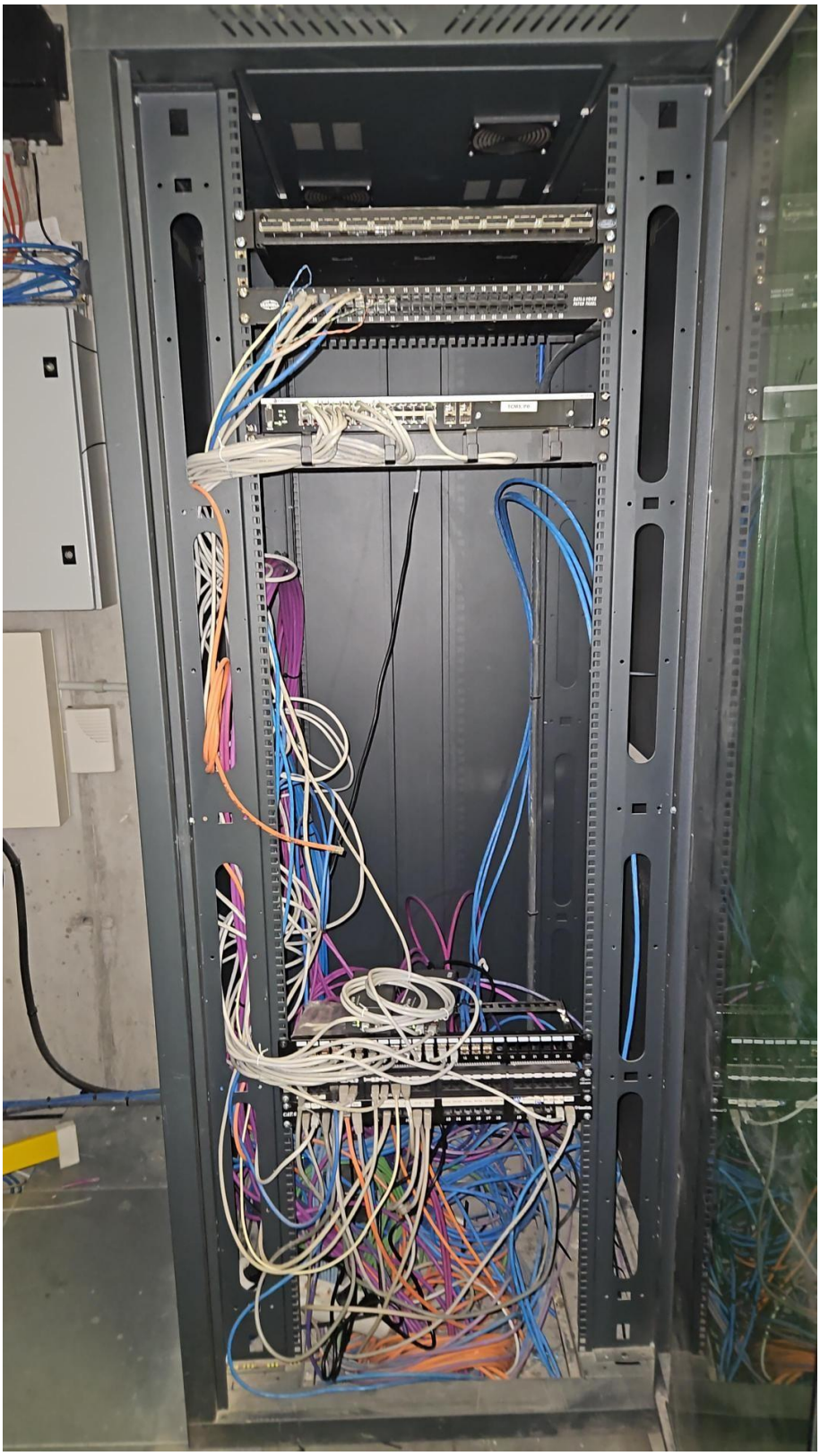
veu_tcm3_p3_front



veu_tcm3_p4_front

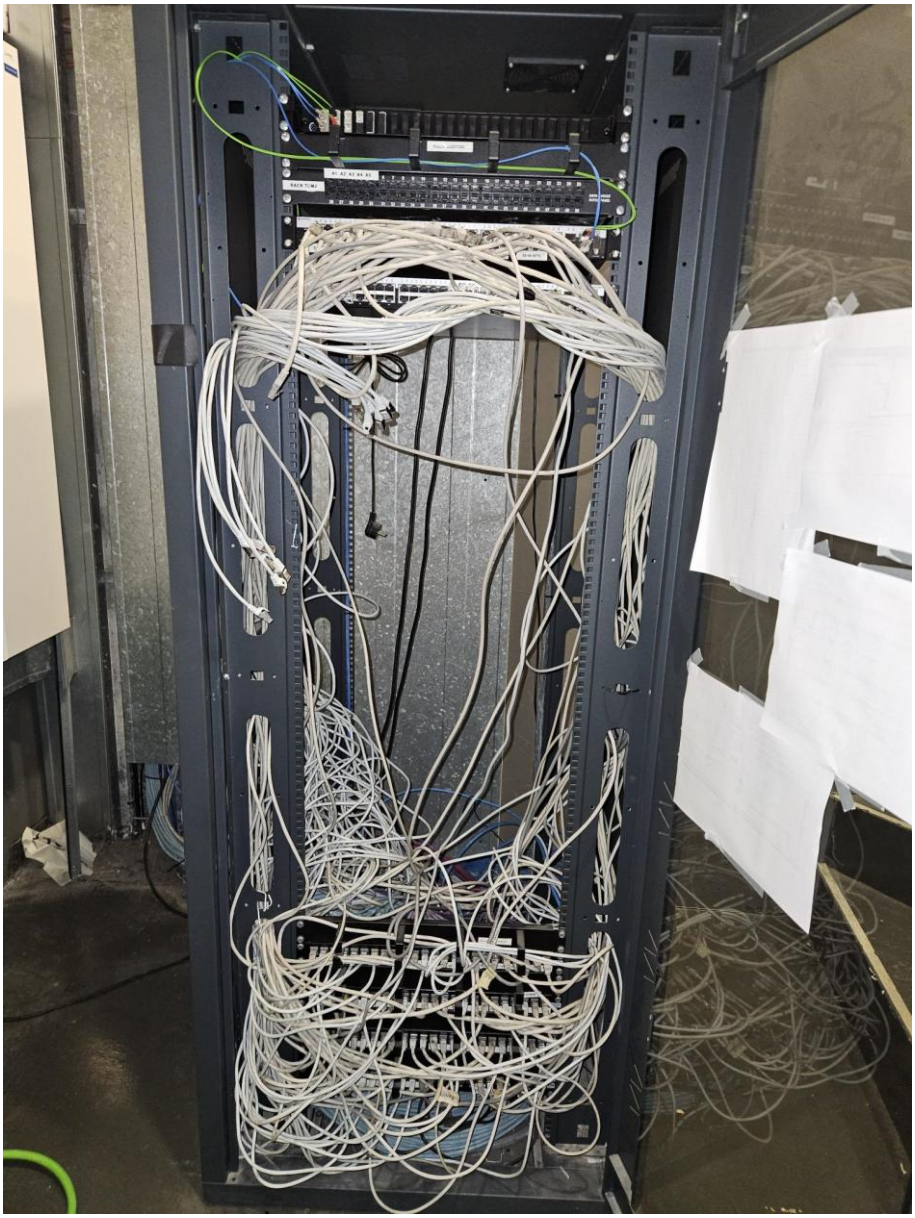


veu_tcm3_p6_front nose que es



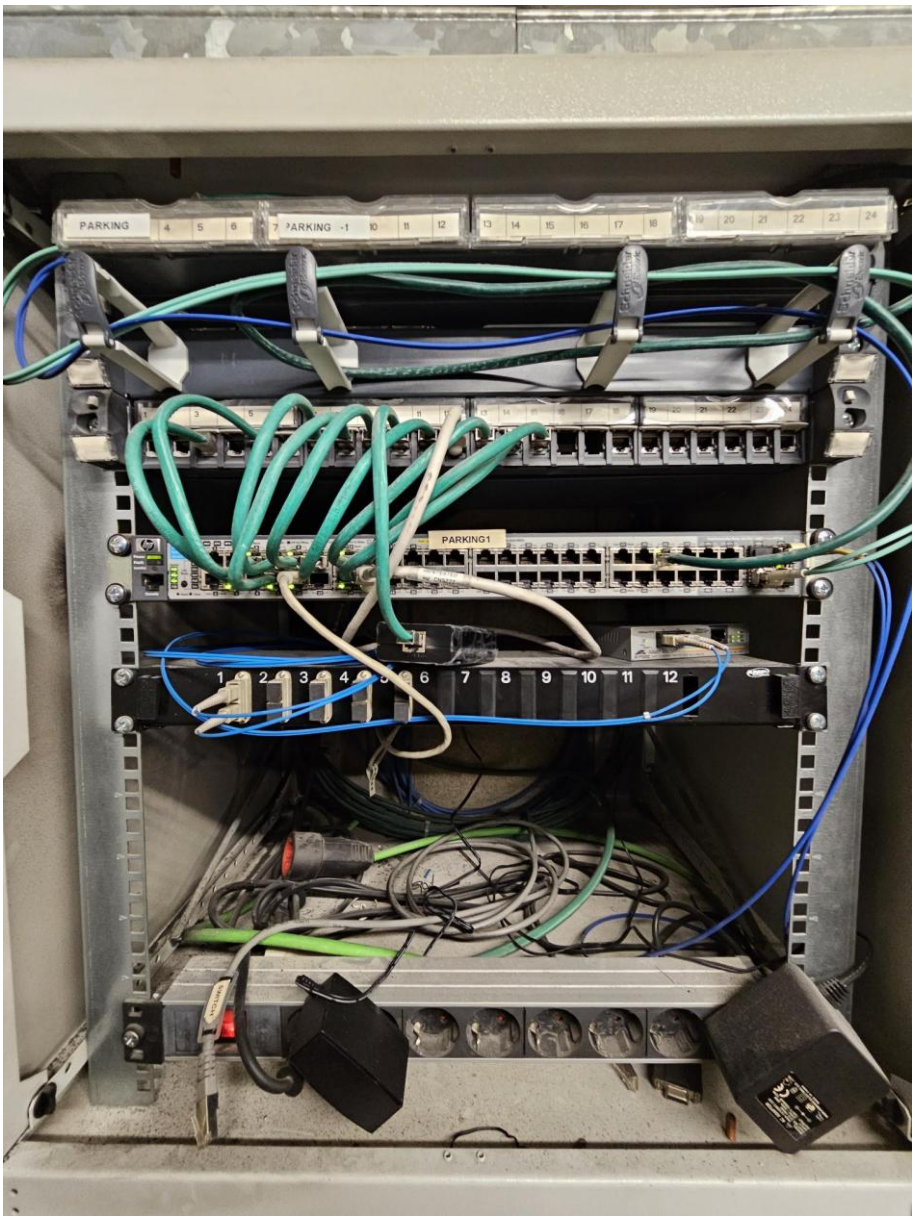
veu_tcm3_pb_front

Edifici TCM4

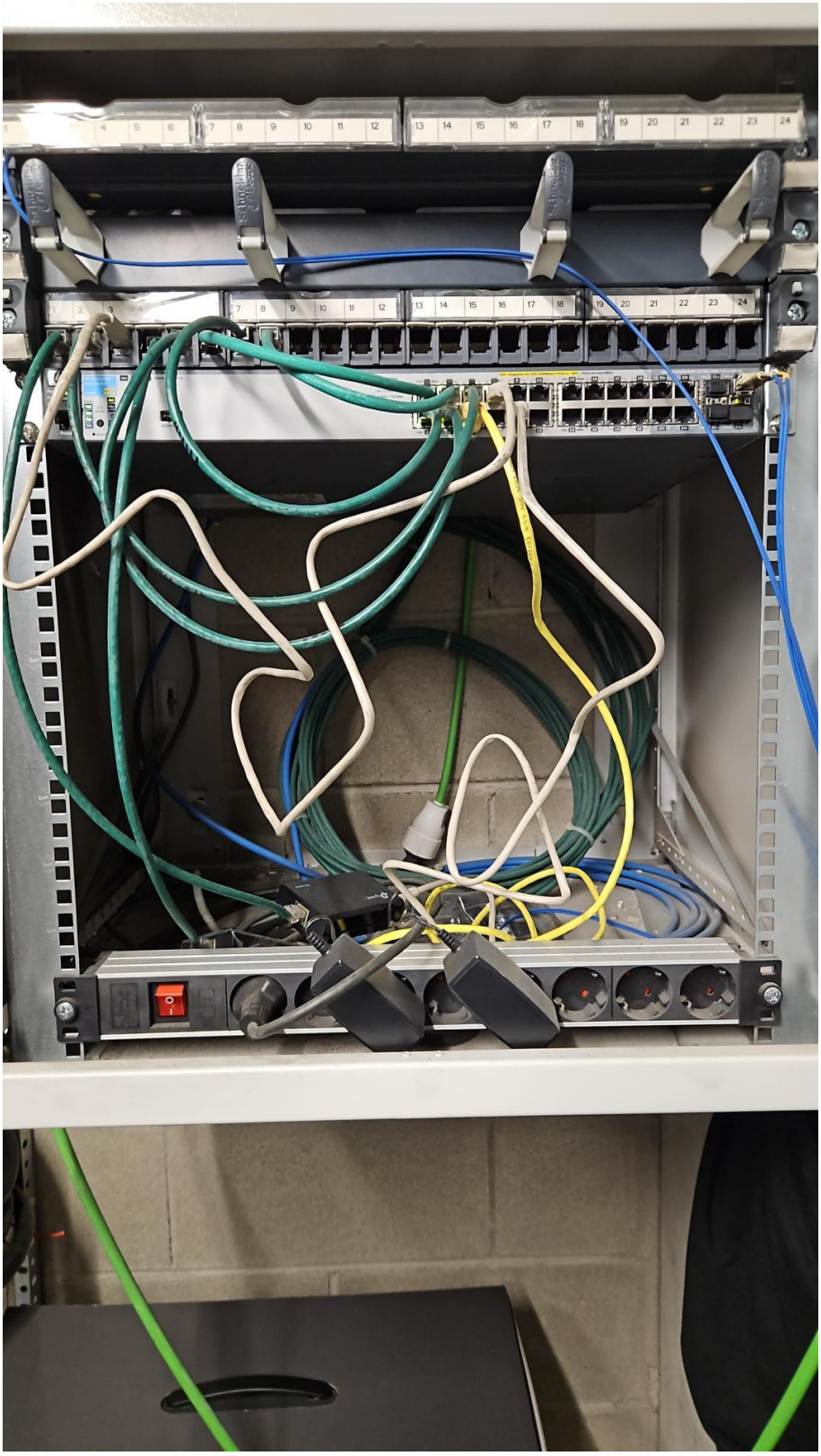


