Especificacions generals per a la integració de sistemes en la infraestructura de TMB

Versió 2.7

Infraestructura de Sistemes

Infraestructura Tecnològica i Operació Tecnològica de Sistemes

Direcció Ejecutiva d'Innovació, Tecnologia i Negoci Internacional

TMB

Contingut

Control de canvis

Versió	Data	Autor	Canvis
1.0		Javier Jarne	
2.0	05/06/2014	Javier Jarne	Redacció en format paràgraf
2.1	07/04/2015	Javier Jarne	Inclusió de la taula de control de canvis. Inclusió dels requisits RA-GN-4, RA-RS-4
2.2	20/10/2018	Javier Jarne	Reflectir canvis organitzatius. Incloure-hi els nous requisits de seguretat que emergeixen de l'existència de la Política.
2.3	14/08/2019	Javier Jarne	Introduir concepte “servei extern”
2.4	08/09/2021	Juan José del Río	Incloure requisits Seguretat TIC.
2.5	13/09/2021		Criteris obligatoris vs. opcionals
2.6	28/10/2021	Juan José del Río	Repàs criteris

1 Introducció

La filosofia del disseny de l'arquitectura física dels sistemes i la manera de treballar de TMB té l'objectiu següent:

Disposar d'una infraestructura:

- **adaptada a la criticitat dels diferents entorns de TMB;**
- **al menor cost d'adquisició, operació i manteniment;**
- **que compleix els criteris de seguretat establerts.**

Per poder aconseguir-lo, hi ha dues grans línies de treball.

- **Consolidació**. TMB ha apostat per disposar d'elements d'infraestructura comuns a tots els sistemes amb l'objectiu que puguin ser utilitzats per a totes les solucions. Aquesta reutilització permet optimitzar les inversions disposant de menys equips i, al seu torn, amb majors funcionalitats.
- **Estandardització.** S'han d'optimitzar els recursos destinats a gestionar i mantenir la infraestructura. Per a això, s'ha de limitar la diversitat d'elements, sistemes operatius, programari, eines…, ja que cada nova tecnologia introdueix una major complexitat en els sistemes i implica un esforç afegit d'administració, a més d'una despesa en formació. D'altra banda, l'estandardització assegura una correcta integració amb les eines de gestió i monitoratge existents.

Això es tradueix que les diferents arquitectures es recolzen en les mateixes capes de maquinari i programari base

	Arquitectura sistema 1		**Arquitectura sistema 2**	**…**	**Arquitectura sistema N**	
Aplicacions SW						
Servidors d'aplicació						
Base de dades						
Sistema operatiu						
Maquinari						
Emmagatzematge						
Comunicacions						
Cablatge						
CPD / Sala Tècnica						

Per tant, els **dissenys de les arquitectures dels sistemes han de fer-se de forma integrada amb la infraestructura ja existent** i amb tecnologies ja existents, i cal descartar solucions que comportin la creació de sitges tecnològiques.

Aquest document recull els **requisits generals** per al disseny, adquisició i operació d'una solució des del punt de vista **del maquinari, del sistema operatiu, de l'emmagatzematge i de la base de dades** (encara que recull també algun requisit de disseny d'altres aspectes).

A causa que per fer el disseny correctament integrat és necessari conèixer la infraestructura ja existent a TMB, **cal comptar, en la fase de disseny, amb la col·laboració del personal especialista de TMB** en instal·lacions físiques, cablatge (Departament d'Instal·lacions), xarxes de comunicacions (Departament de Xarxes i Telecomunicacions), maquinari, sistema operatiu, bases de dades, programari intermediari (Departament d'Infraestructura de Sistemes) i seguretat de la informació (Unitat de Seguretat TIC).

A més, tota la part de **monitoratge, operació i administració dels sistemes haurà de consensuar-se amb OTS** (Operació Tecnologica de Sistemes) per garantir que la solució és **completament operable per TMB una vegada lliurada**.

2 Disseny d'arquitectura

2.1 Generals

RA-GN-1	Obligatori sempre	El disseny de les arquitectures s'ha realitzat de manera que s'integra amb la infraestructura ja existent a TMB.
RA-GN-2	Obligatori sempre	El disseny ha de comptar amb la participació i acceptació dels especialistes d'instal·lacions, xarxes, infraestructura, bases de dades, programació intermèdia i seguretat TIC de TMB.
RA-GN-3	Obligatori sempre	El monitoratge, operació i administració dels sistemes han de ser consensuats amb el personal de TMB.
RA-GN-4	Obligatori si s'usa HW/sistemes a TMB	Tota la solució ha d'estar correctament llicenciada a nom de Ferrocarril Metropolità de Barcelona, SA, i/o Transports de Barcelona, SA, amb llicències que en permetin la reutilització posterior en cas de substitució del maquinari.

2.2 Seguretat

RA-RS-1	Obligatori sempre	El sistema ha de complir la política de seguretat de TMB i totes les seves normatives i directrius associades, incloses les de l'RGPD.
RA-RS-2	Obligatori sempre	El disseny ha de contemplar, des de l'inici, la seguretat com un factor intrínsec al seu disseny i en totes les capes.
RA-RS-3	Obligatori sempre	El disseny ha d'indicar l'RTO (Recovery Time Objective) i l'RPO (Recovery Point Objective) que ha de complir la solució.
RA-RS-4	Obligatori sempre	Si el sistema es considera crític, s'ha de dotar de mecanismes d'alta disponibilitat i contingència en totes les parts fonamentals.
RA-RS-5	Obligatori sempre	Tot equip al qual s'hagi d'accedir directament des d'Internet ha de situar-se en una DMZ.
RA-RS-6	Obligatori sempre	Han d'evitar-se solucions, arquitectures, protocols…, considerats insegurs o amb vulnerabilitats conegudes.
RA-RS-7	Obligatori sempre	Es prohibeix l'ús d'usuaris genèrics o comuns a diferents persones. Els usuaris s'han d'identificar amb l'usuari de domini personal de TMB, tant al sistema com a les aplicacions.

RA-RS-8	Obligatori sempre	Tant el sistema operatiu com les aplicacions que estiguin instal·lades als equips/servidors, PC, estacions de treball..., han de tenir un pla d'actualització per no quedar obsolets.
RA-RS-9	Obligatori sempre	S'ha de disposar d'un pla per a la instal·lació de pedaços als sistemes i aplicacions instal·lades als equips per evitar vulnerabilitats de seguretat.
RA-RS-10	Obligatori sempre per a equips a TMB	Els accessos com a administrador als equips s'hauran de fer mitjançant la solució PAM de TMB, i hi queda expressament prohibit l'accés directe com a administrador.

2.3 Xarxa

RA-RD-1	Obligatori sempre	Només són possibles solucions de comunicacions basades en IP i admeses per la xarxa corporativa. No s'admetran solucions que no utilitzin aquesta xarxa.
RA-RD-2	Obligatori sempre	El disseny s'ha d'adequar a les característiques de la xarxa i ha de detallar els requisits i necessitats de connectivitat entre els equips i la resta de sistemes de TMB (fluxos de comunicació entre equips, IP necessàries, protocols i ports usats, VLAN necessàries, amplades de banda, latències màximes, necessitat de multidifusió, serveis de balanceig...).
RA-RD-3	Obligatori si hi ha equips a TMB	El sistema ha d'adequar-se al pla d'encaminament IP existent a TMB.
RA-RD-4	Obligatori si hi ha equips a TMB	No es poden estendre VLAN de nivell 2 entre centres o entre segments de xarxa separats per tallafocs.
RA-RD-5	Obligatori si hi ha equips a TMB	La connectivitat és a 1000 Mbps per a servidors virtuals o servidors de làmina situats als CPD. Per a un altre tipus de servidors o ubicacions, la connexió pot estar limitada a 100 Mbps.
RA-RD-6	Obligatori sempre	La connexió d'un equip a la xarxa corporativa (sigui cablejada o sense fil) implica l'acceptació i compliment dels requisits de connexió a la Xarxa de TMB vigents.
RA-RD-7	Obligatori sempre que s'empri connexió	Les solucions que impliquen la connexió d'equips amb solucions de connexió de dades de xarxes de telefonia mòbil (4G/5G/...) han d'utilitzar SIM corporatives i APN privat.

