CONTRACTE RELATIU AL SUBMINISTRAMENT SAAS DE LA SOLUCIÓ RIO EDUCATION I SERVEIS ASSOCIATS PER A LA UNIVERSITAT OBERTA DE CATALUNYA

EXPEDIENT HSE00014/2024

PROCEDIMENT OBERT
SUBJECTE A REGULACIÓ HARMONITZADA

PLEC DE PRESCRIPCIONS TÈCNIQUES

1. Antecedents i context

La Universitat Oberta de Catalunya (en endavant, “la UOC”) és una universitat innovadora, arrelada a Catalunya i oberta al món, que forma les persones al llarg de la vida contribuint al seu progrés i al de la societat, alhora que duu a terme recerca sobre la societat del coneixement. El seu model educatiu es basa en la personalització i l'acompanyament de l'estudiant mitjançant l'e-learning; en aquest sentit, es tracta de la primera universitat a la xarxa a l’estat espanyol.

La UOC vol ser una universitat que, connectada en xarxa amb la resta d'universitats del món, impulsa la construcció d'un espai global de coneixement i la recerca frontera en societat del coneixement. Innova en el model educatiu propi que se centra en l'estudiant, oferint una formació de qualitat i personalitzable, per fomentar la seva competitivitat i contribuir al progrés de la societat.

Dins de la universitat, l'Àrea de Tecnologia vetlla per la governabilitat dels Sistemes d’Informació i per l‘evolució tant del Campus Virtual com de les diferents eines que hi donen suport a la gestió.

Com a part de l’estratègia per apostar per solucions administrades sempre que sigui possible (SaaS), la solució RIO Education és la solució escollida en l’àmbit del Sistema d’Informació Estudiantil (SIS). És una plataforma que ofereix una sèrie de funcionalitats i serveis per a la gestió acadèmica i administrativa d’institucions educatives. Aquest procés de transformació s’ha d’executar d’acord a:

- Els reptes estratègics que ha fixat la institució.
- A les noves necessitats de flexibilització i agilitat en el desplegament de l’oferta formativa.
- Proporcionar estandardització, solidesa i eficiència a la gestió acadèmica.
- Modernitzar el parc tecnològic, eliminant obsolescència, creant sistemes d’acoblament feble resilients i fiables tot seguint el full de ruta d’arquitectura tecnològica que fixa l’àrea de Tecnologia.

Aquest procés de transformació, dins de la UOC, s’identifica com el projecte o iniciativa GAUDI.

2. Objecte del contracte

L'objecte de la licitació per a la compra de llicències de la solució de Rio Education inclou els següents aspectes:

- **Adquisició de llicències de la solució de Rio Education**: Aquesta part de l'objecte implica la compra de les llicències necessàries per utilitzar la plataforma de Rio Education sobre Salesforce Education Cloud. Aquesta solució pot incloure funcionalitats com a gestió acadèmica, e-learning, seguiment d'estudiants, comunicació, i altres serveis relacionats amb l'educació o qualsevol altre inclosa al producte.
- **Serveis professionals "RIO Services" sota demanda del fabricant:** Aquesta part de l'objecte inclou el suport tècnic expert directament del fabricant Rio Education, proporcionat a través del licitant i que pot incloure assistència tècnica experta per a la instal·lació, configuració, resolució d'incidències i actualitzacions del sistema entre altres.
- **Serveis professionals sota demanda de l'adjudicatari**: Aquesta part de l'objecte especifica la quantitat d'hores de suport o serveis especialitzats en l'ús i construcció de serveis sobre la plataforma per a complementar amb coneixement expert els projectes que es facin sobre la mateixa en cas que la complexitat ho requereixi. Aquest servei pot ser presencial, telefònic o en línia, i s'utilitza per resoldre dubtes, problemes tècnics o altres consultes relacionades amb l'ús de la solució de Rio Education i que ha de proporcionar el licitant.

En resum, l'objecte de la licitació és **adquirir llicències de la solució de Rio Education** juntament amb **serveis professionals sota demanda** per garantir una implementació i ús eficaços de la plataforma educativa. Aquest aprovisionament comprèn el dret d'ús per part de la UOC per àmbit intern sense facultat de cessió a tercers de les llicències indicades.

3. Abast de la prestació

3.1 Subministrament de llicències per a la plataforma Rio Education

L'adjudicatària subministrarà llicències de la plataforma RIO Education - Student Information System, amb els següents requeriments:

- Servei de manteniment estàndard del fabricant.
- Model de llicència Entreprise Org amb llicències d'usuari RIO il·limitades. El model d'escalat de la tarifa de llicència en els primers anys és més baixa, ja que està dimensionat en base a la planificació, de quan entra en producció el sistema acadèmic amb la totalitat d'estudiants.
- El model de desplegament del projecte de gestió acadèmica de la Universitat planteja una utilització progressiva del sistema acadèmic, en base a la incorporació dels estudiants i personal de gestió previst per les iniciatives a gestionar, per això hi ha imports inferiors de llicència durant els dos primers anys. Els dos primers anys es preveu la posta en marxa de CP's (Cursos Professionalitzadors) que tenen un volum d'estudiants molt menor (actualment uns 800). A partir del tercer any es planteja la incorporació dels Màsters Universitaris de la UOC, de tal forma que es planteja un model de preu de llicències que permet la cobertura de la totalitat de la gestió acadèmica dels estudiants de les iniciatives de CP i MU de la Universitat, així com del col·lectiu de docents i gestors necessaris, amb un escalat de preu en base a aquest desplegament previst
- Aquest model de llicència Enterprise inclou qualsevol tipologia d'usuari del producte, tant per llicències d'administració d'estudiants (Student Admin), com a llicències d'estudiants (Student) com de professor o facultat (Teacher/Faculty) o qualsevol altre tipus de llicència que disposi el producte (o mòduls addicionals) de la solució Rio Education.
- A mode de referència, la UOC disposa de com a mínim prop de 70.000 estudiants, més de 500 usuaris de facultat i més de 300 usuaris administradors als quals ha de poder donar servei, incloent qualsevol increment d'aquesta xifra d'usuaris, sense que això comporti cap increment de cost addicional per la UOC.
- Aquestes llicències del producte seran vàlides per a qualsevol entorn en el que es faci servir: desenvolupament, preproducció o producció.
- Les llicències han de ser vàlides per la versió del producte Rio Education del fabricant WDCI en l'entorn de Salesforce Education Cloud que és la que la UOC vol utilitzar en el seu desplegament.
- RIO garantirà que el producte estarà certificat sobre Education Cloud i tindrà com a mínim les mateixes funcionalitats que l'actual versió de Rio Education 3.15 sobre Salesforce EDA a data de 01/10/2024.
- La disposició de la llicència inclou l'existència de procediments de gestió d'incidents relatius, l'establiment de prioritats i la definició dels responsables referent a qualsevol incidència relativa a l'activació de la llicència.
- Rio ha de garantir que el seu producte és compatible amb l'estàndard de les funcionalitats disponibles en la plataforma de Salesforce Education Cloud sense requerir cap desenvolupament o customització adicional.
- L'empresa adjudicatària garantirà la continuïtat de la llicència de la versió requerida del programari al llarg de tota la vigència del contracte, sense perjudici de que aquesta deixi de tenir accés a aquesta, tal com s'indica a la Clàusula 33 del Plec de Clàusules Particulars.

3.2 Serveis professionals “RIO Services” sota demanda del fabricant.

L’adjudicatària haurà de proporcionar en el marc d’aquesta licitació una sèrie de serveis professionals associats a perfils especialistes del mateix fabricant Rio Education “RIO Services”. Aquests perfils i dedicació són necessaris per a poder assegurar i garantir la correcta implantació i configuració del producte de Rio Education, i assegurar que s’estan seguint els màxims estàndards de qualitat definits pel fabricant en la implantació del seu producte.

Aquests serveis corresponen a les necessitats de perfils experts i d’alta qualificació requerits en la implantació i configuració del producte RIO Education i són necessaris per a la UOC per tal de poder disposar del suport requerit durant la implantació del producte i garantir l’èxit d'aquesta. Les necessitats d'alta qualificació són aquelles que comporten les tasques d’anàlisi i consultoria de processos acadèmics i la seva implementació sobre la solució existent, l’auditoria, revisió, implementació de solucions o configuracions sobre la plataforma que afecten a sistemes crítics, a contextos d'alta concurrència, a processos on es tracten alts volums de dades, actuacions que tenen un alt component d'innovació tecnològica o bé suport en la resolució d'incidències i actualitzacions del sistema que afectin al producte.

Per poder proveïr aquests serveis, és necessari contractar una determinada capacitat de perfils professionals experts oferts pel fabricant Rio Education. La dimensió i composició dels perfils requerits està dimensionat en com a mínim 618 hores anuals de dedicació, d’acord amb la dedicació prevista per les tasques abans comentades. Aquestes hores inclouen les hores de suport expert de fabricant, ofertades pels licitadors (LOT1 i LOT2) en el plec de licitació de Gaudí.

Així mateix, l'adjudicatària haurà de proporcionar sota demanda serveis professionals del catàleg del mateix fabricant Rio Education “RIO Education Implementation Specialists” https://appexchange.salesforce.com/appxConsultingListingDetail?listingId=a0N30000009uRD3EAM per poder cobrir necessitats variables específiques d’alta qualificació en cas que sigui necessari. Les necessitats d'alta qualificació són aquelles que comporten l’auditoria, revisió o implementació de solucions i configuracions sobre la plataforma que afecten a sistemes crítics, a contextos d'alta concurrència, a processos on es tracten alts volums de dades, actuacions que tenen un alt component d'innovació tecnològica o bé suport en la resolució d'incidències i actualitzacions del sistema que afectin al producte. Per poder proveir aquests serveis, el fabricant Rio Education dóna la possibilitat de contractar serveis professionals RIO Services. La dimensió i composició variable d’aquests perfils és l'especificada en el PCP d'acord amb la màxima quantitat d'hores variables previstes.

3.3 Serveis professionals sota demanda de l’adjudicatari

La UOC pot requerir la realització de determinats desenvolupaments d'aplicacions UOC complexes sobre la plataforma RIO Education que requereixin la participació de personal expert en la plataforma amb les certificacions adients. L'adjudicatària haurà de poder proporcionar sota demanda els perfils requerits per portar a terme aquests desenvolupaments evolutius.

Aquest servei consistirà en la provisió sota demanda per part de l'adjudicatària de personal tècnic certificat en el producte RIO Education. L'adjudicatària haurà de proporcionar sota demanda, els següents perfils tècnics que hauran de complir amb la solvència tècnica que es relaciona al plec de clàusules particulars.

En concret, cal preveure activitats com ara:

- Suport i assessorament especialitzat.
- Realització de propostes d'arquitectura, anàlisis, consultories o diagnòstics.
- Desenvolupament i construcció de solucions finalistes específiques.
- Implantació de productes o serveis per cobrir necessitats específiques.

3.3.1 Desenvolupament i construcció

3.3.1.1 Desenvolupament i/o implantació

El servei de desenvolupament sota demanda permet la construcció tant de components com de sistemes digitals finalistes, així com la implantació d'algun producte o servei. Per a la seva correcta execució cal preveure, com a mínim, les tasques i activitats següents.

- Planificació, control i seguiment del projecte
  S'inclouen les activitats de control i seguiment centrades en la preparació, la monitorització de l'estat, la gestió de riscos, la resolució de problemes i el reporting a l'equip de projecte i, en especial, a la persona responsable per part de la UOC, al comité de seguiment i al de direcció del projecte. Aquestes activitats han de permetre fer l'adequat seguiment, corregir desviacions, gestionar riscos i problemes.

- Anàlisi i Disseny
  S'inclouen les activitats d'anàlisi de requeriments funcionals i tècnics, coordinadament amb l'equip UOC definit. S'inclouen també les activitats de disseny tècnic i funcional de la solució, amb especial atenció al disseny d'arquitectura que haurà de ser adequadament validat en els termes que s'estableixi. Igualment, les solucions amb interfícies i/o processos que tinguin impacte a la interacció de l'usuari final, han de passar per una correcta metodologia d'investigació amb usuaris (Research) i de processos de disseny, que assegurin un bon resultat tant en usabilitat com en accessibilitat, tal i com indica la normativa. El disseny de la solució inclourà la documentació necessària per a la seva implementació segons la normativa vigent a la UOC.

- Desenvolupament

S'inclouen les activitats de desenvolupament i construcció de la solució aplicant el model de qualitat UOC. Aquestes activitats de desenvolupament inclouen la codificació, les proves unitàries així com la documentació tècnica corresponent segons els formats i eines que la UOC especifiqui en la normativa corresponent. També s'inclouen les activitats d'integració amb altres sistemes existents, quan s'escaigui. El desenvolupament haurà de passar els controls automàtics de qualitat i de seguretat que estableix la normativa UOC.

- Implantació
  S'inclouen les activitats d'adaptació i configuració de tots els elements de la solució així com la introducció de les dades bàsiques per a una correcta operativització i prova en tots els entorns. Tanmateix, es poden incloure activitats de migració de dades i de migració d'aplicacions i/o funcionalitats quan correspongui.

- Proves
  S'inclouen en aquestes activitats el disseny, desenvolupament, suport, gestió i seguiment de les proves tant d'integració, funcionals, de regressió, de volum, de seguretat i d'adaptació de la solució a posar en producció. També s'inclouen totes les proves necessàries en el cas de migracions a noves versions de qualsevol producte base.
  Aquestes proves estaran encaminades a assegurar el correcte funcionament de la solució en la seva totalitat, tant de les diferents configuracions parcials com dels desenvolupaments, integració amb altres eines i adaptació als sistemes UOC. En tots els casos, s'aplicarà el model de qualitat vigent a la UOC.

- Suport Post-implantació
  S'inclouen les activitats de suport post-implantació tècnic i/o funcional necessàries per assegurar l'estabilitat dels desenvolupaments i/o funcionalitats posades en producció.
  Les activitats de suport poden ser requerides de manera tant presencial com remota.

- Gestió del Canvi
  S'inclouen les activitats derivades de la gestió del canvi habitual en qualsevol implementació o desenvolupament d'una eina informàtica o sistema d'informació.
  S'inclouen també dins d'aquest apartat el disseny, desenvolupament, planificació i formació tant als usuaris responsables de l'aplicació i l'establiment de mesures i polítiques de comunicació que minimitzen l'impacte de la implementació.

- Traspàs a manteniment
  S'inclouen les activitats destinades a traspassar el control del desenvolupament a l'equip estable de manteniment de les solucions UOC. Aquest traspàs es realitza durant la garantia del desenvolupament i finalitza en exhaurir-se el període de garantia.

3.3.1.2 Condicions per la valoració i execució de projectes

- Projectes amb abast tancat
  L'adjudicatària:
  - Construeix la definició detallada de l'abast (descripció de requisits/històries d'usuari).
  - Determina, a alt nivell, el disseny d'arquitectura.
  - Estima l'esforç en hores per cada requeriment/història d'usuari.
  - Determina la composició de l'equip de projecte.
  - Presenta l'oferta per l'execució del projecte que serà iterada amb la persona responsable designada per la UOC.
  - La direcció de la UOC accepta formalment l'oferta final, en un document d'acceptació que dóna fe d'aquest acció.

- Projectes àgils d'abast obert i esforç tancat
  L'adjudicatària:
  - Construeix la definició detallada de l'abast (descripció de requisits/històries d'usuari).
  - Determina, a alt nivell, el disseny d'arquitectura.
  - Determina la composició de l'equip de projecte.
  - Acorda amb la responsable UOC l'esforç mínim i màxim que ha de suposar cada sprint dins el projecte.
  - Realitza el projecte amb tants sprints com es puguin realitzar dins de l'esforç previst pel projecte.
  - Cada sprint finalitzat comptabilitzarà en el projecte amb el valor d'esforç pactat, independentment de l'esforç real que hagi suposat aconseguir-lo.
  - L'abast de cada sprint s'acordarà entre la responsable UOC i el cap de projecte de l'adjudicatària, sempre dins dels marges d'esforç mínim i màxim, i amb temps suficient per acordar l'esforç que suposa i no iniciar cap sprint que no tingui un valor acordat.

- Projectes àgils d'abast obert i esforç obert
  L'adjudicatària:
  - Construeix la definició detallada de l'abast (descripció de requisits/històries d'usuari).
  - Determina, a alt nivell, el disseny d'arquitectura.
  - Determina la composició de l'equip de projecte.
  - Acorda amb la responsable UOC l'esforç mínim i màxim que ha de suposar cada sprint dins el projecte.
  - Realitza el projecte. Al final de cada sprint, l'equip UOC determinarà si cal continuar amb el següent sprint. Quan es decideixi no continuar, es valorarà el projecte en la suma del valor dels sprints que ha executat l'adjudicatari.
  - Cada sprint finalitzat comptabilitzarà en el projecte amb el valor d'esforç pactat, independentment de l'esforç real que hagi suposat aconseguir-lo.
  - L'abast de cada sprint s'acordarà entre la responsable UOC i el cap de projecte de l'adjudicatària, sempre dins dels marges d'esforç mínim i màxim, i amb temps suficient per acordar l'esforç que suposa i no iniciar cap sprint que no tingui un valor acordat.

