



Catàleg de sistemes per a proveïdors

Documentació

06/2025

Registre de Modificacions

Versió	Descripció	Autor	Creació	Aprovador	Data Aprovació
1.0	Creació del document	DSI	21/05/25		

Índex

1	Introducció	4
2	Requisits proposats d'Infraestructura/Plataforma	5
2.1	Servidors Virtuals i Hardware Físic	5
2.2	Sistemes Operatius Homologats.....	5
2.3	Cloud.....	5
2.3.1	Regió i Alta Disponibilitat	5
2.3.2	Ús de Serveis i Eficiència Operativa	5
2.3.3	Connectivitat i Xarxa	6
2.3.4	Seguretat i Governança	6
2.3.5	Automatització i Desplegaments	6
2.3.6	Sistemes Operatius i Compatibilitat.....	6
2.4	Contenidors.....	6
2.4.1	Xarxa	6
2.4.2	Rutes	6
2.4.3	Usuaris	6
2.4.4	Registry	7
2.4.5	Volums	7
2.4.6	Neteja de l'entorn	7
2.5	Emmagatzematge	7
2.5.1	Spectrum Scale.....	7
2.5.2	Entorns amb SVC.....	7
3	Accessos i autenticació	7
3.1	Accés remot	8
3.2	Gestió d'usuaris	8
3.3	Actualitzacions i pegats de seguretat.....	8
3.4	Connectivitat.....	8
3.4.1	Xarxa cablejada	8
3.4.2	Xarxa sense fils.....	8
3.4.3	Xarxa cablejada i sense fils	8
3.4.4	Altres tecnologies de connectivitat	9
3.4.5	Protocols de comunicació	9
3.4.6	Adreçament IP	9
3.4.7	Gestió centralitzada.....	9
3.5	Antivirus.....	9
3.6	Copies de seguretat	9
3.7	Monitorització	10
4	Autenticació d'aplicacions.....	10
5	Integració amb altres sistemes	10
6	Seguretat i compliment.....	10

1 Introducció

L'objectiu d'aquest document és establir un marc tècnic i de seguretat que han de complir les aplicacions de tercers que s'instal·lin en plataformes de l'hospital Clínic Barcelona, garantint:

- Compatibilitat amb la infraestructura existent.
- Seguretat en l'accés i la integració.
- Homogeneïtat en els punts de compliment a proveïdors.

2 Requisits proposats d'Infraestructura/Plataforma

2.1 Servidors Virtuals i Hardware Físic

- Els servidors virtuals han de ser compatibles amb **vSphere 8.0** i desplegats a partir d'una **plantilla** actualitzada amb l'última versió de sistema operatiu i pegats de seguretat.
- El sistema operatiu del servidor virtual haurà d'estar **homologat** per els departaments corresponents de la DSI.
- Ha d'estar reflexat sempre quin tipus de servei o aplicació s'instalarà en el servidor (Oracle, Web Server, Fileserver...) per tal de poder aplicar les Best Practices per entorns virtuals de cada fabricant.
- La configuració per defecte inclou **2 vCPUs**, amb possibilitat d'augmentar segons el consum
- La memòria **RAM** s'ajustarà segons el tipus de servei i les seves necessitats
- Especificar quin tipus de **dades** contindrà el disc/s (BBDD, Logs, Backups, imatge, fitxers...) i una **previsió de creixement**.
- No es permet més d'una **targeta de xarxa** per servidor virtual.
- No es poden instal·lar dispositius **USB** en els servidors virtuals.
- S'ha de buscar un sistema de **llicenciament** que pugui anar per **xarxa**.
- Els **appliance** han de ser compatibles amb **vSphere 8.0** i la versió **20** de **virtual hardware**.
- Els **discos** del appliance (vmdk) hauran de configurar-se amb una controladora **SCSI** virtual amb qualsevol de les opcions (LSI Logic Parallel, LSI Logic SAS, VMware Paravirtual).
- A nivell de seguretat s'afegirà el dispositiu **TPM** per poder encriptar el servidor.

2.2 Sistemes Operatius Homologats

- Linux: Suse, RedHat, AlmaLinux, RockyLinux, Ubuntu, Debian.
- Windows Server: Versions 2022 i 2025 (en suport oficial).
- No s'admeten sistemes obsolets o sense suport oficial.