veu_tcm4_p-1_front

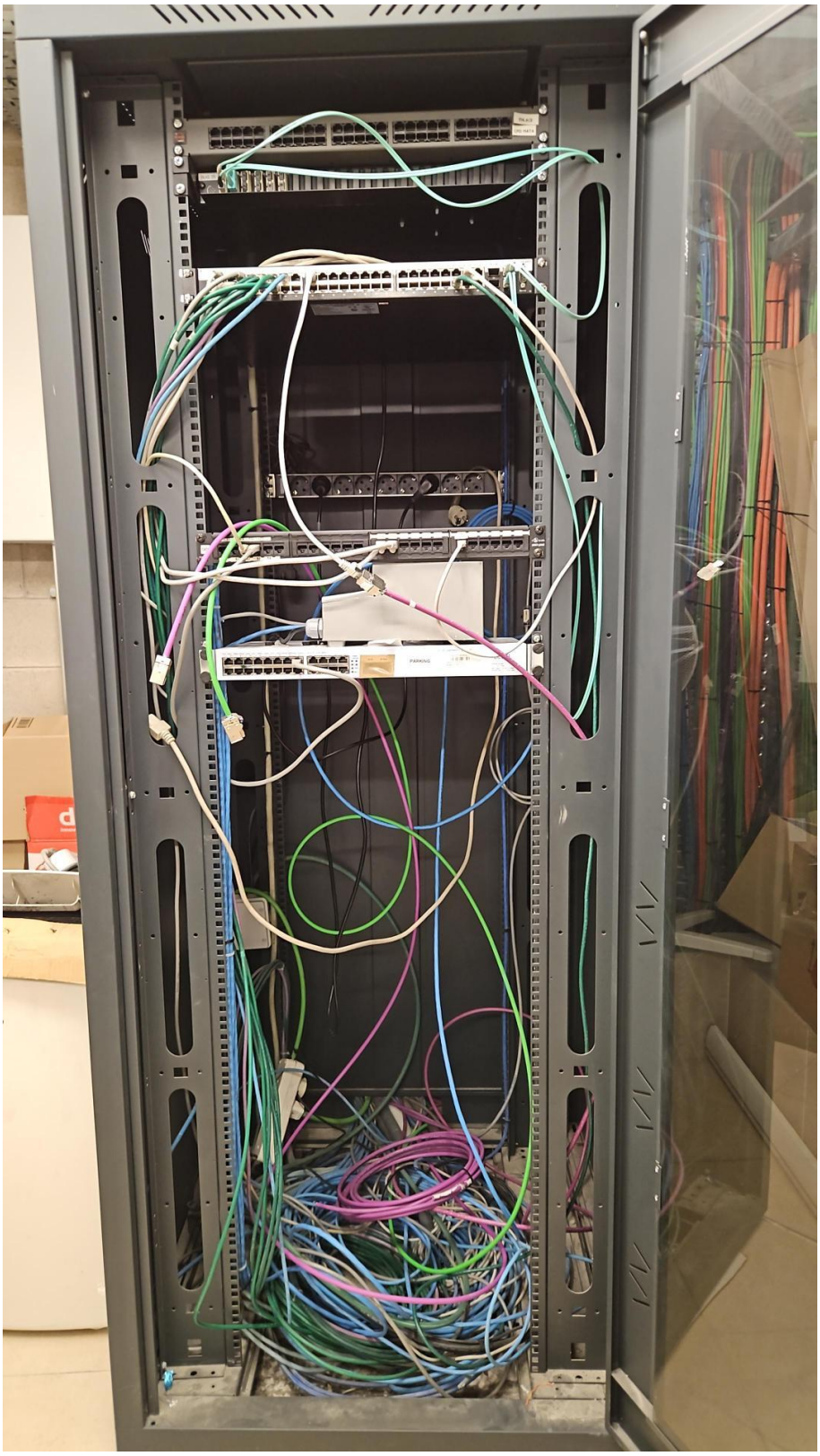
Edifici TCM5



clima_tcm5_p-1_front

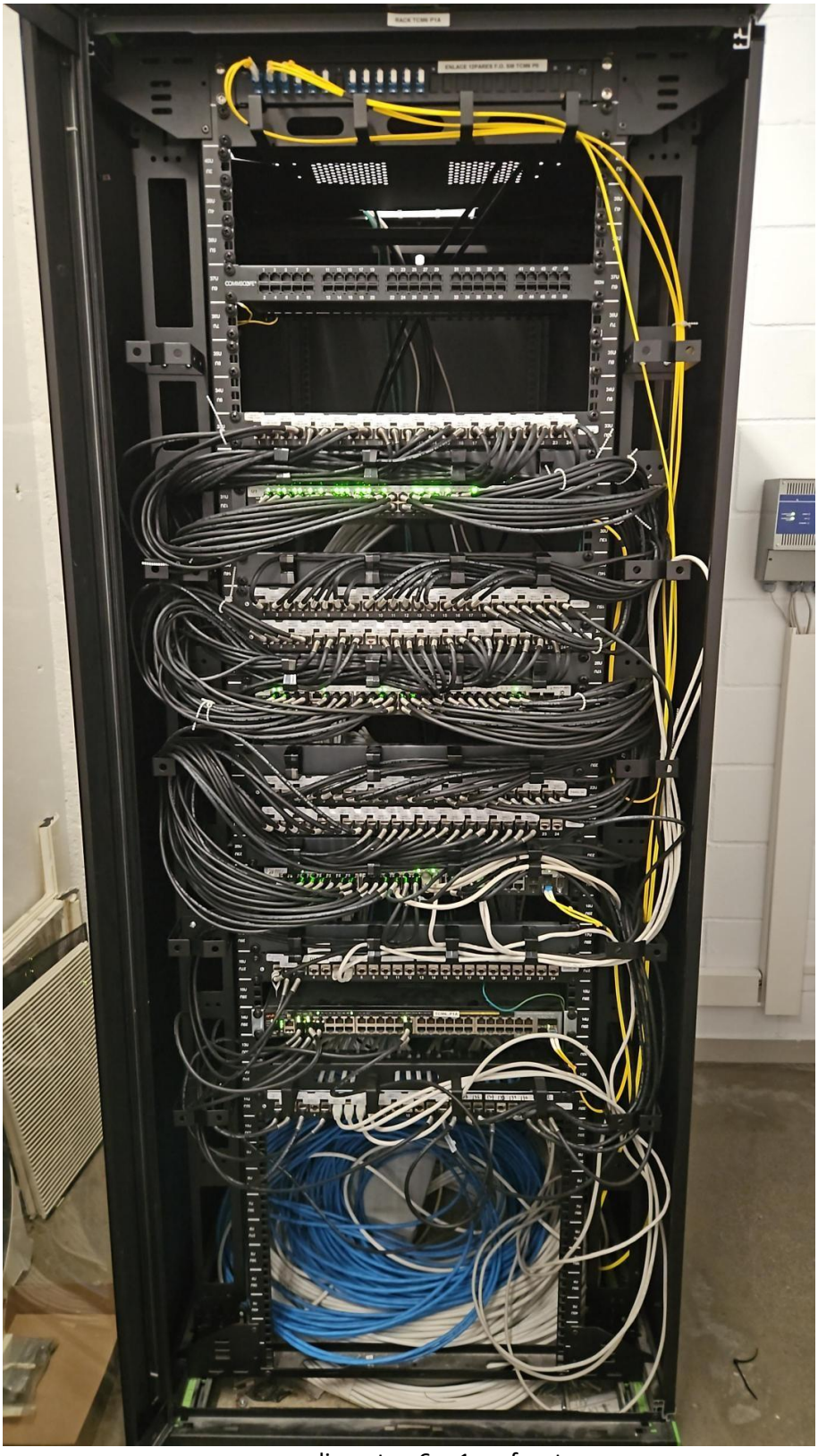


clima_tcm5_p-2_front

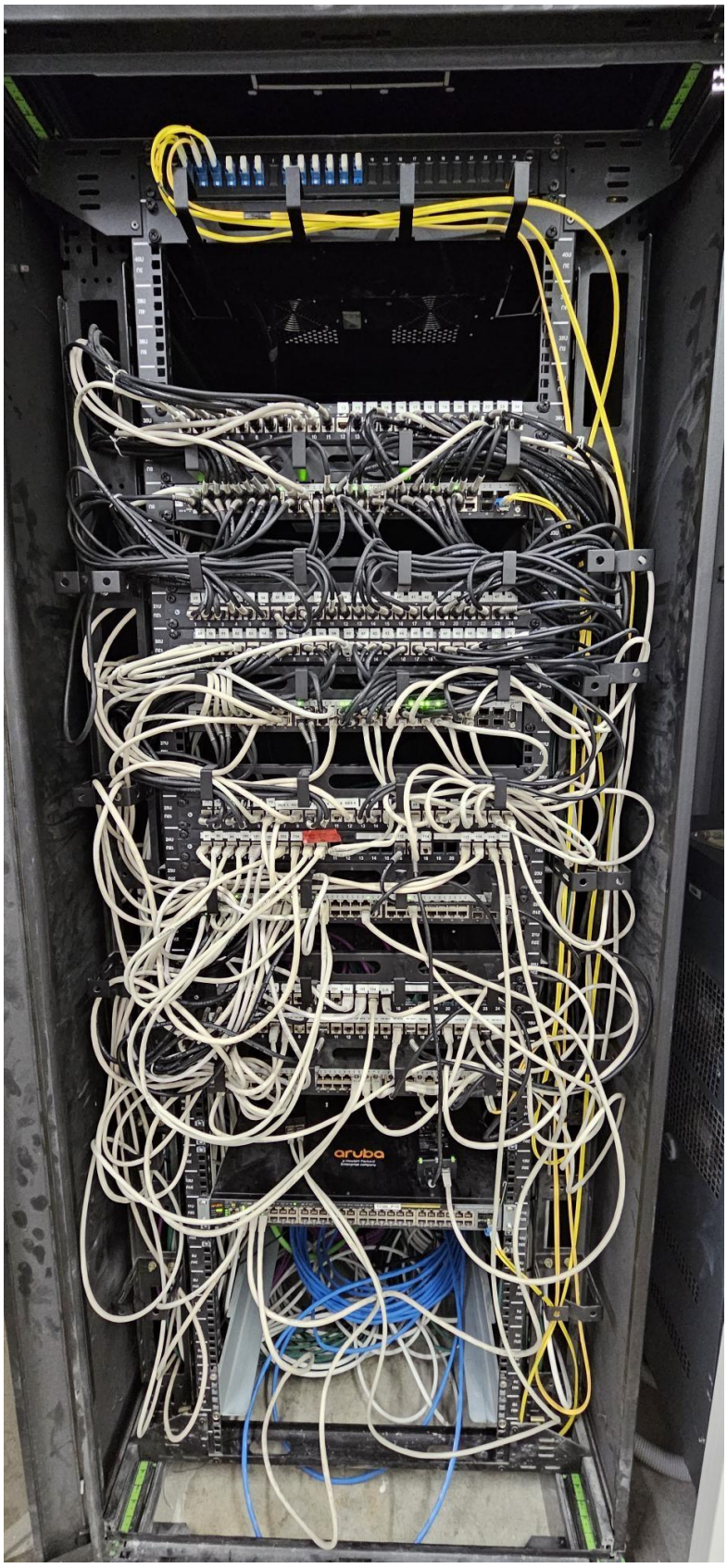


veu_tcm5_p-1_front

Edifici TCM6

