COORDINACIÓ SERVEIS DIGITALS
Exp: 904784/2026

PLEC DE CONDICIONS TÈCNIQUES

OBJECTE DEL CONTRACTE

L'objecte del contracte és la contractació d'una solució de Gestió d'Accés Privilegiat (PAM) per l'Àrea Metropolitana de Barcelona.

ABAST

El present expedient contempla el subministrament de les llicències necessàries per implementar la solució així com els serveis professionals necessaris per garantir una implantació correcta i un ús efectiu per part del personal tècnic de l'AMB.

REQUERIMENTS

Requeriments funcionals:

La solució oferta ha de disposar, com a mínim, de les funcionalitats següents:

Gestió de contrasenyes i credencials privilegiades

La plataforma haurà de disposar d'un repositori centralitzat i xifrat per a l'emmagatzematge de credencials privilegiades. Haurà de permetre:

- Rotació automàtica de contrasenyes segons polítiques configurables per tipus d'actiu i nivell de criticitat.
- Recuperació controlada i auditable de credencials en cas d'emergència (break-glass).
- Xifrat de dades en repòs i en trànsit mitjançant algorismes reconeguts internacionalment, com AES-256 i TLS 1.2 o superior.
- Control d'accés granular a secrets, amb registre complet d'ús i accés.
- Gestió de claus SSH i credencials d'aplicació dins del mateix repositori.

Control d'accés privilegiat

La solució haurà d'implementar un model de control d'accés basat en rols (RBAC) que permeti assignar permisos de manera granular en funció del rol de l'usuari, el tipus d'actiu i el context de l'accés.

A més, haurà de suportar:

- Accés just-in-time (JIT), amb concessions temporals de privilegis i revocació automàtica en finalitzar la tasca o el temps autoritzat.
- Fluxos de sol·licitud i aprovació, si escau, per a l'atorgament d'accés privilegiat temporal.
- Capacitat per aplicar polítiques d'accés condicionals (horari, origen, tipus d'actiu).

EXPOSITO PEREZ, Cristian (1 de 2)
Tècnic/a Serveis Corporatius
Data signatura 09/09/2026 9:41:52
HASH:80DB07609E21587A6BECC81185D5F11ACE421D1A

DE LA MORENA BARRIO, Carlos (2 de 2)
Cap de Servei TIC
Data signatura 09/09/2026 10:14:58
HASH:80DB07609E21587A6BECC81185D5F11ACE421D1A

AREA METROPOLITANA DE BARCELONA - PLEC TECNIC
Codi per a validació: ZXQAP-830V5-ZOYDG
Verificació: https://verificador.amb.cat/verificadorDocumento/home
Aquesta és una còpia impresa del document electrònic referènciat : 1/5.

APROVAT

Gestió i gravació de sessions privilegiades

La plataforma haurà de permetre:

- Establir, supervisar i enregistrar sessions privilegiades sobre protocols com SSH, RDP i interfícies web d'administració.
- Reproducció i cerca dels enregistraments, amb protecció contra manipulació.
- Monitoratge en temps real de les sessions actives.
- Finalització forçosa d'una sessió per part d'un administrador.
- Generació de metadades detallades de sessió per a integració amb SIEM. La solució ha de ser compatible amb la plataforma de gestió centralitzada de logs i analítica de seguretat existent a l'AMB.

Els enregistraments i metadades associades hauran de conservar-se de manera segura i auditable.

Autenticació reforçada

L'accés a la plataforma de gestió requerirà autenticació multifactor (MFA).

La solució haurà de ser compatible amb:

- Factors basats en tokens d'un sol ús (TOTP/HOTP) en format aplicació mòbil, d'acord amb els estàndards RFC 6238 i RFC 4226.
- Integració amb proveïdors d'identitat corporatius que implementin SAML 2.0, RADIUS, LDAP i altres protocols d'identitat estàndard utilitzats habitualment en entorns corporatius.
- Gestió centralitzada de polítiques d'autenticació, incloent-hi usuaris, grups, rols i requisits d'MFA.

Suport multi-plataforma

La solució haurà de donar cobertura, com a mínim, als següents tipus d'actius:

- Servidors Windows i Linux/Unix.
- Bases de dades relacionals (Oracle, SQL Server, PostgreSQL o equivalents).
- Dispositius de xarxa administrats per SSH/Telnet.
- Entorns cloud (AWS, Azure o GCP).

Informes i auditoria

La solució haurà de generar informes d'activitat i auditoria exportables en formats estàndard (PDF, CSV o equivalents), amb capacitat de filtratge per usuari, actiu, rang de dates i tipus d'acció.