Cicles de vida

- Suse : <https://www.suse.com/lifecycle>
- RedHat: <https://access.redhat.com/support/policy/updates/errata>
- AlmaLinux: <https://wiki.almalinux.org/release-notes>
- RockyLinux: <https://wiki.rockylinux.org/rocky/version>
- Ubuntu: <https://ubuntu.com/about/release-cycle>
- Debian: <https://wiki.debian.org/LTS>
- Windows Server 2022: <https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2022>
- Windows Server 2025: <https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2025>

No s'admeten **sistemes obsolets** o sense suport oficial, per garantir la seguretat i la compatibilitat amb les actualitzacions.

2.3 Cloud

2.3.1 Regió i Alta Disponibilitat

- Tots els serveis s'han de desplegar a la regió Irlanda (eu-west-1). Qualsevol excepció ha d'estar degudament justificada i aprovada.
- Si es requereix una arquitectura d'alta disponibilitat, el màxim de zones de disponibilitat seran de dues.

2.3.2 Ús de Serveis i Eficiència Operativa

- Es recomana prioritzar serveis gestionats (PaaS/SaaS) abans que solucions basades en instàncies EC2.

- Els sistemes han d'estar dissenyats amb criteris d'eficiència de costos, escalabilitat i mantenibilitat.

2.3.3 Connectivitat i Xarxa

- Només es poden utilitzar els rang IP proporcionats per l'equip de l'hospital.
- L'accés a instàncies ha de ser segur i restringit, preferiblement mitjançant AWS Systems Manager (SSM). No està permès exposar ports com SSH, RDP o VNC a Internet.
- La creació i gestió de VPCs i components compartits (com Internet Gateway o Transit Gateway) és responsabilitat exclusiva de l'equip d'infraestructura de l'hospital.

2.3.4 Seguretat i Governança

- La gestió d'identitats es realitza mitjançant IAM Identity Center federat amb Active Directory.
- S'aplicarà sempre el principi de mínim privilegi i l'ús de RBAC (control d'accés basat en rols).
- Tots els serveis han de tenir l'auditoria activada mitjançant CloudTrail i estar monitoritzats amb CloudWatch Logs.
- L'etiquetatge de recursos és obligatori.

2.3.5 Automatització i Desplegaments

- Tota la infraestructura s'ha de definir com a codi (IaC), preferiblement amb **Terraform**.
- Es recomana automatitzar els desplegaments per garantir la traçabilitat, la consistència i una gestió eficient.

2.3.6 Sistemes Operatius i Compatibilitat

- Es prefereix l'ús de Linux com a sistema operatiu base a AWS.
- En cas de requerir Windows, es valorarà si s'ha d'implantar a AWS o Azure. Si s'utilitzen ambdós entorns, cal garantir la interoperabilitat entre ells.

2.4 Contenedors

2.4.1 Xarxa

- Rang 172.27.14.0/24
- El driver de Docker ha de ser bridge i NO host.

2.4.2 Rutes

- Tots els desplegaments de contenidors mitjançant Docker Compose ubicats a la ruta /opt/docker-compose.
- Cal que tant /opt/docker-compose, com /var/lib/docker resideixin en volums independents gestionats amb LVM (Logical Volume Manager).

2.4.3 Usuaris

Els proveïdors disposaran d'un **usuari específic** per a la gestió dels projectes de contenidors. Aquest usuari serà el responsable d'executar les operacions següents:

- **docker-compose (comanda)**
- **docker (comanda)**

2.4.4 Registry

Totes les imatges de contenidors generades específicament per als projectes de l'hospital hauran d'estar allotjades de forma obligatòria al nostre entorn **AWS ECR (Elastic Container Registry)**. En cas que per alguna raó no pugui ser així, cal que les imatges estiguin allotjades en algun repositori de forma segura incloent l'escaneig de les mateixes.

2.4.5 Volumes

- Mapeig de volums via docker-compose.yml (ubicats a la següent ruta: **/opt/docker-compose/<nom-del-projecte>/mapejos**)

2.4.6 Neteja de l'entorn

Es requereix fer, de manera periòdica, les següents accions de manteniment:

- **Eliminació d'imatges orfes** (no utilitzades per cap contenidor actiu).
- **Eliminació de contenidors aturats**, xarxes no utilitzades i volums temporals no referenciats.

Execució regular de comandes :

- docker (comanda) prune

2.5 Emmagatzematge

Sempre que sigui possible, la **base de dades** s'ha de crear dins del nostre SQL corporatiu.

Els servidors no podran oferir recursos samba o CIFS.

Si es requereix d'un recurs per a dades, tenir en compte els següent punts.