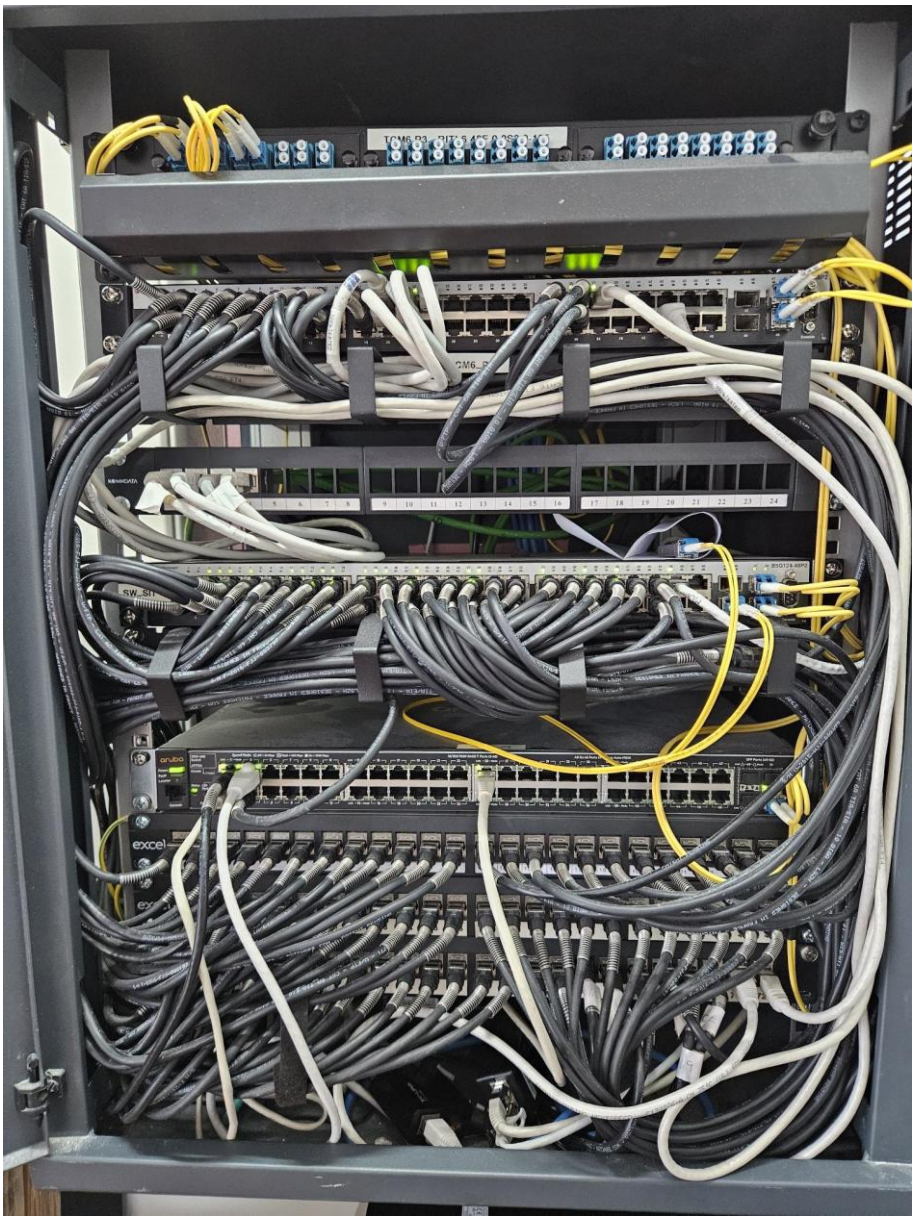


veu_clima_tcm6_p1_a_front

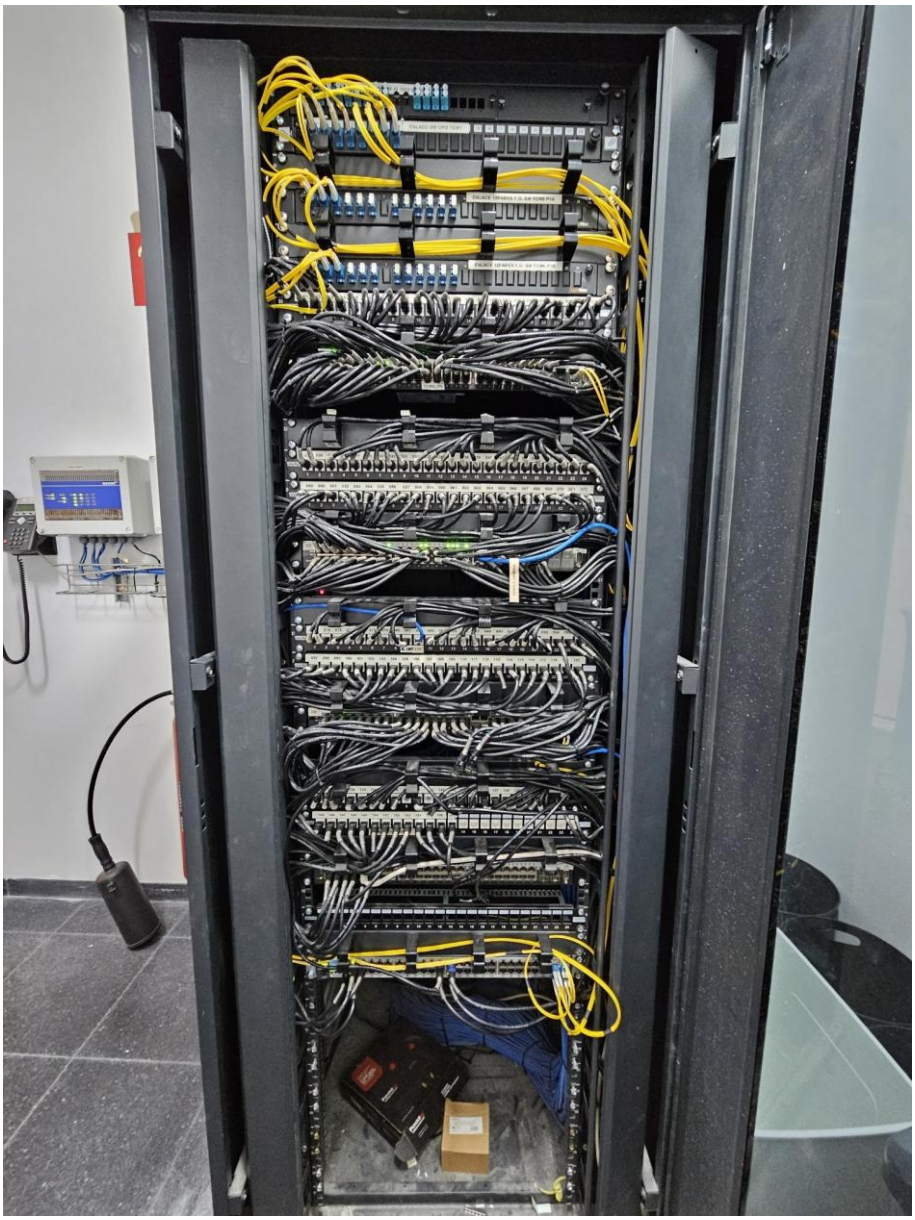


veu_clima_tcm6_p1_b_front

veu_clima_tcm6_p1_d_front



veu_clima_tcm6_p3_sit_front



veu_clima_tcm6_pb_a_front

ANNEX DE DOCUMENTACIÓ REFERIDA AL PLEC DEL PROJECTE DE