	LTE	

2.4 Servidors “on premise”

RA-SR-1	Obligatori amb servidor a TMB	Tot equip servidor ha d'estar situat en un dels CPD corporatius situats a l'edifici de Sagrera (entorns productius) i/o a la cotxera de Triangle (entorns de productius de contingència, preproducció i desenvolupament).
RA-SR-2	Obligatori amb servidor a TMB	Les solucions han d'estar basades en servidors virtuals sobre VMWare. Les úniques excepcions a aquesta premissa són: - Equips que requereixin programari no admès per VMWare o el fabricant dels quals no proporcioni un suport complet sobre VMWare o requereixi excés de llicenciament (com per exemple BD Oracle). - Equips les necessitats de recursos dels quals (I/O, targeta gràfica…) impedeixin o desaconsellin la seva virtualització.
RA-SR-3	Obligatori amb servidor a TMB	En la fase de disseny s'han de dimensionar els servidors des del punt de vista de consum de CPU, RAM i espai d'emmagatzematge (SO i aplicació) per reservar-ne l'espai a la granja de VMWare.
RA-SR-4	Obligatori amb servidor a TMB	Només cal subministrar maquinari de servidor en el cas que justificadament no es pugui muntar la solució sobre servidors virtuals o un responsable de sistemes de TMB indiqui que ha d'ampliar-se la granja de servidors virtuals.

2.5 Emmagatzematge “on premise”

RA-AL-1	Obligatori si hi ha base de dades a TMB	En cas de necessitar emmagatzematge addicional, es prefereix l'emmagatzematge centralitzat a través de NAS o SAN enfront de solucions amb discos locals, que estan desaconsellades.
RA-AL-2	Obligatori amb base de dades a TMB	En fase de disseny s'han d'indicar els requisits necessaris d'emmagatzematge en bloc (criticitat, volum, temps d'accés, necessitat de replicació entre centres, necessitat de snapshots…), així com indicar clarament les necessitats d'espai i creixement futur previst.

		En funció d'aquestes necessitats, TMB indicarà quin nivell d'emmagatzematge és l'adequat i reservarà espai a les cabines corporatives. (All-flash Array)
RA-AL-3	Obligatori si hi ha base de dades a TMB	En cas que no es disposi d'espai a la cabina i sigui necessari adquirir-lo dins del projecte, el responsable d'emmagatzematge de TMB indicarà, una vegada lliurats els requisits, quins elements s'han d'adquirir.
RA-AL-4	Obligatori si hi ha base de dades a TMB	En fase de disseny s'han d'indicar els requisits necessaris d'emmagatzematge de fitxer (volums, replicació…), així com indicar clarament les necessitats d'espai, creixement i permisos necessaris referenciats a grups de directori actiu.
RA-AL-5	Obligatori si hi ha base de dades a TMB	Per a totes les dades d'aplicació que s'utilitzin s'haurà de presentar un pla de gestió d'històrics (arxivament i/o eliminació).
RA-AL-6	Obligatori si hi ha dades a TMB	L'accés a les dades ha d'atorgar-se a identificadors nominals i en funció del que l'usuari necessiti saber o al que hagi d'accedir per desenvolupar el seu treball.
RS-AL-7	Obligatori si hi ha dades a TMB	S'han d'especificar clarament les dades de les quals cal fer còpia de seguretat, així com la periodicitat i retenció d'aquestes. S'ha de lliurar un procediment d'assignació de permisos d'accés a les dades i recursos.

2.6 Bases de dades

RA-BD-1	Obligatori si hi ha base de dades a TMB	En el cas que es necessiti base de dades, en general es prefereix consolidar en bases de dades corporatives a una base de dades dedicada.
RA-BD-2	Obligatori si hi ha base de dades a TMB	Les plataformes de BD actualment admeses són Oracle i SQL (sempre sobre versions amb suport de fabricant vigent). Altres opcions estan desaconsellades, ja que no podran ser gestionades i/o administrades pel personal de TMB.
RA-BD-3	Obligatori si hi ha base de dades a TMB	El disseny ha de proveir una descripció dels permisos necessaris i les estimacions d'espai necessari i creixement anual.
RA-BD-4	Obligatori si hi ha base de	Per a totes les bases de dades que es creïn o s'actualitzin, s'ha de presentar un pla de gestió

	dades a TMB	d'històrics (arxivament i/o eliminació).
RA-BD-5	Obligatori si hi ha base de dades a TMB	Tota creació d'una base de dades també implica la presentació d'una política de manteniment de dades, suport i monitoratge.
RA-BD-6	Obligatori sempre	No s'aconsellen mecanismes de rèpliques entre diferents bases de dades i no es permeten entre les bases de dades corporatives existents.
RA-BD-7	Obligatori si hi ha base de dades a TMB	En el disseny cal preveure l'existència a les bases de dades corporatives d'entorns de desenvolupament, integració i producció i, si el sistema ho requereix, la instal·lació i documentació en tots els entorns.
RA-BD-8	Obligatori si hi ha base de dades a TMB	En cas que la base de dades contingui dades personals subjectes a l'RGPD, s'ha de proporcionar xifratge d'aquestes dades i, en cas que sigui necessària la còpia a desenvolupament o integració, s'ha de proporcionar l'anonimització de les dades personals.
RA-BD-9	Obligatori si hi ha dades a TMB	L'accés a les dades ha d'atorgar-se a identificadors nominals i en funció del que l'usuari necessiti saber o al que hagi d'accedir per desenvolupar el seu treball. S'ha de lliurar un procediment d'assignació de permisos d'accés a les dades i recursos.
RA-BD-10	Obligatori si hi ha dades personals a la BD	En cas que la base de dades contingui dades personals que estiguin afectades per l'RGPD, cal xifrar aquesta informació a la base de dades.

2.7 PC, estacions de treball i altres sistemes distribuïts

En aquesta categoria s'hi inclou tot aquell equipament necessari fora del CPD amb processador i un sistema operatiu. Comunament, són PC, llocs de treball o equips per a control o gestió d'altres dispositius.

Es considera que té necessitats de tipus “equip industrial” tot aquell que, per grandària, ubicació, robustesa, condicions ambientals, consum, característiques de processament en temps real, …, requereix solucions específiques diferents de les d'un PC estàndard.

RA-SD-1	Obligatori sempre que s'usi/instal·li un equip a TMB	Una estació de treball només pot usar-se perquè un usuari interactuï amb el sistema. No poden, per tant, utilitzar-se per a processos en segon pla o tasques per lots propis d'equips centrals.

RA-SD-2	Obligatori sempre que s'usi/instal·li un equip a TMB	En el cas que la funció d'una estació de treball sigui crítica i se n'hagi de garantir el funcionament, s'ha de basar en servidors d'aplicacions o escriptoris centralitzats i amb equips distribuïts exclusivament d'accés remot (PC corporatius, clients lleugers...).
RA-SD-3	Obligatori sempre que s'usi/instal·li un equip a TMB	Els sistemes de seguretat corporatius no estan dissenyats ni operats per treballar amb estacions de treball. Tota informació que necessiti ser protegida ha d'emmagatzemar-se en repositoris centralitzats en equips del CPD.
RA-DS-4	Obligatori sempre que s'usi/instal·li un equip a TMB	Tot equip que s'instal·li a la xarxa de TMB ha de tenir instal·lat un programari antimalware configurat perquè s'actualitzi automàticament per estar al dia. Preferiblement, aquest programari serà el que estigui homologat a TMB.
RA-DS-5	Obligatori sempre que s'usi/instal·li un equip a TMB	Tot equip que s'instal·li a la xarxa de TMB ha de tenir activats els registres d'accés i auditoria del sistema.
RA-DS-6	Obligatori sempre que s'usi/instal·li un equip a TMB	Tot equip que s'instal·li a la xarxa de TMB ha d'actualitzar el sistema conforme a la política d'apedaçament i canvi de sistema de TMB.

2.8 Gestió de l'obsolescència

RO-OB-1	Obligatori si hi ha equips a TMB	El sistema ha d'indicar la fi del suport del fabricant prevista per a cadascun dels components.
RO-OB-2	Obligatori si hi ha equips a TMB	Al moment de l'engegada, el sistema no pot incloure en el seu disseny components sense suport per part del fabricador (obsolets) o amb una fi de suport prevista anterior a la fi de la garantia.
RO-OB-3	Obligatori si hi ha equips a TMB	En cas dels components afectats per obsolescència dins de la vida útil prevista, s'han de proveir els procediments per substituir/actualitzar els elements obsolets i corregir les possibles afectacions a altres components, amb una estimació econòmica dels costos en què cal incórrer.

