B:SM

ANNEX I.A

Estàndards TiC de B:SM

	Documentat per	Revisat per	Aprovat per
Nom	Ivan Gaspar Pujadas	Ivan Gaspar Pujadas	Artur Frigola
Càrrec	Cap d'àrea govern TiC	Cap d'àrea govern TiC	Director corporatiu de Tecnologies de la Informació
Data	01/12/2023	01/12/2023	10/01/2024
Signatura			

B:SM

Índex

B:SM

Control de versions

Versió	Creat	Validat
1.0	01/12/2023	08/09/2023

B:SM

1 Estàndards TiC de B:SM

1.1 Objectiu

L'objectiu d'aquest document annex és **especificar els estàndards tecnològics definits per la Direcció de Tecnologies de la Informació, Comunicacions i Estratègia Digital de B:SM** (en endavant direcció TiC de B:SM), concretament, els components i tendències tecnològiques seleccionades, i les polítiques i procediments que els regeixen per tal de dur a terme les iniciatives i projectes de B:SM.

l'estàndard tecnològic, i polítiques i procediments vigents, establerts per la direcció de sistemes de B:SM, i **d'obligatori compliment** per totes les empreses que participen en processos de contractació.

1.2 Abast

Els estàndards tecnològics considerats en aquest document annex fan referència als següents àmbits tecnològics:

- Bases de Dades
- Desenvolupament de programari
- Sistemes, plataforma i Infraestructura
- Lloc de treball
- Comunicacions i networking
- Seguretat tecnològica

Els estàndards definits per cada àmbit tecnològic, son els actualment vigents a B:SM. I **són d'obligat compliment** per totes les empreses proveïdores de serveis (en endavant proveïdors) que participen en processos de contractació.

1.3 Consideracions

Tots els proveïdors que participen en processos de contractació (procés de licitació o be, amb un o mes contractes vigents) han de tenir en compte els següents aspectes:

- **Durant el procés de licitació** i elaboració d'ofertes, els proveïdors, sense excepcions, **han de tenir en compte les especificacions i estàndards definits en aquest annex**, de la mateixa manera que els requeriments específics del plec tècnic i de condicions particulars.
- Durant tot el cicle de vida de contractació (licitació i execució de contracte), els responsables assignats per la direcció TiC de B:SM, **revisaran el compliment del estàndards TiC** definits en aquest annex. Qualsevol incompliment per part de proveïdor sense causa justificada, pot implicar la **tramitació d'una penalització** i/o la cancel·lació del contracte.
- **Enfront dubtes** en el compliment dels estàndards TiC per part de proveïdor durant tot el cicle de vida de contractació, **el proveïdor l'ha de comunicar de manera oficial** a través dels canals habilitats.
- **Excepcions en el compliment dels estàndards TiC**: Les excepcions, únicament seran acceptades en el cas de que el plec tècnic de la licitació especifiqui algun punt diferenciador sobre el document annex d'estàndards TiC, o be, en el cas que un

proveïdor adjudicatari justifiqui els motius de l'incompliment i presenti una alternativa similar prèviament acceptada pels responsables assignats d ela direcció TiC de B:SM.

2 Estàndard de Bases de dades

En aquest apartat, és defineixen els principis bàsics aplicables als diferents àmbits de les bases de dades a B:SM

2.1 Bases de Dades

Les consideracions, estàndards, tecnologies, i arquitectures definides en l'àmbit de bases de dades a B:SM, són aplicables a les següents casuístiques:

- Bases de dades centralitzades i específiques.

2.1.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Totes les solucions proposades per els proveïdors, de manera **preferent**, han de considerar les **bases de dades centralitzades** que són estàndard de B:SM. Així mateix, per serveis i aplicacions concretes, és permeten bases de dades de caràcter específic (o embegudes) (**veure Annex 9.1 BBDD**).
- En el cas de que un proveïdor proposi una solució de bases de dades diferent al determinat al plec o a l'estàndard, **requerirà l'aprovació de la direcció TiC de B:SM.**
- De manera general, el proveïdor ha de garantir els principis bàsics de backup definits per B:SM (**veure Annex 9.2 Política de Backup BBDD**).
- Així mateix, s'ha de **garantir backup de serveis SaaS**, i per aquest motiu, el proveïdor ho ha d'indicar a la seva proposta, juntament amb el ANS i possibles redundàncies (en cas de servei crític).
- En el cas de que un proveïdor no pugui assolir els requeriments mínims de backup, haurà de presentar una proposta coherent que **requerirà l'aprovació de la direcció TiC de B:SM.**

2.1.2 Arquitectura BBDD

Es resumeixen a alt nivell l'arquitectura de base de dades centralitzades en entorn productiu de B:SM:

A. **Oracle**:
   Entorn On-premise (CDBSM) amb **3 nodes + 1** *Broker Data Guard* com a mètode de HA.
   - **Rèplica** a *Oracle Cloud* amb entorn d'alt rendiment orientat a històric i replicació.
   - Entorn de "recovery" com a contingència externa.

B. **Microsoft SQL Server**:
   2 clústers en entorn productiu amb **3 servidors dins el clúster Windows.**
   - **2 servidors** dins el clúster de SQL Server (FCI) amb varies instancies dins d'aquest clúster.

- **+ 1 servidor SQL Server standalone** a com a servidor de recolzament mitjançant la tecnologia Always ON de SQL Server (permet la continuïtat en cas de fallida del node 1 i del node 2, en base a l'activació manual de la replica del node 3).

3 Estàndard de Desenvolupament

En aquest apartat, és defineixen els principis bàsics aplicables als diferents àmbits de desenvolupament a B:SM

3.1 Desenvolupament

Les consideracions, estàndards i tecnologies definides en l'àmbit de desenvolupament de programari a B:SM, són aplicables a les següents casuístiques:

- Projectes de **construcció de programari**
- Serveis de **manteniment** i evolutiu.