RENOVACIÓ, IMPLANTACIÓ I SERVEI DE MANTENIMENT DE BASE DE LA INFRAESTRUCTURA DE XARXA, SEGURETAT I SERVEIS ASSOCIATS DEL TECNOCAMPUS MATARÓ-MARESME

Exp. Número ES_LA0011122_2026_EXP_34

La documentació referida a aquest annex ha estat referenciada al PPT d'aquest contracte i queda disponible per al seu tractament i consulta amb millor qualitat i autonomia. Qualsevol documentació que el licitador consideri incomplerta o faltant pot demanar-la al Tecnocampus per les vies habituals.

Ubicació física de TecnoCampus	Ubicacio de Tecnocampus.pdf
Esquema lògic de la Xarxa de TecnoCampus	Esquema logic 2023.pdf
Esquema físic de la Xarxa de TecnoCampus	Esquema fisic 2023.pdf
Resum dels principals enllaços de fibra dels edificis	1_Visio general de les fibres de tecnoca
Proposta de nou esquema lògic d'alt nivell	Nou Esquema logic Alt Nivell.pdf
Proposta de nou esquema lògic nivell 1	Nou Esquema logic nivell1.pdf
Esquema de seguretat lògic actual	Esquema seguretat fisic 2023.pdf
Proposta de la política de seguretat nova	Nova Politica de seguretat Alt Nivell.p