Amb independència del model d'execució triat per la UOC, les tasques i activitats que condueixen a disposar d'una valoració en esforç s'inclouen dins el servei recurrent i s'hauran de regir pels ANS següents:

- Propostes preliminars i d'alt nivell, que corresponen a una primera aproximació a la solució, al seu disseny d'arquitectura i rang d'esforç s'hauran de respondre en un termini màxim de 5 dies laborables, a partir de la data d'entrega de les necessitats per part de la Universitat a l'adjudicatària..
- Propostes detallades que corresponen a l'aproximació definitiva segons l'esquema mencionat anteriorment s'hauran de respondre en un termini màxim de 12 dies laborables, a partir de la data d'entrega de les necessitats per part de la Universitat a l'adjudicatària..

3.3.2 Realització de propostes d'arquitectura, anàlisis, consultoria i diagnòstics

La UOC podrà sol·licitar sota demanda la realització de propostes d'arquitectura, anàlisi de solucions, consultoria o diagnòstic.

Aquestes activitats seran sol·licitades i aprovades pels responsables interns UOC i el circuit d'execució serà:

- El responsable UOC descriu i realitza la petició.
- L'adjudicatària estima l'esforç en hores.
- El responsable UOC accepta la proposta i es fixa el calendari.

3.3.3 Assessorament especialitzat i actuacions extraordinàries

3.3.3.1 Assessorament

La UOC podrà solicitar sota demanda formacions expertes tant funcionals, com tecnològiques en qualsevol àmbit vinculat a l'objecte del contracte.

Els assessoraments seran sol·licitats i aprovats pels responsables interns UOC i el circuit d'execució serà:

- La UOC descriu la necessitat.
- L'adjudicatària presenta una composició d'equip i oferta.
- El responsable UOC accepta la proposta i es fixa el calendari
- Els materials generats/entregables seran propietat de la UOC qui ostenta la titularitat plena autoritzant el seu ús a l'adjudicatària i/o subcontractista exclusivament amb l'abast necessari per tal d'executar el servei durant la vigència

del present contracte d'acord amb la clàusula/apartat del PCP "Drets de propietat intel·lectual i industrial dels entregables i materials generats".

3.3.3.2 Formació

La UOC podrà sol·licitar sota demanda formacions expertes en les tecnologies que componen qualsevol de les plataformes objecte del plec.

Aquestes formacions estan adreçades a personal de la UOC o equips de projecte.

Les formacions seran sol·licitades i aprovades pels responsables interns UOC i el circuit d'execució serà:

- Conjuntament amb els responsables interns UOC del Servei, es fa la definició detallada de l'abast (descripció de mòduls formatius i exercicis).
- Conjuntament amb els responsables interns UOC del Servei, es determinen les necessitats tecnològiques per dur-la a terme, així com les infraestructures on es faran les formacions.
- Els materials generats per la formació, seran propietat de la UOC.
- L'adjudicatària estima l'esforç en hores.
- L'adjudicatària determina la composició de l'equip de formació.
- L'adjudicatària presenta l'oferta per l'execució de la formació.
- El responsable UOC accepta la proposta i es fixa el calendari.

3.3.3.3 Guàrdies i actuacions fora d'horari laboral/Suport funcional estès/Atenció especial en activitats clau

La guàrdia serà un servei sota demanda i consistirà en el suport per a cobrir la resolució d'incidències o donar suport a processos crítics de la UOC que, d'una manera o altra, fan ús de les plataformes digitals, fora de l'horari laboral. Aquest suport podrà ser requerit de forma presencial a les oficines de la UOC, encara que habitualment, no serà necessari.

També es podrà requerir sota demanda el suport a la realització d'activitats tècniques que s'hagin de realitzar fora de l'horari laboral (dilluns a divendres de 08:30 a 18:30 amb el calendari de festius de la ciutat de Barcelona).

La UOC avisaria amb 1 setmana d'antelació per actuacions planificades que necessitin supervisió i 8 hores per incidentals crítics que s'hagin d'atendre fora de l'horari laboral.

Sobre les actuacions fora d'horari s'aplicarà una tarifa equivalent a 1,5 multiplicat pel preu/hora per perfil requerit i gestionat a través de la part variable del contracte.

3.4 Perfils professionals

Per a la realització de qualsevol d'aquestes activitats, la UOC pot sol·licitar la confecció d'un equip amb qualsevol combinació dels perfils professionals següents:

- Cap de projecte
  - Responsable de dirigir i gestionar els projectes d'implementació de Salesforce Rio Education a la UOC. Coordina els recursos, supervisa els cronogrames, assegura que es compleixin els objectius del projecte i gestiona la comunicació amb els òrgans establerts de direcció i seguiment del projecte a més de la comunicació amb els interessats entre d'altres.
- Desenvolupador integrador RIO o Salesforce (DIRS)
  - Perfil amb capacitat per desenvolupar, integrar, desplegar solucions personalitzades i realitzar test dins de la plataforma Salesforce Rio Education per satisfer les necessitats específiques de la UOC.
- Consultor (CS)
  - Expert en la configuració i la personalització de la plataforma Salesforce i la solució Rio Education. Assessora la UOC sobre com millorar els processos acadèmics i administratius utilitzant la tecnologia Salesforce.
- Assegurament de la qualitat (QA)
  - Responsable d'assegurar la qualitat dels productes i els processos relacionats amb la implementació de Salesforce Rio Education a la UOC. Realitza proves funcionals, identifica i reporta errors i col·labora amb l'equip de desenvolupament per resoldre-los.
- Arquitecte (cloud o salesforce) (ARC)
  - Perfil especialista d'alt nivell capaç de dissenyar arquitectures complexes tenint en compte totes les variables (capacitat, sostenibilitat, gestió de l'obsolescència i del deute tècnic, costos, integracions, etc.).
  - Es requereix alguna de les certificacions indicadas al plec de clàusules particulars
- RIO Education Implementation Specialist
  - Perfil especialista certificat pel fabricant Rio Education amb capacitats de implementació, desenvolupament d'aplicacions, migració de dades, integració, suport o millores relatives al producte Rio Education sobre la plataforma Salesforce.

Els equips seran sol·licitats i aprovats pels responsables interns UOC i el circuit d'execució serà:

- La UOC configura necessitat d'equip i capacitat.
- L'adjudicatària proposa un equip i calendari.
- El responsable UOC accepta la proposta.

4. Condicions del subministrament

En el termini màxim de 15 dies de la data de cada comanda realitzada durant la vigència del contracte, l'adjudicatària haurà de lliurar a la UOC un certificat conforme el fabricant RIO Education ha registrat per a la UOC les llicències o serveis oficials del fabricant RIO Education demanats a la comanda.

Els subministraments relacionats en el punt 3.1 comprenen el dret d'ús amb els requeriments descrits a l'apartat 3 sense facultat de cessió a tercers l'ús de les llicències durant el període de contracte.

La UOC tindrà dret a l'ús del programari contractat sobre infraestructura Cloud de Salesforce Education Cloud al servei de la UOC.

Les característiques del servei i condicions d'ús d'aquest programari seran les estàndard establertes per l'empresa RIO Education, propietària del programari.

Les comunicacions tècniques, tant amb l'empresa adjudicatària com amb RIO Education, hauran de ser en algun dels següents idiomes: català, castellà o anglès.

Pel que fa als serveis professionals sota demanda expressats en els punts 3.2 i 3.3:

- L'adjudicatària configurarà l'equip sol·licitat en base a hores de dedicació per perfil sol·licitades, havent de disposar del mateix en un termini no superior a 20 dies naturals des de la petició formal.
- Els encàrrecs que es faran sota a aquest concepte estan orientats a la construcció d'equips tècnics que realitzaran configuracions sobre la plataforma sota la forma de projectes. La sol·licitud de servei es realitzarà indicant la configuració desitjada de l'equip en base als diferents perfils establerts i el temps de dedicació de cadascun d'ells. Aquesta sol·licitud es realitzarà a través de correu electrònic o JIRA (eina de gestió de peticions corporativa de la UOC) al responsable del servei de l'adjudicatària .
- L'adjudicatària s'encarregarà de fer arribar a la persona responsable del contracte un informe mensual que recollirà el conjunt de tasques realitzades, així com la

previsió per al següent període. Aquest informe s'haurà d'entregar, com a màxim, dins dels 10 primers dies naturals del mes següent. La UOC es reserva el dret de demanar canvis en els equips en cas que les tasques realitzades difereixin significativament de les previstes, prèvia justificació per part de la UOC. El canvi s'haurà de fer en un màxim de 10 dies naturals des de la sol·licitud per part de la UOC.

- L'adjudicatària tramitarà el servei del fabricant en un termini no superior a 15 dies des de la data de recepció de la petició.
- L'adjudicatària s'encarregarà de proporcionar els elements necessaris a la UOC perquè pugui tenir accés al Suport Tècnic del fabricant en cas necessari així com la totalitat dels serveis expressats en el punt 3.2 i 3.3.
- Els encàrrecs que es faran sota aquest concepte estan orientats a tasques de suport especialitzades per part del fabricant per cobrir actuacions d'alta complexitat tal i com s'han descrit en el punt 3.2. La sol·licitud es realitzarà a través de correu electrònic o JIRA al responsable del servei de l'adjudicatari.

5 Mecanismes de control i reporting

En aquest apartat es defineixen els mecanismes de control i reporting per assegurar els correctes indicadors que s'han de complir durant l'execució del projecte.

5.1 Acords de Nivell de Servei (ANS) del servei de suport post-implantació

Els ANS serviran per definir el compromís de servei acordat entre la UOC i l'adjudicatària del contracte i s'hauran d'aplicar els mecanismes de gestió necessaris per controlar el seu grau de compliment.

Cada ANS està determinat pels següents paràmetres:

- Indicadors de mesura.
- Valors acceptables pels indicadors.
- Objectiu de compliment de l'ANS.
- Freqüència de les mesures.

Acords de Nivell de Servei mínims

Els indicadors són els següents:

● Indicadors d'activitat: Mesuren volums i dedicació i són indicatius, sense estar sotmesos a cap ANS.

● Indicadors de Compromís: Mesuren el grau de compliment del servei en termes d'eficiència i efectivitat del servei i estan sotmesos a acords de nivell de servei:

- Temps d'avaluació i compromís de peticions.
- Temps màxim en circuit de les peticions.
- Temps de resolució de peticions.

Els valors i objectius de compliment mínims dels indicadors de compromís per les accions d'operació són:

Temps d'avaluació i compromís

Prioritat	Objectiu ANS	Objectiu Servei
Alta	6h	90%
Blocker, Critical	3h	95%
Minor, Trivial	25h	85%
Normal	16h	88%

Temps de resolució

Prioritat	Objectiu ANS	Objectiu Servei

Blocker , Critical	6h	95%
Alta	15h	90%
Normal	36h	88%
Minor, Trivial	60h	85%

Temps màxim en circuit

Prioritat	Objectiu ANS	Objectiu Servei
Blocker , Critical	12h	98%
Alta	90h	98%
Normal	90h	95%
Minor, Trivial	90h	95%

Les prioritats s'assignen a partir de l'avaluació de l'afectació de la incidència i el comportament dels serveis digital impactats, i pot ser modificada a posteriori pel gestor de la petició o per algun responsable UOC, si es considera oportú.

Es mesuraran els temps a partir del calendari laboral del servei, el seu horari i en visió servei (descomptant els temps en els quals la petició està pendent d'informació, o en espera d'actuació d'un tercer).

Model del càlcul dels ANS segons estats de Jira

ANS	Start Status	End Status	Pause Status
Temps d'avaluació i compromís	[Open]	[Closed] [En Valoració] [In progress] [Pendent Info] [Pendent OT] [Pendent PRE] [Pendent PRO] [Resolved]	[On Hold] [Pendent Info]
Temps de resolució	[In progress] [Open] [Pendent PRE] [Pendent PRO] [Reopened]	[Closed] [Resolved]	[On Hold] [Pendent Info] [Pendent OT] [Pendent PRE] [Pendent PRO]

Temps màxim en circuit	[In progress] [Open] [Pendent PRE] [Pendent PRO] [Reopened]	[Closed] [Resolved]	[On Hold] [Pendent Info] [Pendent OT] [Pendent PRE] [Pendent PRO]

6 Resolució de contracte

La resolució del contracte correspon al moment en el qual el Comitè de Direcció del projecte avalua l'estat d'assoliment dels objectius segons la metodologia descrita en aquest plec i determina si els incompliments de caràcter [GREU] fan inviable la consecució dels objectius. En aquest cas, el Comitè de Direcció pot determinar que cal iniciar el procés de resolució del contracte.

En cas d'acumular més de 5 penalitzacions de tipus GREU (no resoltes) al llarg de la durada del contracte, el comitè de direcció decidirà motivadament sobre la possible resolució del contracte.

El criteri per la resolució del contracte tindrà en compte els següents factors:

- No disposar de totes les funcionalitats del producte de Rio Education versió Salesforce EDA, desplegades sobre Salesforce Education Cloud.
- Incompliment en el subministrament de llicències per a la plataforma Rio Education.
- Incompliments en els serveis contractats sota demanda.
- Incompliments en el serveis contractats del fabricant.
- No respectar les condicions relatives a la subcontractació especificades al Plec de Clàusules Particulars.

- Addicionalment, serà d'aplicació la causa de resolució unilateral prevista al PCP.

Signa,

Sr. Enric Espejo Martínez
Director de l'Àrea de Tecnologia

Universitat Oberta de Catalunya

7 Annex - Principis de Tecnologia

7.1 Principis estratègics

1. Els **nous sistemes i aplicacions** es regiran pels principis de **cloud first** (i preferentment a **cloud públic**), **mobile first** (en el sentit de **multidispositiu**) i seran **data-centric** (la dada com a actiu més important de l'organització)

2. Si existeix un **SaaS**, utilitza'l

3. Si no existeix un **SaaS**, però existeixen productes:

    - Si és un **problema comú**, utilitza **Opensource**

    - Si és un **problema poc comú**, **compra**

4. Si no existeix, ets únic: **construeix**

    - sempre, redueix al mínim les línies de codi, ja que el codi d'avui serà el legacy de demà.

5. En construir, es farà sobre **serveis administrats** (això és, operació inclosa en el servei) de manera que et **focalitzis en la lògica de negoci**, en el **codi**. Això aplica tant:
    - als **building blocks** de desplegament: PaaS, CaaS, FaaS, SaaS per sobre de IaaS/VM
    - als **serveis existents en els clouds de referència**: serveis de notificacions, cues, CDN, storage, …, per sobre de solucions desenvolupades a mida

6. Ponderar sempre **tecnologia vs negoci**: la millor tecnologia no sempre és la millor solució per a l'organització → s'han de balancejar **aspectes tecnològics, de govern, funcionals, organitzatius i econòmics**

7.2 Principis sobre el disseny d'aplicacions

1. **Segregació de funcions/responsabilitats**: les aplicacions han d'estar estructuralment dividides en blocs independents per funcionalitats, processos de negoci o serveis, per tal d'**evitar els monòlits** → patró de microserveis:

    - Aquest principi és d'**aplicació a totes les capes**: la divisió lògica de les funcionalitats també s'hauria de correspondre a una divisió "física" en el desplegament → un servei, una base de dades

2. La **presentació** (client/frontend) i el **backend**/negoci estaran **desacoblats**. Veure concepte Component Tècnic.

3. **Orientació a serveis**. Les aplicacions poden ser consumides externament o bé han d'integrar-se amb 3rs. Els backend han d'exposar la seva funcionalitat de negoci via serveis per facilitar-ho. Aquests serveis seran, a més, fàcilment integrables en un '**API Gateway o Bus de Serveis (com Mulesoft)**, per a ser securitzats i governats de manera centralitzada.

4. **Emmagatzema a la memòria cau** tot allò que sigui possible. Per fer-ho, utilitza la tecnologia que millor s'adapti tant a client (html5 cache, localstorage , etc.) com a servidor (Redis, Varnish, Memcache, caché personalitzada, etc.)
5. **Desacobla** de la interfície d'usuari aquells **processos que consumeixin molts recursos** (cpu, ram) o que **puguin ser executats de manera asíncrona**: utilitza una **cua** que informi via **events** a un nou **procés** que s'executarà **sota demanda** i amb una concurrència X (preferiblement per a aquest cas d'ús utilitzarem tecnologies serverless)

6. Tingues present sempre la **compatibilitat cap a enrere dels teus serveis**: si exposes una API REST i actualitzes el teu servei, que sigui compatible amb versions anteriors per a evitar actualitzacions innecessàries als teus consumidors i d'aquesta manera poder evolucionar el servei lliurement.

7. **Dissenya** l'aplicació o servei tenint present els conceptes **d'elasticitat** (enlloc de per a suportar els pics de càrrega), **d'alta disponibilitat**, **d'alta concurrència** i ***zero downtime***.

8. Pensa en la **portabilitat de les aplicacions**, això és, que es puguin moure amb facilitat d'un cloud privat a un cloud públic, per exemple.