3 Servidors

3.1 Requisits de maquinari

RS-HW-1	Obligatori si el servidor és a TMB	El maquinari ha de ser un model homologat a TMB, d'última generació. Actualment, el model estàndard són servidors tipus blade HPE Synergy.
RS-HW-2	Obligatori si el servidor és a TMB	Tot servidor ha d'anar instal·lat en un rack del CPD de Sagrera o al de Triangle.
RS-HW-3	Obligatori si el servidor és a TMB	Almenys tres mesos abans de la instal·lació, caldrà detallar les necessitats d'espai físic al rack, alimentació elèctrica (només monofàsica), refrigeració, punts de xarxa de dades i punts de xarxa de SAN i tipus de connectors (endolls, cables de xarxa…).
RS-HW-4	Obligatori si el servidor és a TMB	Els processadors han de ser Intel.
RS-HW-5	Obligatori si el servidor és a TMB	En el cas de servidors de làmina, sempre s'hi inclouran 4 ports de LAN 100/1000 i 2 de canal de fibra. En cas de servidors "stand-alone", inclouran un port de xarxa addicional independent per a l'accés a la gestió remota. També inclouran 2 ports de canal de fibra si és necessària la connexió a la SAN.
RS-HW-6	Obligatori si el servidor és a TMB	L'alimentació de l'equip ha de ser monofàsica.
RS-HW-7	Obligatori si el servidor és a TMB	L'equip ha d'estar equipat amb una segona font d'alimentació redundant.
RS-HW-8	Obligatori si el servidor és a TMB	El disc del sistema operatiu ha d'estar en "mirror".
RS-HW-9	Obligatori si el servidor és a TMB	Tot servidor físic ha de portar ILO amb la corresponent llicència per a la gestió remota avançada.
RS-HW-10	Obligatori si el servidor és a TMB	Tots els equips i cables han de quedar correctament col·locats, etiquetats i documentats segons la normativa vigent a TMB.
RS-HW-11	Obligatori si	Tot el material sobrant de la instal·lació (caixes,

	el servidor és a TMB	embalatges…) ha de ser retirat pel mateix proveïdor després de la instal·lació.

3.2 Sistema operatiu

RS-SO-1	Obligatori si el servidor és a TMB	El sistema operatiu ha d'estar homologat i admès per TMB. **Actualment estan admesos Windows Server** o **Red Hat Enterprise Linux** en l'última versió vigent.
RS-SO-2	Obligatori si el servidor és a TMB	El sistema operatiu s'ha de subministrar actualitzat a l'última versió i últim nivell de ServicePack i pedaços.
RS-SO-3	Obligatori si el servidor és a TMB	El sistema operatiu haurà d'estar correctament llicenciat a nom de Ferrocarril Metropolità de Barcelona, SA, i/o Transports de Barcelona, SA, amb llicències que en permetin la reutilització posterior en cas de substitució del maquinari.

3.3 Requisits de seguretat

RS-SG-1	Obligatori sempre	La plataforma/SO ha de garantir l'accés i emmagatzematge segur: a les dades, als dispositius i als serveis que ofereix.
RS-SG-2	Obligatori sempre	La plataforma/SO ha de garantir que només les actualitzacions generades per entitats acreditades puguin actualitzar el sistema.
RS-SG-3	Obligatori sempre	Tot sistema ha d'incorporar un programari antimalware o el mecanisme de control de llista blanca corporatius i el tallafoc local activat i configurat.
RS-SG-4	Obligatori si el servidor és a TMB	En cas de disposar de sistemes de contingència, la seva activació ha de ser transparent per a la resta de sistemes amb els quals s'integri.
RS-SG-5	Obligatori sempre	Les aplicacions s'han d'executar en un compte d'usuari amb el menor privilegi possible. Han de ser comptes de servei que no permetin iniciar sessió des d'un terminal.
RS-SG-6	Obligatori si el servidor és a TMB	Totes les funcionalitats supèrflues del sistema operatiu han d'estar desinstal·lades o, en defecte d'això, deshabilitades.
RS-SG-7	Obligatori si hi ha equips	Totes les contrasenyes d'usuari han de poder-se canviar de forma centralitzada (en el cas d'equips Windows, és

	a TMB	automàtic amb la pertinença al domini).
RS-SG-8	Obligatori si el servidor és a TMB	El servidor ha d'integrar-se amb els sistemes de còpies de seguretat corporatius, per la qual cosa s'haurà d'especificar de quins directoris s'ha de fer còpia de seguretat i amb quina periodicitat i retenció. (NOTA) La integració amb els sistemes corporatius pot implicar la instal·lació d'un agent a l'equip.
RS-SG-9	Obligatori si l'equip és a TMB	Cal seguir les recomanacions de ciberseguretat de TMB per a servidors.
RS-SG-10	Obligatori si l'equip servidor és a TMB	S'han d'eliminar els usuaris 'convidat', canviar la contrasenya per defecte dels usuaris que hi hagi definits, sobretot el d'administrador.

3.4 Altres requisits d'instal·lació

RS-OT-1	Obligatori si hi ha equips a TMB	Els equips Windows han d'integrar-se amb un dels dominis corporatius basats en Microsoft Active Directory per facilitar la gestió d'usuaris i equips.
RS-OT-2	Obligatori si hi ha equips a TMB	Els equips Linux han d'integrar-se amb les eines de gestió centralitzada de configuracions (Ansible) i pedaços (SuSEManager).
RS-OT-3	Obligatori si hi ha equips a TMB	Tots els equips han de sincronitzar l'hora mitjançant protocol NTP amb els servidors de temps de TMB (en el cas d'equips Windows, és automàtic amb la pertinença al domini).
RS-OT-4	Obligatori si hi ha equips a TMB	El servidor ha de permetre la instal·lació dels agents necessaris per a la correcta integració amb les eines de gestió (còpia de seguretat, monitoratge, gestió de la SAN, planificador, distribució de programari i pedaços…).
RS-OT-5	Obligatori si hi ha equips a TMB	Als servidors s'hi accedirà únicament mitjançant l'eina PAM de TMB per a la seva gestió i administració remota.

3.5 Programari i aplicacions

RS-SW-1	Obligatori si hi ha equips a TMB	Les aplicacions han de fer ús del DNS per a la comunicació amb altres equips. No pot haver-hi adreces IP en el codi o en fitxers de configuració de les

		aplicacions.
RS-SW-2	Obligatori si hi ha equips a TMB	Les aplicacions que no requereixin intervenció de l'usuari han de funcionar sense necessitat que hi hagi una sessió iniciada.
RS-SW-3	Obligatori si hi ha equips a TMB	El sistema ha d'estar totalment operatiu després d'un reinici sense necessitat d'intervenció per part d'un operador o un usuari.
RS-SW-4	Obligatori si hi ha equips a TMB	En cas de necessitat de planificació de tasques periòdiques automatitzades, aquestes s'han d'integrar amb el planificador de tasques corporatiu.
RS-SW-5	Recomanació	En la mesura que sigui possible, cal automatitzar el desplegament de les solucions per si s'han de repetir en el futur, facilitar el manteniment o, senzillament, facilitar la documentació de tot el que s'ha instal·lat i configurat.

4 PC i estacions de treball

4.1 Requisits de maquinari

RE-HW-1	Obligatori si hi ha equips a TMB	El maquinari de tots els llocs d'operació necessaris s'ha d'adequar als equips homologats per TMB.

4.2 Requisits de sistema operatiu

RE-SO-1	Obligatori si hi ha equips a TMB	El sistema operatiu per PC i estacions de treball ha de ser Windows 11 Professional OEM.
RE-SO-2	Obligatori si hi ha equips a TMB	Tots els equips (incloent-hi els monitors o altres) han d'incorporar una garantia de fabricant de 4 anys.
RE-SO-3	Obligatori si hi ha equips a TMB	És obligatori fer la seqüència de tasques a través de SCCM per obtenir una maqueta.
RE-SO-4	Obligatori si hi ha equips a TMB	El desplegament massiu dels equips ha d'estar basat en la distribució mitjançant SCCM (Microsoft System Center Configuration Manager).
RE-SO-5	Obligatori si hi ha equips a TMB	Tant els equips com els comptes d'usuari, així com els recursos en xarxa necessaris, han d'estar integrats sota un Active Directory (d'ara endavant AD).
RE-SO-5	Obligatori si hi ha equips a TMB	Les polítiques a l'AD han d'estar documentades amb detall i cal descriure'n l'objectiu clarament. L'estructura d'Organitzational Unit s'haurà d'establir mitjançant un acord amb TMB.
RE-SO-6	Obligatori si hi ha equips a TMB	Tots els equips han de permetre les actualitzacions mensuals de Microsoft sense minvament de la disponibilitat de les aplicacions que s'han d'executar a l'equip.
RE-SO-7	Obligatori si hi ha equips a TMB	Les aplicacions han de disposar de les actualitzacions necessàries per a la seva computabilitat amb l'actualització del sistema operatiu i controladors.
RE-SO-8	Obligatori si hi ha equips a TMB	Les aplicacions han de ser compatibles amb qualsevol monitor, KVM, projectors o qualsevol altre que tingui compatibilitat amb el sistema operatiu.

