E-302500/07-06-24

Plec de prescripcions tècniques

El present plec té com a objecte definir les condicions tècniques en les que s'ha de regir la contractació específica d'una eina de gestió d'identitats i gestió d'accessos en modalitat de servei al núvol ("Identity as a Service" o IDaaS) per a la UPF amb els serveis addicionals d'instal·lació, configuració i parametrització, suport, formació i evolutiu, per al període 2024-2026.

La contractació conté tres prestacions diferenciades però inseparables:

1. Contractació de les llicències (dret d'ús) de la plataforma de gestió d'identitats en modalitat servei al núvol ("Identity as a Service" o IDaaS), amb tots els elements que calgui per a proporcionar el servei a la UPF. Aquesta llicència en un primer terme i mentre es realitza el procés d'implantació tindrà una capacitat d'usuaris actius mensuals (MAU) que s'incrementarà al finalitzar la implantació i per la resta de la durada del contracte, per poder assumir la capacitat que necessita la UPF.

2. Tasques d'implementació, configuració, adaptacions i desenvolupaments necessaris per la posada en marxa de la llicència d'ús de la plataforma de gestió d'identitats per la UPF de manera que cobreixi tot el que ara ja s'està fent més les noves necessitats descrites en el plec.

3. Servei evolutiu amb gestió de petits desenvolupaments que s'hagin de realitzar un cop implementada la solució, per atendre noves demandes o prestar suport a la UPF en la realització d'aquestes, per exemple, per la incorporació als sistema de nous programaris.

Els objectius d'aquesta contractació són:

a) Permetre centralitzar la informació sobre els usuaris, els perfils i rols i els drets d'accés que han de tenir, unificant els diferents repositoris d'usuaris i fonts autoritatives d'informació. Disposar d'un magatzem d'identitats que comporti la representació de la Identitat digital amb un model d'identitat i cicle de vida.

b) Disposar de capacitat per a la gestió de comptes i accessos amb integració de sistemes i aplicacions tant al núvol com de la infraestructura local de la UPF (on premises), seguint l'estàndard SCIM (System for Cross-domain Identity Management) i permetent l'automatització de processos, compatible amb un model RBAC (Role-based access control).

c) Incorporar un model de gestió, basat en l'automatització d'accions i events i de sol·licituds d'accés i aprovació a través de fluxos de treball, sense necessitat d'implementació de codi (no code o low code). Poder gestionar la neteja o modificació dels permisos d'accés dels usuaris en cas de baixes o canvis d'adscripcions, perfils o rols que han d'estar contemplats a la plataforma, així com poder disposar d'informes d'adopció i d'auditoria de la tota la informació i les accions dels usuaris. Tot això, per permetre reduir riscos de compliment i seguretat.

1. Requeriments de les llicències (dret d'ús) de la plataforma de gestió d'identitats en modalitat servei al núvol ("Identity as a Service" o IDaaS)

La plataforma objecte del contracte ha de ser una solució integral i unificada per a totes les necessitats de gestió d'identitat i gestió d'accessos amb seguretat, de la UPF.

Ha de ser una plataforma en modalitat servei al núvol (IDaaS) ja desenvolupada i plenament operativa, que ja estigui funcionant en multitud de clients. No es contempla la possibilitat de desenvolupar una plataforma ad hoc més enllà de la implementació necessària per complir amb els requeriments d'integració amb la lògica de negoci del serveis de UPF i de personalització i configuració.

Ha de complir d'un nivell de servei (SLA) alt pel que fa a disponibilitat, estabilitat i historial d'incidents, en els termes definits a l'annex ENS del plec de clàusules administratives particulars

La plataforma ha de disposar d'un ampli catàleg d'integracions, predefinides i ja disponibles com a opció del producte, amb aplicacions i serveis: ha de proporcionar integracions amb connectors ja disponibles cap a aplicacions empresarials populars on, com a mínim, cal que inclogui els que s'indiquen en el punt 16 de taula de requeriments: A. Característiques globals de la plataforma.

Ha d'incloure el suport i manteniment de la plataforma (manteniment correctiu, evolutiu, adaptatiu i perfectiu) i de les integracions, assegurant que les connexions es mantinguin segures i funcionals a mesura que les aplicacions i serveis a integrar evolucionen.

La plataforma ha de disposar d'eines gràfiques i visuals que permetin a la UPF automatitzar les tasques de gestió d'identitat, amb fluxos de treball dins de la gestió del cicle de vida de la Identitat.

La solució ha de proporcionar una àmplia gamma de recursos de documentació i suport que incloguin: guies, tutorials, i un equip de suport dedicat per tal de facilitar la solució de problemes i l'optimització de la implementació. La documentació s'haurà de mantenir accessible en tot moment i al dia, d'acord amb l'evolució de la plataforma i les seves integracions.

La solució ha d'estar dissenyada per a poder augmentar o disminuir la capacitat (escalar) fàcilment, segons les necessitats de la Universitat, assegurant que la implementació segueixi essent eficient i efectiva a mesura que l'entorn universitari s'amplia o varia.

Addicionalment, la solució a contractar ha de facilitar l'autonomia de la Universitat, de manera que no necessiti de la intervenció de l'empresa proveïdora per a futures integracions o activar nous serveis i aplicacions a no ser que la UPF vulgui contractar ajuda de manera volguda per manca de temps o recursos.