9. A l'hora de dissenyar el teu sistema cal incorporar **aspectes qualitatius al cicle de vida**:
    - **Proves** per a verificar la qualitat del codi, el suport de càrrega o requisits no funcionals del sistema. Veure Etapa d'anàlisi i disseny de proves
    - **Documentació detallada** del projecte (descripció d'arquitectura, document funcional, manual de desplegament, manual d'explotació, …).
    - **Control de versions**. El sistema en el seu conjunt ha de ser tractat com un producte amb les seves versions majors, menors, etc
    - **Desplegament automatitzat**, execució de proves automàtiques que verifiquin la instal·lació i integració contínua.

10. Si has d'emprar dades d'un altre sistema, millor consumeix-les via serveis. Les dades d'aquell sistema han de ser "l'**única font de la veritat**"
11. Delega les decisions d'autenticació, utilitzant o bé el protocol **SAML** o bé **OAuth** (si es tracta d'una SPA, aplicacions mòbils o bé d'APIs). Les decisions d'autorització s'haurien de prendre en l'àmbit de l'aplicació, però preferiblent amb les dades proporcionades pel sistema d'autenticació de la UOC (perfils, tipus d'usuari...).

7.3 Principis sobre la tecnologia

1. **Utilitza la tecnologia que millor encaixi al cas d'ús**, si cal combinant tecnologies, ja que en un mateix sistema en poden conviure diverses: per exemple, en dividir les aplicacions en serveis, no tots tenen perquè estar construïts en els mateixos llenguatges o utilitzar les mateixes bases de dades.

2. Els **serveis** (backend) exposaran el seu negoci preferentment **mitjançant REST i en format JSON**.

3. En el cas d'aplicacions web, **la presentació estarà construïda amb tecnologies estàtiques** (html5/javascript/css) i consumirà els serveis que li proporcioni el backend.

4. Davant solucions estàndards utilitzarem preferentment les tecnologies del **Full de Ruta Tecnològic**. Aquest fet no exclou que per a noves solucions es puguin utilitzar altres tecnologies, que eventualment passaran a formar-ne part.

5. **Planifica i gestiona l'obsolescència tecnològica** (sistemes operatius, middlewares, frameworks de desenvolupament, productes, ...): és una **inversió que reduirà riscos.**

6. Qualsevol **nou sistema creat, renovat o refactoritzat**, s'haurà de fer amb les versions més modernes de middlewares, llenguatges, frameworks, mòduls disponibles, i en cas de dubte, utilitzar versions LTS, sempre alineat amb el Full de Ruta de Programari.
7. De la mateixa manera s'ha de disposar d'un pla d'actualització i millora continua sobre els components tecnològics utilitzats.

7.4 Principis sobre el cost i manteniment de les solucions

1. **Cal tenir presents els costos d'infraestructura i el model de llicenciament** requerits per a posar en marxa una solució ja que representen un cost recurrent.

2. Pensa en els **costos** i en la seva **optimització:**

    1. **Monitoritza** els teus serveis per a identificar necessitats d'ampliació o reducció de recursos i poder ajustar els costos en conseqüència

    2. Arquitectura/dissenya les **càrregues de treball** amb els costos en ment

3. A l'hora de triar entre utilitzar un **producte** (opensource o comercial) o fer un **desenvolupament** a mida cal fer una avaluació del **cost vs. benefici** de l'opció triada respecte a les altres.
4. Pensa en l'**impacte d'actualització** que pugui tenir un canvi de sistema operatiu, middleware o producte allà on corre l'aplicació: quant **menys acoblament** amb el sistema de base i **utilitzant estàndards**, més senzilla serà l'actualització o l'ampliació de funcionalitats de l'aplicació.

8 Annex - Normativa de Lliurables

8.1 Introducció

Definim un lliurable com un objecte resultat de l'execució d'un projecte. Els lliurables els podem categoritzar com a lliurables de gestió del projecte que ens permeten fer el seguiment i control de projecte, o lliurables que esdevenen resultats de l'execució del projecte en sí mateixos, l'obtenció dels quals, és el motiu pel qual executem el projecte.

D'altra banda, es defineixen una sèrie d'artefactes del projecte què, tot i no ser lliurables, requerim que es mantinguin actualitzats al llarg del projecte per a garantir la correcta execució, seguiment i control del projecte.

Abast

La Normativa és aplicable a tot el cicle de vida d'un projecte.

8.2 Propòsit

L'objectiu de la Normativa de Lliurables és donar als diferents participants involucrats en el desenvolupament, integració, evolució o manteniment de software de la UOC, la normativa sobre els lliurables mínims que cal entregar en un projecte.

Es descriuen també aspectes generals normatius, terminis, nomenclatura i quins són els repositoris on desar cada tipus de lliurable.Per a cada un dels lliurables mínims normatius, es descriuen les fases i les fites associades

8.3 Audiència

Aquest Normatiu està dirigit a tots aquells proveïdors de l'Àrea de Tecnologia de la UOC que estiguin oferint els seus serveis actualment o ho vulguin fer en un futur així com per als membres de l'equip propi de l'Àrea de Tecnologia UOC.

8.4 Lliurables

En la fase inicial de validació del pla de projecte, es determinaran els entregables (i el contingut dels mateixos), que s'hauran d'anar lliurant per part del licitador en les diferents fases del projecte.

8.5 Normativa de lliurables

Els lliurables han de garantir els aspectes següents:

8.5.1 Aspectes generals sobre lliurament de documentació

- Tots els lliurables han de ser proporcionats en el format que defineixi la UOC i sobre les plataformes indicades en cada moment.
- Cal fer servir les eines que la UOC posa a disposició per a la gestió dels projectes. A la descripció de cada lliurable i de cada activitat s'indica quin és el repositori que cal fer servir.
- Tots els lliurables han de tenir un format que permeti la seva edició, incloent els diagrames incrustats als documents. Si es lliura un document pdf per algun motiu particular, caldrà lliurar una còpia en format editable.
- Els lliurables no han de contenir logotips de cap adjudicatària, només els logos corporatius vigents de la UOC.
- La UOC és la propietària de tots els lliurables elaborats pels diferents adjudicataris
- Tant a la documentació de projectes com a la d'aplicacions, cal mantenir el registre de lliurables actualitzat així com la resta d'artefactes descrits més endavant.
- Cal produir i mantenir actualitzada la documentació mínima que faciliti la correcta comprensió del projecte o el manteniment del servei.
- Els proveïdors de projectes mantindran actualitzada la documentació associada a un projecte fins a la finalització de la garantia del mateix. De la mateixa manera, el servei de manteniment d'una aplicació o sistema, haurà de mantenir actualitzats els lliurables corresponents fins a la devolució del servei.
- L'adjudicatària tindran accés a les aplicacions corporatives sempre amb el seu correu UOC

8.5.2 Lliurables i artefactes mínims obligatoris de cada fase del projecte

- A més a més dels lliurables destinats a la gestió del projecte, cal mantenir la documentació de les aplicacions o components implicats en el projecte.

- En fase de contractació del projecte, es poden requerir lliurables addicionals seguint recomanacions d'UX, Qualitat, Seguretat o Arquitectura, que caldrà afegir al registre de lliurables del projecte. Tal com s'indica en el punt 10.5, es definiran en la fase inicial del projecte.
- Quan un lliurable d'aplicació va acompanyat d'una "n" indica que cal fer tants lliurables d'aquell tipus com nombre d'aplicacions hi hagi implicades al projecte.
- Els artefactes de seguiment i control serveixen per a poder consultar en qualsevol moment l'estat del projecte. El proveïdor ha de mantenir actualitzats obligatòriament els artefactes el màxim possible.

9 Annex - Normativa de Qualitat

9.1 Introducció

La Normativa de Qualitat es basa en el Model de Qualitat de la UOC i n'extreu els indicadors bàsics i Normatius que s'han de complir i les condicions en les quals s'ha de fer.

9.2 Abast

La Normativa és aplicable a tot el cicle de vida d'un projecte o aplicació i durant tot el període que dura el contracte amb un proveïdor.

9.3 Propòsit

L'objectiu d'aquest document és donar a conèixer als col·laboradors de l'Àrea de Tecnologia la normativa que aplica als projectes en termes de qualitat. Aquesta normativa es basa en la (ISO/IEC 25010) System and software quality models i en l'ISTQB.

La missió és assegurar que, en termes generals, **els projectes SEMPRE milloren la qualitat dels sistemes d'informació de la UOC** basat en els estàndards oficials aplicant-los sobre el context de la UOC.

9.4 Audiència

Aquest Normatiu està dirigit a tots aquells proveïdors de l'Àrea de Tecnologia de la UOC que estiguin oferint els seus serveis actualment o ho vulguin fer en un futur i evidentment, per als membres de l'equip propi de l'Àrea de Tecnologia UOC.

9.5 Responsable de document

Els responsables d'aquest document es mostren a la capçalera del document.

9.6 Indicadors Normatius

La Normativa de l'Àrea de Tecnologia posa focus en el compliment dels següents Indicadors primaris d'obligat compliment.

Indicadors de Qualitat	Característiques relacionades	Categoria	Mètriques	Normatiu
Compliment de la doble A d'accessibilitat	Usabilitat - Accessibilitat	Accessibilitat	→ Compliment dels criteris de conformitat **a nivell de pàgina web** Per a cada un dels criteris de conformitat, s'avalua si: ● **passa:** la plana, per a aquest criteri, ha estat avaluada satisfactòriament. És a dir, no es detecta cap error d'aquest criteri. ● **no passa:** la plana, per aquest criteri, no ha estat avaluada satisfactòriament. És a dir, es detecta com a mínim un error d'aquest criteri. ● **N/A:** no s'ha pogut analitzar la plana per aquest criteri ja que no hi ha elements amb les característiques necessàries per fer les comprovacions requerides S'exclouen les planes on no és aplicable aquest criteri. → Compliment dels criteris de conformitat **a nivell d'Aplicació o lloc web (per a la declaració d'accessibilitat)** ● **Accessible - Conforme:** com a mínim un 90% de les planes han estat	**Les aplicacions (llocs web) que tenen interfície han d'estar catalogades com a "Accessible - Conforme".** **(S'informa aquest valor a la fitxa d'aplicació al camp "Accessible").codi font**

			avaluades satisfactòriament com a "passa" • **No Accessible - Parcialment Conforme**: entre el 50% i el 90% de les planes han estat avaluades satisfactòriament com a "passa" • **No Accessible - No conforme:** menys del 50% de les planes han estat avaluades satisfactòriament com a "passa" • **N/A**: L'Aplicació no té interfície.	
Quality Gate	Fiabilitat, Mantenibilitat, Seguretat	Anàlisi estàtic de codi font	Segons Quality Gate aplicada al repositori de Codi Font	**Ha de passar OK (SUCCESS) per poder promocionar a Producció**

Els indicadors principals es composen dels següents indicadors secundaris, també d'obligat compliment. Amb el compliment dels primaris, es compleixen directament els secundaris.

Indicadors de Qualitat	Característiques relacionades	Categoria	Mètriques	Normatiu

Rati de Seguretat	Seguretat	Anàlisi estàtic de codi font	A = 0 Vulnerabilitats B = com a mínim 1 Vulnerabilitat Minor C = com a mínim 1 Vulnerabilitat Major D = com a mínim 1 Vulnerabilitat Critical E = com a mínim1 Vulnerabilitat Blocker	Sempre que no s'especifiqui el contrari al projecte, si el resultat és: A poden promocionar d'entorns B,C,D,E no poden promocionar entre entorns

<table>
<tr>
<td>Cobertura de Codi</td>
<td>Fiabilitat</td>
<td>Anàlisi estàtic de codi font</td>
<td>(literal de Sonarqube)

It is a mix of Line coverage and Condition coverage.

Coverage = (CT + CF + LC)/(2*B + EL) where

• CT = conditions that have been evaluated to 'true' at least once
• CF = conditions that have been evaluated to 'false' at least once
• LC = covered lines = linestocover - uncovered_lines
• B = total number of conditions
• EL = total number of executable lines (lines_to_cover)

*Cobertura de línia i condition coverage no s'avaluen de forma independent.</td>
<td>
<table>
<tr><th colspan="5">TAULA RESUM COBERTURES DE CODI</th></tr>
<tr><td></td><td colspan="2">CODI NOU</td><td colspan="2">CODI LEGACY</td></tr>
<tr><td></td><td>New code</td><td>Overall Code</td><td>New code</td><td>Overall Code</td></tr>
<tr><td>NAQ ALT</td><td>80 %</td><td>30%</td><td>60 %</td><td>20%</td></tr>
<tr><td>NAQ MIG</td><td>60 %</td><td>15%</td><td>40 %</td><td>10%</td></tr>
<tr><td>NAQ BAIX</td><td>30 %</td><td>10%</td><td>20 %</td><td>5%</td></tr>
</table>
CODI NOU: (els components tècnics que es despleguen amb DEPLOY)
CODI LEGACY: (els components tècnics que es despleguem amb INSTALL o DISTRIBUCIO)

Cobertura > Cobertura Inicial al projecte
</td>
</tr>
</table>

Vulnerabilitats	Seguretat	Anàlisi estàtic de codi font	1. **BLOCKER** Bug with a high probability to impact the behavior of the application in production: memory leak, unclosed JDBC connection, ... The code MUST be immediately fixed. 2. **CRITICAL** Either a bug with a low probability to impact the behavior of the application in production or an issue which represents a security flaw: empty catch block, SQL injection, ... The code MUST be immediately reviewed. 3. **MAJOR** Quality flaw which can highly impact the developer productivity: uncovered piece of code, duplicated blocks, unused parameters, ... 4. **MINOR** Quality flaw which can slightly impact the developer	Sempre que no s'especifiqui el contrari al projecte, si el resultat és: Vulnerabilitats = 0; poden promocionar d'entorns Vulnerabilitats > 0; NO poden promocionar d'entorns

			productivity: lines should not be too long, "switch" statements should have at least 3 cases, ... 5. **INFO** Neither a bug nor a quality flaw, just a finding.	

Code Smells	Mantenibilitat	Anàlisi estàtic de codi font		Inclòs a l'Indicador Quality Gate
Nombre de Bugs al Codi	Fiabilitat	Anàlisi estàtic de codi font		Segons Quality Gate aplicada al repositori de Codi Font
Deute Tècnic	Mantenibilitat	Anàlisi estàtic de codi font		

Nombre de Defectes	Fiabilitat	Testing Funcional	1. Blocker = Defectes que bloquegen completament una funcionalitat de l'aplicació i no es pot accedir de cap manera 2. Critical = Defectes que bloquegen parcialment la funcionalitat de l'aplicació causant greus problemes per fer servir la funcionalitat 3. Major = Defectes greus que no bloquejen la funcionalitat 4. Normal = Defectes de criticitat mitja 5. Minor = Defectes de criticitat baixa 6. Trivial = Defectes estètics o ortogràfics	Veure Severitat dels Defectes

10 Annex. Normativa UX

10.1 Introducció

La normativa de UX estableix els requeriments, lliuraments i marc de treball a tenir en compte en els projectes de l'Àrea de Tecnologia, per assegurar que els clients i usuaris dels productes i serveis digitals desenvolupats i oferts per la UOC, tinguin una experiència d'usuari satisfactòria, incloent també com a experiència satisfactòria, l'accessibilitat, cuya normativa es troba ampliada a l'annex 13.

Aquesta normativa defineix, per tant:

- Requeriments en matèria de UX, frontend i accessibilitat
- Tipologia i característiques dels lliuraments UX d'Accessibilitat demanats
- Marc de treball de les activitats UX en els projectes

S'ha d'assegurar el seu compliment

- En les propostes de solució
- Durant l'execució dels projecte
- La definició i execució del pla de proves

El grau i abast del compliment s'ajustarà en funció de la naturalesa i objectius dels projectes, en consens entre les parts implicades.

10.2 Abast

Aquesta normativa s'aplica en tots aquells projectes, tasques i actuacions sobre productes digital on les seves interfícies i/o funcionalitats es vegin modificades i/o s'hagin de crear des de zero.

És a dir, s'aplica tant en projectes on l'objectiu sigui conceptualitzar un producte digital des de zero, així com en projectes/tasques consistents en modificar, evolucionar i/o afegir una funcionalitat, la implementació de la qual provoqui que les interfícies d'usuari s'hagin de modificar per poder donar solució a aquesta funcionalitat objecte del projecte/tasca.

La normativa s'aplica tant en productes a mida (nous o legacy), com en productes de mercat, i en productes per a usuaris de gestió com a usuaris client (estudiants, potencials estudiants, docents, etc).

En funció de les característiques del producte i del projecte/tasca, es podran fer excepcions a la normativa.

10.3 Propòsit

El propòsit de la normativa és, en últim terme, assegurar en la mesura del possible que els usuaris dels productes i serveis digitals de la UOC tinguin una bona experiència d'usuari, és a dir, que trobin els productes i serveis de la UOC fàcils d'utilitzar, útils, accessibles, agradables en el seu ús i amb sentit.

En la mesura que aquesta normativa es compleix, s'assegura el control dels riscos que poden provocar desviacions en l'objectiu d'oferir una bona experiència d'usuari als usuaris de la comunitat UOC.

10.4 Audiència

Aquesta normativa està dirigit a tots aquells proveïdors/partners de l'Àrea de Tecnologia de la UOC que estiguin oferint els seus serveis actualment o ho vulguin fer en un futur i evidentment, per als membres de l'equip propi de l'Àrea de Tecnologia UOC.