3.1.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Tots els desenvolupaments requereixen de **proves funcionals i d'estres** dels sistemes abans de la posada en producció.
- Així mateix, es realitzaran **proves de rendiment** en base a l'eina *Apache JMeter* per tal de garantir la disponibilitat i recursos implementats.
- Com a norma general, i en el cas de que estigui determinat, **s'utilitzarà el llenguatge de programació indicat en el plec tècnic**. En el cas de que no estigui determinat al plec, preferentment s'utilitzarà un llenguatge estandarditzat per B:SM (**veure Annex 9.3 Llenguatges i frameworks**).
- En el cas de que un proveïdor proposi un llenguatge diferent al determinat al plec (sigui estàndard B:SM o no), o un llenguatge no estandarditzat, **requerirà l'aprovació de la direcció TiC de B:SM.**
- Els proveïdors han de **complir amb les bones practiques** de codificació, disseny, i polítiques de seguretat recomanades. Les necessitats especifiques de cada projecte seran indicades per la direcció TiC de B:SM en el plec tècnic.

3.2 Desenvolupament de serveis (API)

Les consideracions, estàndards, i tecnologies definides en l'àmbit de desenvolupament de serveis (API), són aplicables a les següents casuístiques:

- **Interfícies de programació** entre aplicacions i integracions entre sistemes.

3.2.1 Consideracions

S'han establert una sèrie de metodologies, bones practiques i tecnologies que conformen els estàndards de B:SM per a la construcció de serveis (API). A continuació s'especifiquen els aspectes clau relacionats amb aquest àmbit:

- Els proveïdors gestionaran els desenvolupament API en base a les plataformes estandarditzades per B:SM (**veure Annex 9.4 Plataforma d'integració i gestió API**). De la mateixa manera, La plataforma a utilitzar **es determinarà en funció del projecte** i es definirà al plec tècnic
- És requeriment **proporcionar un mètode de *Health* per cada API** a implementar.
- És requeriment **complir amb els principis de disseny *Api Restful* i l'especificació *Opendata*** a l'hora de disenyar i codificar API.
- Com a norma general, es dona preferència al disseny de l'API versus la codificació ***(API Design-first)***, amb el suport d'eines de disseny, construcció i documentació (ex. *Swagger OpenAPI*) que actuen com a contracte, i faciliten la comprensió i el treball dels usuaris sobre les API.

3.3 Gestió del codi font

Les consideracions, estàndards, i tecnologies definides en l'àmbit de gestió del codi font, són aplicables a les següents casuístiques:

- Projectes de **construcció de programari**
- Serveis de **manteniment** i evolutiu.

3.3.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Com a norma general, el sistema de control de versions a utilitzar pel software de referència (de tots els entorns excepte SAP) és el **GIT**, a través de una distribució "On-premise" de la plataforma **GITlab** de B:SM.
- En el cas de que un proveïdor proposi una solució diferent l'estàndard, **requerirà l'aprovació de la direcció TiC de B:SM.**

3.4 Gestió i centralització de logs

Les consideracions, estàndards, i tecnologies definides en l'àmbit de gestió i centralització de Logs, són aplicables a les següents casuístiques:

- Programari i **aplicacions**
- **Servidors** d'aplicació

3.4.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- La generació i registre de logs és requeriment a B:SM per garantir l'emmagatzemament dels diferents registres d'esdeveniment, generats per aplicacions i sistemes en base a una base de dades centralitzada (sistema centralitzat de logs).
- B:SM ha definit 2 sistemes de centralització estàndard per emmagatzemar esdeveniments; **Dynatrace** (Servei SMOU) i **Graylog** (resta de serveis). Totes les solucions dels proveïdors han de **considerar un d'aquets sistemes** per registrar els esdeveniments.

- Les aplicacions o sistemes que formen part de la solució han d'estar **configurats per enviar** els esdeveniments al servidor mitjançant un protocol determinat, en funció del sistema de centralització determinat. Aquesta comunicació es farà en un **fil d'execució separat de la aplicació** per tal de no afectar al seu rendiment.
- En el cas de que un proveïdor proposi una solució diferent l'estàndard, **requerirà l'aprovació de la direcció TiC de B:SM.**
- No és pot desplegar un desenvolupament o sistema que no sigui integrat al sistema de centralització de logs. **El cost d'aquesta integració anirà a càrrec del proveïdor.**

3.5 Gestió i centralització de Jobs

Les consideracions, estàndards, i tecnologies definides en l'àmbit de gestió i centralització de Jobs, són aplicables a les següents casuístiques:

- Programari i **aplicacions**
- **Servidors** d'aplicació

3.5.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- B:SM ha definit 1 sistema estàndard de programació de Jobs per centralitzar i monitoritzar els processos batch:
  - **Quartz engine** (Open source)

- La solució dels proveïdors ha de **considerar el sistema estàndard** de B:SM per gestionar la programació de Jobs.
- En el cas de que un proveïdor proposi una solució diferent l'estàndard, **requerirà l'aprovació de la direcció TiC de B:SM.**

3.6 Gestió de la seguretat en programari

Les consideracions, estàndards, i tecnologies definides en l'àmbit de gestió de la seguretat de programari, són aplicables a les següents casuístiques:

- Projectes de **construcció de programari**
- Serveis de **manteniment** i evolutiu.

3.6.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Tots els desenvolupaments han de seguir les metodologies i bones pràctiques per garantir un desenvolupament segur, i garantir, **com a mínim**, la robustesa enfront riscos i bretxes de seguretat recomanats pel framework *OWASP Top 10 2021* (**veure Annex 9.5 Llistat riscos desenvolupament Web**).
- Totes les dades d'entorns **no productius han d'estar xifrades.**
- Tots els desenvolupaments han de complir amb els **estàndards definits per l'àrea de Seguretat** TiC de B:SM per protegir els accessos, les dades i les pròpies aplicacions.