La plataforma ha de disposar d'una URL pròpia amb el domini de la UPF (upf.edu) per tal d'accedir-hi de manera segura (https). Aquesta personalització ha d'estar inclosa en les tasques d'implementació i configuració.

La plataforma ha de ser accessible per als administradors amb tota la seva gamma de serveis i components, i a tota la comunitat universitària (estudiants, PDI i PTGAS) per a gestionar les ~~seves~~ credencials d'accés a les diferents aplicacions que correspongui a cadascú.

En qualsevol cas, s'ha d'incloure l'allotjament, manteniment, suport i execució de la plataforma en modalitat de servei al núvol (IDaaS) de manera que no suposi per a la UPF cap feina de gestió, manteniment, instal·lació, canvi de versió, etc., per tal de mantenir el programari funcionant, integrat, al dia tecnològicament i amb compliment de la legalitat vigent en aquesta matèria.

Específicament estaran inclosos tots els serveis, provisions, subministraments, que siguin necessaris per a l'execució total i completa del contracte en els termes detallats en aquest plec de prescripcions tècniques.

La plataforma que es proposi haurà d'ajustar-se als següents requisits, que cobreixen els aspectes generals que s'han de considerar per a la implementació i ús d'una eina d'aquestes característiques per a una universitat pública:

La plataforma i el servei hauran de complir el reglament 2016/679 del Parlament Europeu i el Consell de la Unió Europea, la GDPR (General Data Protection Regulation) i l'Esquema Nacional de Seguretat. En aquest sentit, haurà de disposar de:

- el certificat de l'Esquema Nacional de Seguretat (ENS) de nivell alt.

- el certificat del codi de conducta del núvol de la UE de nivell 2. (EU Cloud Code of Conduct Level 2)

L'empresa que prestarà el servei IdaaS i l'adjudicatària han de garantir la permanent actualització de la plataforma als canvis legals i tecnològics que es puguin produir en el futur durant la vigència del contracte.

Els requeriments que es consideraran en relació a les plataformes es descriuen a continuació agrupant-se segons temàtica i, a més, per tal de concretar el mètode d'avaluació es classifiquen en els següents termes:

(I) Imprescindible	Necessari per al projecte. En cas de no complir aquest requeriment la plataforma queda descartada
(D) Desitjable	Es valorarà que la plataforma l'incorpori

Ref.	A. Característiques globals de la plataforma	Tipus
1	Ha de permetre la gestió tant d'Identitats com d'accessos: capacitat de gestionar usuaris, perfils, rols, grups i dispositius.	**(I)**
2	Ha de disposar de funcionalitats i automatismes per a gestionar l'aprovisionament, la modificació i la baixa d'usuaris i dels seus permisos d'accés a les diferents aplicacions i serveis de la UPF.	**(I)**
3	La plataforma i la solució ha de permetre l'encriptació de dades en trànsit i en repòs i a les còpies de seguretat	**(I)**
4	Disposar d'un directori al núvol com a repositori central d'informació que permeti: personalitzar, organitzar i gestionar qualsevol conjunt d'atributs d'usuari des de múltiples fonts d'identitat amb un magatzem d'usuaris flexible. Aquest directori ha de ser l'autoritat central per a la informació sobre un usuari concret, com a "única font de veritat" per als usuaris de la comunitat universitària.	**(I)**
5	Permetre la gestió del cicle de vida de la identitat (comptes d'usuari) automatitzant la incorporació i la baixa dels usuaris i assegurant una comunicació segura i sense interrupcions entre directoris com: Active Directory i LDAP, i altres aplicacions o sistemes gestionats mitjançant les capacitats d'aprovisionament SCIM (System for Cross-domain Identity Management) i connectors a desenvolupar en cas necessari.	**(I)**
6	La integració de directoris ha d'incloure regles de pertinença a grups.	**(I)**
7	Disposar d'una capa API (Interfície de Programació d'Aplicacions), API REST i de SDKs (Software development Kits), per a integracions personalitzades. amb accés al nucli de la plataforma, que permeti que interactuïn les aplicacions i altres serveis que es relacionen amb la plataforma. Així mateix, ha de permetre implementar funcions d'autenticació bàsiques com iniciar la sessió dels usuaris en aplicacions i serveis i gestionar programàticament els atributs de la identitat de l'usuari dins el directori.	**(I)**