10.5 Requeriments UX, Front-end i accessibilitat

Aquests requeriments han de ser tinguts en compte per part del proveïdor/partner en els projectes que se'ls encarregui, s'ha d'assegurar que es planifiquin i executin el conjunt d'activitats i lliuraments necessàries pel seu compliment, i s'ha de poder evidenciar això en les fases de:

- Proposta de solució
- Kick-off
- Durant l'execució del projecte
- La definició i execució del pla de proves
- Tancament

L'objectiu d'aquesta Taula i la seva inclusió en les fases anteriors són:

- Conjuntament amb el Lead UX de cada GO, definir i decidir, en las fases de maduració de la iniciativa, tot allò que pot permetre tenir un impacte en la millora de la UX i en la consecució dels objectius de la iniciativa, així com les activitats i lliurables necessaris per aconseguir-ho
- Possibilitar al Lead UX dels GO la participació en la maduració d'iniciatives
- Alinear expectatives entre Proveïdor, Lead UX dels GO, Cap de projecte i Negoci en matèria d'UX
- Facilitar l'explicació de riscos i costos d'oportunitat
- Facilitar la presa de decisions sobre què entra en l'abast i què no
- Compartir amb Negoci l'abast de les activitats UX i la seva justificació
- Assegurar la traçabilitat de l'abast, plantejament d'objectius i consecució d'objectius

Cal destacar que no cal que tots els projectes han de complir amb tots els requeriments, ja que dependrà del context, objectiu i abast de cada projecte, però s'ha de poder explicar i justificar per què no es compleix amb un requeriment determinat, si es complirà a mitges, o com es complirà. Per exemple, dins de la taula ja es planteja els escenaris amb actuacions sobre aplicacions legacy i productes de mercat.

El responsable de què aquesta taula estigui inclosa és el Responsable UX del servei. i la valida el Lead UX del GO corresponent.

A continuació, la Taula de requeriments:

REQUERIMENTS	DESCRIPCIÓ	EVIDÈNCIES

Disseny Centrat en l'Usuari (ISO 9241-210:2019)	Rellevant per projectes de transformació o d'alt impacte en la UX i en el disseny de servei • El disseny està basat en una comprensió explícita d'usuaris , tasques i entorns. • Els usuaris estan involucrats durant el disseny i el desenvolupament. • El disseny està dirigit i refinat per avaluacions centrades en usuaris. • El procés és iteratiu. • El disseny està dirigit a tota l'experiència de l'usuari. • L'equip de disseny inclou habilitats i perspectives multidisciplinars. Aplicable també en productes legacy i productes de mercat que contempli certes possibilitats de personalització i/o tinguin impacte en el disseny i/o l'experiència d'ús d'un servei digital.	Existeix fase de research amb metodologies com entrevistes, workshops, benchmarking, design thinking, card sorting etc. amb usuaris final, a més d'un informe de resultats del research i/o un entregable que permet entendre i conèixer les necessitats de l'usuari final (intern o extern) com Service Blueprint, Roadmaps, Journeys, Personas/Jobs to be done, Escenaris. etc. Existeixen activitats adreçades a l'avaluació de la UX, com test d'usabilitat, guerrilla test, heurístic, etc, a més d'un informe de resultats. Es fa ús dels entregables mencionats en els punts anteriors que procedeixen d'altres projectes. Existeixen iteracions previstes amb usuaris finals i està explicitat en la planificació. Existeixen iteracions previstes sobre el producte, està descrit la naturalesa de les mateixes, i està explicitat en la planificació. Existeix el detall dels perfils inclosos en l'execució del projecte (researcher, UI, UX, etc).

Usabilitat i disseny d'interacció	Ús d'estàndards , bones pràctiques, i principis bàsics d'usabilitat i interacció Aplicació d'heurístics de Nielsen. Disseny d'interacció homogeni amb la resta d'espais digitals de la UOC i la guia d'estil UOC En aplicaciones legacy i de mercat amb poques capacitats de personalització, es prioritza el disseny d'interacció proposat per la pròpia aplicació per preservar la homogeneïtat de la UX dins de l'aplicació.	Existeix un test usabilitat/test guerrilla, en desktop i responsive, amb usuaris finals amb un informe de resultats. Existeix un heurístic, en desktop i responsive, amb un informe de resultats. Les decisions sobre disseny d'interacció i usabilitat estan justificades en el user research, benchmarking i/o bones pràctiques. Existeix un lliurable de wirerame i/o disseny gràfic i funcional d'interacció El perfil UX/UI del proveïdor revisa i valida les diferents iteracions del producte/lliurable i el resultat final El Lead UX de AT revisa i valida les diferents iteracions del producte/lliurable i el resultat final. El responsable de negoci valida el resultat final del producte/lliurable.

Layout, estructura, navigation, AI	El producte/eina digital ha de poder oferir un layout d'interfície (estructura i ubicació d'elements en la interfície) igual o similar als layouts ja existents en el conjunt d'espais web de la UOC. El producte/eina digital ha de poder oferir una navegació igual a les ja existents en el conjunt d'espais web de la UOC En desktop, 12 columnes a 1200 pixels. En aplicacions legacy i de mercat amb poques capacitats de personalització, es prioritza el layout i navegació proposat per la propia aplicació, per preservar la homogeneïtat de la UX dins de l'aplicació	Existeix un lliurable de wireframe i/o disseny gràfic, i funcional d'interacció Existeix un lliurable d 'arbre de continguts, arquitectura d'informació, o similar. El perfil UX/UI del proveïdor revisa i valida les diferents iteracions del producte/lliurable i el resultat final El Lead UX de AT ha revisa i valida les diferents iteracions del producte/lliurable i el resultat final. El responsable de negoci valida el resultat final del producte/lliurable.
Estil gràfic	La interfície gràfica segueix els estils gràfics de la UOC indicats en la Guia d'estil UOC.	Existeix un lliurable de disseny gràfic. Existeix un lliurable de front-end amb l'estil gràfic aplicat. El perfil UX/UI del proveïdor revisa i valida les diferents iteracions del producte/lliurable i el resultat final El Lead UX de AT ha revisa i valida les diferents iteracions del producte/lliurable i el resultat final.

		El responsable de negoci valida el resultat final del producte/lliurable
Front-end	L'eina permet escollir un framework per desenvolupar un tema propi. En cas de no ser possible realitzar certes personalitzacions, s'ha de complir amb les millors pràctiques del mercat. Es fa càrrega asíncrona i els arxius JS estan minimitzats i optimitzats. HTML vàlid (demostrable a https://validator.w3.org/) o HTML5 semàntic, basat en estàndards internacionals de W3C (https://www.w3.org/standards/) En aplicacions legacy, el front-end resultant és continuïsta amb el de l'aplicació.	Existeix un entregable de front-end

Responsive	Si l'eina és una webapp, haurà de ser responsive per als 4 mínims punts de tall (breakpoints) descrits a la Normativa per als diferents Viewports; XS, SM, MD, LG. (Viewport XL, opcional). En desktop, 12 columnes a 1200 pixels. Es persegueix trobar dissenys responsive, no únicament adaptatius. Les aplicacions legacy o de mercat són les que determinaran les capacitats de responsiveness.	Existeix un lliurable de wireframe i/o disseny gràfic on es pugui visualitzar la interfície responsive. Existeix un entregable de front-end on es visualitza la interfície responsive. El perfil UX/UI del proveïdor revisa i valida les diferents iteracions del producte/lliurable i el resultat final El Lead UX de AT ha revisa i valida les diferents iteracions del producte/lliurable i el resultat final. El responsable de negoci valida el resultat final del producte/lliurable
Crossbrowsing	L'eina haurà de tenir una correcta visualització i compatibilitat amb els principals navegadors de mercat. ● Desktop (dues últimes versions dels navegadores): ○ Windows: Chrome, Firefox i Edge (ie11, navegable. Es conserva i s'asegura l'accés al contingut)	Existeix un lliurable on es demostra la correcta visualització en els diferents navegadors del producte entregat.

	○ iOS: Chrome, Firefox o Safari ○ Linux: Firefox ● Tablets / Mobile: ○ Android - Android Browser, Chrome ○ iOS - Safari	
Perfomance i Optimització	Bon rendiment, mesurat amb PageSpeed Insights: ● Per sobre de 89%. ● Entre el 90 i el 100% ● 100% en desenvolupaments nous. Optimització: Icones en format font o svg, CSS optimitzades i minimitzades.	Existeix un lliurable on es demostra la correcta performance del producte entregat.
Multidioma	La plataforma haurà de ser multi-idioma, i hauran d'estar disponibles en els idiomes: català, castellà i anglès. Així doncs, haurà de ser compatible amb caràcters llatins com pot ser el cas dels accents, la "ñ" i la "ç" (UTF-8)	-

Accessibilitat	Compliment de les pautes d'accessibilitat per a les pàgines webs, aconseguint com a mínim el nivell AA de les directrius d'accessibilitat per a continguts web 2.0 del W3C / WAI. Compliment de la Norma UNE-EN 301549 V3.2.1:2022, "Requisits d'accessibilitat de productes i serveis TIC aplicables a la contractació pública a Europa "-" Accessibility requirements suitable for public procurement of ICT products and services in Europe". Es contempla només l'accessibilitat que correspongui a l'abast de l'actuació, no al conjunt de la aplicació on es preveu fer l'actuació.	Existeix el lliurable anotacions d'accessibilitat Existeix un informe de conformitat Existeix un test-run d'accessibilitat i informe de proves corresponent.

11 Annex. Normativa d'Accessibilitat

11.1 Introducció

La UOC està des dels seus orígens compromesa amb la inclusió social de les persones amb discapacitat, i per tant procura facilitar l'accessibilitat de la universitat per a tothom qui vulgui formar part dels diferents col·lectius de la nostra comunitat (estudiants, docents col·laboradors, professorat i personal de gestió).

Tenint en compte que la UOC és una universitat privada que rep fons públics, ens és d'aplicació el RD 193/2023 de 21 de març, pel qual es regulen les condicions bàsiques d'accessibilitat i no discriminació de les persones amb discapacitat per a l'accés i utilització dels béns i serveis a la disposició del públic". Aquest Reial decret 193 /2023,

especifica que tots els llocs web i aplicacions mòbils el contingut de les quals es refereixi a béns i serveis a la disposició del públic han de complir amb la norma d'accessibilitat UNE-EN 301549.

A part, com a universitat cal tenir en compte el que estableix la "Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario", que estableix que "en matèria d'accessibilitat, les universitats han de garantir a persones amb discapacitat un accés universal als edificis i els seus entorns físics i virtuals, així com al procés d'ensenyament-aprenentatge i avaluació". Especialment i, tal com s'indica al Article 37. Equitat i no discriminació. Punt 2, d'aquesta mateixa llei Orgànica:

"Les universitats afavoriran que les estructures curriculars dels ensenyaments universitaris resultin inclusives i accessibles. En particular, adoptaran mesures d'acció positiva perquè l'estudiantat amb discapacitat pugui gaudir d'una educació universitària inclusiva, accessible i adaptable, en igualtat amb la resta de l'estudiantat, realitzant ajustos raonables, tant curriculars com metodològics, als materials didàctics, als mètodes d'ensenyament i al sistema d'avaluació.

Les universitats facilitaran a les persones usuàries de les llengües de signes la seva utilització quan es precisi".

Per tot això, tots els productes i serveis digitals de la UOC han de complir les pautes WCAG 2.1 publicades per la WAI al nivell AA (doble A), això vol dir què s'hauran de complir els punts de verificació de prioritat 1 i 2 de les pautes.

11.2 Abast

Aquesta Normativa estableix quins són els requisits que s'han de seguir en el desenvolupament de les interfícies web, en quant a criteris d'accessibilitat durant tot el cicle de vida d'un projecte o aplicació, marcant com a estàndard les pautes d'accessibilitat recollides a la WCAG 2.1 (Web Content Accessibility Guidelines) especificats en la norma EN 301 549 V3.2.1 (2021-03). Requisits d'accessibilitat per als productes i serveis de les TIC ", o en vigor.

11.3 Propòsit

L'objectiu de la Normativa d'accessibilitat és donar als diferents participants involucrats

en el desenvolupament, integració o manteniment de software de la UOC, unes línies mestres en les quals basar l'accessibilitat de totes les interfícies web i aplicacions mòbils. Tots alineats amb les bones pràctiques reconegudes internacionalment però adaptades a les necessitats i especificitats de l'Àrea de Tecnologia de la UOC.

11.4 Audiència

Aquesta normativa està dirigit a tots aquells proveïdors de l'Àrea de Tecnologia de la UOC que estiguin oferint els seus serveis actualment o ho vulguin fer en un futur i evidentment, per als membres de l'equip propi de l'Àrea de Tecnologia UOC.

La Normativa s'ha escrit per a persones familiaritzades amb aquesta disciplina. Per a adquirir coneixements complementaris amb aquesta disciplina, disposem de documentació complementària que afegeix bibliografia.

11.5 Activitats

La Normativa d'accessibilitat la conformen les activitats següents:

- Lliurar la proposta de Solució
- Integrar accessibilitat en la fase disseny
- Executar el heuristic d'accessibilitat
- Definir la paleta de colors
- Definir estratègia de proves d'Accessibilitat
- Executar el test d'Accessibilitat al TestRail
- creació informe resultat proves accessibilitat
- Declaració d'accessibilitat

A continuació es descriuen a alt nivell:

11.5.1 Lliurar la proposta de solució

Cal tenir en ment aquests punts a l'hora de fer la Proposta de Solució:

- Ha de considerar-se durant la planificació fer el contingut accessible i assegurar-se que ho és, no com una etapa posterior: L'accessibilitat no és un afegit. Cal tenir-la

en compte des del principi del projecte.

- L'accessibilitat no implica més cost de desenvolupament. "Costa el mateix afegir una imatge de forma accessible que inaccessible. Costa el mateix fer un formulari accessible que inaccessible"
- El bon desenvolupament web comença amb l'accessibilitat. Cada línia de codi escrita sense pensar en ella es una línia que haurà de ser reescrita més tard: És molt costós arreglar els errors després. "Si fem un error, aquella línia de codi caldrà reescriure-la. I en la majoria de casos implica reescriure de nou la funcionalitat amb problemes d'accessibilitat".
- No és acceptable cap error d'accessibilitat en eines i espais web que s'hagin creat de nou. Qualsevol error no solucionat haurà d'anar acompanyat de la seva justificació per poder ser acceptat.
- En cas d'haver d'utilitzar una eina d'un tercer o servei extern per un projecte, ja sigui en codi obert o propietari, caldrà escollir la més accessible.
- En la plantilla de checklist per Acceptació de la proposta de solució hi ha un apartat d'accessibilitat on s'ha de recollir com es pretén assolir aquesta accessibilitat.

A l'hora d'escriure els requeriments cal tenir en compte (entre altres) les següents recomanacions

- Accessible Rich Internet Applications (WAI-ARIA) 1.2
- WAI-ARIA Authoring Practices
- Requeriments dels diàlegs modals
- Requeriments dels formularis
- Requeriments de les apps amb angular
- Navegació amb teclat i lector de pantalla

per veure en més detall com tenir en compte l'accessibilitat en la fase de recollida de requeriments, es pot consultar la plana Requeriments d'accessibilitat.

11.5.2 Integrar accessibilitat en la fase disseny

Es proposa seguir la metodologia següent per aconseguir una bona integració accessibilitat. Aquests passos s'haurien d'aplicar a l'hora de crear els wireframes i dissenys gràfics per tal de poder generar una maqueta amb un bon codi html.

11.5.3 Executar heuristic d'accessibilitat

Com hem indicat anteriorment l'accessibilitat cal tenir-la en ment durant totes les fases del desenvolupament d'una aplicació. Com més a prop de la posta en producció es detecta un error d'accessibilitat més és el cost de solucionar aquest error.

per aquesta raó, es recomana passar el Heuristic d'accessibilitat en el lliurable wireframe. També pot ser útil emprar aquest heuristic a l'hora de definir els requeriments funcionals o en altres fases del projecte on no hi ha un codi font que es pot validar amb el test d'accessibilitat que es comenta més avall.

11.5.4 Definir la paleta de colors

Dins de la fase de disseny del projecte cal validar que totes les combinacions de colors que es fan servir compleixen la relació indicada en la pauta 1.4.3. On s'indica que El text o les imatges de text han de tindre una relació de contrast de al menys 4.5:1 . En el cas de text gran o en negreta seria de 3:1.

Caldrà entregar amb el disseny gràfic, més específicament en el lliurable Disseny gràfic una llista de les combinacions de colors emprades i el seu valor de contrast (Anotacions dels colors emprats en el disseny) per tal de validar que son correctes.

11.5.5 Definir estratègia de proves d'Accessibilitat

Dins del document d'Estratègia de Proves del projecte és necessari contemplar les proves d'Accessibilitat per a cada una de les aplicacions implicades al projecte. El W3C te definida una metodología per poder seleccionar l'abast, mostra de planes que seran l'objectiu d'aquesta anàlisi, etc (WCAG-EM (Website Accessibility Conformance Evaluation Methodology)). Veure activitat Definir estratègia de Proves per més informació.

En especial, cal tenir en consideració el lliurable pla de proves d'accessibilitat.