- Tots els desenvolupaments requereixen de **proves de seguretat** prèviament a la pujada a producció per tal de validar que aquest **és robust enfront riscos de seguretat** o atacs maliciosos de manera independent a mesures de seguretat agregades.
- L'Àrea de seguretat revisarà i escanejarà els desenvolupaments per tal de garantir els requeriments de seguretat de programari. **Tots els costos correctius sobre aquest àmbit, aniran a càrrec del proveïdor**.

4 Estàndard Comunicacions i Networking

En aquest apartat, és defineixen els principis bàsics aplicables als diferents àmbits de comunicacions a B:SM

4.1 Comunicacions

Les consideracions, estàndards, tecnologies, i arquitectures definides en l'àmbit de comunicacions i networking, són aplicables a les següents casuístiques:

- **Connectivitat extrem a extrem** entre seus de B:SM

4.1.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Tota aplicació o servei proposat pels proveïdors ha de ser **compatible i eficient amb la arquitectura de comunicacions** i balancejadors proposada per B:SM (veure apartat 9.11 Arquitectura de xarxa).
- Sense excepcions, tots els elements tallafocs (firewalls) requerits per donar servei a B:SM, han de **ser proveïts** pels proveïdors **en el seu extrem** per garantir la separació entre ambdues xarxes**.** i **han de ser auditables** (accés lectura) per B:SM.
- Tota nova aplicació o servei proposat pels proveïdors, com a norma general, requerirà **redundar els elements balancejadors** requerits.

4.1.2 Arquitectura de xarxa

Es resumeixen a alt nivell l'arquitectura, mecanismes i elements de xarxa i comunicacions de B:SM:

- B:SM disposa d'una seu central amb 2 centres de processament de dades (en endavant CPD). Existeixen diferents seus que B:SM emparà dins del seu àmbit, a les que dona suport i manté com a pròpies (**veure Annex 9.6 Llistat de seus B:SM**).
- Connectivitat **MPLS**, **amb redundàncies i sortida a internet** per tots els CPD de B:SM.
- Elements balancejadors de ***Citrix Netscaler***.

5 Estàndard Sistemes i Infraestructura

En aquest apartat, és defineixen els principis bàsics aplicables als diferents àmbits de sistemes, infraestructura i plataformes a B:SM

5.1 Sistemes i infraestructura

Les consideracions, estàndards, tecnologies, i arquitectures definides en l'àmbit de sistemes i infraestructures, són aplicables a les següents casuístiques:

- Sistemes, infraestructura i plataformes **"on-premise"**
- Sistemes, infraestructura i plataformes **SaaS**

5.1.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- De manera general, totes les solucions de proveïdor que requereixin sistemes, infraestructura i plataformes, **prioritzaran una solució SaaS** fora de l'entorn "on-premise" dels CPD de B:SM.
- En el cas de que la solució de proveïdor requereixi ubicar sistemes, infraestructura i plataformes a l'entorn "on-premise", hauran de complir amb els requeriments del model i arquitectura "on-premise" (**veure apartats 5.1.2 i 5.1.3**) d'aquest document.

5.1.2 Model d'infraestructura

S'exposen les següents aspectes rellevants en referència al model d'infraestructura actual y futur:

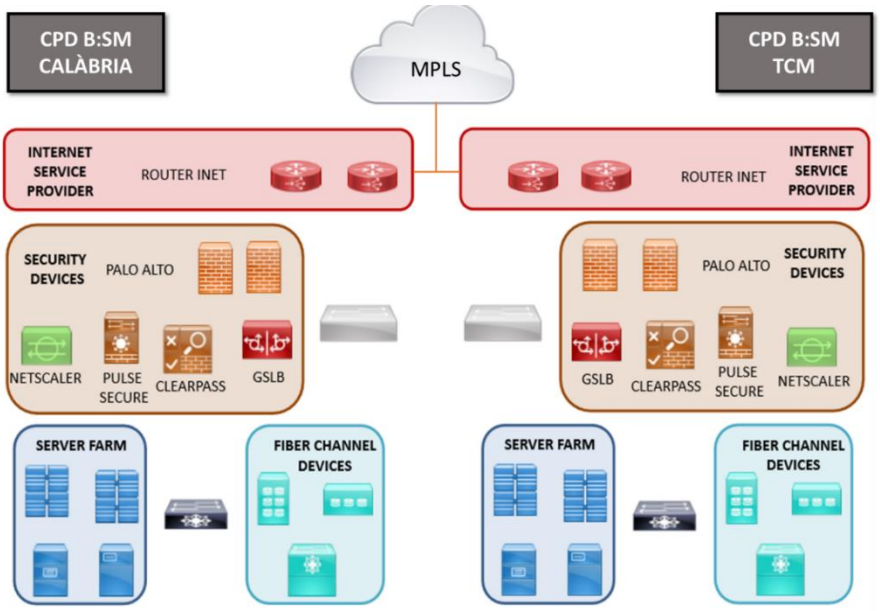
- Actualment, B:**SM compta amb dues sales de processament de dades**; CPD de Calabria (entorn no productiu) i un CPD extern (entorn productiu).
- El **model actual es basa en una estratègia de creixement de serveis preferiblement de tipus SaaS.** En els cassos que no sigui possible es valorarà l'opció cloud públic o ubicació en alguns dels dos CPD gestionats per BSM.
- El **serveis d'accés a Internet i crítics estan redundats en ambdós CPD**. D'aquesta manera, en el cas de que hi hagi una caiguda de tràfic al CPD de Calabria, permet redirigir-lo pel CPD extern, garantint la connectivitat dels usuaris mitjançant tecnologia GSLB.
- El **model futur** (ja en desplegament) es basa en una estratègia d'integració al cloud públic (principalment amb *Azure* i *AWS*). Aquesta integració considera les línies (*Express Route i Direct Connect*) i estratègia de backup recomanat pels serveis cloud públics.
- Actualment, B:SM ja disposa de molts serveis SaaS i està començant a introduir serveis de DR al Cloud.