8a	Gestió d'Accés a l'API (API Access Management): Disposar d'una implementació seguint l'estàndard OAuth 2.0 que integri la gestió d'accés a l'API amb implementacions amb OpenID Connect per a l'autenticació. (OpenID Connect (OIDC) és un protocol d'autenticació d'identitat que és una extensió de l'autorització oberta (OAuth) 2.0 per estandarditzar el procés d'autenticació i autorització dels usuaris quan inicien sessió per accedir als serveis digitals).	**(I)**
8b	Proporcionar una API de gestió d'usuaris per a la incorporació, monitoratge i retirada d'aplicacions a usuaris. També ens ha de permetre conèixer els passos sobre com afegir l'autenticació als nostres possibles catàleg i punts d'API.	**(I)**
9a	Ser multi-idioma per a totes les funcionalitats a què tenen accés els usuaris finals. L'usuari ha de poder escollir en quin idioma vol navegar.	**(I)**
9b	Ha de tenir una interfície d'accés web suportada en múltiples sistemes operatius (Windows, Linux, MacOS) i en les últimes versions dels navegadors, mínim Chrome, Firefox, Safari i Edge.	**(I)**
10a	S'ha de poder personalitzar amb el disseny i imatge gràfica de la UPF a través de la configuració, amb capacitats que no impliquin afegir o desenvolupar codi dins de l'administració de l'eina.	**(I)**
10b	Cal que la pàgina on els usuaris inicien sessió pugui mostrar el fons i el logotip de la UPF.	**(I)**
10c	Si els usuaris troben un error, aquesta pàgina cal que mantingui el mateix tema gràfic de la UPF.	**(I)**
10d	El quadre de comandament d'usuari final cal que estigui personalitzat amb els criteris visuals de la UPF.	**(I)**
10e	De la mateixa manera les plantilles i missatges de correu electrònic en el recordatori de la contrasenya han de poder ser amb el disseny gràfic de la UPF	**(I)**
11a	Disposar de funcionalitats d'accés tipus passarel·la (Gateway) que permetin protegir l'accés a les aplicacions hostatjades en local (on premises) que no admeten federació amb les capacitats d'autenticació d'usuaris i inici de sessió únic.	**(I)**
11b	Disposar de funcionalitats de passarel·la d'accés (Access Gateways) que permetin comunicar-se a través de IPv6 amb servidors IP que escolten direccions IPv6 i servidors d'identitats que es comuniquen a través de IPv6 amb magatzems d'usuaris LDAP	**(I)**
11c	Ha de permetre protegir l'accés tant a les aplicacions locals com al núvol híbrid sense incorporar canvis en les aplicacions.	**(D)**
11d	Ha de permetre als usuaris externs accedir a aplicacions web locals sense la necessitat de VPNs tradicionals.	**(D)**
12a	Ha de disposar de funcionalitats d'accés avançat a servidors (Privileged Access).- Proporcionar gestió d'identitat i accés de confiança zero per a la infraestructura en el núvol i local. Utilitzant la plataforma com a font de veritat i reconciliar comptes per gestionar l'accés SSH i RDP a servidors Linux i Windows.	**(I)**

12b	Ha de permetre ampliar l'accés privilegiat segur als usuaris, automatitzant la gestió del cicle de vida dels comptes de servidor i eliminant la necessitat de gestionar credencials.	**(I)**
13a	Cal que incorpori la funcionalitat d'inici de sessió únic (SSO). Que és una eina d'autenticació que permet als usuaris accedir de manera segura a múltiples aplicacions i serveis utilitzant un únic conjunt de credencials, eliminant la necessitat de recordar diferents contrasenyes per a cada servei. L'SSO ha de proporcionar un senzill widget[1] emergent o pàgina d'inici de sessió amb una sola contrasenya que proporciona accés a totes les aplicacions integrades.	**(I)**
13b	Els protocols i estàndards a tenir en compte quan s'identifica i es treballa amb l'SSO cal que incloguin: Saml, Oauth, OIDC i altres.	**(I)**
14a	Cal que la plataforma inclogui, sense incorporació d'altres productes de tercers, d'una autenticació multifactor (MFA) com a mètode de verificació d'identitat que afegeixi una capa addicional de seguretat a les credencials com noms d'usuari i contrasenyes, proporcionant una major certesa que un usuari és qui diu ser abans de concedir-li accés a una aplicació, compte en línia o xarxa corporativa. La solució MFA amb d'incloure / permetre aquests tipus: OTP, SMS, factors biomètrics (en cas que la UPF finalment els adopti).	**(I)**
14b	Cal que la plataforma disposi d'algun tipus d'autenticació adaptativa basada en el risc, on s'analitzin les dades de: clients, dispositius i esdeveniments d'autenticació, amb l'objectiu d'obtenir informació sobre el comportament dels usuaris finals per restringir l'accés quan es detectin comportaments anòmals. L'objectiu és el de protegir de manera proactiva els recursos sensibles sense afectar els usuaris autèntics.	**(D)**
15	En relació amb els punts anteriors (9,14a i 14b) la plataforma ha d' incloure solucions d'autenticació sense contrasenya basades en regles, escenaris o dispositius registrats, orientades a facilitar l'experiència dels usuaris en l'accés als serveis i aplicacions.	**(D)**

[1] Widget: Petita aplicació o programa que són executats per un motor de ginys o Widget Engine. Entre els seus objectius estan donar fàcil accés a funcions freqüentment utilitzades i proveir informació visual. Els widgets solen ser utilitzats per ser "encastats" en una altra pàgina web