11.5.6 Executar el test d'Accessibilitat al TestRail

Com ja hem dit, tota aplicació ha de ser accessible a nivell doble A.

S'ha dissenyat un Pla de proves d'accessibilitat a confluence al TestRail de la UOC. Cada una de les aplicacions implicades en un projecte han de superar el test per tal de que sigui acceptada l'entrega del projecte.

Val a dir que el Test Plan d'Accessibilitat definit al TestRail, no contempla totes les

validacions que serien necessàries per garantir doble A. Esdevé un recull que ens sembla essencial que tot projecte compleixi. Per tant, això vol dir que cal complir amb totes les validacions proposades per la WAI, no només les recollides al Test Plan.

El primer pas del test suite consisteix en fer un test automatic. Hi ha eines automàtiques que ens poden ajudar en aquesta tasca però, cal tenir en compte que no son totalment fiables. Amb una revisió automàti ca obtindrem un nivell aproximat de revisió d'accessibilitat del 32%, pel que es recomana una combinació de test manual i eines automàtiques. El W3C té una plana on recull les diferents eines per fer un test automatic (veure apartat bibliografia).

11.5.7 Creació informe resultat proves accessibilitat

Quan passem el test d'accessibilitat, ja sigui via el Pla de proves d'accessibilitat a Confluence o seguint la metodologia del proveïdor, anirem recollint per cada criteri si passa, falla o no aplica. A més a m és d'exemples on el test falla (veure “Generació informe compliment accessibilitat”, per veure una llista d'eines per recollir les dades de passar el test).

Tota aquesta informació (si passa o no el criteri i els comentaris amb les evidències dels errors detectats) s'han de recollir en un informe de Resultat de Proves d'accessibilitat.

Si es detecten errors s’haurien de solucionar per tal de poder complir el primer requeriment de la normativa que l’eina ha de ser accessible. No hauria de passar a mantenimen t cap eina si avanç no s’han solucionat els errors d’accessibilitat detectats en l’auditoria.

11.5.8 Declaració d'accessibilitat

Quan l'eina es doni com a correcte des del punt de vista de l'accessibilitat es fa ús de l’informe de resultats de proves d'acc essibilitat per poder omplir la "declaració d'accessibilitat".

Aquesta declaració d'accessibilitat s'hauria de mostrar a l'enllaç "accessibilitat" que cal afegir en el peu de tota aplicació web. Si es tracta d'una aplicació mòbil si ha de poder accedir desde l'app.

11.5.9 Lliurables

S’ha de lliurar l'Informe de Resultats de Proves conforme s’ha passat el pla de proves d'accessibilitat. Més concretament l’ Informe resultats proves accessibilitat a TestRail

sobre els següents lliurables:

- Front end
- Producte en entorn preproducció

Aquest informe es el que ens permet lliurar la Declaració d'accessibilitat.

11.5.10 Control d'aplicació de la Normativa

Per demostrar l'acompliment d'aquestes pautes, cal que l'Informe de Resultats de Proves d'Accessibilitat passi OK completament en fase maqueta i fase pre.

Principalment, serà el cap de projecte (o algú en qui delegui) qui vetllarà per l'aplicació correcta de la Normativa. En tot cas, qualsevol membre de l'Àrea de Tecnologia podrà aixecar alertes sobre incompliments en termes d'accessibilitat.

12 Annex - Normativa de seguretat

12.1 Plataformes SaaS

Per a les plataformes SaaS es defineixen els criteris següents:

• La solució ha de garantir l'existència de rols i permisos que es puguin assignar a usuaris específics per garantir que només accedeixen a les dades i recursos necessaris pel desenvolupament de les seves funcions.
• La solució ha de registrar les dades de cada intent d'accés, incloent informació relativa a la identificació unívoca de l'usuari, data i hora, informació accedida i tipus d'accés. Aquests registres s'hauran de custodiar durant un mínim de 12 mesos
• La solució ha de poder oferir la possibilitat de tenir un registre actualitzat d'usuaris. El registre ha de reflectir l'associació de cada codi d'usuari amb la persona que el té assignat, el seu perfil i els accessos autoritzats. Aquest registre ha de reflectir tots els canvis en el mapatge: altes, baixes i possibles

modificacions.
• La solució ha de disposar de mecanismes necessaris que permetin registrar l'activitat dels usuaris i custodiar aquests registres durant un mínim de 12 mesos
• La solució ha de tenir mecanismes de logging i de control de canvi en les dades, registrant tota la informació necessària que permeti la traçabilitat dels successos.
• La solució ha de garantir el processat immediat de les baixes dels usuaris mitjançant les eines d'administració de les aplicacions, inhabilitant l'accés a les mateixes amb el codi d'usuari donat de baixa. La baixa d'un usuari implica el seu bloqueig temporal, abans de procedir a la seva eliminació definitiva.
• L'adjudicatària ha d'informar a la UOC sobre la ubicació de les Dades que seran emmagatzemades abans de la contractació del Servei. Durant el període de duració del Servei, qualsevol canvi en la ubicació de les Dades haurà de ser comunicat a la UOC amb anticipació, i no podrà ser efectuat fins rebre l'autorització de la UOC.
• La solució ha de garantir que tota la informació ha de viatjar xifrada (amb clau mínima 256 bits) i s'ha d'emmagatzemar de forma xifrada. Fent especial èmfasi a les dades de caràcter personal que pugui proporcionar la UOC.
• La solució ha de disposar de les mesures de seguretat adequades en tots els entorns per garantir la confidencialitat, integritat i disponibilitat de les dades de la UOC, així com podrien ser: Firewall, Sistemes de Detecció i Prevenció de Intrusos (IDS/IDPS), Zona Desmilitaritzada (DMZ), Xarxes Privades Virtuals (VPN) i Proxy a la infraestructura. I garantir que aquests elements disposen dels logs o registres de traçabilitat suficients per analitzar una intrusió o fuga d'informació en cas necessari.
• L'adjudicatària ha d'actuar proactivament instal·lant les actualitzacions i pegats de seguretat publicats pels corresponents fabricants. Ha de tenir una política de vigilància d'alertes de seguretat i detecció de vulnerabilitats.
• L'adjudicatàriaha de realitzar totes aquelles auditories legalment exigibles, tant de manera interna com externa, sobre aquells sistemes involucrats en el servei prestat a la UOC, deixant a disposició de la UOC els informes de auditoria generats.
• Gestió avançada d'autoritzacions i permisos amb assignació de rols d'autoria, aprovació, supervisió, eliminació de continguts, etc. La plataforma haurà de permetre l'assignació d'autoritzacions i permisos de forma que cada usuari pugui accedir només i exclusivaments als continguts als que està autoritzat pel

seu rol.
• Possibilitat de definir IP Blacklist
• Caducitat de sessió en cas d'inactivitat (configurable)
• Disposar d'eines de revisió d'anàlisi forense
• Compliment amb tota la normativa definida en la GDPR
• Disposar d'un sistema de mitigació de riscos i impactes per atacs DDOS
• Possibilitat d'integrar doble factor d'autenticació en diferents rols de la eina, fen èmfasi en els administradors
• La solució haurà de garantir que s'empraran mecanismes d'eliminació segura d'informació. Aquests inclouran els casos de reciclatge de suports i de finalització del Servei. Amb aquestes mesures, la UOC s'assegura que la informació no és enviada sense aprovació a altres ubicacions i que no es pot extreure informació dels suports després del seu ús.

12.2 Desenvolupaments i configuracions

Per els desenvolupaments i configuracions cal aplicar com a mínim els criteris següents. Aquests criteris s'han de tenir en compte alhora d'elaborar qualsevol dels artefactes del projecte, en cas contrari, generaran penalitats que es tipifiquen en l'apartat 8.2.

Seguretat Arquitectural
L'aplicació garanteix que tots els components que estan presents a la mateixa estan identificats (bé sigui un component individual o bé siguin grups d'arxius de codi font, llibreries i/o executables)
L'aplicació garanteix que tots els components que no formen part de la mateixa aplicació, però en els que aquesta hi confia, estan identificats
Existeix una arquitectura d'alt nivell per a l'aplicació
Autenticació
L'aplicació garanteix que tots els camps de contrasenya tenen el "eco" desactivat i que els camps de contrasenya o els formularis que contenen aquests camps tenen

Seguretat Arquitectural
l'atribut "d'autocompletat" desactivat
L'aplicació garanteix el control en si s'ha excedit el nombre màxim d'intents durant el procés d'autenticació, el compte quedarà bloquejat durant un període prou llarg de temps que impedeixi els atacs per força bruta
L'aplicació garanteix que tots els controls d'autenticació s'apliquen a la banda servidora
L'aplicació garanteix que tots els controls d'autenticació (incloses les llibreries que criden a serveis d'autenticació externs) tenen una aplicació centralitzada
L'aplicació garanteix que tots els controls d'autenticació fallen de forma segura
L'aplicació garanteix que la robustesa de les credencials d'autenticació són suficients per resistir els atacs típics
L'aplicació garanteix que totes les funcions de gestió de les comptes d'usuaris són al menys tan resistents a un atac (de força bruta o d'enginyeria inversa) com el mecanisme d'autenticació principal
L'aplicació garanteix que els usuaris poden canviar de forma segura les seves credencials i amb algun mecanisme que sigui, almenys, tant resistent com el mecanisme d'autenticació principal
L'aplicació garanteix que cal una re-autenticació abans de permetre operacions "realment" sensibles
L'aplicació garanteix que totes les decisions (tant el que fa als èxits com als fracasos) d'autenticació s'estan enregistrant
L'aplicació garanteix que que totes les contrasenyes de les comptes d'usuari es "salten" amb una "sal" (en criptografía, la sal compren bits aleatoris que són usats como una de les entrades en una funció derivadora de claus) exclusiva d'aquesta compta (pex. l'ID d'usuari, la data de creació de la compta, ... etc) y que s'emmagatzema un hash i no la contraseña en clar
L'aplicació garanteix que totes les credencials d'autenticació per accedir a serveis externs (accessos a la DB, WX, ... ect) estan xifrades i que s'emmagatzemen en un lloc protegit (i no en el codi font o fitxers accesibles de configuració)
Gestió de la sessió
L'aplicació utilitza algun "framework" de gestió de les sessions
L'aplicació garanteix que les sessions s'invaliden quan l'usuari tanca la sessió
L'aplicació garanteix que les sessions caduquen (expiren) després d'un període d'inactivitat

Seguretat Arquitectural
L'aplicació garanteix que totes les pàgines que necessiten autenticació per accedir a elles tenen vincles (anchors, buttons, imatges, ... etc) de tancament de sessió
L'aplicació garanteix que l'identificador de la sessió no es "divulga o publica", particularment a les adreces de les URL i missatges d'error. Això inclou garantir que l'aplicació no admet la reescriptura de la URL ni les cookies de sessió
L'aplicació garanteix que l'identificador de sessió es canvia a l'inici de la sessió
L'aplicació garanteix que l'identificador de sessió es canvia quan es fa una re-autenticació
L'aplicació garanteix que l'identificador de sessió es canvia o s'esborra en sortir de l'aplicació o servei
L'aplicació garanteix que només els identificadors de sessió generats per el "framework" de l'aplicació són reconeguts com a vàlids per l'aplicació
Control d'accés
L'aplicació garanteix que els usuaris només poden accedir a les funcions protegides per a les que tinguin una autorització específica
L'aplicació garanteix que els usuaris només poden accedir a les adreces URL per a les que tinguin una autorització específica
L'aplicació garanteix que els usuaris només poden accedir als arxius de dades per els que tinguin una autorització específica
L'aplicació garanteix que les referències directes a objectes estan protegides, de tal manera que un usuari només té accés als objectes als que ha estat autoritzat
L'aplicació garanteix que está deshabilitada la vista de contingut dels directoris del servidor Web, exceptuant que es vulgui fer de forma deliberada
L'aplicació garanteix que els usuaris només poden accedir als serveis per als que tenen una autorització específica
L'aplicació garanteix que els usuaris només poden accedir a les dades per a les que tenen una autorització específica
L'aplicació garanteix que el control d'accés falla de forma segura
L'aplicació garanteix que s'apliquen les mateixes regles d'accés a la capa de presentació que en la banda del servidor
L'aplicació garanteix que tots els atributs d'usuari i de dades i que la política d'informació usats en el control d'accessos no poden ser manipulats per usuaris finals sense una autorització expressa
L'aplicació garanteix que tots els controls d'accés s'apliquen en el servidor
L'aplicació garanteix que hi ha un mecanisme centralitzat per a protegir l'accés a

Seguretat Arquitectural
cada tipus de recurs protegit (incloses les llibreries que necessiten d'autorització de serveis externs
L'aplicació garanteix que les limitacions imposades per "les regles de negoci", tant pel que fa a l'entrada de dades com en l'accés a l'aplicació (pex. límits diaris de transacció) no poden ser anul·lades o ignorades
L'aplicació garanteix que totes les decisions de control d'accés es poden enregistrar i que tots els fallos en decisions de control s'estan enregistrant
Validació de l'entrada de dades
L'aplicació garanteix que l'entorn d'execució del programari no es susceptible a desbordaments de buffer. O que en el seu defecte, els controls de seguretat prevenen dels desbordaments de buffer
L'aplicació garanteix que s'aplica un patró de validació positiva per a totes les entrades de dades de l'aplicació
L'aplicació garanteix que totes les fallades de validacions d'entrada donen com a resultat el rebuig de l'entrada o el "sanejament" de la mateixa
L'aplicació garanteix que s'especifica una conjunt de caràcters, com pot ser UTF8, per a totes les possibles fonts d'entrada de dades
L'aplicació garanteix que la validació de totes les entrades de dades es realitzen a la part servidora
Codificació i escapament dels caràcters de sortida
L'aplicació garanteix que totes les dades emeses per la sortida HTML i que no són de confiança estan degudament escapats (incloent-hi els elements HTML, els atributs, valor de les dades JavaScript, blocs CSS i atributs URL)
L'aplicació garanteix que tots els controls de codificació i escapament dels caràcters de sortida estan implementat a la part servidora
L'aplicació garanteix que tots els controls de codificació i escapament dels caràcters de sortida codifiquen aquests caràcters com "no segurs" per al llenguatge intèrpret (HTML, JavaScript, CSS, XML, JSON, ... etc)
L'aplicació garanteix que totes les dades que "no són de confiança" emeses per ser usades per un intèrpret SQL, utilitzen interfícies parametritzades, del tipus "prepared statement", o bé estan correctament escapats
L'aplicació garanteix que totes les dades que no són de confianza emeses per a ser usades amb un intèrpret XML utilitzen interfícies amb paràmetres o caràcters d'escapament apropiats
L'aplicació garanteix que totes les dades que no siguin de confiança utilitzats en consultes LDAP estan escapats correctament

Seguretat Arquitectural
L'aplicació garanteix que totes les dades que no siguin de confiança i que poden ser paràmetres de comandaments del sistema operatiu estan escapats correctament
L'aplicació garanteix que totes les dades que no són de confiança per a qualsevol intèrpret (dels no mencionats anteriorment) estan escapats correctament
Criptografia i xifrat
L'aplicació garanteix que totes les funcions criptogràfiques i de xifrat usades per protegir els "secrets" de l'aplicació s'executen a la banda servidora
L'aplicació garanteix que tots els mòduls criptogràfics fallen de forma segura
Gestió d'errors i gestió de logs
L'aplicació garanteix que no es generen missatges d'error ni traces que continguin dades sensibles que un atacant podria usar (com ara la informació personal)
L'aplicació garanteix que tots els errors de la part servidora estan gestionats des de la mateixa part servidora
L'aplicació garanteix que tots els controls de registre estan implementats en la part del servidor
L'aplicació garanteix que la lògica de controls d'errors en els controls de seguretat denega l'accés per defecte
L'aplicació garanteix que el registre de seguretat ofereix la possibilitat d'enregistrar tant els esdeveniments d'èxit com els de fracàs o error (entre la sèrie d'esdeveniments identificats com a rellevants)
L'aplicació garanteix que cada esdeveniment de registre inclou: un segell de temps d'una font confiable (pex. NTP), el nivell de gravetat de l'esdeveniment, una indicació de que es tracta d'un esdeveniment de seguretat pertinent (si es barreja amb d'altres registres), la identitat de l'usuari que ha ocasionat l'esdeveniment (en el cas que hi hagi un usuari associat a l'esdeveniment), l'adreça IP de l'origen de la sol·licitud associada a l'esdeveniment, el grau d'èxit de l'esdeveniment i una descripció de l'esdeveniment
L'aplicació garanteix que tots els esdeveniments que inclouen dades que no són de confiança no s'executarà com a "codi" en el programari de visualització de logs
L'aplicació garanteix que els esdeveniments (registres d'activitat, logs, ...) estan protegits contra l'accés no autoritzat i la modificació
L'aplicació garanteix que només hi ha una única implementació d'enregistrament d'esdeveniments i que és la que usa l'aplicació
L'aplicació garanteix que no enregistra dades sensibles que poguessin ajudar o donar pistes a un atacant, com ara informació personal o sensible de l'entorn o