2.5.1 Spectrum Scale

Per determinar la ubicació adequada de les dades en el sistema d'emmagatzematge, cal disposar de la següent informació per part del proveïdor o sol·licitant:

- **Tipus de dada:** Si es tracta de dades amb accés freqüent (**dades calentes**) o bé dades històriques, amb accés esporàdic, accés ofimàtic o amb un gran volum. (**dades fredes**)
- **Freqüència d'accés**
- **Volum estimat inicial i creixement previst** (expressat en GB/any)
- **Qui accedirà a les dades**

Aquestes dades són imprescindibles per evitar el malbaratament de recursos com els **discos SSD**, destinant-los únicament a dades que realment requereixin altes prestacions.

2.5.2 Entorns amb SVC

En entorns amb sistemes **SVC (SAN Volume Controller)**, caldrà especificar:

- Si es requereix una **LUN dedicada**, per si s'ha d'adjuntar un volum específic exclusiu per a l'aplicació o sistema sol·licitat

3 Accessos i autenticació

A continuació es detalla el suport per a entorns corporatius Wifi SomClinic, accés des de xarxa interna, i compliment de polítiques de còpia de seguretat, monitoratge, actualitzacions, pegats de seguretat i recuperació.

3.1 Accés remot

- L'**accés remot** a la xarxa de l'Hospital es realitzarà amb un client VPN proporcionat per la DSI. Aquests accessos són de caràcter nominal i hauran de ser sol·licitats per personal de l'Hospital.
- Per a permetre la connexió mitjançant VPN l'equip origen ha de complir amb els següents requisits:
- Sistema operatiu **Windows actualitzat** amb els últims pegats de seguretat aplicats
- **Antivirus operatiu i actualitzat.**
- L'**accés** als servidors que es trobin en la infraestructura del Clínic es realitzarà mitjançant l'accés remot via guacamole per <https://remot.clinic.cat>. (FortiPAM en el futur).
- L'accés remot a les estacions de treball no està permesa per part dels proveïdors. En cas necessari caldrà coordinar-se amb el SAU per a gestionar la petició.

3.2 Gestió d'usuaris

li

- La **gestió d'accessos i contrasenyes** dels usuaris s'ha de realitzar mitjançant el nostre directori actiu.
- L'aplicatiu o recurs que faci ús dels usuaris corporatius haurà de tenir segmentació d'accessos basat en rols i amb el mínim privilegi.
- No es permeten aplicatius amb usuaris locals.

3.3 Actualitzacions i pegats de seguretat

- Els servidors s'hauran d'**actualitzar mensualment** amb les actualitzacions crítiques i de seguretat dins de les finestres de manteniment establertes.

3.4 Connectivitat

Tots els dispositius que requereixin connectivitat a la xarxa de l'Hospital (com ara ordinadors, impressores, equipament mèdic, dispositius IoT, etc.) hauran de complir els següents requisits tècnics.

3.4.1 Xarxa cablejada

- Interfície Ethernet amb connexió RJ45
- Velocitat: autonegociació 10/100/1000 Mbps
- Mode dúplex: autonegociació half/full

3.4.2 Xarxa sense fils

- Interfície inalàmbrica basada en l'estàndard **IEEE 802.11ac** o superior
- Compatibilitat amb protocols de roaming: **802.11k**, **802.11r** i **802.11v**
- **no es permeten dispositius amb connexió wifi mitjançant WPA2 personal**

3.4.3 Xarxa cablejada i sense fils

- Suport per a **autenticació 802.1x** amb usuari i certificat digital
- no es permeten aplicatius que funcionin mitjançant multicast
- no es permeten solucions que requereixin connectivitat entre dispositius de la mateixa xarxa, només estan permeses solucions de comunicació mitjançant client servidor

3.4.4 Altres tecnologies de connectivitat

El licitador haurà de proporcionar informació detallada sobre altres tecnologies de connectivitat inalàmbrica que incorporin els dispositius, com ara **Bluetooth**, **NFC**, o altres basades en transmissió radioelèctrica. A aquestes hauran de complir els següents requisits:

- **Xifratge:** Tota transmissió inalàmbrica ha d'estar xifrada
- **Freqüències:** No es podran utilitzar bandes de freqüència que ja estiguin assignades a altres solucions de l'Hospital (WiFi, RFID, lectors de temperatura, etc.)