16	La plataforma ha de disposar d'un ampli catàleg d'integracions predefinides amb aplicacions i serveis, ja disponibles com a opció del producte. Ha de proporcionar connectors ja disponibles cap a aplicacions empresarials populars on, com a mínim hi ha d'haver **totes** les següents: 1. Salesforce 2. Zoom 3. Google Workspace user and devices administration 4. Google Gmail 5. Google Drive 6. Google Calendar 7. Google Cloud 8. Google Docs per a interaccionar amb documents a Google Docs 9. Google Sheets per a gestionar events i autoritzacions i fer accions a Google Sheets 10. Liferay 11. Microsoft (Office) 365 12. Azure Active Directory 13. Adobe User Management 14. Atlassian (Jira i Jira Service Management) 15. AWS S3 16. AWS Lambda 17. AWS Multi-Account Access 18. Excel online per a autoritzar i fer accions a l'Excel online 19. Microsoft Teams 20. Microsoft Onedrive 21. OpenAI 22. Oracle HCM 23. Sendgrid 24. SFTP 25. ASANA	**(I)**
17	Cal que la plataforma es pugui integrar amb sistemes SIEM (Security Information and Event Management) per millorar la seguretat i la visibilitat en la infraestructura TI de la Universitat. Això es pot fer mitjançant l'enviament dels logs d'auditoria que contenen informació detallada sobre els esdeveniments de seguretat, com ara intents d'inici de sessió, canvis de contrasenya, assignacions d'aplicacions i altres esdeveniments d'administració o mitjançant APIs que permeten l'extracció de dades d'esdeveniments de seguretat.	**(I)**
18	Cal que la plataforma permeti la integració, de manera nativa, amb serveis EDR (Endpoint Detection and Response) per augmentar la seguretat general de la Universitat, combinant la gestió d'identitats amb les capacitats de detecció i resposta d'amenaces en els llocs de treball (endpoints) proporcionades pels serveis EDR i permetent enviar a la plataforma les senyals recollides per l'EDR i avaluar-les amb les polítiques d'autenticació i seguretat que s'hagin configurat.	**(I)**
19	La plataforma nativa que es serveix com a IDaaS ha d'incloure tots els elements necessaris per a cobrir el servei, tant per a la gestió d'identitats com per a la gestió i autorització d'accessos de manera que no calgui desplegar part dels components en local o altres ubicacions diferents.	**(I)**

20	La solució adjudicada i a implementar, per al seu funcionament, no pot tenir ni generar necessitat d'altres despeses que no siguin les explícitament contemplades en els documents d'aquesta licitació (invitació)	**(I)**

Ref.	**B. Motor d'Identitat, casos d'ús a integrar i configurar**	**Tipus**
1	Implementar la gestió d'usuaris: cada usuari ha de disposar d'un perfil únic dins la plataforma. Cal poder gestionar els usuaris en grups o individualment.	**(I)**
2a	Integració amb directoris des de CSV: integrar directoris, com a mínim l'Active Directory (AD) i Lightweight Directory Access Protocol (LDAP).	**(I)**
2b	Disposar d'una opció que permeti crear integracions personalitzades per a sistemes locals des de fitxers CSV, que contenen identitats d'usuari. Mitjançant aquest component, s'ha de poder ingerir aquests fitxers de manera recurrent, important usuaris i els seus atributs a la gestió d'identitats i als directoris (Active Directory i LDAP). Ha de permetre totes les funcionalitats disponibles en altres fonts com ara el mateix Active Directory, que inclouen importacions programades, a nivell d'atributs, regles de concordança i un conjunt ric de possibles atributs d'usuari.	**(I)**
3	Disposar d'una llançadora o portal d'aplicacions que incorpori les aplicacions amb les que l'eina ja s'integra de manera nativa i que s'hi puguin configurar de manera personalitzada les de la Universitat	**(D)**
4	Ha de permetre assignar usuaris administradors per gestionar i mantenir tots els aspectes de l'experiència de l'usuari final dins la Universitat.	**(I)**
5	Zones de xarxa: ha de poder definir perímetres de seguretat al voltant dels quals poder restringir o limitar l'accés dels usuaris a la nostra organització.	**(I)**
6	Polítiques i regles d'inici de sessió: poder disposar d'una política de sessió global i polítiques d'autenticació. El motor de gestió de la identitat ha de requerir que es satisfacin aquestes polítiques abans que l'usuari final accedeixi a una aplicació.	**(I)**
7	L'autenticació multifactor ha de disposar de la possibilitat de configurar els "autenticadors" que els usuaris han de proporcionar per a la verificació per part d'una aplicació o servei.	**(I)**
8	Permetre la puntuació de riscos de manera que es proporcioni un motor de control de riscos que permeti determinar la probabilitat d'un esdeveniment d'inici de sessió anòmal.	**(I)**
9	La plataforma ha d'estar monitoritzada en el seu funcionament i disponibilitat les 24h del dia, de cada dia de la setmana i de l'any.	**(I)**
10	Ha de disposar d'informes i consultes del registre del sistema sobre l'assignació d'aplicacions, l'accés a les aplicacions, l'aprovisionament (altes) i modificació, baixa o desactivació dels usuaris.	**(I)**
11	Cal que ofereixi informes, lligats amb alertes de seguretat i possibles accions automatitzades, que permetin ajudar a detectar possibles riscos de seguretat i a entendre com els usuaris consumeixen les aplicacions i serveis.	**(I)**

12	La plataforma oferirà una aplicació d'autenticació multifactor (MFA) disponible en els principals dispositius (Ordinadors, tauletes, dispositius mòbils i smartphones) i sistemes operatius (Windows, Linux, MacOS, IOS, Android, etc.) que permeti als usuaris confirmar la seva identitat quan inicien sessió al seu compte o accedeixen a recursos protegits i que s'integri amb els diferents serveis de la plataforma o inclús en serveis de tercers.	**(I)**