RE-SO-9	Obligatori si hi ha equips a TMB	La resolució de vídeo ha de ser adaptable i compatible amb qualsevol dispositiu de vídeo, mentre aquest sigui compatible amb el sistema operatiu, sense que es deformi el format de sortida.

4.3 Requisits de seguretat

RE-SG-1	Obligatori si hi ha equips a TMB	Tot PC i estació de treball ha d'integrar-se sota l'antivirus i programari antimalware o el mecanisme de control de llista blanca corporatius.
RE-SG-2	Obligatori si hi ha equips a TMB	Els comptes dels usuaris han d'estar integrats sota l'eina de Gestió d'Identitats de TMB (en aquest cas només en són usuaris aquelles persones que inicien sessió en la màquina i disposen d'un escriptori amb accés a les aplicacions i dades, inclou MFA). En qualsevol cas, la solució sempre ha de garantir la traçabilitat de l'ús que es faci des de l'equip (quin, qui, com, quan, on). Si la solució proposa un equip multiusuari en mode quiosc només mostrarà la/les aplicació/ons que garanteixin la traçabilitat a través dels comptes usuaris nominals. Pel que fa als usuaris utilitzats per arrencar serveis (quan siguin necessaris) als equips han d'estar integrats al DA de TMB.
RE-SG-3	Obligatori sempre	Les aplicacions han d'executar-se en un compte d'usuari amb el menor privilegi possible.
RE-SG-4	Obligatori si hi ha equips a TMB	Totes les contrasenyes d'usuari han de poder-se canviar de forma centralitzada (en el cas d'equips Windows, és automàtic amb la pertinença al domini).
RE-SG-5	Obligatori si l'equip és a TMB	Cal seguir les recomanacions de ciberseguretat de TMB per a estacions de treball.

4.4 Altres requisits

RE-OT-1	Obligatori si hi ha equips a TMB	Tot PC i estació de treball han d'integrar-se amb un dels dominis corporatius basats en Microsoft Active Directory per facilitar la gestió d'usuaris i equips (si n'hi ha per a aquests elements d'OT) i, en cas contrari, hauria de generar-se'n un de nou per a la posterior federació amb l'existent a TMB.

RE-OT-2	Obligatori si hi ha equips a TMB	Les aplicacions han de fer ús del DNS per a la comunicació amb altres equips. No pot haver-hi adreces IP en el codi o en fitxers de configuració de les aplicacions.
RE-OT-3	Obligatori si hi ha equips a TMB	Tots els PC i estacions de treball han de sincronitzar l'hora mitjançant protocol NTP amb els servidors de temps de TMB (en el cas d'equips Windows, és automàtic amb la pertinença al domini).
RE-OT-4	Obligatori sempre per a equips a TMB	Per a la distribució d'aplicacions en PC, s'ha de seguir el següent model: • Distribució mitjançant Microsoft App-V. Distribució de programari mitjançant Microsoft SCCM. En tots els casos, s'ha de documentar el procediment de generació dels paquets i instal·lació.

5 Sistemes distribuïts industrials

5.1 Requisits de maquinari

RI-HW-1	Obligatori si hi ha equips a TMB	El disseny de l'equip ha de ser industrial, des de l'ús de CPU de rang industrial (variants industrials de CPU amb arquitectura x86 AMD, Intel o ARM), així com tots els seus components/perifèrics (targeta gràfica, expansió de ports, mòdem, mòduls de comunicacions, I/O…), fins al disseny del xassís que l'allotja.
RI-HW-2	Obligatori si hi ha equips a TMB	Els connectors han de ser de tipus industrial amb fixacions que admetin les normatives corresponents en cada cas i permetin un manteniment senzill. Per exemple, connectors resistents a les vibracions, al desgast, a la degradació per calor, etc.
RI-HW-3	Obligatori si hi ha equips a TMB	Els mitjans d'emmagatzematge no han de ser fàcilment accessibles des de l'exterior per seguretat, però sí que han de facilitar en la mesura del possible el seu manteniment.
RI-HW-4	Obligatori si hi ha equips a TMB	El criteri per definir si el connector femella es col·loca a la placa o al cable és el següent: és més valuosa la instal·lació que els equips, sempre que la reparació i/o canvi suposi una llarga immobilització del vehicle/tren o una complexa substitució de la instal·lació fixa. En aquest sentit, es prefereix el connector femella al cable en comptes de ser a l'equip perquè és més robust i menys propens a una intervenció (substitució i/o reparació).
RI-HW-5	Obligatori si hi ha equips a TMB	L'equip ha de disposar d'un fusible ràpid (d'accés exterior) que el protegeixi de sobreintensitats.
RI-HW-6	Obligatori si hi ha equips a TMB	L'equip ha de complir les normatives específiques en el cas d'anar embarcat en un vehicle de transport de passatgers o les normatives ferroviàries en el cas d'anar embarcat en un tren i, a més, ha d'estar acompanyat de totes aquelles certificacions oficials que acreditin el compliment d'aquestes normatives. Per exemple, normatives: marcatge I-mark, mediambientals, mecàniques, vibració, temperatura, humitat, elèctriques i electromagnètiques, immunitat, emissions radiades i conduïdes, compatibilitat electromagnètica.
RI-HW-7	Obligatori si hi ha equips	Els mitjans d'emmagatzematge han de ser de tipus industrial per garantir robustesa, durabilitat i fiabilitat. Si l'equip industrial ha de ser embarcat en vehicle/tren o

	a TMB	susceptible de vibracions, s'han d'emprar mitjans d'emmagatzematge no mecànics com ara SSD de rang industrial (discos d'estat sòlid) o CF industrials (Compact Flash). CF industrials (Compact Flash). No es recomana l'ús de memòries flaix tipus NAND (flaix usb, SD…) per la seva poca robustesa enfront de corrupcions de dades, en el seu lloc es prefereixen memòries de tipus NOR o híbrides que conjuminin el millor de les dues tecnologies (EFD, ORNAND, OneNAND, mDOC…).
RI-HW-8	Obligatori si hi ha equips a TMB	Tots els connectors han d'anar correctament fixats al xassís mitjançant elements de subjecció que evitin que s'afluixin o es degradin en manipular-los i rebre xocs i vibracions.
RI-HW-9	Obligatori si hi ha equips a TMB	El disseny del xassís ha d'afavorir la dissipació de calor i la circulació d'aire, així com la disposició de components, dispositius i plaques d'expansió a l'interior de la CPU.
RI-HW-10	Obligatori si hi ha equips a TMB	La ranura del mitjà d'emmagatzematge, sigui de tipus compact flash o disc dur d'estat sòlid, ha de tenir un sistema de subjecció ferm, robust i durador enfront de vibracions, xocs i manipulacions.
RI-HW-11	Obligatori si hi ha equips a TMB	L'equip ha d'estar fixat correctament preferiblement mitjançant element estàndard tipus bastidor o carril DIN. En el cas d'anar embarcat i en funció de les vibracions a què pugui ser sotmès, es recomanen l'ús de sistemes d'absorció de vibracions.
RI-HW-12	Obligatori si hi ha equips a TMB	La disposició de l'equip o dels equips i dels perifèrics ha de facilitar la dissipació de calor i la circulació d'aire.
RI-HW-13	Obligatori si hi ha equips a TMB	La disposició de l'equip o dels equips i dels perifèrics ha de facilitar el manteniment, tant per a la substitució de l'equip com per al canvi d'un perifèric, per exemple tipus CF o disc SSD.
RI-HW-14	Obligatori si hi ha equips a TMB	El proveïdor de l'equip industrial ha de facilitar un programa de test de maquinari i diagnòstic, tant de l'equip/s, perifèrics, plaques de I/O, així com del diagnòstic de tot el conjunt.

5.2 Requisits de fiabilitat tècnica

RI-FT-1	Obligatori si hi ha equips a TMB	Els requisits de maquinari del sistema hauran de ser els mínims possibles per complir totes les funcionalitats actuals i futures. S'ha de minimitzar el consum d'energia i CPU, cosa que implica una temperatura de treball

		menor i un augment de la fiabilitat en general.
RI-FT-2	Obligatori si hi ha equips a TMB	L'arquitectura d'integració ha de ser tan simple com sigui possible per afavorir la fiabilitat, el manteniment i l'impacte en la resta del sistema en què s'integri l'equip.