Seguretat Arquitectural
l'aplicació
L'aplicació garanteix que hi ha una eina disponible que permeti a l'analista realitzar cerques de registres d'esdeveniments basat en la combinació de criteris de cerca
Protecció de les dades
Tot el sistema està construït sota el principi de privacitat per disseny per garantir ple compliment de totes les disposicions del RGPD
L'aplicació garanteix que tots els formularis que contenen informació sensible tenen deshabilitada la "cache" d'informació en la banda del navegador, o client, incloent-hi les característiques d'autocompletat
L'aplicació garanteix que hi ha una llista identificada de dades confidencials processades per cadascuna de les aplicacions, i que hi ha una política explícita d'accés a aquestes dades, i quan aquestes dades han d'estar xifrades (tant en l'emmagatzemament com en el trànsit)
L'aplicació garanteix que totes les dades confidencials s'envien al servidor en el cos del missatge o protocol HTTP, es a dir, no s'utilitzen paràmetres de la URL per transmetre dades
L'aplicació garanteix que les còpies en cache o temporals de dades confidencials trameses als clients estan protegides contra el accés no autoritzat i que aquestes caches són porgades o invalidades després de que el propi usuari hagi accedit a dades sensibles (és a dir: les capçaleres HTTP tenen establerts els paràmetres de No-cache i No-Store Cache-Control)
L'aplicació garanteix que totes les còpies en cache o temporals de les dades emmagatzemades a la part servidora estan protegides contra l'accés no autoritzat i que aquestes cahes són porgades o invalidades després que l'usuari hagi accedit a dades sensibles
Seguretat de les comunicacions
L'aplicació garanteix que per a cada certificat SSL es pot construir una ruta de verificació cap a una CA (Certification Authority) de confiança, i que cada certificat de servidor és vàlid
L'aplicació garanteix que una fallada en la connexió SSL no comporta que s'estableix una connexió NO segura
L'aplicació garanteix que s'utilitza SSL a totes les connexions autenticades o referides a dades o funcions sensibles (tant pel que fa a les connexions externes com cap a les da back-end)
L'aplicació garanteix que el back-end de connexions SSL enregistra les fallades de connexió

Seguretat Arquitectural
L'aplicació garanteix que els certificats de client utilitzen ancoratges ("anchors") de confiança (per a construir la ruta cap a la CA) i informació de revocació
L'aplicació garanteix que totes les connexions a sistemes externs que manipulan informació o funcions sensibles estan autenticades
L'aplicació garanteix que totes les connexions a sistemes externs que manipulen funcions o informació sensible utilitzen un compte que ha estat creada per a tenir els privilegis mínims per a que l'aplicació funcioni correctament
Seguretat HTTP
L'aplicació garanteix que les redireccions NO inclouen dades no validades
L'aplicació garanteix que només accepta un conjunt definit de mètodes de sol·licitud HTTP, com poden ser GET i POST
L'aplicació garanteix que cada resposta HTTP conté un encapçalament de tipus de contingut que especifica un conjunt de caràcters segurs (pex. UTF-8)
L'aplicació garanteix que l'indicador HTTPOnly s'utilitza a totes les cookies que no precisen específicament d'accés JavaScript
L'aplicació garanteix que l'indicador "secure" s'utilitza a totes les cookies que contenen informació confidencial, incloent-hi la cookie de sessió
L'aplicació garanteix que els encapçalaments HTTP, tant a les peticions com a les respostes, contienen només caràcters ASCII imprimibles
Verificació dels requeriments de Seguretat
L'aplicació garanteix que tota la informació de configuració rellevant per a la seguretat, s'emmagatzema a llocs que estan protegits accessos no autoritzats
L'aplicació garanteix que es deneguen tots els accessos, si l'aplicació no pot accedir a la seva informació sobre la configuració de seguretat
Com l'aplicació dona compliment del RGPD i a la llei LOPDgdd

12.3 Mesures de seguretat

Les mesures de seguretat s'apliquen en casos en que hi ha tractament de dades personals per part de l'adjudicatària.

Aquest model de mesures de seguretat s'aplica en el següent cas:

A. El servei es presta completa o parcialment en les instal.lacions de l'adjudicatària?	Sí
B. Per la prestació del servei s'usen aplicacions (o se'n desenvolupen de noves) i/o infraestructures de l'adjudicatària o de tercers (no UOC)?	Sí
C. L'adjudicatària per a la prestació del servei ha d'emmagatzemar dades personals en els seus propis sistemes o en sistemes de tercers (no UOC)?	No
D. L'adjudicatària per a la prestació del servei ha d'enviar emails en nom de la UOC?	No

12.3.1 Consideracions prèvies

- S'autoritza expressament el tractament de dades personals en les instal·lacions de l'adjudicatària per les finalitats recollides en el contracte a que es refereixen el serveis de l'adjudicatària. Tanmateix, s'autoritza explícitament la sortida de suports i documentació que continguin informació amb dades personals, si procedeix, per la prestació dels serveis contractats. Pel trasllat de suports i documents, l'adjudicatària aplicarà en tot cas, les mesures de seguretat establertes per donar compliment al present document o a la normativa vigent.

- L'adjudicatàriaemprarà els recursos d'informació i/o les dades propietat de la UOC en el marc del desenvolupament de la prestació de serveis encomanada i amb la finalitat prèviament establerta.

12.3.2 Confidencialitat de les persones

- Tot el personal de l'adjudicatària que, amb motiu de la prestació del Servei, o per qualsevol altra circumstància, sigui coneixedor d'informació relacionada amb la UOC mantindrà la màxima confidencialitat sobre aquesta, i no podrà comunicar-la a tercers en cap moment, ja sigui abans, durant o després de la prestació del Servei,

per altres finalitats que no siguin les de la prestació del propi servei. L'adjudicatària i el seu personal, únicament podrà emprar la informació amb la finalitat prevista en l'objecte d'aquest Contracte, responent davant de la UOC pels danys i perjudicis que del incompliment poguessin derivar-se per la UOC.

- En cas de que L'adjudicatària vulgui subcontractar, necessita l'autorització expressa de la UOC per fer-ho. En aquest cas, el mateix és responsable de que es respecti i compleixi el mateix criteri de confidencialitat i les normes sobre la informació relacionada amb la UOC descrites en les clàusules anteriors.

12.3.3 Confidencialitat de la informació

- Amb caràcter general, L'adjudicatària ha de tractar la informació de la UOC com informació sensible, i adoptar les mesures adequades per aquesta classificació.

- El tractament de la informació ha de permetre traçabilitat, entenent-la com la capacitat de conèixer quines persones, i en quin moment, han accedit i tractat la informació de la UOC. S'entendrà com a tractament qualsevol operació realitzada amb la informació, com són, tot i que no únicament, la seva lectura, escriptura, modificació, copia, transmissió, gravació o arxivat mitjançant mitjans manuals o amb aplicacions informàtiques.

12.4 Protecció de dades personals

12.4.1 Compliment de la legislació

- L'adjudicatària està obligat a complir estrictament allò establert per la legislació vigent relativa a dades de caràcter personal, tractades durant el transcurs de la prestació dels Serveis.

- L'adjudicatària ha de tractar les Dades amb absoluta confidencialitat i d'acord amb les instruccions que rebi de la UOC en relació amb la finalitat, contingut i ús del tractament.

- L'adjudicatària ha d'emprar aquestes Dades, única i exclusivament, per les finalitats que figuren en el Contracte de serveis i sempre conforme a les instruccions que li dicti la UOC, i s'ha d'abstenir de reproduir-les així com de cedir-les o comunicar-les en qualsevol forma a terceres persones, ni tan sols per la seva conservació, per altres finalitats que no siguin les de la prestació del propi servei.

- L'adjudicatària ha de posar a disposició de la UOC els mecanismes necessaris i suficients a l'objecte que aquest pugui dur a terme l'execució dels drets dels interessats de manera àgil i efectiva, en cas de que la seva aplicació suposi la intervenció en els sistemes d'informació i documents de l'adjudicatària.

- L'adjudicatària ha de complir respecte a les Dades esmentades, amb totes les obligacions que resultin de la normativa aplicable en la seva condició d'Encarregat del Tractament i en particular, però sense que aquesta enumeració tingui caràcter exhaustiu, s'obliga a:

    i. Vetllar per la seguretat de les Dades i adoptar, a tal efecte, les mesures necessàries d'índole tècnica, legal i organitzativa que garanteixin la seguretat de les mateixes i evitin la seva alteració, pèrdua, tractament o accés no autoritzat de conformitat amb allò que estableix la legislació vigent.
    ii. Guardar el més estricte secret sobre el contingut de les Dades.
    iii. Retornar a la UOC totes les Dades a les que hagi tingut accés en virtut del Contracte de serveis en qualsevol moment en que la UOC li sol·liciti, i, en tot cas, un cop finalitzada la prestació contractual per la realització de la qual es van facilitar les Dades, sense que, en cap cas, L'adjudicatària pugui conservar cap còpia de les Dades facilitades per la UOC.

- L'adjudicatària es fa responsable davant de la UOC, i mantindrà a la UOC indemne davant de qualsevol dany i perjudici que li pugui causar i que siguin conseqüència de la inobservança per part de l'adjudicatària de les obligacions contingudes en aquesta clàusula, incloent tots els que es deriven de reclamacions de tercers o de procediments sancionadors oberts per l'Agència de Protecció de Dades.

12.4.2 Document de seguretat

- L'adjudicatària ha de disposar d'un Document de Seguretat que inclogui les mesures d'índole tècnica i organitzativa adoptades en el tractament de les dades personals, de conformitat amb la normativa vigent. Aquest document ha de reflectir i identificar a l'encarregat del tractament i els fitxers afectats, i, això, s'ha de detallar en el contracte.

- L'adjudicatària ha de mantenir actualitzat el document esmentat, tant en allò relatiu a l'organització com a la legislació vigent, essent objecte de revisió periòdica, com a mínim, anual.

- L'adjudicatària ha de definir i mantenir actualitzades periòdicament les funcions i obligacions de cadascun dels usuaris que accedeixen a dades de caràcter personal, així com la seva divulgació eficient.

- L'adjudicatària ha de garantir, mitjançant procediments interns eficients, el coneixement continuat per part del personal involucrat, de la política i normativa de seguretat.

12.4.3 Responsabilitat proactiva

- L'adjudicatària es compromet a realitzar una anàlisi de riscos que li permeti determinar les mesures tècniques i organitzatives més apropiades per garantir i poder demostrar que el tractament de dades personals es duu a terme d'una forma responsable, segura, respectant la privacitat i els drets dels interessats, i que dona compliment a la legislació vigent. Aquestes mesures hauran d'adoptar un enfocament preventiu en lloc de correctiu, i ser revisades de forma periòdica per garantir que es mantenen actualitzades.

- Aquests principis s'hauran de tenir en consideració des del propi disseny de tots els projectes o iniciatives relacionades amb el tractament de dades personals, pel que s'hauran d'integrar en tot el seu cicle de vida.

12.5 Seguretat de la informació

12.5.1 Esquema de control

- L'adjudicatària accepta i s'obliga a complir l'esquema de control aplicable al servei prestat segons la classificació resultant de l'avaluació del risc del servei objecte del contracte, realitzada per la UOC.

- L'adjudicatària ha d'establir els controls de seguretat adequats amb la finalitat de reduir el risc d'accés i modificació no autoritzats de la informació rellevant continguda en els sistemes (aplicacions, sistemes operatius i bases de dades) que se suporten en el servei, i evitar la pèrdua, sostracció, indisponiblitat i tractament no autoritzat dels actius d'informació de la UOC.

- Els requeriments de seguretat indicats en aquest contracte són d'aplicació al Proveïdor, ja que emprarà els recursos d'informació i/o dades propietat de la UOC en el marc del desenvolupament de la prestació de serveis encomanada i amb la finalitat prèviament establerta. En el cas en que L'adjudicatària subcontracti, al seu torn, a un tercer, serà responsable de que els requeriments de seguretat siguin satisfets també per part d'aquest tercer.

- La UOC es reserva la facultat de modificar en qualsevol moment els requeriments de seguretat continguts en aquest contracte i en els seus annexes, i comunicarà les modificacions realitzades al Proveïdor, amb indicació de les dates previstes per la seva entrada en vigor.

12.5.2 Accés a la informació

- L'adjudicatària ha d'establir una segregació de funcions adequada que determini les mesures suficients i necessàries que assegurin que els drets d'accés (rols i perfils) de cada usuari del servei s'assignen d'acord amb les necessitats funcionals de cadascun.

- L'adjudicatària ha d'establir els controls suficients i necessaris per tal d'assegurar que l'accés físic als sistemes que tenen informació rellevant, es controla d'acord amb els requisits establerts per la UOC.

- L'adjudicatària ha d'establir les mesures suficients i necessàries per tal d'assegurar que es realitzen revisions periòdiques sobre els permisos i controls d'accés configurats en els sistemes involucrats en el servei.

12.5.3 Gestió de canvis

- L'adjudicatària ha d'establir els controls de seguretat adequats en relació amb els canvis que puguin ser necessaris realitzar sobre les aplicacions o sistemes involucrats en el servei. Aquests controls han de cobrir, com a mínim, autoritzacions, realització de proves, aprovacions de l'usuari final i una separació adequada dels entorns previs respecte de l'entorn de producció.

12.5.4 Adquisició i desenvolupament d'aplicacions

- L'adjudicatària ha d'establir els controls de seguretat adequats en relació amb l'adquisició i desenvolupament de noves aplicacions o l'adquisició de nous sistemes durant la prestació del servei. Aquests controls han de cobrir, com a mínim, autoritzacions, realització de proves, aprovacions de l'usuari final i una separació adequada dels entorns previs respecte de l'entorn de producció.

12.5.5 Gestió d'operacions

- L'adjudicatària ha d'establir els controls de seguretat adequats a l'objecte d'assegurar que les operacions realitzades sobre les aplicacions i sistemes involucrats en el servei, són autoritzades i programades d'acord amb els requeriments acordats entre la UOC i el Proveïdor. En concret, les operacions a considerar en el servei es refereixen a la generació de còpies de seguretat i la gestió d'incidències de seguretat tecnològica.

- L'adjudicatària ha de tenir establertes una sèrie de polítiques en què s'especifiquin les mesures que s'han de dur a terme per la realització de còpies de seguretat, incloent els procediments a seguir per la recuperació dels sistemes.

- L'adjudicatària ha de tenir establertes una sèrie de mesures en les que s'especifiquin les accions que s'han de dur a terme per a una correcta gestió (detecció, resolució i comunicació a la UOC) de les incidències de seguretat tecnològica que succeeixin durant la prestació del servei.

12.6 Organització de la seguretat

12.6.1 Marc normatiu de seguretat TI

- L'adjudicatària ha d'establir un marc normatiu de seguretat TI que asseguri una correcta implantació de les mesures de seguretat indicades, i que estigui alineat amb els criteris de la UOC en relació amb la seguretat aplicable a la informació tractada.

- L'adjudicatària ha d'actualitzar de manera convenient l'esmentat marc normatiu de seguretat, d'acord amb les modificacions del servei i amb les noves lleis, normatives o estàndards que puguin sorgir en matèria de seguretat tecnològica i protecció de la informació i les dades de caràcter personal.

- Aquest marc normatiu ha de contenir, com a mínim, els següents procediments:
    a. Codi de conducta;
    b. Gestió d'usuaris;
    c. Control d'accés i gestió de logs d'activitat;
    d. Gestió d'incidències:
    e. Gestió de la continuïtat del servei;
    f. Gestió de les operacions;
    g. Gestió del canvi;
    h. Devolució del servei;
    i. Gestió de canvis de software;
    j. Desenvolupament de software i noves adquisicions de sistemes;
    k. Política de contrasenyes;

l. Procediment de divulgació i emmagatzemament;
m. Model de relació i notificació amb la UOC.

- Cada un dels procediments indicats ha de ser verificat i aprovat per la UOC.

- L'adjudicatària ha de garantir que els procediments d'assignació, distribució i emmagatzemament de contrasenyes han estat formalitzats per escrit, sense que existeixin més excepcions que les que es puguin incloure en els procediments esmentats.

- L'adjudicatària ha de comunicar el Codi de Conducta i el marc normatiu als seus treballadors encarregats de la prestació de serveis a la UOC, registrant l'acceptació per part d'aquests.

12.6.2 Identificació de responsabilitats

- L'adjudicatària ha de disposar d'una figura de Responsable de Risc Tecnològic i Seguretat de la Informació formalment establerta, a l'objecte de vetllar pel compliment de les polítiques de seguretat i el seguiment dels controls per assegurar la integritat, confidencialitat i disponibilitat de les Dades i sistemes, així com del compliment de totes aquelles normatives i lleis que siguin d'aplicació, prestant especial atenció a les lleis relatives a la protecció de dades de caràcter personal.

- El Responsable de Seguretat ha de realitzar el control i la coordinació de les mesures de seguretat aplicades pel Proveïdor, en especial d'aquelles destinades a la protecció del tractament de les dades personals objecte de la prestació de servei, i realitzar revisions periòdiques a l'objecte de verificar el compliment dels aspectes establerts en el Document de Seguretat.