Ref.	**C. Fluxos de treball: processos d'identitat complexos amb una plataforma d'automatització i orquestració sense codi (no code/low code)**	**Tipus**
1a	L'eina de fluxos de treball ha de permetre amb una desenvolupament sense codi (no code o low code) provisionar (donar d'alta) i donar de baixa comptes d'aplicacions. Això vol dir: tant crear automàticament la identitat de l'usuari a les aplicacions com establir els permisos d'usuari i de grup i assignar espais de carpeta.	**(I)**
1b	De manera anàloga quan un usuari deixa la relació amb la Universitat cal poder desactivar el compte d'usuari, transferint els seus actius digitals a un gestor i després desactivar el compte d'usuari després d'un temps de cortesia.	**(I)**
2	L'eina de fluxos de treball de la plataforma ha de permetre seqüenciar accions amb lògica i temporització. Cal poder crear comptes no activats en les aplicacions, un temps abans de la data d'inici d'un nou usuari, i després activar-lo el primer dia que li correspongui començar a la Universitat	**(I)**
3	Enviar notificacions per als diferents esdeveniments del cicle de vida. Per a un esdeveniment del cicle de vida, com ara l'assignació d'una aplicació o la suspensió d'un usuari, l'eina de fluxos de treball ha de poder enviar una notificació als interessats a través de correu electrònic i altres eines de comunicació (sms, slack).	**(I)**
4	Registrar i compartir els esdeveniments del cicle de vida. L'eina de fluxos de treball ha de poder consultar les API de la plataforma i els esdeveniments del Registre del Sistema i executar lògica (tasques, accions i operacions lògiques) si s'escau i notificar-ho per correu electrònic als nostres equips o responsables de l'event.	**(D)**
5	Cal que la plataforma disposi de plantilles predefinides de fluxos de treball que, a part de poder-se utilitzar, mostrin les possibilitat i funcionalitats de la pròpia eina per tal de definir-ne d'altres. Ha de disposar d'alguna mena de col·lecció o catàleg de plantilles que puguem adaptar fàcilment per satisfer les necessitats de la Universitat. El catàleg cal que estigui dirigit a casos d'ús que incloguin la provisió d'usuaris i la gestió d'identitats.	**(I)**

Ref.	**D. Prestació del servei**	**Tipus**
1	S'ha de proveir un servei de suport en l'ús de la plataforma als usuaris administradors de l'eina, ja siguin personal d'informàtica de la UPF com usuaris amb perfil administrador de la UPF.	**(I)**

2	S'ha de proveir als administradors de la plataforma a la UPF un servei de suport 24x7 tots els dies de la setmana amb els requeriments de l'annex d'ENS del Plec de clàusules administratives particulars.	**(I)**
3	S'ha de proporcionar suport des d'una plataforma de tíqueting o correu electrònic.	**(I)**
5	Cal proporcionar en tot moment un entorn de preproducció o sandbox per a poder fer proves i comprovar les novetats i canvis abans no es despleguin a l'entorn de producció	**(I)**
6	S'haurà d'implementar en el termini d'1 mes des de la formalització del contracte un portal contrasenyes multi-idioma (català, castellà, anglès), específic per a la UPF, que ha de permetre la gestió de la contrasenya i la possibilitat de recuperar la contrasenya (fer reset) en cas d'oblit o la primera vegada que s'accedeix	**(I)**

1. Altres característiques de la llicència

Disposar lde llicenciament de tipus empresarial (Enterprise) específic pel món educatiu amb nombre personalitzat de connexions i nivells (tiers) que han de permetre connexions amb la plataforma, rols i accions d'administració per tota la comunitat Universitària en forma de nombre d'usuaris actius mensuals o MAU (Montly active Users), possibilitat d'anar creixent de forma escalada i per trams en cas de necessitat.

Ha d'incloure complements com protecció contra atacs i certificacions HIPAA BAA (Business Acces Agreement) & PCI (customers' payment information), requerits per organismes internacionals amb els que la Universitat col.labora.

La subscripció ha d'incloure uns Identificadors únics (SKU) per llicència, botiga d'usuaris, autenticació, autorització bàsica, multifactor d'autenticació (MFA) bàsic, rols d'administrador i registre i polítiques bàsiques de sessió d'usuari.

Les SKU han d'incloure capacitats o funcionalitats de: directori, inici de sessió únic (SSO), autenticació social, contrasenya d'un sol ús (OTP: One-Time Password), gestió d'API limitada a un servidor d'autorització i funcions de personalització de la interfície d'usuari.

La plataforma ha de permetre la gestió del cicle de vida de la identitat de l'usuari a totes les aplicacions pròpies i externes ja estiguin en local o al núvol. Els usuaris i els seus dispositius cal que disposin d'accés gairebé instantani a les aplicacions i serveis que necessitin.

El repositori central de la plataforma, el directori, ha de tenir en compte el cicle de vida d'un usuari que pot ser: activat, suspès, desactivat i suprimit, en funció dels esdeveniments de canvi d'estat del cicle de vida.

- Activat: Usuari d'alta amb els seus perfils i rols actius que pot accedir a tots els recursos, serveis i aplicacions que se li han definit segons els perfils, rols i grups als que pertany.
- Desactivat. usuari d'alta però al que encara no se li permet accedir als recursos, serveis i aplicacions.
- Suspès. Usuari a la plataforma al que se li han suspès o bloquejat temporalment l'accés als recursos, serveis i aplicacions.
- Suprimit. Usuari que al que s'ha donat de baixa tot i que mantenim la informació dels perfils, rols, grups i recursos, serveis i aplicacions als que havia tingut permís i accés.