5.1.3 Arquitectura CPD

Els serveis es distribueixen entre dos CPD:

- Calabria: Ubicat a les oficines centrals de B:SM de Carrer Calabria (**entorn no productiu**)
- Extern: Ubicat al Tecno Campus Mataró (TCM), destinat a allotjarà tots el serveis i aplicacions crítiques de B:SM (**entorn productiu**).

L'arquitectura simplificada es descriu en el següent esquema:



Es detalla el contingut d'alguns elements mostrats en l'esquema anterior (server farm) (**veure Annex 9.7 Detall dels components i continguts de la granja de servidors**).

5.2 Eines de monitorització

Les consideracions, estàndards, tecnologies, definides en l'àmbit de eines de monitorització, són aplicables a les següents casuístiques:

- Tots els components d'infraestructura requerits per les solucions i nous serveis proposats

5.2.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Sense excepcions, els proveïdors hauran de **presentar una proposta de monitorització dels serveis o aplicacions a implementar**, i així mateix, facilitar la informació necessària als equips interns de la direcció TiC de B:SM
- Les propostes de monitorització, han de cobrir els requeriments definits per B:SM (**veure Annex 9.8 Requisits monitorització de serveis B:SM**).

5.3 Entorns i Sistemes operatius (SO)

Les consideracions, estàndards, tecnologies, definides en l'àmbit d'entorns i Sistemes operatius (SO), són aplicables a les següents casuístiques:

- Tots els components d'infraestructura requerits per les solucions i nous serveis proposats

5.3.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Els sistemes o serveis implementats, han de disposar **com a mínim** d'entorns PRE/PRO (serveis no crítics) i DES/PRE/PRO (serveis crítics).
- Com a norma general, els entorns de desenvolupament (DES) i pre-producció (PRE) s'ubicaran al CPD de Calabria, mentre que entorns productius (PRO) al CPD de TCM (Tecno Campus Mataró) sempre i quant és consideri servei crític
- Els proveïdors han d'adoptar els estàndards de sistemes operatius definits per B:SM, tant a nivell de fabricant (determinat al plec per B:SM) com versió (**veure Annex 9.9 Estàndard SO**).

5.4 Control d'accés a serveis i aplicacions

Les consideracions, estàndards, tecnologies, definides en l'àmbit de control d'accés a serveis i aplicacions a, són aplicables a les següents casuístiques:

- Tots els serveis i aplicacions

5.4.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Com a norma general, és requeriment que l'accés a tots els serveis i aplicacions a B:SM es realitzi a través de **grups i usuaris del Active Directory** i amb una única identitat **single sign on (SSO)**. En el cas de que un proveïdor proposi una solució de control d'accés diferent, **requerirà l'aprovació de la direcció TiC de B:SM.**
- Tota validació d'accés a serveis i aplicacions haurà de passar per l'arquitectura d'**ADFS** si es un servei publicat a Internet, o en el seu defecte, validació LDAP per el AD intern corporatiu.
- B:SM està impulsant la **autentificació de doble factor (2FA)** en la majoria de les seves aplicacions i plataformes. Com a norma general, és requeriment establir doble factor (2FA) considerant les següents premisses:
  - Aplicacions publicades internament (excepte les configurades amb single sign on **sempre i quant s'implementi 2FA al primer accés**).
  - Aplicacions obertes a internet.

  En funció del servei a implementar el proveïdor haurà de consensuar el seu ús amb la direcció TiC de B:SM

6 Estàndard de Lloc de Treball

En aquest apartat, és defineixen els principis bàsics aplicables als diferents àmbits de lloc de treball a B:SM

6.1 Entorn del lloc de treball

Els nous serveis i aplicacions desplegats, han de complir amb les consideracions i requeriments definits per B:SM

6.1.1 Ecosistema i equipament

L'ecosistema de lloc de treball a B:SM, de manera general està composat pel següent equipament:

- Equipament workstation o portàtil (Windows) units al domini B:SM
- Equipament mòbil Android i IOS

6.1.2 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- Tot l'equipament que formi part de B:SM, **ha d'estar integrat al domini B:SM amb el software de seguretat i de gestió** de lloc de treball, definit per l'equip d'explotació de la direcció TiC de B:SM i ha de complir amb les versions mínimes de S.O definits en cada moment per la direcció TIC.
- Tot l'equipament nou, ha de seguir els requeriments definits a l'estàndard d'equipament de B:SM **(veure Annex 9.10 Estàndard d'equipament).**
- L'alta d'equipament a la infraestructura ha de seguir el **procediment d'alta d'actiu de B:SM.** Així mateix, han de ser integrats al domini de B:SM per part de l'equip d'explotació, i inventariats amb les eines de seguretat i gestió instal·lades.
- Els proveïdors que ofereixin serveis de gestió d'incidències, han de fer ús de l'eina corporativa de gestió d'incidències i peticions de B:SM (*easyvista*).
- Les intervencions on el proveïdor hagi d'accedir a la màquina de l'usuari final, es realitzaran de manera coordinada amb l'equip de lloc de treball, i a través dels mecanismes establerts per B:SM per a habilitar la connexió.
- Si un usuari ha d'accedir a algun lloc fora de la xarxa de B:SM, caldrà sol·licitar-ho a l'equip d'explotació de la direcció TiC de B:SM, per a permetre l'accés tant des de la xarxa interna com a través de la VPN.
- Sense excepcions, els accessos de VPN i a la plataforma O365, s'habiliten **amb doble autentificació.**

7 Estàndard de Seguretat de la Informació

En aquest apartat, és defineixen els principis bàsics aplicables als diferents àmbits de la seguretat de la informació a B:SM

7.1 Seguretat de la informació

Les consideracions, estàndards, tecnologies, i arquitectures definides en l'àmbit de seguretat de la informació, són aplicables a les següents casuístiques:

- Infraestructura, plataformes i aplicacions que gestionin informació de B:SM

7.1.1 Requeriments generals de seguretat a B:SM.

Es detallen els principals requisits generals de seguretat:

A. Política de Seguretat

B:SM disposa de protocols, processos i procediments per a garantir el compliment de política de seguretat TiC establerta sota el marc genèric descrit a continuació:

- El proveïdor ha de respectar totes aquelles mesures de seguretat, tècniques o organitzatives establertes per B:SM per garantir la confidencialitat, disponibilitat, traçabilitat, autenticitat i integritat de la informació que contingui dades personals, així com de la informació, serveis i tecnologies tractades a B:SM.
- Complir amb les polítiques, normatives i procediments de seguretat que formen part del marc normatiu de l'Esquema Nacional de Seguretat (ENS).
- Les polítiques, normatives, i procediments apliquen a tots els actius d'informació que són creats, rebuts, emmagatzemats, processats, transmesos o impresos a qualsevol sistema o mitjà d'emmagatzematge, així com dels sistemes d'informació que donen suport a la gestió dins de B:SM.
- Les polítiques de seguretat de B:SM seran revisades i, si escau, actualitzades amb periodicitat anual, d'acord amb l'exigència de la normativa actual en matèria de seguretat de la informació, havent-se de realitzar les accions requerides per a adequar-se a les modificacions realitzades.
- L'incompliment per part de tercers podrà suposar la rescissió del contracte pertinent amb B:SM o entitat operativa.

B. Consideracions

Tots els proveïdors que ofereixin **plataforma i/o infraestructura** de serveis i solucions, **han de garantir l'ús de components autoritzats per CCN** d'acord amb els requisits establerts en l'ENS. Per a això, el proveïdor haurà d'utilitzar del Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació (CPSTIC) del CCN, per a seleccionar els productes o serveis subministrats que hagin de formar part de l'arquitectura de seguretat del sistema.

C. Avaluació de Riscos

B:SM seguint les normes de l'ENS, avalua els riscos basats en la metodologia Magerit, en la qual s'avaluen tots els actius dels diferents serveis que s'usen en els seus Sistemes.
Són requisits dins dels serveis de B:SM, les següents accions per part del proveïdor amb relació a la gestió de riscos a B:SM:

- Avaluar els riscos amb periodicitat anual per identificar les amenaces i vulnerabilitats específiques de B:SM.
- Classificar els actius segons la seva importància i risc.

D. Accés i Autenticació

S'estableixen els següents requisits al proveïdor dins de l'àmbit del control d'accés als recursos de B:SM, així com els permisos d'accés a aquests:

- Implementar sistemes de control d'accés per limitar qui pot accedir a quins recursos.
- Implementar el principi del "menys privilegi": proveir als usuaris únicament els permisos necessaris per realitzar les seves funcions.
- Establir polítiques de contrasenyes fortes i el canvi regular de les mateixes.
- Implementar l'autenticació de dos factors (2FA) **(veure apartat 5.4.1. Consideracions)**
- Limitar l'accés a sistemes i dades sensibles només a personal autoritzat.

- Control, monitoratge i gestió dels comptes d'accés privilegiats a través de l'eina PAM de B:SM.

E. Avaluació de la Seguretat

S'estableixen controls pel garantir el seguiment i actualització dels sistemes i gestió de vulnerabilitats que son responsabilitat del proveïdor de serveis a B:SM:

- Mantenir el programari i sistemes actualitzats amb les últimes solucions de seguretat.
- Establir un pla d'acció continu per a mantenir aquests sistemes actualitzats.
- Realitzar auditories de vulnerabilitats a la xarxa i sistemes interns de manera periòdica i/o a petició de B:SM per a garantir el correcte estat dels sistemes de B:SM.
- El departament de seguretat de B:SM ha de tenir accés al codi font de totes les aplicacions desenvolupades per a B:SM per poder auditar les aplicacions i poder identificar possibles vulnerabilitats a través d'anàlisis estàtiques (SAST) i dinàmiques (DAST).
- Executar l'anàlisi de vulnerabilitats en base a eines corporatives (*Nessus, Qualys, Nexpose, Veracode, SonarQube*) tant per a l'anàlisi de sistemes com de l'entorn web.
- Executar tests d'intrusió (pentest) amb periodicitat anual, per a verificar l'abast de possibles amenaces dins dels sistemes de B:SM,
- Tots els desplegaments de nous projectes seran avaluats a través d'una anàlisi de vulnerabilitats, de sistemes o web, en funció de la naturalesa del projecte. El resultat obtingut serà determinant per a validar el desplegament, de tal manera que, si com a resultat del mateix són detectades vulnerabilitats de nivell alt, hauran de ser solucionades abans de passar a l'entorn de producció.

F. Protecció de la informació

Es requeriment per part del proveïdor establir mesures per garantir la protecció de la informació en trànsit o emmagatzemada (en repòs) en els sistemes de B:SM. L'eina usada per a aquesta protecció haurà de cobrir tant informació estructurada (Bases de dades) com no estructurada, i considerarà les següents accions independentment de l'entorn on est trobin (productiu o no productiu):

- Establir xifrat o aplicació de tècniques de ofuscació i anonimització de **dades en repòs** (**veure Annex 9.12 Requeriments de protecció de la informació**).
- Garantir requeriments de **dades en transit** establerts per B:SM (VPN, HTTPS) **i auditoria** sobre connexions que són responsabilitat de proveïdor o compartida amb B:SM:
  - Punt a punt (en extrem de proveïdor)
  - Connexió implementada sobre entorns de proveïdor SAAS.
  - Qualsevol altre connexió sobre tercers
- Definir polítiques per a la retenció i destrucció segura de dades.

G. Prevenció de codi maliciós (Malware)

Son requeriment les següents mesures per part de proveïdor en tots els sistemes, dispositius i usuaris que interactuïn amb els sistemes de B:SM, i en relació a la protecció d'amenaces de malware:

- Les eines de protecció i/o detecció de malware actuals en B:SM seran *Sophos* (anti-malware) i *Palo Alto Cortex* amb XDR.