- L'adjudicatària ha de designar un Coordinador encarregat de la gestió dels aspectes de seguretat amb la UOC. Aquest Coordinador de l'adjudicatària haurà d'assistir al Comitè de Coordinació mixt, entre L'adjudicatària i la UOC, en cas de que aquest sigui convocat per la UOC, a l'objecte de realitzar un seguiment oportú del servei i definir els plans d'acció necessaris per tal de garantir el correcte desenvolupament dels serveis.

- L'adjudicatària comunicarà a través dels canals establerts amb la UOC, qualsevol canvi que es produeixi respecte de la designació inicial de responsables del servei.

A tal efecte, els responsables designats per la UOC, així com per el proveïdor, per efectuar el tractament objecte d'encàrrec, són identificats en el següent quadre resum:

Responsable del Fitxer:	UOC
Encarregat del tractament de les Dades:	Indicar
Responsable de Seguretat per part de l'adjudicatària	Indicar
Tipus de Mesures: ESTÀNDARDS	Tipus de Tractament: MIXT

12.6.3 Anàlisi de riscos

- L'adjudicatària ha de realitzar un procés d'anàlisi de riscos contemplant els riscos involucrats en el Servei prestat a la UOC de forma periòdica i quan es produeixin canvis rellevants en l'entorn tecnològic. També ha de supervisar l'efectivitat de les accions definides pel tractament dels riscos.

- L'adjudicatària ha d'implementar un procés de monitorització de vulnerabilitats de la infraestructura tecnològica del Servei, identificant i tractant les vulnerabilitats oportunament sense exposar la informació de la UOC als riscos esmentats. Addicionalment, periòdicament haurà de realitzar l'avaluació de seguretat de la xarxa interna i perimetral amb recursos propis o emprant un tercer independent.

12.6.4 Plans de formació/conscienciació

- L'adjudicatària implementarà plans de formació i conscienciació en matèria de seguretat de la informació que incloguin a tots els treballadors que prestin Servei a la UOC.

- L'adjudicatària ha de desenvolupar de manera explícita un pla de conscienciació sobre la importància de les Dades de caràcter personal i la seva confidencialitat.

- L'adjudicatària ha d'implementar de manera explícita un pla de formació relatiu a la importància del desenvolupament segur de codi.

12.6.5 Notificació

- L'adjudicatària ha de notificar a la UOC qualsevol succés que excedeixi del acord contractual assolit amb la UOC.

- L'adjudicatària ha de notificar a la UOC qualsevol canvi sorgit durant la prestació del servei, ja sigui en la forma de prestar-lo (canvi en el procés) o en els sistemes emprats per subministrar el servei (canvi en la infraestructura).

12.7 Mesures tecnològiques

12.7.1 Control d'accés

12.7.1.1 Controlar l'accés a aplicacions i sistemes

- L'adjudicatària ha d'implantar els mecanismes necessaris per evitar l'existència d'usuaris genèrics, llevat d'aquells requerits per les tecnologies emprades.

- L'adjudicatària ha d'implantar els mecanismes necessaris que permetin tenir identificats de manera inequívoca al seus usuaris amb accés als sistemes que formen part del servei prestat a la UOC. No han de compartir-se codis d'usuari entre persones. En tot moment, els codis d'usuari emprats per accedir a les aplicacions han de permetre al Proveïdor identificar inequívocament a la persona que hi accedeix.

- L'adjudicatària ha de registrar les Dades de cada intent d'accés, incloent informació relativa a l'usuari, data i hora, fitxer accedit i tipus d'accés.

- L'adjudicatària ha d'implantar els mecanismes necessaris que permetin tenir un registre actualitzat d'usuaris. L'adjudicatària ha de mantenir un registre actualitzat per cadascun del sistemes o aplicacions implicats en el servei prestat a la UOC. El registre ha de reflectir l'associació de cada codi d'usuari amb la persona que el té assignat, el seu perfil i els accessos autoritzats.

- El registre ha de reflectir tots els canvis en el mapatge: altes, baixes i possibles modificacions.

- L'adjudicatària ha d'implantar els mecanismes necessaris que permetin el processat immediat de les baixes dels usuaris. Les baixes dels usuaris han d'executar-se de forma immediata mitjançant les eines d'administració de les aplicacions, inhabilitant l'accés a les mateixes amb el codi d'usuari donat de baixa. La baixa d'un usuari implica el seu bloqueig temporal, abans de procedir a la seva eliminació definitiva.

- L'adjudicatària ha d'instal·lar una protecció antivirus en els sistemes emprats per prestar el servei a la UOC, que s'ha de mantenir operativa i actualitzada en tot moment.

- L'adjudicatària ha d'implantar els mecanismes necessaris que permetin disposar de mecanismes de registres de l'activitat usuària.

- L'adjudicatària ha d'implementar controls per restringir els dispositius de sortida, com USB, unitat lectora/enregistradora de CD/DVD o altres, que permetin l'extracció de dades del mateix.

- L'adjudicatària ha d'implantar els mecanismes necessaris que permetin restringir l'accés a Internet o a qualsevol tipus de connexió que possibiliti la fuga d'informació de les Dades tractades en els mateixos.

- L'adjudicatària ha de definir una Política de Control d'accés/Contrasenyes que estableixi un marc normatiu de control d'accés en base als requisits del servei i de Seguretat de la Informació.

- L'adjudicatària ha d'implementar aquells controls per garantir que tots els elements amb els que prestarà el Servei s'administren i exploten de forma segura. Aquests controls han d'estar disponibles per la UOC, en cas de que així ho sol·liciti.

- Els controls indicats en el punt anterior han d'incloure:

    a. Polítiques d'usuaris/contrasenyes dels operadors i administradors de sistemes o productes, incloent expressament gestors de bases de dades.
    b. Accés als sistemes mitjançant eines que protegeixin la confidencialitat de les contrasenyes dels administradors, per exemple SSH a UNIX.
    c. Protecció dels sistemes servidors davant d'accessos no autoritzats.
    d. En casos d'accés a informació confidencial, el Servei haurà de proporcionar mecanismes d'autenticació multi-factor.

- L'adjudicatària ha d'incloure en la seva Política de Contrasenyes un procediment de distribució de contrasenyes que garanteixi que la contrasenya únicament és coneguda per l'usuari.

- L'adjudicatària ha d'incloure en la seva Política de Contrasenyes un procediment per a controlar la caducitat de les contrasenyes i l'emmagatzemament ininteL·ligible d'aquestes.

- L'adjudicatària ha d'implantar els mecanismes necessaris per concedir permisos d'accés als sistemes que presten servei a la UOC, únicament al personal autoritzat en el Document de Seguretat i en els llistats d'usuaris de cadascun dels sistemes.

- L'adjudicatària ha d'establir un mecanisme que limiti el nombre d'intents reiterats d'accés no autoritzat.

- L'adjudicatària ha d'establir una segregació de funcions adequada, que estableixi les mesures suficients i necessàries per tal d'assegurar que els drets d'accés (rols i perfils) de cada usuari del Servei s'assignen d'acord amb les necessitats funcionals de cadascun.

- L'adjudicatària ha d'establir controls suficients i necessaris que assegurin que l'accés lògic als sistemes que tenen informació rellevant es controla d'acord amb els requeriments establerts per la UOC.

- L'adjudicatària ha d'establir les mesures suficients i necessàries a l'objecte d'assegurar la realització de revisions periòdiques sobre els permisos d'accés i els controls d'accés configurats en els sistemes involucrats en el Servei.

- L'adjudicatària ha d'establir les mesures suficients i necessàries a l'objecte d'assegurar que els accessos remots a l'entorn tecnològic siguin controlats i monitoritzats.

- L'adjudicatària ha d'assegurar que la informació relacionada amb el Servei prestat no és tramesa a tercers sense la prèvia autorització de la UOC, i queda dintre del marc legal de la legislació.

12.7.1.2 Controls físics i ambientals

- L'adjudicatària serà responsable de la implantació de mesures de seguretat física per la protecció dels sistemes d'informació ubicats en les seves instal·lacions davant accessos no autoritzats i danys físics.

- L'adjudicatària ha d'establir controls suficients i necessaris a l'objecte d'assegurar l'accés físic a les instal·lacions en què es troben ubicats els sistemes d'informació que tenen informació rellevant.

- Es mantindrà actualitzada la base de dades del personal amb accés autoritzat i es controlarà d'acord amb els requeriments establerts per la UOC.

12.7.1.3 Autorització i autenticació

- L'adjudicatària ha de garantir l'emmagatzemament xifrat de les contrasenyes en els sistemes de tractament de la informació.

- L'adjudicatària ha d'implantar els mecanismes necessaris que permetin tenir identificats de forma inequívoca els accessos de cadascun dels usuaris, permetent únicament l'accés a les Dades i recursos necessaris pel desenvolupament de les seves funcions.

- L'adjudicatària ha d'implantar els mecanismes necessaris per evitar que els usuaris siguin administradors locals dels seus llocs de treball, llevat que es produeixi un requeriment explícit i una validació per part de la UOC.

- En cas de que el Servei requereixi atendre a clients, L'adjudicatària ha d'implantar les mesures de seguretat necessàries i suficients a l'objecte d'assegurar que l'autenticació dels clients esmentats es realitza mitjançant mecanismes de doble factor, com a mínim, per l'execució d'operacions o la consulta d'informació confidencial.

12.7.2 Desenvolupament i adquisició de sistemes de proveïdors amb accés a dades

Tots aquells desenvolupaments que es realitzin amb l'objecte de prestar serveis a la UOC, seran autoritzats per la UOC, havent l'adjudicatària de:

- Abstenir-se d'emmagatzemar dades de la UOC sense que aquest n'estigui al corrent, ho autoritzi i/o ho auditi.

- Realitzar una revisió de seguretat del codi font de qualsevol software que no hagi estat desenvolupat per la UOC, de manera prèvia a la seva posada en producció d'acord als principis i les bones pràctiques de desenvolupament segur.

- En cas de que es realitzin desenvolupaments de software per a la UOC, L'adjudicatària ha de posar a disposició de la UOC tots aquells desenvolupaments de software fets a mida, incloent el codi font, el codi objecte, els manuals i qualsevol altra informació rellevant.

- Estar en disposició de realitzar una avaluació de l'entorn de control, hacking ètic o qualsevol altra avaluació de seguretat prèvia a la posada en producció de qualsevol versió del sistema, en qualsevol moment que la UOC així ho requereixi.

- Aquells entorns diferents del de producció no poden contenir dades reals.

- Assegurar que els desenvolupaments realitzats per la prestació dels Serveis a la UOC i les eines emprades, compleixen les lleis de propietat intel·lectual i no vulneren cap legislació, normativa, contracte, dret, interès o propietat de tercers.

- Establir els controls de seguretat adequats en relació amb l'adquisició o el desenvolupament de noves aplicacions o sistemes durant la prestació del Servei. Aquests controls han de cobrir, com a mínim, l'anàlisi de la viabilitat, les autoritzacions, la realització de proves, les aprovacions de l'usuari final i una separació adequada dels entorns previs respecte de l'entorn de producció.

- En cas de que es desenvolupi software que pugui estar sotmès a regulació PCI-DSS, s'han de seguir les millors pràctiques de desenvolupament de software segur d'acord amb els requeriments de l'estàndard, evitant la introducció de vulnerabilitats conegudes.

- Els equips de desenvolupament hauran d'estar situats en segments de xarxa i entorns dedicats exclusivament al desenvolupament d'aplicacions, sense accés a entorns de producció ni a dades reals de la UOC.

- L'adjudicatària ha d'establir controls de seguretat adequats en relació a la validació de la integritat dels desenvolupaments en els entorns de producció.

12.7.3 Comunicacions

- L'adjudicatària ha d'establir tots els mecanismes necessaris per a que les comunicacions a través de xarxes públiques o xarxes sense fils de comunicacions electròniques estiguin xifrades.

- La connexió del CPD de l'adjudicatària amb els sistemes de la UOC únicament es podrà realitzar establint les mesures de control que determini la UOC , després d'una anàlisi detallada de les necessitats.

- Les comunicacions amb el CPD de la UOC han d'estar redundades.

- L'adjudicatària ha de posar a disposició de la UOC, quan així li sol·liciti, un mapa complert de la xarxa del prestador del Servei de comunicacions, en que s'identifiquin perfectament tots els elements de comunicació que hi intervenen, així com els elements de seguretat.

- L'adjudicatària ha de disposar, com a mínim, de les següents mesures de seguretat perimetral: Firewall, Sistemes de Detecció i Prevenció de Intrusos (IDS/IDPS), Zona Desmilitaritzada (DMZ), Xarxes Privades Virtuals (VPN) i Proxy.

12.7.3.1 Seguretat en l'ús del correu electrònic

Quan L'adjudicatària realitzi enviaments de correu en nom de la UOC o amb informació que faci referencia al mateix, ha de complir les següents mesures:

- Les direccions web (URL) incloses en els correus electrònics i els continguts dels mateixos han de ser supervisats prèviament pel responsable del servei de la UOC

- El responsable del servei de la UOC ha de conèixer les Dades de la UOC que seran incloses en els correus. Aquestes no han de ser confidencials ni secretes, i es determinarà si han de ser emmascarades i de quina manera.

- La UOC ha de rebre:
    a. L'avís previ de l'enviament dels correus electrònics.
    b. Una breu explicació del contingut del correu electrònic.
    c. Un exemple del correu electrònic/SMS que rebran els clients.

d. Conèixer la bústia origen de l'enviament del correu electrònic que rebran els clients.

- Hauran de quedar rastres i evidències (logs) de quan i a qui s'envien els correus des del servidor de correus emprat per l'enviament dels correus electrònics, tant si es realitza en la infraestructura de la UOC com en la de l'adjudicatària.

- En el registre d'activitat (logs) haurà de quedar registrada la data i hora d'enviament, compte d'origen amb el que s'envia el correu i destinataris del correu.

- Els correus han d'incloure els avisos/recomanacions acordades amb el departament de Prevenció Tecnològica del Frau.

- Els correus hauran de ser emesos amb un domini registrat a nom de la UOC.

- El departament de Missatgeria (en el cas de ser la UOC qui realitza l'enviament), o L'adjudicatària del Servei, haurà d'arbitrar mecanismes de control sobre les llistes negres de SPAM per controlar que els dominis de la UOC no hi apareguin.

- Els correus enviats als clients han de passar els controls necessaris per estar lliures de virus. És a dir, s'hauran d'explorar els correus amb les eines antivirus existents a la UOC o, en cas de que es subcontracti, al Proveïdor del Servei.

12.7.4 Incidències

- L'adjudicatària ha de disposar d'un procediment de gestió i notificació d'incidències de Seguretat i de protecció de dades personals, havent d'informar oportunament a la UOC d'una potencial incidència de seguretat o de l'ocurrència d'una incidència de seguretat i de la manera de resolució, en el seu cas. Aquest procediment haurà de ser divulgat per a que serveixi de coneixement i conscienciació de tots els seus treballadors.

- L'adjudicatària ha d'adoptar les mesures adequades per tal de que es solucioni l'anomalia generadora de la incidència en el menor temps possible.

- De cada incidència succeïda, L'adjudicatària ha de registrar: tipus d'incidència, descripció, moment en què s'ha produït o detectat, persona que la notifica, persona a la que se li comunica, efectes derivats, mesures correctores aplicades, procediments realitzats de recuperació de dades, persona que els executa, dades restaurades i enregistrades manualment.

- El Responsable del fitxer ha d'autoritzar l'execució dels procediments de recuperació de dades (en cas de ser necessari).

- L'adjudicatària ha de prestar el suport requerit a la UOC en el cas de que aquest decideixi iniciar una avaluació independent de seguretat o una investigació d'incidències.

- L'adjudicatària ha de definir un mitjà de comunicació segur per comunicar incidències, situacions inusuals, o de qualsevol altre tipus relacionades amb la confidencialitat de la informació de la UOC en un termini màxim de 24 hores.

- L'adjudicatària ha d'informar immediatament a la UOC en el cas de que es detecti o es tingui una sospita d'una incidència de seguretat.

- L'adjudicatària ha d'acordar amb la UOC els criteris per la notificació d'una incidència de seguretat, en els casos de fuita d'informació, disrupció del servei, atacs que afectin a la reputació de la UOC i qualsevol altre cas que sigui acordat.

- La falta de notificació d'una incidència crítica de la que s'hagi tingut coneixement, podrà ser considerada com una falta contra la seguretat dels fitxers, podent constituir un menyscapte de la bona fe contractual.

- El registre d'incidències ha d'estar a disposició de la UOC, que podrà sol·licitar la seva consulta en qualsevol moment, quan així ho requereixi.

12.7.5 Gestió de les operacions

12.7.5.1 Manteniment de sistemes

- L'adjudicatària podrà proposar proactivament la instal·lació d'actualitzacions i pegats de seguretat. Haurà d'existir una política de vigilància d'alertes de seguretat i d'actualització dels pegats de seguretat publicats pels corresponents fabricants.

- En tot cas, el desplegament de pegats s'haurà de provar en entorns previs, a l'objecte d'evitar possibles impactes sobre el Servei.

- Amb independència del software base que doni suport a la plataforma i de les seves versions (sistemes operatius, base de dades, servidor web, etc.), ha d'existir una política de vigilància d'alertes de seguretat i d'actualització dels pegats de seguretat publicats pels corresponents fabricants.