Els equips informàtics han de poder crear fluxos d'autoservei CIAM (Customer Identity and Access Management)) que envien i gestionen una sol·licitud d'accés a una aplicació, servei o responsable final.

Dins de la gestió del cicle de vida (LCM Life cycle management) cal disposar de les següents funcions o característiques:

- Regles de pertinença al grup: en funció dels atributs dels usuaris (per exemple, posició/departament/geografia), un usuari es pot assignar automàticament a un grup determinat donant dret a l'usuari a un determinat conjunt d'aplicacions i drets dins de l'aplicació.
- Aplicacions com a font (apps as source): connectors ja existents que permeten obtenir els atributs d'usuari dins del directori propagant canvis d'atributs o actualitzacions, en cas necessari. Els administradors cal que puguin definir la prioritat de les fonts del perfil d'una tipologia d'usuari.
- Obtenció a nivell d'atributs: la capacitat d'obtenir diferents atributs d'un mateix usuari de diferents fonts autoritatives. Un usuari pot tenir els seus atributs definits per varies fonts.
- Flux de treball de sol·licitud d'accés: flux de treball de sol·licitud d'accés d'autoservei de diversos passos on els usuaris poden sol·licitar qualsevol aplicació del catàleg d'aplicacions que no tinguin i les sol·licituds s'envien automàticament als responsables adequats dins o fora del Servei d'Informàtica.

L'activació de la subscripció per a la gestió del cicle de vida cal què es mesuri pel nombre d'usuaris en un estat actiu assignats a aplicacions que tenen la provisió activada o equivalent incloent els fluxos de treball de sol·licitud d'accés.

2. Localització física i característiques de la plataforma

El servei es prestarà en modalitat servei (SaaS) amb els mitjans de que disposi el propi proveïdor o de tercers. Els servidors i infraestructures amb els que se suportin els serveis estaran ubicats dins la Unió Europea i les dades s'ubicaran en tot moment a la Unió Europea. Així mateix, compliran el reglament i totes les normatives vigents en cada moment en matèria de protecció de dades i de propietat intel·lectual de la UE.

3. Manteniment i suport

L'empresa adjudicatària oferirà, durant tota la vigència del contracte, un servei d'atenció als administradors i al personal TIC que contempla:

- Avisar al personal de TI de les incidències que es produeixin en el servei.
- Atenció per a atendre consultes i la resolució de problemes o incidències en el servei i la plataforma i siguin comunicades pels administradors i personal de TI de la UPF.
- Avisar, per part del proveïdor, de les accions de manteniment planificat que puguin tenir incidència en el servei.
- Comunicar els canvis evolutius del sistema, amb un mínim de 3 setmanes d'anticipació, indicant les accions que puguin requerir del personal de TI i informant dels canvis incorporats
- Lliurament d'informes de qualitat: continuïtat del servei, índex d'incidències i la seva durada.

A tal efecte l'adjudicatari i el responsable del contracte designaran els interlocutors.

El subministrador oferirà un servei d'atenció sobre l'ús de la plataforma, amb les eines definides anteriorment.

Cas que el proveïdor hagi de fer alguna actuació programada en el sistema que requereixi l'aturada del servei, ho notificarà als usuaris amb un mínim de quinze dies (15) dies d'antelació per tal de causar el menor inconvenient possible. Sempre que sigui possible, aquestes actuacions es planificaran dintre de períodes no lectius o entre les 23:00h i les 8:00h de la matinada (hora catalana). Amb aquesta finalitat proporcionarà informació sobre:

- La data i hora de l'aturada
- La durada estimada
- Els serveis o prestacions afectades

2. Implementació, configuració, adaptacions i desenvolupaments necessaris per la posada en marxa de la llicència d'ús de la plataforma de gestió d'identitats per la UPF

2.1 Objectius

La implantació de la nova Plataforma de gestió d'Identitats com a solució a la UPF té diversos objectius, a destacar:

- Modernizar la gestió i provisió d'accés als serveis i aplicacions amb un sistema CIAM (Customer Identity and Access Management).
- Obsolescència tecnològica de l'actual solució, Oracle Identity Manager (OIM) Problemes de disponibilitat, necessitat d'una plataforma estable.
- Gestió moderna de la identitat, amb una millor usabilitat i facilitat d'operació.
- Assentar les bases per simplificar la infraestructura CIAM (Customer Identity and Access Management), basada en un paradigma cloud (IDaaS) que permeti estalviar costos indirectes i una millora de l'eficiència i seguretat.