- El servei o sistema haurà de garantir que es pugui actualitzar el sistema anti-malware i XDR.
- Per part del proveïdor, es requeriment que tots els seus sistemes relacionats amb el suport o implementació del neu servei/aplicació tinguin instal·lats sistemes anti-malware i XDR actualitzats per a garantir la no propagació als sistemes de B:SM.

H. Resposta a Incidents

Es requeriment per part del proveïdor seguir el pla de resposta a incidents establert en B:SM, de manera detallada i que inclogui procediments clars per gestionar i mitigar incidents de seguretat. Dins del mateix és necessari disposar d'un equip de resposta a incidents.

I. Monitoratge

Es requeriment per part del proveïdor facilitar sistemes de monitoratge de seguretat per detectar activitats sospitoses en tots els sistemes desplegats en B:SM. Tots els sistemes hauran de proporcionar la informació dels logs al SIEM de B:SM.
La recopilació de registres d'esdeveniments es realitzarà amb una mínima configuració de les fonts, i es podrà dur a terme a través de diferents mecanismes: *Syslog, GELF o SNMP (traps o polling)* per a la majoria de servidors i dispositius de xarxa o de seguretat perimetral; lectura directa de fitxers de logs en sistemes de fitxers per a recol·lectar la informació rellevant d'una aplicació específica i consulta.

J. Conscienciació

Es requeriment per part del proveïdor garantir la formació en matèria de seguretat de tots els usuaris que participin en la implementació, manteniment o operació dels serveis proporcionats a B:SM, garantint que tinguin uns mínims de formació i conscienciació en matèria de Seguretat de la Informació. De manera general, es requereixen:

- Realitzar formacions regulars de conscienciació sobre seguretat de la informació per al personal que accedeixi als sistemes de B:SM.
- Fomentar una cultura i procediments de seguretat en què els empleats siguin capaces d'informar de possibles amenaces o incidents.

K. Continuïtat

Es requeriment per part del proveïdor garantir alts nivells de disponibilitat per assegurar que els usuaris puguin accedir als serveis quan els necessitin. De manera general, es requereixen:

- Establir sistemes de còpia de seguretat i redundància per evitar pèrdues de dades o interrupcions prolongades en cas de fallades.
- Determinar períodes de retenció de les dades en funció de la tipologia de projecte.

7.2 Estàndard al Cloud

Les consideracions, estàndards, tecnologies, i arquitectures definides en l'àmbit de seguretat al núvol, són aplicables a les següents casuístiques:

- Serveis SAAS, PAAS i IAAS.

7.2.1 Consideracions

Es consideraran els següents aspectes clau relacionats amb aquest àmbit:

- **Tots els serveis al núvol** de B:SM, independentment de si són de tipus SAAS, PAAS o IAAS, sense excepcions, han de **complir uns requisits bàsics** per garantir la seguretat, privacitat, disponibilitat, confidencialitat, autenticitat, traçabilitat i compliment normatiu.
- Tots els proveïdors que ofereixin serveis o solucions al núvol, han de garantir el compliment del marc de control obligatori per servei**s** SAAS definit per B:SM **(ANNEX I_B - Requeriments de control serveis SAAS v10**), i així mateix, determinar el grau d'aplicabilitat amb la finalitat de complir amb els requisits i estàndards exigits.
- Tots els proveïdors que ofereixin **plataforma i/o infraestructura** de serveis i solucions, **han de garantir l'ús de components autoritzats per CCN** d'acord amb els requisits establerts en l'ENS. Per a això, el proveïdor haurà d'utilitzar del Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació (CPSTIC) del CCN, per a seleccionar els productes o serveis subministrats que hagin de formar part de l'arquitectura de seguretat del sistema.

7.2.2 Requeriments de l'Esquema Nacional de Seguretat (ENS).

Es detallen els principals requisits per a cada domini:

A. Seguretat

Els serveis del núvol hauran de ser integrats en un sistema de gestió d'identitats per habilitar les següents mesures de seguretat:

- Mecanismes d'autenticació forts per assegurar que només els usuaris autoritzats puguin accedir als recursos.
- Controls d'autorització per garantir que els usuaris només tinguin accés als recursos que estan autoritzats a utilitzar.
- Sistema de gestió d'accés que permeti revocar els privilegis dels usuaris que ja no necessitin accedir als serveis.
- Les dades han de ser xifrades tant en trànsit com en repòs per protegir la informació de possibles accessos no autoritzats.
- Sistemes de detecció i prevenció d'intrusions per detectar activitats sospitoses o atacs.

B. Privacitat

- Els serveis al núvol de B:SM, han de complir amb les regulacions i lleis de protecció de dades aplicables per garantir la privacitat de la informació dels usuaris (RGPD).
- El responsable del tractament de dades sempre serà B:SM, que determina els fins i mitjans del tractament, és a dir, qui és el responsable d'informar sobre la finalitat del tractament i els mitjans elegits.
- El proveïdor del servei o solució al núvol serà l'encarregat del tractament de dades que realitza per compte de B:SM. Així mateix, ha d'informar si les dades seran tractades per tercers.
- Les dades personals han de ser tractades amb el consentiment explícit dels usuaris i ser únicament utilitzades per a les finalitats establertes.

- És necessari comptar amb procediments per gestionar les sol·licituds dels usuaris relacionades amb les seves dades personals, com el dret a l'oblit i la portabilitat de dades.

C. Disponibilitat

- Els proveïdors dels serveis o solucions al núvol de B:SM, han de garantir alts nivells de disponibilitat per assegurar que els usuaris puguin accedir als serveis quan els necessitin.
- Aquests serveis o **solucions** han de disposar de sistemes de còpia de seguretat i redundància per evitar pèrdues de dades o interrupcions prolongades en cas de fallades.
- Els períodes de retenció, seran determinats en funció del projecte.