5.3 Requisits del sistema operatiu

RI-SO-1	Obligatori si hi ha equips a TMB	L'equip ha de tenir un sistema operatiu de tipus industrial, siguin versions basades en Linux industrials o personalitzades a aquest efecte, o bé solucions comercials per a entorns embeguts o industrials tipus Windows Embedded.
RI-SO-2	Obligatori si hi ha equips a TMB	El sistema operatiu ha de ser totalment robust enfront de talls d'alimentació, reinicis continuats i corrupcions.
RI-SO-3	Obligatori si hi ha equips a TMB	El sistema operatiu ha de ser tan eficient i tan reduït, tant en espai com en consum de recursos, com sigui possible.
RI-SO-4	Obligatori si hi ha equips a TMB	Els sistemes de fitxers emprats i el particionament del mitjà d'emmagatzematge han de ser robusts enfront de corrupcions de dades. El tipus de sistema de fitxers ha de garantir que, davant talls de corrent o reinicis, el sistema operatiu i les aplicacions no es corrompin, i que les dades perdudes siguin mínimes. Per aquesta raó, es recomana l'ús de particions o fins i tot dispositius d'emmagatzematge diferenciats per a SO/aplicacions vs. dades.
RI-SO-5	Obligatori si hi ha equips a TMB	L'encapsulament del sistema operatiu ha de permetre d'una forma tan simple com sigui possible la seva actualització completa, parcial, així com del nucli i les aplicacions de manera desatesa.
RI-SO-6	Obligatori si hi ha equips a TMB	El sistema ha de quedar completament operatiu després d'un reinici, sense necessitat d'intervenció manual i arrencant en el menor temps possible.
RI-SO-7	Obligatori si hi ha equips a TMB	Els sistemes que no requereixin interactuar amb l'usuari per funcionar no han d'iniciar sessió, i tot el programari ha d'executar-se en mode servei.
RI-SO-8	Obligatori si hi ha equips a TMB	La plataforma de SO ha de facilitar la integració, de la manera més transparent possible, dels diferents tipus de maquinari, és a dir, s'advoca per solucions de plataforma úniques que integrin els diferents evolutius de maquinari i no requereixin el manteniment de diverses plataformes

		de SO en funció del maquinari.
RI-SO-9	Obligatori si hi ha equips a TMB	La plataforma SO ha d'integrar la gestió energètica del maquinari, per exemple, per monitorar els voltatges i la temperatura del maquinari.
RI-SO-10	Obligatori si hi ha equips a TMB	La plataforma SO ha de disposar d'un mecanisme d'administració remota que faciliti tasques d'administració, manteniment i configuració.
RI-SO-11	Obligatori si hi ha equips a TMB	La plataforma SO ha de ser robusta i tenir mecanismes de prevenció, avaluació i reparació de corrupcions lògiques i físiques dels mitjans d'emmagatzematge.

5.4 Requisits de seguretat

RI-SG-1	Obligatori sempre	La plataforma/SO ha de garantir l'accés i emmagatzematge segur: a les dades, als dispositius i als serveis que ofereix.
RI-SG-2	Obligatori sempre	La plataforma/SO ha de garantir que només les actualitzacions generades per entitats acreditades puguin actualitzar el sistema.
RI-SG-3	Obligatori sempre	Tot sistema ha d'incorporar el programari antimalware o el mecanisme de control de llista blanca corporatius.
RI-SG-4	Obligatori sempre	Tot sistema ha d'incorporar un sistema de tallafoc que habiliti únicament el que és necessari i bloquegi la resta.
RI-SG-5	Obligatori sempre	En cas de disposar de sistemes de contingència, la seva activació ha de ser transparent per a la resta de sistemes amb els quals s'integri.
RI-SG-6	Obligatori sempre	Les aplicacions han d'executar-se en un compte d'usuari amb el menor privilegi possible.
RI-SG-7	Obligatori sempre	Totes les funcionalitats supèrflues del sistema operatiu han d'estar desinstal·lades o, en defecte d'això, deshabilitades.
RI-SG-8	Obligatori sempre per a equips a TMB	Totes les contrasenyes d'usuari han de poder-se canviar de manera centralitzada o per mitjà del sistema d'actualització de manera desatesa sense necessitat d'actualitzar tot el SO.
RI-SG-9	Obligatori sempre	Els sistemes de còpia de seguretat corporatius no estan dissenyats ni operats per treballar amb equips distribuïts. Tota informació que necessiti ser protegida, ha d'emmagatzemar-se en repositoris centralitzats en

		equips del CPD, o bé la plataforma del sistema ha de garantir el seu propi sistema de còpia de seguretat i contingència.
RI-SG-10	Obligatori sempre per a equips a TMB	Tots els accessos als equips han de quedar traçats en un format de només lectura que en no permeti la modificació posterior.

5.5 Altres requisits

RI-OT-1	Obligatori si hi ha equips a TMB	Tots els equips Windows han d'integrar-se amb un dels dominis corporatius basats en Microsoft Active Directory per facilitar la gestió d'usuaris i equips. En el cas d'equips, Linux han de proveir-se mecanismes i eines per gestionar de forma centralitzada els usuaris.
RI-OT-2	Obligatori sempre	Les aplicacions han de fer ús del DNS per a la comunicació amb altres equips. No pot haver-hi adreces IP en el codi o en fitxers de configuració de les aplicacions.
RI-OT-3	Obligatori si hi ha equips a TMB	Tots els equips han de sincronitzar l'hora mitjançant protocol NTP amb els servidors de temps de TMB (en el cas d'equips Windows, és automàtic amb la pertinença al domini).
RI-OT-4	Obligatori si hi ha equips a TMB	En el cas d'instal·lació mitjançant maqueta, s'han de lliurar els procediments per al manteniment i actualització posteriors.

6 Operació i manteniment

6.1 Monitoratge

RO-MO-1	Obligatori si es necessita suport de TMB	Tot equip que, en cas de mal funcionament, necessiti intervenció per part d'OTS (Operacions de Tecnologies i Sistemes) o pugui afectar un servei de l'Àrea de Tecnologia de TMB ha d'estar monitorat i integrat en la consola corporativa de monitoratge per als operadors d'OTS.
RO-MO-2	Obligatori si es necessita suport de TMB	Els sistemes s'han de monitorar des de dos punts de vista. • Visió de sistema (monitoratge agregat). L'objectiu és construir una visió de l'estat del servei/sistema *com a suma dels estats individuals de tots els components*. Per a això, cal identificar tots els components tecnològics individuals i les seves relacions. Aquesta informació ha de ser degudament incorporada o actualitzada en la CMDB corporativa. • Visió de client (monitoratge directe). L'objectiu és construir una visió de l'estat del servei/sistema *el més semblant possible al que percep el client final*.
RO-MO-3	Obligatori si es necessita suport de TMB	Tot el monitoratge ha d'estar basat en una de les següents tecnologies: • Enviament per part dels equips de traps SNMP basats en MIB. • Interrogació directa de l'estat per algun element de la infraestructura de monitoratge a través de protocols estàndard (SSH, WMI, SNMP, Web Services…). Si cap d'aquests protocols habituals no està disponible, no es pot garantir el monitoratge.
RO-MO-4	Obligatori si es necessita suport de TMB	Amb la informació de relacions proporcionada anteriorment, cal subministrar, a més, la informació necessària (pesos, dependències) amb la qual es pugui implementar la gestió d'impacte a les eines corporatives i que permeti a Operació prioritzar les seves actuacions.
RO-MO-5	Obligatori si es necessita	Amb la unió dels esdeveniments detectats o rebuts de la visió de sistema i la visió de client s'ha de construir un *Catàleg d'esdeveniments* del servei o sistema, que

	suport de TMB	ha de recollir tots els esdeveniments sigui generat per interrogació o generat pel mateix sistema mitjançant traps SNMP.
RO-MO-6	Obligatori si es necessita suport de TMB	Si és possible l'ús d'interrogació remota, per a cada tipologia de component que cal monitorar s'ha d'indicar com supervisar i comprovar l'estat de funcionament (llista dels paràmetres que cal monitorar i els llindars de generació d'alarma).
RO-MO-7	Obligatori si es necessita suport de TMB	Per a cada tipologia de component que cal monitorar s'ha d'indicar quins esdeveniments poden originar, que seran enviats a la plataforma de monitoratge de TMB juntament amb la seva severitat i/o criticitat, que s'ha de mostrar.
RO-MO-8	Obligatori si es necessita suport de TMB	Tota alarma ha de tenir documentat el procediment d'operació corresponent per resoldre la situació de degradació o no disponibilitat del servei/sistema.
RO-MO-9	Obligatori si es necessita suport de TMB	Tota alarma ha de tenir la contraalarma corresponent per garantir la integritat i coherència del monitoratge.