4. 2.2 Arquitectura actual

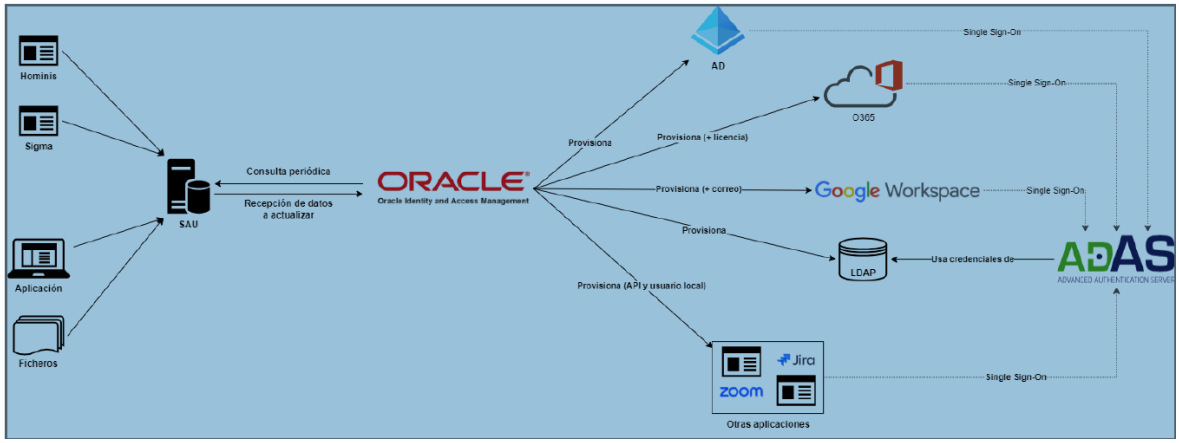
La solució actual de la UPF per a la gestió d'identitats és Oracle Identity Manager (OIM). OIM utilitza les identitats de SAU i les aprovisiona cap a la resta de sistemes. El procés d'aprovisionament d'aquestes identitats consisteix que, des de SAU, a les entrades d'usuari, tenen un camp a la base de dades que serveix per indicar que aquesta entrada conté algun tipus d'actualització, i aquesta actualització ha de ser replicada a OIM. D'altra banda, des d'OIM, té un job, que s'executa periòdicament, l'objectiu del qual és recórrer la informació d'usuari continguda a la base de dades de SAU i, quan troba aquest camp indicant que s'ha actualitzat informació, rèplica i actualitza els usuaris actualitzats a OIM.

Directoris i integracions que es provisionen des de OIM:

- LDAP
- Active Directory
- AdAS
- Microsoft 365
- Google
- Zoom
- Altres aplicacions que s'integren fent crides a l'API de l'aplicació (Jira, MS Insight, Liferay, etc.). Des d'OIM s'aprovisionen els usuaris d'aquestes aplicacions fent ús de les API pròpies i creant usuaris locals en ells.

L'objectiu principal del projecte serà substituir l'OIM per la nova plataforma de gestió d'identitats, per tant, caldrà migrar tota la funcionalitat que fa actualment OIM i addicionalment configurar el nou gestor com a solució de gestió d'identitats i accessos (IAM - Identity and Access Management)

En aquest diagrama es representa l'arquitectura actual:



Fonts autoritatives i el Servei d'Autenticació d'Usuaris

Pel que fa a l'origen de les identitats, hi ha diverses fonts autoritatives:

- Universitas XXI i Ulisses (desenvolupament propi) per les dades del personal (PDI i PTGAS).
- SIGMA per les dades dels estudiants.
- Formularis d'alta d'usuaris o càrregues a través de fitxers per a altres col·lectius i grups d'usuaris del grup UPF per exemple.

Totes aquestes dades provisionen identitats a un sistema propi anomenat SAU (Servei d'Autenticació d'Usuaris).

L'objectiu de SAU és unificar perfils en un únic sistema. A causa de la naturalesa de la UPF, hi ha la possibilitat que una identitat pugui tenir diversos perfils dins del sistema (perquè és o continua sent estudiant d'un màster o doctorat i passa a ser PDI o situacions similars). Per això aquest sistema s'encarrega de, quan s'hi aprovisionen identitats, detectar (de manera automàtica mitjançant un algorisme) si la identitat ja existeix al sistema i, en cas afirmatiu, vincula els diferents perfils dins d'una mateixa identitat.

2.3 Desenvolupament de la implantació

Per portar a terme les tasques esmentades en l'abast i tal i com s'ha descrit en l'inici de l'apartat. Caldrà dissenyar i presentar un pla de projecte que incorpori les diferents fases clau:

- Preparació i planificació.
    - Recopilació d'informació de la situació actual de la GID (gestió d'Identitats).
    - Anàlisi de les integracions a realitzar.
    - Anàlisi i disseny de la solució final.
    - Arquitectura tècnica de la solució final.
    - Sol·licitud d'infraestructura al núvol de la UPF per desplegar els components necessaris.
    - Definició i planificació de l'estratègia de migració.
- Implementació, personalització, integració, posada en explotació de la plataforma i del projecte de migració i gestió del servei.
    - Integracions amb els sistemes Actuals i SAU a mida: LDAP, AD, AdAS, Salesforce, Zoom, Google Workspace, Google Drive, Google Cloud, Liferay, suite d'Atlassian, Microsoft (Office) 365, Moodle, Azure Active Directory, Adobe User Management, AWS S3, AWS Lambda, AWS Multi-Account Access i d'altres aplicacions amb capa Rest (p.e. Insight, Liferay, JIRA) amb una lògica de negoci aplicable al grup UPF.
    - Migració de les funcionalitats disponibles a l'actual GID (gestió d'Identitats) d' Oracle cap a la nova plataforma.
    - Tancament del projecte d'implentació. Que ha d'incloure una formació a l'equip de tècnics de la UPF per transferir el know-how del projecte, com es descriu més endavant.

En cada funcionalitat o integració que s'implementi caldrà sempre fer la cobertura de proves i desplegaments; personalitzacions, posada en explotació i gestió del nou servei.

Al final de la implementació l'empresa haurà de fer entrega dels principals procediments operatius de les tasques més comunes per a monitoritzar, gestionar i fer funcionar la plataforma.