Esquema del servei VPN actual	Esquema Servei VPN.pdf
Esquema del servei NAC actual	Esquema servei NAC.pdf
Esquema Radius	Esquema Radius.pdf
Esquema servei DNS actual	Esquema DNS.pdf
Esquema serveis DHCP + NTP + IPAM	Esquema DHCP NTP IPAM.pdf

ANNEX DE DOCUMENTACIÓ SOBRE LA PLATAFORMA BÀSICA PROPOSADA DEL TECNOCAMPU3S - PROJECTE DE RENOVACIÓ, IMPLANTACIÓ I SERVEI DE MANTENIMENT DE BASE DE LA INFRAESTRUCTURA DE XARXA, SEGURETAT I SERVEIS ASSOCIATS DEL TECNOCAMPUS MATARÓ-MARESME

Exp. Número ES_LA0011123_2026_EXP_34

A continuació es llisten i concreten les propostes mínimes extretes d'auditoria interna per donar servei als requeriments de la xarxa del TecnoCampus, aplicant els percentatges de reducció de ports i unificació de xarxes i serveis

En base a la auditoria interna d'equipament i proposta mínima de requeriments de connectivitat sobre la que el licitador podrà començar a treballar indiquem:

Equipament base proposat

- Core de veu i dades:
  - 2 switches core.
- Accés de veu i dades – equipament multigigabit:
  - 10 switches veu i dades multigigabit 48 ports, dels quals un mínim de 12 ports han de suportar MGIG (1/2.5/5 GB) POE+ o PE++ com a opció de millora
- Accés de veu i dades restant:
  - 30 switches veu i dades 48 ports.
  - 18 switches veu i dades 24 ports.
- Core de CCTV i Clima:
  - 1 switch core.
- Accés CCTV i Clima:
  - 1 switches veu i dades 48 ports.
  - 6 switches veu i dades 24 ports.

A fi de disposar d'una electrònica de xarxa correctament dimensionada s'ha realitzat una auditoria d'us efectiu de ports per a la nova plataforma:

- Equipament proposat de 48/24p.
- Classificació entre equipament de tipus core, dades o clima.
- Ubicacions i notes on hi ha més d'un armari rack amb enllaços separats de clima i dades.

Ubicació	Equipament 48p proposats	Equipament 24p proposats	Dades / Clima / Core	Notes
TCM4_PS (Garita Parking)	0	1	Clima	Armaris clima i dades separats (*)
		1	Dades	Armaris clima i dades separats (*)
TCM4_PS2 (Parking)	0	1	Clima	
TCM2_PS_CPD2	2	0	Core	**Equips Core** + SW d'accés en racks separats (**)
		1	Dades	**Equips Core** + SW d'accés en racks separats (**)
TCM1_Planta1_A	**3**	0	Dades	
TCM1_Planta1_B	**3**	0	Dades	
TCM1_Planta1_C	0	1	Dades	
TCM1_Planta2_A	**2**	1	Dades	
TCM1_Planta2_B	**2**	0	Dades	

TCM1_Planta2_C	0	1	Dades	
TCM1_PlantaB_A	0	1	Clima	Armaris clima i dades separats (*)
	0	1	Dades	Armaris clima i dades separats (*)
TCM1_PlantaB_B	**1**	0	Core	**Equip Core Clima (***)**
	1	0	Clima	Mateix armari equip core clima
	2	1	Dades	Armaris clima i dades separats (*)
TCM1_PlantaB_C	0	1	Clima	Armaris clima i dades separats (*)
	0	1	Dades	Armaris clima i dades separats (*)
TCM1_PS_C_Reimagina	1	0	Dades	
TCM1_PS_B_CPD	**2**	0	Dades	
TCM1_PS_A_Plato	**1**	0	Dades	
TCM2_PS_Auditori	**2**	0	Dades	
TCM2_Planta0	1	1	Dades	
TCM2_Planta1	1	1	Dades	
TCM2_Planta2	1	1	Dades	
TCM2_Planta3	2	0	Dades	
TCM2_Planta4	2	1	Dades	
TCM2_Planta5	2	0	Dades	
TCM2_Planta6	2	0	Dades	
TCM3_PS_Gimmas	0	1	Clima	
TCM3_Planta0	0	1	Dades	
TCM3_Planta4_OpenSpace	1	0	Dades	
TCM3_Planta1	1	0	Dades	
TCM3_Planta3	0	1	Dades	
TCM3_Planta4	1	0	Dades	
TCM3_Planta6	0	1	Dades	
TCM6_P0	**2**	1	Dades / Clima	
TCM6_P0_MasterChef	**0**	1	Dades / Clima	
TCM6_P1A	2	0	Dades / Clima	
TCM6_P1B	**2**	0	Dades / Clima	
TCM6_P1D	1	0	Dades / Clima	
TCM6_P3_SIT	1	1	Dades / Clima	
TCM2_PS_Montant	0	1	Clima	
Equipament total proposat	**44**	**24**	**Total SWs**	**68**
Ports previstos	**2112**	**576**	**Total Ports**	**2688**

(*) Dins la mateixa sala tècnica a una distancia màxima de uns 5 metres.
(**) Dins el CPD amb connexions habilitades entre armaris de fibra i coure.
(***) Dins rack mural de petites dimensions. Consultar fotografies en cas de dubtes.