6.2 Manteniment reactiu

RO-MR-1	Obligatori si hi ha equips a TMB	Tot element de maquinari ha de portar associat un manteniment de substitució o reparació de peces d'acord amb la seva criticitat.
RO-MR-2	Obligatori si hi ha equips a TMB	En el cas de l'equipament central, el maquinari de l'equip ha de tenir un manteniment 24 x 7 in situ amb un temps de resposta de, com a màxim, 4 hores per a equips crítics i de 8 x 5 in situ amb resposta en següent laborable per a la resta.
RO-MR-3	Obligatori si hi ha equips a TMB	Els servidors i appliance que s'adquireixin hauran de tenir una extensió de garantia d'almenys 4 anys amb el fabricant.
RO-MR-4	Obligatori si hi ha equips	El sistema ha de preveure els mecanismes i els procediments més automatitzats possibles per a la

	a TMB	restauració del sistema i la seva configuració després d'una incidència.
RO-MR-5	Obligatori si hi ha equips a TMB	En cas de ser necessària la interacció remota amb la sessió oberta per a la resolució d'incidències o el manteniment, el sistema ha de permetre la captura de sessió.
RO-MR-6	Recomanació	(RECOMANACIÓ) Els sistemes distribuïts haurien d'integrar-se amb l'eina de control remot corporativa, que pot implicar la instal·lació d'un agent a la màquina.

6.3 Manteniment preventiu i actualitzacions

RO-MP-1	Obligatori si hi ha equips a TMB	El sistema ha de proveir d'algun mètode o eina i d'un procediment que permeti el desplegament i actualització de l'equip pel que fa a SO i aplicacions de forma remota (Ethernet, wireless, 3G/4G…) i desatesa.
RO-MP-2	Obligatori si hi ha equips a TMB	El sistema ha de proveir d'algun mètode o eina que permeti el desplegament i actualització de l'equip pel que fa a SO i aplicacions de manera local (tipus clau USB…).
RO-MP-3	Recomanació	(RECOMANACIÓ) Els sistemes distribuïts haurien d'integrar-se amb l'eina de distribució de programari corporativa, que pot implicar la instal·lació d'un agent en la màquina.
RO-MP-4	Obligatori si hi ha equips a TMB	El sistema operatiu de tots els equips ha de ser actualitzat a últim nivell de pedaços almenys dues vegades cada any, sense excloure que s'hagi de realitzar una actualització per una vulnerabilitat greu.
RO-MP-5	Obligatori si hi ha equips a TMB	Els sistemes Windows s'han d'integrar amb l'eina de distribució de programari, pedaços i inventari, que actualment és Microsoft SCCM.
RO-MP-6	Obligatori si hi ha equips a TMB	La política de distribució de pedaços implica la distribució de tots aquests de manera gradual a tots els equips. Si el sistema no s'adapta a aquesta política s'han de proporcionar mecanismes i recursos ad hoc per validar quins pedaços es distribueixen i distribuir-los.
RO-MP-7	Obligatori si hi ha equips a TMB	El sistema ha de poder permetre fer un inventari de les aplicacions instal·lades en cada equip i la seva versió.

6.4 Documentació

RO-DC-1	Obligatori	S'ha de lliurar la documentació, en el format indicat per TMB, de tot el sistema muntat. La documentació ha d'incloure almenys aspectes de: - Arquitectura física i lògica del sistema - Guies d'operació (arrencada i parada del sistema, consulta d'estat, consulta de logs…) - Paràmetres a monitorar, llindars i guia d'accions correctores a executar per a cada alarma o trap SNMP que el sistema enviï - Guies d'administració/manteniment i resolució d'incidències - Llistat de directoris i tipus d'informació de què s'ha de fer còpia de seguretat - Tasques planificades - Consums: elèctric, refrigeració, espai a CPD…
RO-DC-2	Obligatori	S'ha d'actualitzar la CMDB amb la informació relativa als sistemes.
RO-DC-3	Obligatori	Si el sistema crea o modifica un servei o producte de TMB (segons el model de bones pràctiques ITIL implementades a TMB), ha d'actualitzar-se la documentació corresponent.
RO-DC-4	Obligatori	S'ha de lliurar la documentació original relativa a les llicències adquirides.
RO-DC-5	Obligatori	S'ha de lliurar la documentació de tota formació realitzada.

7 Integració de sistemes, serveis i dades

7.1 Requisits generals

REQ-INT-01	Obligatori	Si cal **autenticació,** se n'ha d'implementar una de basada en **SAML 2.0** i **OpenID Connect (OIDC)** per integrar-se amb els proveïdors d'identitat de **TMB**.
REQ-INT-02	Obligatori	Totes les comunicacions han d'estar protegides mitjançant **HTTPS** amb **TLS 1.2** o superior.
REQ-INT-03	Recomanat	Implementar un sistema de **logging centralitzat** per recopilar i gestionar "logs" de totes les aplicacions i serveis.
REQ-INT-04	Recomanat	Utilitzar **agents de monitoratge** per supervisar el rendiment i l'estat dels sistemes, assegurant un impacte mínim en el rendiment. Es recomanen agents com **Filebeat, NXLog, Vector.dev** o similars. Es recomana oferir endpoints de health compatibles amb Prometheus per a les mètriques.
REQ-INT-05	Obligatori	Els serveis han de complir amb els **estàndards de seguretat** i regulacions aplicables de l'**Esquema Nacional de Seguretat (ENS)**.
REQ-INT-06	Obligatori	Les API han de gestionar errors de manera consistent, utilitzant codis d'estat HTTP correctes i missatges d'error clars sense revelar informació sensible.
REQ-INT-07	Recomanat	S'ha de proveir **documentació actualitzada** de les API utilitzant **OpenAPI (Swagger)** d'aquells serveis que s'ofereixin.
REQ-INT-08	Recomanat	Cal implementar **control de versions** a les API per facilitar la gestió de canvis i mantenir compatibilitat cap enrere.
REQ-INT-09	Obligatori	Les integracions internes s'han de fer a través d'**API RESTful** segures, seguint convencions estàndard i utilitzant l'autenticació corporativa. Recomanable via **OIDC,** disponible també via **APIKey.**
REQ-INT-13	Obligatori	Cal complir amb els estàndards interns de seguretat i polítiques de **gestió de dades** de TMB.
REQ-INT-14	Obligatori	Per a les integracions amb sistemes OT. Han de complir amb la **norma IEC 62443** per garantir la seguretat. Cal aplicar **segmentació de xarxes** i principis de **mínim privilegi.**

REQ-INT-16	Obligatori	Les integracions en sistemes OT interns s'han de fer a través de **protocols segurs** i **API controlades**, evitant accessos directes o connexions natives.
REQ-INT-17	Recomanat	Cal fer **avaluacions de risc** i anàlisi d'impacte regularment en aquestes integracions.
REQ-INT-18	Obligatori	Les integracions amb sistemes externs han de fer-se a través d'**API REST** segures, utilitzant autenticació robusta i control d'accés. Preferiblement publicades per **TMB API.**
REQ-INT-19	Obligatori	Cal implementar **xifratge de dades en trànsit** per a totes integracions amb sistemes externs.**I en repòs** també per a allò que contingui dades confidencials.
REQ-INT-21	Obligatori	Cal evitar mètodes insegurs, directes o antiquats com **FTP**, **SFTP, SOAP** en integracions amb sistemes interns o externs.
REQ-INT-22	Obligatori	Cal aplicar **segmentació de xarxes** i establir **zones desmilitaritzades (DMZ)** per a connexions amb sistemes OT, sobre la base de l'IEC 62443.
REQ-INT-23	Obligatori	Cal mantenir **registres d'auditoria** de totes les interaccions als sistemes. Per facilitar el seguiment i la resolució d'incidències.
REQ-INT-24	Obligatori	Les integracions amb sistemes externs han de passar per **passarel·les de seguretat** i complir amb les polítiques de seguretat de **TMB.** En aquells entorns segmentats per xarxa, especialment al món OT, no hauran ser directes. Podran fer ús de la DMZ, i preferiblement aniran a l'**API de TMB**.
REQ-INT-25	Obligatori	Implementar **validació i sanitització** de totes les dades provinents de sistemes externs. Sobretot en serveis de fitxers.
REQ-INT-26	Obligatori	Cal utilitzar l'**API Gateway de TMB** per gestionar i protegir les API exposades externament, incloent-hi autenticació, autoritzacions i rate limiting.
REQ-INT-27	Obligatori	Les dades confidencials han de ser **xifrades** i complir amb les polítiques de protecció de dades de l'organització i regulacions com l'**RGPD**.
REQ-INT-28	Recomanat	Totes aquelles integracions de dades, que requereixin d'un flux constant, hauran d'usar el **broker corporatiu** basat en **Apache Kafka** per a l'streaming de dades.
REQ-INT-29	Recomanat	Per a aplicacions que requereixin comunicació lleugera i eficient, cal considerar l'ús del **protocol MQTT del broker corporatiu.**

REQ-INT-30	Recomanat	Els logs s'han d'emmagatzemar en un **sistema centralitzat** i estar disponibles per a anàlisi i auditoria, evitant-ne la transferència manual.
REQ-INT-31	Obligatori	Cal implementar **retenció i eliminació segura** de logs d'acord amb les polítiques internes i regulacions aplicables, com **ISO 27001**, i el bloqueig i eliminació per a aquells afectats per **l'RGPD.**
REQ-INT-32	Obligatori	Els sistemes externs han de complir també les polítiques i el cos normatiu de seguretat de TMB, especialment, els del capítol 15 del cos normatiu de TMB que fixen la relació amb proveïdors.
REQ-INT-33	Obligatori	El disseny ha de preveure els mecanismes perquè TMB pugui controlar, revisar i auditar regularment la provisió de serveis del proveïdor.
REQ-INT-34	Obligatori	Prèviament a l'execució dels serveis, tots els requisits relacionats amb la seguretat tecnològica i de la informació s'establiran i acordaran amb cada proveïdor per delimitar i complir les competències i responsabilitats de cadascuna de les parts.