2.4 Formació

Caldrà realitzar una formació per als administradors funcionals de la plataforma i pel personal TIC de la UPF responsable del servei.

Coincidint amb el desplegament del sistema (de manera coordinada dins les fases del procés d'implementació), s'organitzarà un curs en el que s'explicaran els detalls tècnics del desplegament, de la configuració del sistema i de totes les seves opcions, del manteniment del sistema i de les pautes d'actuació en cas de disfuncions o fallades.

Aquesta formació serà presencial o a distància.

L'horari de formació s'adaptarà a les necessitats de la UPF.

Aquesta formació haurà d'anar recolzada per tots els mitjans necessaris per tal d'obtenir els objectius esmentats, com ara pàgines web i manuals d'instruccions que caldrà mantenir actualitzats durant el període de vigència del contracte.

La durada de la formació serà d'un mínim de 8h repartides en dues o més sessions.

Les empreses licitadores han d'incloure a la seva proposta un pla de formació al personal responsable de la UPF en la gestió dels serveis contractats que ha d'incloure com a mínim els requeriments indicats anteriorment.

3. Servei evolutiu amb gestió de petits desenvolupaments que s'hagin de realitzar un cop implementada la solució

Disponibilitat d'una bossa d'hores mensual d'un equip o d'una oficina tècnica dins de l'empresa adjudicatària que pugui atendre es necessitats que tingui la UPF, ja sigui de suport en la implementació de noves integracions o fluxes de treball o d'efectuar canvis en els existents o que directament se li pugui encarregar que implementi aquestes noves necessitats.

Per a prestar aquesta part del servei s'haurà de disposar com a mínim d'un equip format per un consultor i un projecte manager i s'estima una dedicació mensual de 40h per al consultor i de 8h per al project manager.

S'haurà de donar resposta a les demandes de manera mensual en base a l'estimació d'hores establerta i així mateix, aquest servei es facturarà mensualment.

4. Calendari d'execució del projecte

4.1 Llicències

Les llicències s'han d'instal.lar l'1/11/2024 o el dia següent a la formalització del contracte si es fes en data posterior i tindran una vigència de 3 anys, amb les següents característiques evolutives, que es mesuren en usuaris mensuals actius (MAU), amb un mínim de 16.000 i un màxim de 20.000, considerant que durant l'estiu pot baixar aquest mínim, considerem 18.000 com a mitjana:

<table>
<tr><th>Període</th><th>Concepte</th><th>Unitats</th><th>Observacions</th></tr>
<tr><td rowspan="6">1r any</td><td>Subscripció de la versió enterprise del producte (i API)</td><td rowspan="4">100.000 MAU /any</td><td rowspan="6">Mentre es realitza la implementació són les llicències requerides</td></tr>
<tr><td>API* per integració del directori</td></tr>
<tr><td>API* d'accés únic (SSO) amb un mínim de 5 apps integrades i workflows il·limitats</td></tr>
<tr><td>API* de gestió del cicle de vida amb 10 Apps Integrades (mínim)</td></tr>
<tr><td>Suport de nivell silver (24x7x365) segons criteris descrits a l'annex d'ENS del plec de clàusules administratives particulars (PCAP)</td><td rowspan="2">Anual</td></tr>
<tr><td>Entorn de prova (sandbox)</td></tr>
<tr><td>2n any</td><td>Subscripció de la versió enterprise del producte (i API)</td><td>200.000</td><td></td></tr>
</table>

	API* per integració del directori	MAU /any	
	API* d'accés únic (SSO) amb un mínim de 5 apps integrades i workflows il·limitats		
	API* de gestió del cicle de vida amb 10 Apps Integrades (mínim)		
	Suport de nivell silver (24x7x365) segons criteris descrits a l'annex d'ENS del PCAP	Anual	
	Entorn de prova (sandbox)		
3r any	Subscripció de la versió enterprise del producte (i API)	200.000 MAU /any	En cas de necessitat es poden ampliar llicències
	API* per integració del directori		
	API* d'accés únic (SSO) amb un mínim de 5 apps integrades i workflows il·limitats		
	API* de gestió del cicle de vida amb 10 Apps Integrades (mínim)		
	Suport de nivell silver (24x7x365) segons criteris descrits a l'annex d'ENS del PCAP	Anual	
	Entorn de prova (sandbox)		

4.2. Serveis addicionals d'implementació

S'han d'iniciar en el moment en què s'instal.la la plataforma i s'hauran de completar en un termini màxim d'1 any.

4.3 Serveis evolutiu.

S'han de realitzar des de la fi de la implementació i fins a la fi de la durada del contracte.

5. Model de governança i gestió per a la prestació del servei

La UPF i l'empresa adjudicatària determinaran els procediments a seguir per tal de gestionar els diferents processos:

- Tecnològics (temes tècnics i personal de TI)
- Operatius (respecte als administradors i usuaris)
- Administratius (contractació i facturació)

Per a cada un dels tres processos es determinaran:

- Els interlocutors
- La via d'accés (mail, telèfon, videoconferència,....)
- Protocols de comunicació

6. Tancament i finalització del contracte

Un cop finalitzat el contracte, l'adjudicatària haurà de retornar les dades a la UPF i prestar-li el suport necessari per a fer la migració d'aquestes a la nova solució informàtica d'aquesta necessitat.

Jordi Mas Parareda
Cap de la Unitat de Desenvolupament i Operacions
Servei d'informàtica