3.4.5 Protocols de comunicació

- Totes les comunicacions s'hauran de realitzar mitjançant el protocol **TCP/IP**
- La configuració haurà de garantir transmissions segures, d'acord amb les guies del **Centro Criptológico Nacional (CCN)**
- S'hauran d'utilitzar **rangs de ports acotats**, que caldrà comunicar per permetre la definició de regles específiques als tallafocs corporatius

3.4.6 Adreçament IP

- Tots els dispositius, excepte els servidors, hauran d'obtenir una adreça IP automàticament a través del servidor **DHCP corporatiu**
- La implementació del protocol DHCP haurà de seguir els **estàndards internacionals** i garantir la compatibilitat amb els mecanismes de seguretat de l'Hospital (com la protecció contra **IP spoofing**)
- Qualsevol configuració que requereixi comunicació amb un altre sistema haurà d'usar configuracions mitjançant noms FQDNs (Fully Qualified Domain Name) i no mitjançant configuracions que indiquin direccions IPs

3.4.7 Gestió centralitzada

- En casos de desplegament massiu de dispositius, serà necessari disposar d'una **consola central de gestió**
- Aquesta ha de permetre executar accions sobre múltiples dispositius de forma simultània, evitant la configuració individual equip per equip

3.5 Antivirus

D'acord amb els estàndards de **seguretat i compliment normatiu** de l'organització, **tots els servidors** que s'implementin dins de la infraestructura corporativa hauran de tenir instal·lat l'antivirus **Microsoft Defender for Endpoint (EDR)** i completament operatiu.

És indispensable que el sistema estigui **configurat de manera que compleixi totes les polítiques de seguretat establertes per l'organització**, sense necessitat d'excepcions ni ajustos que puguin comprometre el **rendiment**, la **protecció** o la **estabilitat de l'entorn**.

3.6 Còpies de seguretat

Per tal de garantir una protecció adequada de les dades, caldrà que es proporcioni la següent informació:

- **Tipus de dades** que conté el servidor/sistema
- Existència de **base de dades**
- **Tipus de backup**
- **Horari** preferent per a l'execució de les còpies de seguretat

En absència d'indicacions específiques, s'aplicarà per defecte la següent metodologia:

- **Màquines virtuals (VMs):** còpia per **snapshot**
- **Servidors físics:** còpia **d'arxius a nivell de sistema**

Aquest plantejament busca garantir la protecció bàsica del sistema amb el mínim impacte en el rendiment, però podrà ser ajustat segons les necessitats concretes de cada projecte o entorn.

3.7 Monitorització

Per garantir la supervisió proactiva i la detecció d'incidències, **tots els servidors i serveis associats hauran d'estar integrats en el sistema de monitorització corporatiu**, basat en **Check MK**.

Els requeriments mínims són els següents:

- El sistema haurà de permetre la instal·lació de l'**agent de Check MK**
- Caldrà facilitar la documentació bàsica del servei
- **Nom del servei o servidor**
- **Funcionalitat principal**
- **Mètriques rellevants a monitoritzar**
- En cas de serveis crítics, s'haurà de definir conjuntament amb l'Hospital quins **checks específics** cal configurar.

4 Autenticació d'aplicacions

A continuació es detalla el procés d'Integració amb el sistema corporatiu d'identitat, Accés mitjançant Single Sign On (SSO) amb protocols com SAML2, OAuth2 o OpenID Connect i el suport per a autenticació multifactor (MFA)

- Qualsevol aplicació que es vulgui integrar amb l'**LDAP corporatiu** haurà de fer-ho mitjançant protocols d'autenticació basats en **SAML** o **OAuth**, que seran de caràcter obligatori.
- En cas que no sigui possible la integració amb l'LDAP de l'Hospital, el sistema haurà de disposar d'un **mètode propi de doble autenticació**, que garanteixi un nivell de seguretat equivalent.
- Tota aplicació tant SaaS com onprem haurà d'utilitzar l'autenticació corporativa Microsoft EntraID.

5 Integració amb altres sistemes

A continuació es detalla la comunicació mitjançant HTTPS, REST APIs, Web Services (SOAP) o estàndard com HL7/FHIR i la capacitat de federació per a interoperabilitat amb sistemes clínics i administratius.

Comunicació Segura: Tots els intercanvis de dades s'han de realitzar a través d'un canal segur utilitzant **xifrat TLS/SSL** amb certificat vàlid.

Format dels Missatges: Els missatges han d'estar estructurats en **estàndard HL7**, utilitzant **XML** com a sintaxi.

Codificació de Documents: Qualsevol document adjunt o contingut binari ha d'anar **codificat en Base64** i incrustat dins del missatge HL7

6 Seguretat i compliment.

El proveïdor ha de garantir:

- Compliment del ENS i del RGPD.

- Registre de traçabilitat, xifrat de dades en trànsit i en repòs.
- Declaració d'aplicabilitat i certificacions de seguretat del proveïdor.
- Connexió remota VPN.