7.2 Aplicacions i gestió d'usuaris

RX-AU-1	Obligatori sempre	Si la plataforma requereix una App per l'ús des de mòbil, cal proporcionar l'APK corresponent per a la distribució als mòbils corporatius des de l'eina d'MDM que utilitza TMB (actualment VMware Workspace ONE).
RX-AU-2	Obligatori sempre	La plataforma no ha de tenir gestió d'usuaris desvinculada, s'ha d'integrar via federació SAML o OIDC amb la gestió d'identitats corporativa de TMB. Quant a autoritzacions, es permet la gestió local sobre la base de rols que es definiran en l'LDAP corporatiu i s'hi accedirà a través de la federació SAML o OIDC.
RX-AU-3	Obligatori sempre	En el moment del registre de l'usuari (1r accés) cal presentar un *disclaimer* legal amb el text que determini TMB per ser acceptat per l'usuari. Sense l'acceptació, s'haurà d'impedir l'accés a la plataforma i no podrà emmagatzemar-se cap dada personal de la qual es disposés sobre ell. S'haurà de guardar constància d'aquesta acceptació (data i text acceptat).

7.3 Gestió del servei

RX-GS-1	Obligatori si es necessita suport de TMB	El servei ha de permetre conèixer els ANS pactats amb TMB durant la fase de disseny i el valor d'aquests al llarg del contracte.
RX-GS-2	Obligatori si es necessita suport de TMB	S'han de proveir URL per al monitoratge del servei que permetin conèixer a cada moment l'estat d'aquest.
RX-GS-3	Obligatori si es necessita suport de TMB	S'han de proveir mecanismes per a l'escalat d'incidències, integrat amb el sistema de gestió de tiquets de TMB (actualment basat en FootPrints).
RX-GS-4	Obligatori si es necessita suport de TMB	Independentment de les mètriques proporcionades per temes funcionals, s'ha de generar un log de traçabilitat que guardi, com a mínim, el detall de cada accés (qui hi accedeix, quan i des de quin dispositiu).

7.4 Solucions tipus IaaS o PaaS

RX-IA-1	Obligatori si el sistema és al núvol	Les comunicacions amb serveis tipus IaaS allotjats en núvols públics o privats sense gestió directa per part de TMB hauran de protegir-se mitjançant l'ús de túnels VPN o línies dedicades.
RX- IA -2	Obligatori si el sistema és al núvol	Els sistemes situats en núvols públics o privats sense gestió directa per part de TMB només podran accedir a serveis publicats en la DMZ corporativa, mai a serveis interns. En cas que calgui accedir a serveis que actualment no es troben publicats, s'haurà de preveure en el disseny del projecte la seva publicació segura.
RX- IA -3	Obligatori si el sistema és al núvol	Si l'operació i manteniment de la solució IaaS o PaaS l'ha de fer en algun moment directament personal de TMB, haurà de complir amb els mateixos requisits de les solucions on-premise (a excepció dels relatius a l'HW o altres característiques lligades a aquest o als CPD de TMB).
RX-IA-4	Obligatori en IaaS	Si el que s'instal·la és infraestructura com a servei, aquesta ha de seguir les mateixes condicions de seguretat que la resta d'equips de TMB.

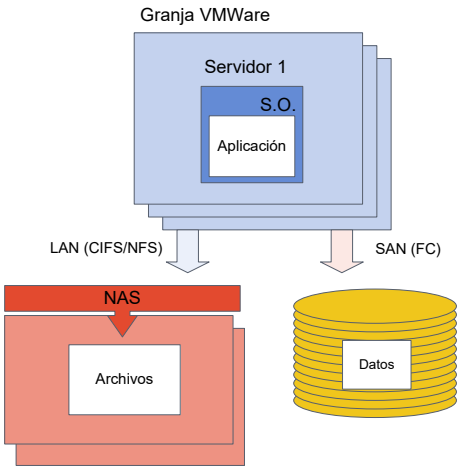
8 Annex. Arquitectures típiques de sistemes centrals “on premise”

A continuació, s'indiquen arquitectures típiques de sistemes centrals a TMB. Per facilitar la implantació i el manteniment posterior, les solucions s'haurien d'adaptar a aquestes arquitectures o a combinacions d'aquestes.

Els elements comuns, com la granja de VMWare, clúster de bases de dades, caixes de discos, NAS, balancejadors, infraestructura LAN/SAN, tallafocs…, existeixen ja a TMB i són comuns per a tota la infraestructura.

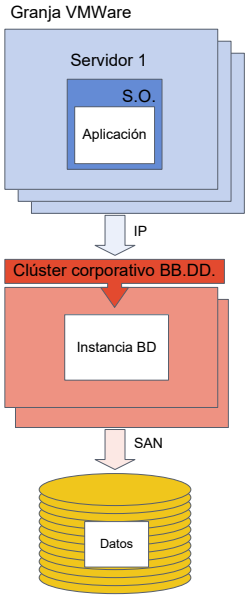
8.1 Servidor amb emmagatzematge extern

Descripció: servidor(s) amb SO Windows o Linux, que s'executa en una granja de VMWare, amb necessitat d'emmagatzematge extern en NAS (accés mitjançant CIFS o NFS) i/o *file systems* en cabines de disc externes (accés mitjançant FC).



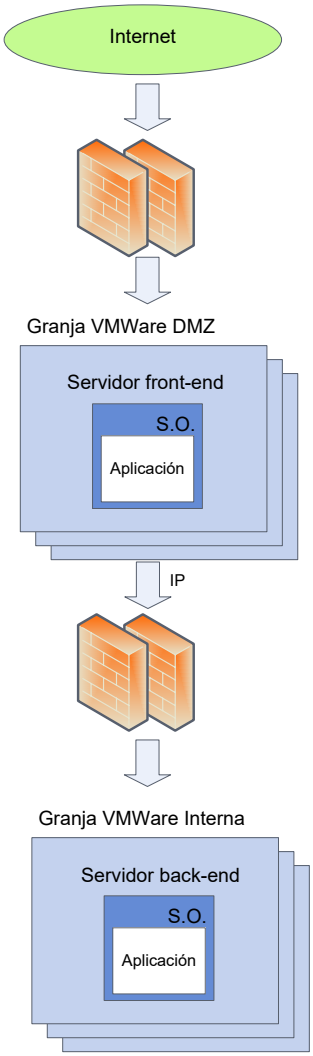
8.2 Servidor amb base de dades

Descripció: servidor(s) amb SO Windows o Linux, que s'executa en una granja de VMWare, accedint a una instància de BD en un clúster corporatiu (compartit amb altres instàncies).



8.3 Servidor per a continguts publicats a Internet

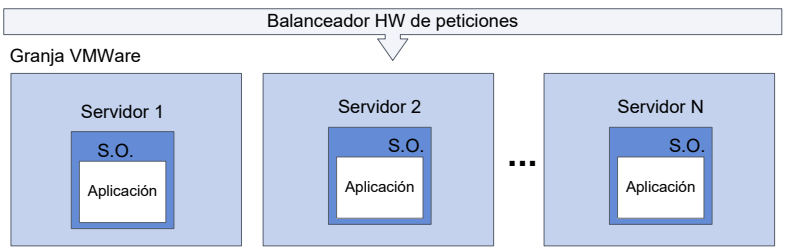
Descripció: servidor de front-end amb SO Windows o Linux en la granja de VMWare situada en la DMZ i un back-end sobre la granja VMWare corporativa (interna).