D. Confidencialitat

- Els serveis al núvol de B:SM han d'implementar mesures tècniques i organitzatives per mantenir la confidencialitat de la informació, evitant l'accés no autoritzat.
- Els proveïdors de serveis i solucions al núvol, han de tenir polítiques clares sobre com gestionar la informació confidencial i garantir la formació dels seus empleats

E. Compliment normatiu

- Els serveis i solucions al núvol de B:SM, han de complir amb les regulacions i normatives vigents en matèria de seguretat i privacitat de les dades.
- Els serveis i solucions al núvol de B:SM, han de ser auditats i certificats segons els requisits establerts a l'Esquema Nacional de Seguretat (ENS) per garantir el compliment normatiu.

F. Interoperabilitat

- Els serveis i solucions al núvol de B:SM, han de ser compatibles amb estàndards i protocols reconeguts per permetre la integració amb altres sistemes i aplicacions.
- Cal garantir la comunicació i interacció adequada amb altres serveis, plataformes en el núvol i en entorns locals de manera segura i complint els requisits de seguretat.

G. Monitoratge

- Cal proporcionar una supervisió constant dels recursos per identificar i respondre ràpidament a possibles incidents o problemes de rendiment.
- Tots els sistemes i serveis en el núvol hauran de proporcionar la informació dels logs al SIEM de B:SM.
- La recopilació de registres d'esdeveniments es realitzarà amb una mínima configuració de les fonts. Es podrà dur a terme a través de diferents mecanismes: SMTP per a la recepció de notificacions de correu electrònic generats per altres sistemes; serveis web basats en *SOAP, XML-RPC o REST* per a la consulta d'informació sobre sistemes o eines que comptin amb aquestes interfícies, com les que permeten gestionar plataformes en el núvol (*Microsoft Office 365, Microsoft Azure, Amazon Web Services*).

H. Actualització

- Els proveïdors de serveis i solucions al núvol han d'establir procediments per planificar actualitzacions de manera regular i garantir que els serveis a B:SM estiguin actualitzats

per oferir protecció enfront amenaces, com ara noves vulnerabilitats o programari maliciós.

I. Avaluació

- És necessari realitzar revisions periòdiques per avaluar i millorar la seguretat i eficiència dels serveis.
- Tots els desplegaments de nous projectes seran avaluats a través d'una anàlisi de vulnerabilitats, en base a l'avaluació del programari base (sistema) o l'aplicatiu (web), depenent de la naturalesa del projecte.
- Totes les vulnerabilitats detectades amb caràcter greus o alta, hauran de ser resoltes prèviament al traspàs a producció.

8 Revisió i manteniment dels estàndards TiC a B:SM

La direcció TiC de B:SM actualitzarà periòdicament els estàndards TIC amb l'objectiu de garantir la seva idoneïtat per donar resposta les necessitats de les unitats de negoci de B:SM, i així mateix, que estan alineats amb les tecnologies i bones practiques del sector TIC.

9 Annex

9.1 BBDD

A continuació, s'especifiquen les bases de dades centralitzades (d'us general) i específiques estandarditzades per la direcció TiC de B:SM segons aplicació o servei:

Tipologia	Estructura	Servei	Versió
Centralitzada	**Oracle**	- Ús general	mínim **versió 19c entreprise**
Centralitzada	**Microsoft SQL**	- Ús general	mínim **versió 2016**
Especifica	**MySQL**	- eCommerce - Aplicacions que no sigui viable /recomanable clústers d'Oracle o SQL. - Aplicacions monolítiques no crítiques	Última versió estable de fabricant
Especifica	**MariaDB**	- Entorns web específics	Última versió estable de fabricant

Especifica	**MongoDB**	- Sharings	Última versió estable de fabricant

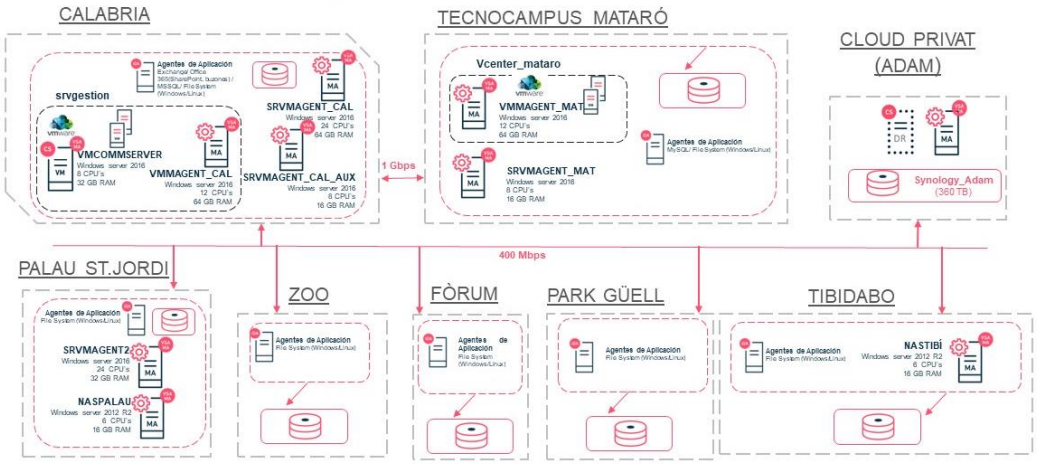
9.2 Política de Backup de BBDD

A continuació, s'especifiquen els principis mínims de Backup de les BBDD a B:SM:

Freqüència	Tipologia	Retenció
Mensual	Complerta	3 anys
Diària	Complerta	30 dies

BS:M disposa i té en funcionament la plataforma Commvault Simpana backup and recovery, amb la següent estructura actual:

Backup B:SM:



9.3 Llenguatges de programació i frameworks

A continuació, s'especifiquen els llenguatges estandarditzats per la direcció TiC de B:SM segons tipologia i necessitats de desenvolupament:

Servei	Llenguatge	Tipologia	Versió

Aplicacions de gestió back-office, middleware	**.NET** **JAVA** **PHP**	A mida	Última versió estable de fabricant
Front web	**HTML** **JAVA SCRIPT** **CSS** **ANGULAR**	A mida	Última versió estable de fabricant
Front APP	**MAUI** **KOTLIN** **SWIFT** **IONIC**	A mida	Última versió estable de fabricant
Gestió continguts (CMS)	**DRUPAL**	Plataforma fabricant	Última versió estable de fabricant

9.4 Plataforma d'integració i gestió API

S'han establert dues plataformes diferenciades que son estàndard a B:SM per residir i gestionar els desenvolupaments API durant tot el cicle de vida (des-de el desenvolupament fins a la publicació):

Servei	Plataforma
SAP*	**SAP BTP Integration Suite**
Salesforce*	**Mulesoft**
Resta de sistemes	**WSO2**

***NOTA:** Sistemes en desplegament previst durant 2024.*

9.5 Llistat riscos desenvolupament Web

Llistat de riscos habituals a mitigar en desenvolupament Web (OWASP 2021 top 10)

OWASP ID	Risk
A01	Brocken Access Arrow
A02	Cryptographic Failures
A03	Injection
A04	Insecure design
A05	Security Misconfiguration
A06	Vulnerable and Outdated Components
A07	Identification and Authentication Failures
A08	Software and Data Integrity Failures
A09	Security Logging and Monitoring Failures
A10	Server-side Request Forgery

9.6 Llistat de seus B:SM

Llistat de seus en abast dins l'àmbit de comunicacions de B:SM

SEU
Cementiris Ibermática (Call Center)
Base Agents cívics Provença
Park Güell
Anella
Port Olímpic
Estació d'Autobusos
Bases Àrea
ZOO
Tibidabo
Fòrum
Aparcaments
Dipòsits

9.7 Detall dels components i continguts de la granja de servidors (Server Farm)

CONTINGUT SERVER FARM
Entorn VMWARE 6.7-6.0
Entorn d'Oracle RAC 19c
Entorn SQL 2016 AlwaysOn
Entorn MongoDB
Aplicacions de negoci (webs/apps/serveis crítics)
Commvault Backup
VDI
FW i serveis de balancejadors Netscalers

9.8 Requisits de monitorització de serveis

Requisits de monitorització mínima en funció del servei

Servei	Requisit
Sistemes i Comunicacions	Monitorització tradicional que ha d'incloure: - Llindars - Serveis del sistema o de l'aplicació específics - Rendiments, evolució i tendències - Consultes BBDD i API (Nagios-OP5)
Webs i APPs	Monitorització sintètica/robotitzada. (ISM-Selenium)
Serveis SaaS	Consultes sobre plataformes, pàgines de Health, etc.

9.9 Estàndards SO

Estàndards B:SM d'us de sistemes operatius i versions

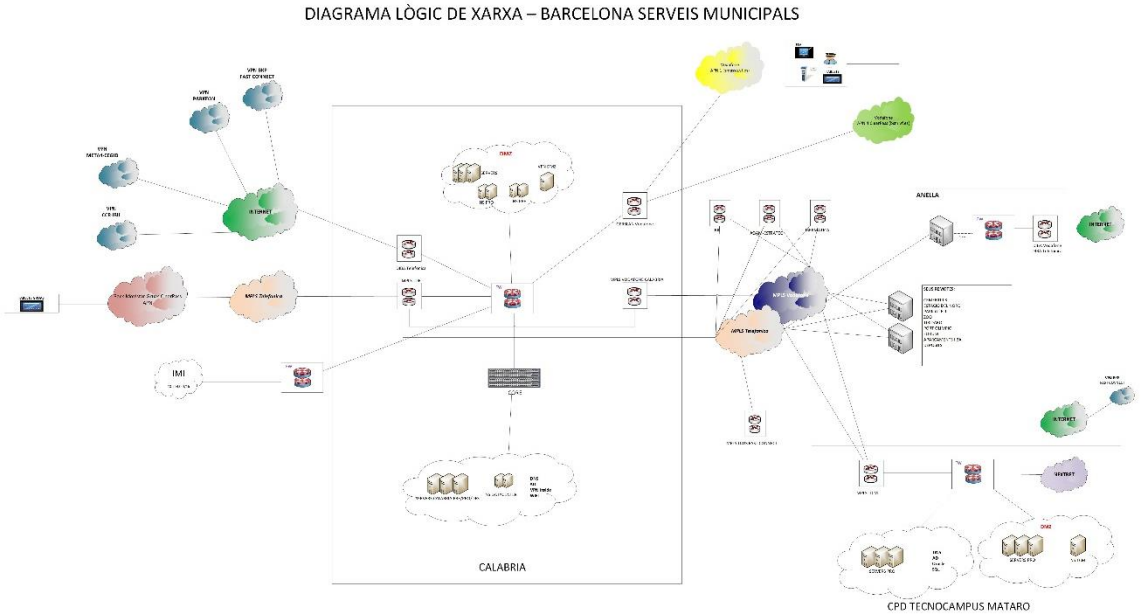
Fabricant	Versió

Microsoft	Windows server 2019
Linux	Redhat 9

9.10 Estàndard d'equipament

Àmbit	Requeriment
Garantia	Mínim 4 anys
Eina de gestió lloc de treball	Compatibilitat amb Workspace One
Programari equips d'usuari	- Office 2016 - Windows 10 PRO - Sophos i Cortex (Protecció) - O365 Suite

9.11 Arquitectura de xarxa



B:SM

9.12 Requeriments de protecció de la informació

Taula resum que relaciona el tractament segons nivell de la informació

Nivell d'Informació	Descripció	Xifrat
Reservada	– Informació altament restringida. – Impacte alt enfront pèrdua o divulgació.	**X**
Confidencial	– Informació restringida. – Impacte alt enfront pèrdua o divulgació.	**X**
Interna	– Informació interna. – Impacte mig/baix.	
Pública	– Informació pública. – Sense impacte	