Els informes i registres generats hauran de proporcionar la traçabilitat i evidències necessàries per donar suport al compliment de les obligacions derivades de l'ENS, el RGPD i la Directiva NIS2.

DE LA MORENA BARRIO, Carlos (2 de 2)
Data signatura: 09/09/2026 10:14:58
HASH:80DB07609E21587A6BECC81185D5F11ACE421D1A

EXPOSITO PEREZ, Cristian (1 de 2)
Data signatura: 09/09/2026 9:41:52
HASH:80DB07609E21587A6BECC81185D5F11ACE421D1A

AREA METROPOLITANA DE BARCELONA - PLEC TECNIC
Codi per a validació: ZXQAP-830V5-ZOYDG
Verificació: https://verificador.amb.cat/verificadorDocumento/home
Aquesta és una còpia impresa del document electrònic referènciat : 2/5.

APROVAT

Requeriments d'integració:

Directori actiu corporatiu

La solució haurà d'integrar-se nativament amb Active Directory i/o LDAP, incloent-hi:

- Autenticació delegada.
- Sincronització automàtica d'usuaris i grups.
- Mapeig de rols basat en grups.
- Detecció de canvis de manera periòdica i configurable.

API d'integració

La solució haurà de disposar d'una API REST completa, documentada i versionada, que permeti:

- Integració amb ticketing i ITSM.
- Automatització de rotació de credencials.
- Gestió de sessions i aprovacions.
- Consulta i gestió de secrets i rols.

Requeriments d'arquitectura i seguretat:

Model de desplegament

La solució haurà de poder desplegar-se en modalitat on-premises, en núvol privat o en mode híbrid, d'acord amb les necessitats i la política de seguretat de l'AMB.

A més, és requisit indispensable que la plataforma:

- Sigui plenament compatible amb entorns de virtualització basats en VMware, incloent-hi com a mínim VMware vSphere/ESXi en versions suportades pel fabricant.
- Permeti el desplegament en màquines virtuals estàndard sense necessitat d'appliances propietaris o maquinari dedicat.

Capacitat d'escalabilitat i concurrència

La solució haurà de garantir, com a mínim:

- 50 usuaris concurrents accedint simultàniament a la plataforma o a sessions privilegiades gestionades per aquesta.
- Capacitat per gestionar un mínim de 150 usuaris definits amb autenticació reforçada basada en tokens d'un sol ús (TOTP/HOTP) sense degradació del rendiment. El licitador haurà d'incloure en la seva oferta les llicències necessàries per cobrir un mínim de 150 usuaris.

Zero Trust i mínim privilegi

L'arquitectura de la solució haurà de ser coherent amb el model Zero Trust, de manera que cap accés privilegiat no sigui permanent per defecte i tots els accessos siguin autenticats, autoritzats i auditats de forma individual.

EXPOSITO PEREZ, Cristian (1. de 2)
Entitat: Consorci de Serveis Informàtics
Data signatura: 09/09/2026 9:41:52
HASH:800B07609E21587A6BECC81185D5F11ACE421D1A

DE LA MORENA BARRIO, Carlos (2. de 2)
Entitat: Consorci TIC
Data signatura: 09/09/2026 10:14:58
HASH:800B07609E21587A6BECC81185D5F11ACE421D1A

AREA METROPOLITANA DE BARCELONA - PLEC TECNIC
Codi per a validació: ZXQAP-830V5-ZOYDG
Verificació: https://verificador.amb.cat/verificadorDocumento/home
Aquesta és una còpia impresa del document electrònic referènciat : 3/5.

APROVAT

Gestió de certificats i secrets

La plataforma haurà de gestionar de manera segura els certificats digitals, claus SSH i secrets d'aplicació (API keys, tokens, etc.) associats als sistemes gestionats.

Requeriments del servei de posada en marxa:

El licitador ha de presentar una proposta de pla de projecte per a la posada en marxa que inclogui, com a mínim, les fases i les tasques descrites a continuació, amb una estimació de la dedicació i el calendari d'execució:

- Fase d'anàlisi: revisió de l'entorn existent i definició de l'arquitectura de desplegament.
- Fase d'instal·lació i configuració: desplegament de la plataforma i configuració dels paràmetres inicials.
- Fase pilot: incorporació d'un conjunt inicial d'actius i comptes privilegiats acordat amb l'AMB.
- Fase de validació: execució del pla de proves i acceptació formal per part de l'AMB.
- Documentació tècnica de la implantació: lliurament dels manuals d'administració, d'operació de la solució i d'un document d'arquitectura as-built, que contingui:
    - Diagrama actualitzat de l'arquitectura desplegada, amb tots els components de la solució, les seves relacions i la ubicació dins la infraestructura de l'AMB (xarxes, segments, DMZ, etc.).
    - Detalls de la màquina virtual que forma part de la solució, amb les seves especificacions (sistema operatiu, versió, recursos assignats) i les adreces IP o noms DNS corresponents.
    - Detall dels paràmetres de configuració aplicats: polítiques de rotació de contrasenyes, temps d'expiració de sessions, regles d'accés just-in-time, configuració de MFA i qualsevol altre paràmetre rellevant per a l'operació.
    - Descripció de les connexions establertes amb sistemes externs (Active Directory, LDAP, SIEM, sistemes de ticketing, etc.), incloent-hi el tipus de protocol, els ports utilitzats i el compte de servei emprat per a cada integració.
    - Relació dels comptes privilegiats i actius donats d'alta durant la posada en marxa, com a punt de partida per a la gestió posterior.
    - Instruccions per a les tasques d'administració més habituals: còpies de seguretat i restauració, gestió de certificats, etc.
    - Qualsevol desviació o adaptació que s'hagi produït durant la implantació respecte al disseny d'arquitectura prèviament acordat, amb la justificació corresponent.

Requeriments del servei de formació:

La corporació requereix que el proveïdor adjudicatari imparteixi un programa de formació adreçat al personal tècnic responsable de l'administració i l'operació de la solució. La formació ha de complir els requisits següents:

- Modalitat i durada: formació presencial o en línia (o combinada), amb una durada mínima de 6 hores lectives, cobert dins el preu del contracte.

EXPOSITO PEREZ, Cristian (1. de 2)
Tècnic/a Sistemes Informàtics
Data signatura 10/09/2026 9:41:52
HASH:80DB07609E21587A6BECC81185D5F11ACE421D1A

DE LA MORENA BARRIO, Carlos (2. de 2)
Cap/a de Servei TIC
Data signatura 10/09/2026 10:14:58
HASH:80DB07609E21587A6BECC81185D5F11ACE421D1A

AREA METROPOLITANA DE BARCELONA - PLEC TECNIC
Codi per a validació :ZXQAP-830V5-ZOYDG
Verificació :https://verificador.amb.cat/verificadorDocumento/home
Aquesta és una còpia impresa del document electrònic referènciat : 4/5.

APROVAT

- Continguts mínims: administració i configuració de la plataforma, gestió del cicle de vida de les credencials, supervisió de sessions, generació d'informes d'auditoria i resposta davant incidències.
- Nombre de participants: la formació ha de poder ser aprofitada per un mínim de 4 tècnics de la corporació sense cost addicional.

Gestió de garantia

El subministrador cobrirà les errades de configuració que siguin detectades durant un termini d'un any a partir de la signatura de l'acta de recepció.

Acta de recepció

En superar-se la posada en marxa de la solució l'ÀMB signarà una acta de recepció indicant la seva acceptació dels treballs efectuats. El termini de suport i garantia s'iniciarà l'endemà de l'esmentada signatura.

REQUERIMENTS D'EXECUCIÓ

Tasques a realitzar

Les tasques a realitzar es desenvoluparan seguint una filosofia claus en ma incloent, de forma conjunta, totes les activitats involucrades.

Metodologia de treball

Les tasques d'instal·lació no hauran d'interferir significativament en l'operativa dels equips en producció. Qualsevol necessitat d'actuacions que puguin alterar l'activitat normal requerirà de l'aprovació prèvia del Servei TIC i s'haurà d'efectuar dins de l'horari establert per aquest.

En cap cas s'admetran accions no aprovades que puguin posar en risc serveis, dades o equipaments en producció, que atemptin contra la seguretat de la instal·lació o que suposin un perjudici en el nivell de servei ofert. Tota actuació que pugui tenir alguna afectació en qualsevol d'aquests aspectes requerirà l'autorització prèvia del Servei TIC i s'haurà d'efectuar d'acord a les indicacions del mateix.

En cap cas es desplegarà un producte de programari o maquinari sense el consentiment del Servei TIC. Tot producte instal·lat quedarà sota el control d'aquest.

DE LA MORENA BARRIO, Carlos (2 de 2)
Cap de Servei TIC
Data signatura: 09/09/2026 10:14:58
HASH:800B07609E21587A6BECC81185D5F11ACE421D1A

EXPOSITO PEREZ, Cristian (1 de 2)
Enginyer informàtic
Data signatura: 09/09/2026 9:41:52
HASH:800B07609E21587A6BECC81185D5F11ACE421D1A

AREA METROPOLITANA DE BARCELONA - PLEC TECNIC
Codi per a validació: ZXQAP-830V5-ZOYDG
Verificació: https://verificador.amb.cat/verificadorDocumento/home
Aquesta és una còpia impresa del document electrònic referènciat : 5/5.