8.4 Servidors de front-end balancejats

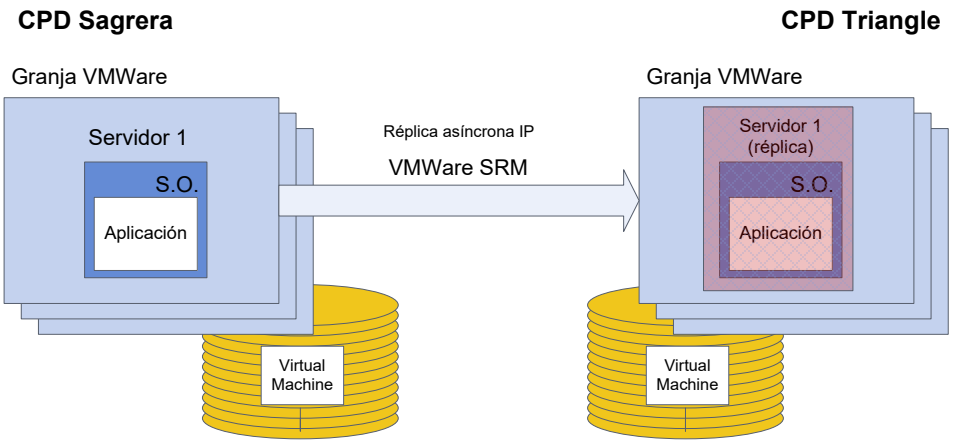
Descripció: granja de servidors de front-end (idealment iguals) amb SO Windows o Linux, repartits en diferents servidors d'una granja de VMWare. Les peticions (http, https) són balancejades per balancejadors HW.

Aquesta solució està disponible tant per a serveis interns (intranet) com externs a la DMZ (internet).



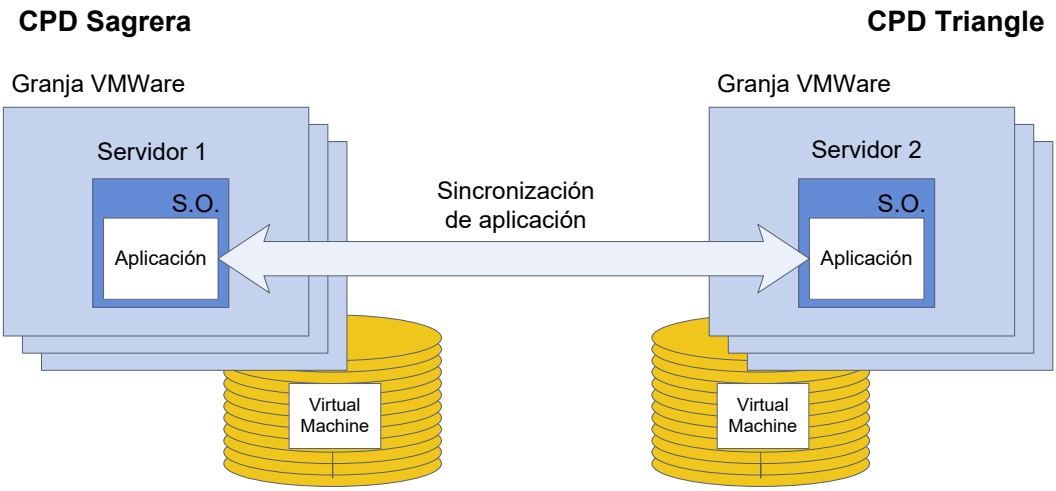
8.5 Sistemes amb contingència

Descripció: servidor(s) amb SO Windows o Linux, que s'executa en una granja de VMWare al CPD de Sagrera, amb la funcionalitat de VMWare Site Recovery Manager (SRM) activada i rèplica per IP.



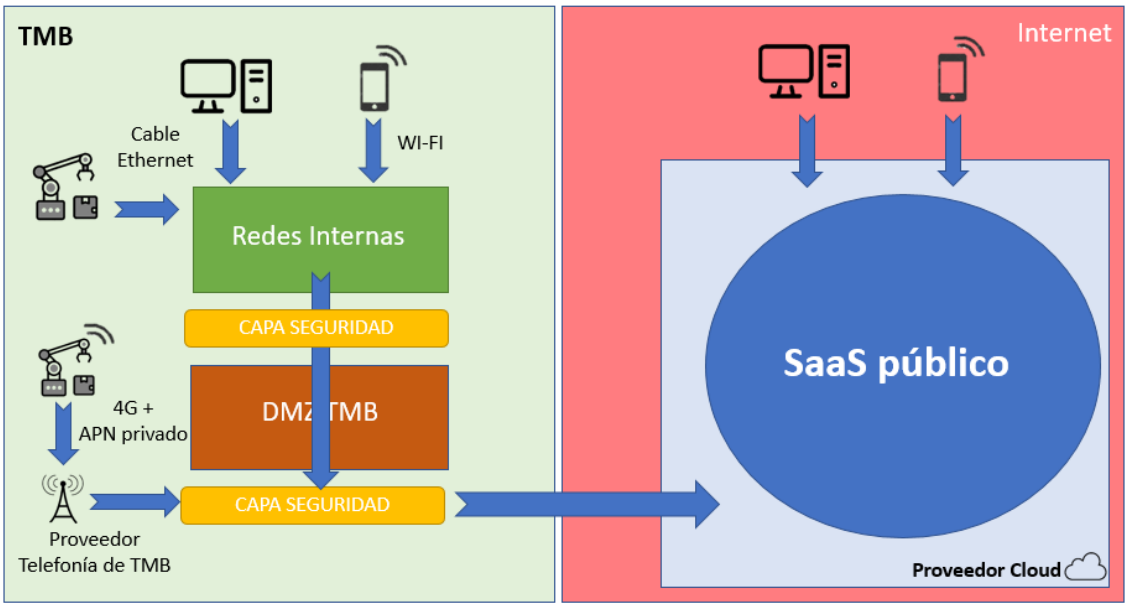
8.6 Sistemes ininterromputs (RTO ≈ 0)

Descripció: servidors amb SO Windows o Linux, que s'executen en una granja de VMWare al CPD de Sagrera i al de Triangle, amb l'aplicació activa simultàniament en cadascun dels centres. Quin centre ataca cada client i la sincronització de les dades a cada centre és un aspecte gestionat per mecanismes intrínsecs a l'aplicació.

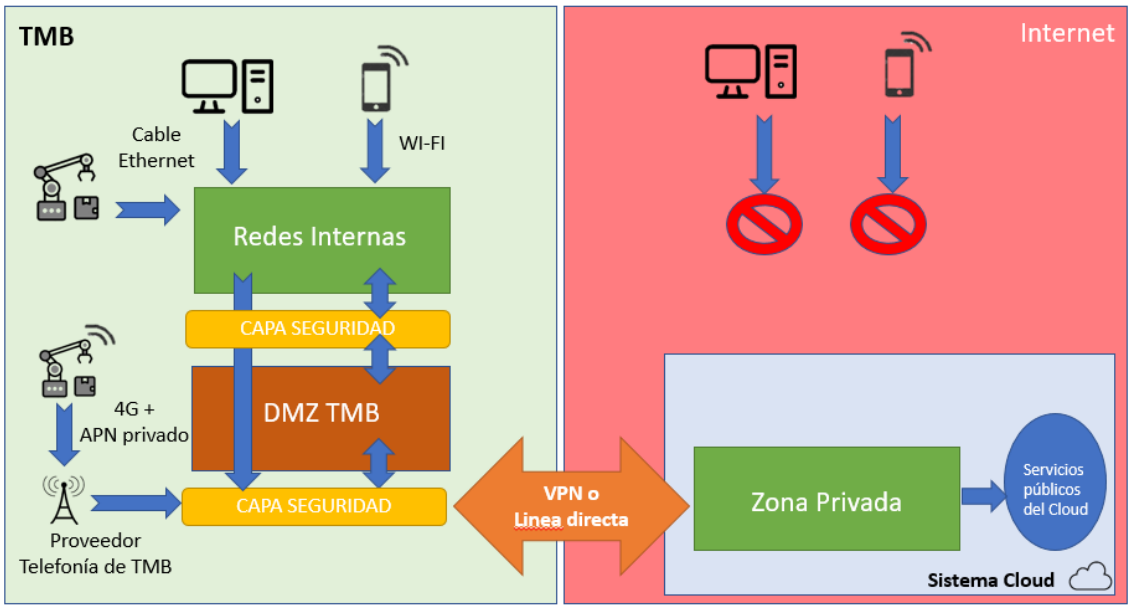


9 Annex. Arquitectures admeses per a sistemes al núvol

9.1 Sistemes públics



9.2 Sistemes privats



9.3 Sistemes híbrids