- Els temps d'actuació no han de superar les 24 hores en casos d'errades en la seguretat classificades pel fabricant amb un caràcter greu/alt.

- L'adjudicatària ha d'establir els controls de seguretat adequats en relació amb els canvis que poguessin ser necessaris aplicar sobre les aplicacions, o sistemes involucrats en el Servei. Aquests controls han de cobrir, com a mínim, sol·licituds de canvis, anàlisi d'impacte, autoritzacions, realització de proves, aprovacions de l'usuari final i una separació adequada dels entorns previs respecte de l'entorn de producció.

- L'adjudicatària ha d'establir els mecanismes necessaris per administrar i operar els dispositius de seguretat, sempre que la UOC realitzi una delegació expressa d'aquestes funcions.

12.7.5.2 Ubicació de dades

- L'adjudicatària ha d'informar a la UOC sobre la ubicació de les Dades que seran emmagatzemades abans de la contractació del Servei. Durant el període de duració del Servei, qualsevol canvi en la ubicació de les Dades haurà de ser comunicat a la UOC amb anticipació, i no podrà ser efectuat fins rebre l'autorització de la UOC.

- L'adjudicatària ha d'implementar mecanismes de control de canvi en els fitxers emmagatzemats en el Servei, registrant tota la informació necessària que permeti la traçabilitat dels successos.

12.7.5.3 Gestió de suports d'informació

- L'adjudicatària ha de disposar d'un inventari d'actius d'informació que identifiqui el tipus d'informació continguda en cadascun d'ells. La identificació dels suports es realitzarà amb un sistema d'etiquetatge únicament comprensible pels usuaris autoritzats.

- L'adjudicatària ha de xifrar les Dades en la distribució de suports i en els dispositius portàtils, evitant el tractament en dispositius portàtils que no permetin el xifrat, adoptant mesures que tinguin en compte els riscos en entorns desprotegits.

- L'adjudicatària ha de garantir l'emmagatzemament segur dels suports que continguin informació de la UOC en una ubicació amb accés restringit al personal autoritzat.

- L'adjudicatària ha d'implantar els mecanismes suficients per garantir la custòdia segura dels suports amb informació de la UOC quan aquests no estiguin emmagatzemats en ubicacions segures.

- L'adjudicatària ha de disposar d'un Procediment de Gestió de Suports en el que defineixi els mètodes de custòdia dels suports d'informació i els responsables d'autoritzar els accessos als mateixos.

- L'adjudicatària ha de garantir que qualsevol tipus de recepció o enviament de suports sigui efectuat exclusivament per personal autoritzat.

- Quan es procedeixi al trasllat de documentació continguda en un fitxer, s'han d'adoptar mesures dirigides a impedir l'accés o la manipulació de la informació continguda.

- L'adjudicatària ha de mantenir un registre d'entrada i sortida de suports que permeti conèixer el tipus de suport o document, la data i hora, l'emissor i/o receptor, el tipus d'informació, la forma d'enviament i la persona responsable.

- L'adjudicatària ha d'adoptar mesures per evitar accessos indeguts a la informació en cas d'abandonament de suports.

12.7.5.4 Fitxers temporals

- El Proveïdor, en cas d'emprar fitxers temporals o auxiliars per la prestació del servei, ha de protegir-los amb les mateixes mesures de seguretat emprades en els fitxers principals, i haurà d'esborrar-los, eliminar-los o destruir-los de forma segura un cop hagin deixat de ser necessaris per les finalitats que van motivar la seva creació, garantint que no es permeti la seva posterior recuperació.

- Els responsables dels sistemes de informació, designats a tal efecte, hauran de verificar periòdicament la possible existència de fitxers temporals creats automàticament com a conseqüència del mal funcionament dels sistemes.

- Llevat de que el servei així ho requereixi, s'evitarà la impressió en paper de dades personals des de les aplicacions de gestió de les mateixes.

12.7.5.5 Servei compartit

- L'adjudicatària ha d'implementar les mesures suficients per garantir la seguretat de la infraestructura tecnològica en cas de que sigui compartida amb altres clients de l'adjudicatària. La infraestructura tecnològica del Servei haurà de posseir canals de comunicació xifrats entre altres serveis que ofereixi L'adjudicatària i les connexions del personal responsable de l'administració de la infraestructura. Per exemple; SSH, VPN amb IPSEC, etc.

- L'emmagatzemament de dades del Servei prestat a la UOC haurà d'estar aïllat, lògicament d'altres repositoris d'emmagatzemament aliens. El Servei de l'adjudicatària haurà de tenir la capacitat de xifrar la informació emmagatzemada, mitjançant algoritmes forts de xifrat, en cas de ser requerit.

12.7.6 Revisió

12.7.6.1 Revisions realitzades per la UOC

- La UOC podrà realitzar revisions de caràcter:

    a. Ordinari, com a part de l'avaluació de la prestació del Servei.
    b. Extraordinari, com a conseqüència d'una incidència en la seguretat, o en cas de produir-se alguna ampliació, regressió dels serveis o donar-se circumstàncies que duguin a la UOC a considerar oportuna la seva realització.

- L'adjudicatària acceptarà la realització d'aquestes revisions assumint el seu cost en aquells casos que la UOC estimi oportuns.

- La UOC realitzarà aquestes revisions en funció de l'esquema de control, seguint un mètode d'avaluació, abast, mètode de seguiment i periodicitat establerts per la UOC.

- L'adjudicatària ha de prestar tota la col·laboració que sigui necessària per donar un adequat compliment als requeriments de la revisió que puguin ser formulats per la UOC, les persones o empreses designades per la UOC, i ha de entregar tota la documentació i/o evidències que li siguin sol·licitades a efectes d'aquesta revisió.

- Addicionalment, la UOC exercirà el control sobre els riscos tecnològics associats al Servei, rebent de l'adjudicatària la següent informació quan li sigui requerida:

    a. Revisió d'informes d'auditoria i/o certificacions referits a:

i. Informes d'auditoria interna /control intern.
ii. Informes emesos per tercers independents (SOC 2 tipus 2, ISAE 3402, SSAE 16, etc.).
iii. Certificacions de seguretat (ISO 27001, etc.).
iv. Certificacions de qualitat del Servei (ISO 9001, ISO 2000, etc.).

- Addicionalment als informes presentats, la UOC haurà de tenir la capacitat de desenvolupar un pla d'avaluació de controls de risc tecnològic i d'executar-lo d'acord amb els terminis de temps, abast i procediments que s'acordin amb el Proveïdor. Aquest pla pot incloure:

  a. Supervisió periòdica d'indicadors de seguretat del Servei:
     i. Els indicadors a supervisar acordats prèviament a la firma del contracte, que hauran de ser revisats periòdicament.
     ii. Accés a quadres de comandament o consoles per part de la UOC, que li permetin la monitorització continua del risc tecnològic.
  b. Notificació de successos rellevants per part de l'adjudicatària:
     i. Incidències de seguretat.
     ii. Proves de recuperació davant de desastres.
  c. Informació sobre la infraestructura tecnològica que dona suport a la UOC (en cas de que L'adjudicatària utilitzi infraestructura pròpia per la prestació del Servei):
     i. Arquitectura de xarxa.
     ii. Arquitectura de seguretat perimetral
     iii. Servidors i bases de dades.
     iv. Protocols de xarxa i comunicacions.
     v. Altres necessaris per a que la UOC pugui exercir adequadament les funcions de control.
  d. Informació de la monitorització realitzada sobre els sistemes que presten servei a la UOC , així com el model de relació establert per la comunicació d'aquesta informació quan es consideri necessari.

- L'adjudicatària ha de solucionar les debilitats de control identificades per la UOC en les revisions realitzades seguint els plans d'acció acordats.

12.7.6.2 Control intern de l'adjudicatària

- L'adjudicatària ha de disposar d'una funció de control intern que vetllarà pel compliment de tots els controls requerits per la UOC.

- L'adjudicatària ha de descriure i posar a disposició de la UOC, quan així ho sol·liciti, els procediments i controls que articularà internament a l'objecte d'assegurar que els requisits enunciats es compleixen.

- L'adjudicatària ha de realitzar totes aquelles auditories legalment exigibles, tant de manera interna com externa, sobre aquells sistemes involucrats en el servei prestat a la UOC, deixant a disposició de la UOC els informes de auditoria generats.

- L'adjudicatària ha de realitzar revisions de seguretat sobre els seus sistemes quan es realitzin canvis substancials en els sistemes d'informació, deixant a disposició de la UOC l'informe de l'esmentada revisió, sobre l'adequació a les mesures, les deficiències identificades, i proposarà mesures correctores.

12.7.6.3 Controls coordinats amb la UOC

- La UOC i L'adjudicatària acordaran els procediments per tal que tota incidència de seguretat sigui comunicada diligentment a la UOC. Es definiran protocols de comunicació específics per aquells casos en els que es requereixi una actuació immediata per part de la UOC a l'objecte de mitigar l'impacte d'incidències de seguretat.

- La UOC podrà verificar en qualsevol moment el compliment dels requisits tècnics, tant mitjançant visites a les instal·lacions de l'adjudicatària, com a través de l'ús de mitjans segurs d'accés remot als sistemes involucrats que s'acordaran amb el Proveïdor.

- Aquells aspectes que s'observin en aquestes revisions i que la UOC consideri una violació del present acord o que puguin posar en risc els sistemes de la UOC seran denunciats al Proveïdor, al qual es donarà un termini de temps per la seva resolució,

amb el consegüent compromís contractual de que aquest doni compliment als aspectes observats segons allò acordat amb la UOC.

12.7.6.4 Devolució del Servei

- La UOC i L'adjudicatària hauran de definir i acordar procediments de devolució del servei de manera que s'asseguri un emmagatzemament segur dels suports i, en el seu cas, una destrucció segura de la informació emprada per l'adjudicatària durant la prestació del Servei.

- L'adjudicatària haurà de garantir que s'empraran mecanismes d'eliminació segura d'informació. Aquests inclouran els casos de reciclatge de suports i de finalització del Servei. Amb aquestes mesures, la UOC s'assegura que la informació no és enviada sense aprovació a altres ubicacions i que no es pot extreure informació dels suports després del seu ús.

12.7.7 Seguretat perimetral i d'infraestructura

- L'adjudicatària informarà a la UOC sobre la infraestructura tecnològica desplegada per donar-li Servei, amb el nivell de detall requerit per la UOC per permetre realitzar les tasques de supervisió/monitorització establertes per la UOC.

- L'adjudicatària ha de desenvolupar una infraestructura tecnològica per la prestació del servei, de manera que es faciliti la migració modular a un altra ubicació o una migració tecnològica.

12.7.7.1 Seguretat dels servidors

- Els servidors es trobaran a la plataforma corresponent seguint les bones pràctiques reconegudes i, únicament es trobaran actius els serveis necessaris.

- S'ha de garantir la protecció de les Dades i assegurar que no són visibles excepte en el cas de la UOC. Les Dades, ja resideixin en bases de dades o en sistemes de fitxers, únicament seran accessibles des de les aplicacions que les processin, i, en cap cas, hauran de ser accessibles de manera pública des de xarxes externes.

- El Servidor de la base de dades s'haurà d'ubicar en un sistema diferent al d'execució de l'aplicació, habilitant únicament la comunicació amb el servidor en què s'allotgi l'aplicació, no havent de ser directament accessible des d'Internet.

- Els servidors es trobaran adequadament tancats/precintats a l'objecte de que qualsevol manipulació pugui ser detectada visualment.

- Els servidors hauran de disposar de protecció antivirus, que haurà de mantenir-se operativa i actualitzada en tot moment.

12.7.7.2 Seguretat perimetral

- El servidor que allotgi l'aplicació haurà d'estar protegit d'accessos de tercers mitjançant un Firewall.

- En cas de que existeixin aplicacions exposades a Internet, l'accés a les mateixes ha d'estar apantallat per un dispositiu que funcioni com a proxy invers, ubicat en una DMZ protegida per una doble barrera de Firewall.

12.8 Monitorització

14.8.1 Monitorització de la seguretat dels sistemes

- L'adjudicatària posarà a disposició de la UOC, quan així li ho sol·liciti, els procediments i controls que implementarà per monitoritzar i alertar sobre possibles violacions de la seguretat dels sistemes.

12.8.2 Custòdia i explotació dels logs de seguretat

- Pel que fa als successos que generen logs, la UOC especificarà el format i contingut dels registres, i el període de custòdia. L'adjudicatària ha de generar logs (accés, autenticació, administració i activitat), com a mínim, dels següents successos:

    a. Comunicacions;
    b. Enviament de fitxers (sistemes involucrats en la transmissió, tant en origen com a destinació, i sistemes intermedis d'emmagatzemament temporal);
    c. Aplicacions web;
    d. Sistemes de virtualització (arquitectura client-servidor); i,
    e. Back-end (servidors i aplicacions).

- Supervisió de la configuració de seguretat dels elements que conformen la infraestructura tecnològica que proporciona Servei a la UOC.

12.9 Suport, continuïtat i contingència

- L'adjudicatària ha d'establir i aplicar una política de realització de còpies de suport que inclogui la seguretat sobre les còpies i els procediments de prova i recuperació. L'adjudicatària tindrà controls implementats per assegurar la correcta manipulació i transport dels mitjans d'emmagatzemament de les còpies de seguretat, assignant responsables, controls d'accessos físics i lògics, cadena de custòdia i inventaris periòdics.

- L'adjudicatària ha d'implementar controls en la seva política de còpies de seguretat que garanteixin la recuperació de les Dades en l'estat en què es trobaven en el moment de produir-se una incidència de modificació, pèrdua o destrucció.

- L'adjudicatària ha de realitzar còpies de seguretat dels seus sistemes de forma periòdica que compleixi amb allò que s'estableix en els Temps Objectius de

Recuperació i el Punt Objectiu de Recuperació, que han de ser inclosos en el Pla de Continuïtat del Negoci i Recuperació davant un desastre.

- L'adjudicatària ha d'establir procediments per la realització, com a mínim, setmanal de còpies de seguretat, llevat que en aquest període no s'hagués produït cap actualització de les Dades.

- L'adjudicatària ha d'incloure en la seva política de còpies de seguretat, la verificació i realització de proves semestrals de l'efectivitat dels procediments de còpia per part del responsable del fitxer.

- Únicament es treballarà amb dades reals si s'assegura el nivell de seguretat corresponent al tipus de fitxer tractat.

- L'adjudicatària disposarà d'un Pla de Continuïtat del Negoci i Recuperació davant un Desastre, que li permeti recuperar el Servei de sistemes d'informació formalment documentat i provat de forma periòdica, alineat amb el servei prestat a la UOC.

12.10 Mesures específiques

- L'adjudicatària es compromet a complir amb totes aquelles polítiques, dictàmens i documents específics de seguretat realitzats per la UOC durant tot el cicle de vida de la externalització del Servei, aplicables a la prestació del servei en l'àmbit del contracte.

En cas de que el Servei tracti informació subjecta a certificacions de seguretat, L'adjudicatària haurà de presentar a la UOC les certificacions aplicables, quan així li ho requereixi.

13 Annex - Full de Ruta de Programari

Criteris de selecció de versions:

1. La versió ha d'estar suportada pel fabricant en el moment del disseny del sistema (si la versió "suportada" UOC no estigués alineada amb el fabricant, es selecciona l'última suportada pel fabricant).

2. Preferiblement s'han d'utilitzar "versions recomanades".

			Obsolet	Suportat	Recomanat UOC	Distribució / Observacions
Llenguatges i runtimes	Golang		<= 1.17	>= 1.18	1.19	
	Java		< 11	11, 17	17	Només s'accepten versions LTS
	NodeJS		<= 14	16, 18	18	Només s'accepten versions LTS
	Python		<= 3.7	>= 3.8	3.11	
	PHP	Només manteniment	<= 8.0	>= 8.1	8.2	Només per a WordPress o Drupal que estiguin en manteniment, no per a aplicacions noves. Ni WP ni Drupal són els gestors de continguts recomanats per l'Àrea de Tecnologia

Frontal web	Angular		<= 12	13	14	Només s'accepten versions LTS
	React		<= 16	17	18	
	Vue		<= 2.6.x	>= 2.7.x	3.2.x	
Gestió de dependències	Maven (Java)		<= 3.6	>= 3.8	3.8	
	NPM (NodeJS)		< 7.10	>= 7.10	9.3	
	Go Modules (Golang)		<= 1.16	>= 1.17	1.18	
	PiP (Python)		<= 21.x	22.x	22.x	

Frameworks de Desenvolupament	Spring Framework (Java)		<= 4.3.x, <= 5.2.x	5.3.x	6.0.x	Alineades amb les version de JDK 11-17
	Flutter (desenvolupament apps natives)				Stable Channel	SDK de Google basat en Dart per a accelerar el desenvolupament d'apps Android i iOS. Recomanada l'última "Stable channel"
	Serverless Framework		< 3.19.x	>= 3.19.x	3.27.x	Es pren de referència la darrera minor version en data 31/1/2023
	Hugo (webs estàtiques)		< 0.91.x	>= 0.101.x	0.109.x	Es pren de referència la darrera minor version en data 31/1/2023
	Gatsby (webs estàtiques)		< 4.17.x	>= 4.17.x	5.5.x	Es pren de referència la darrera minor version en data 31/1/2023

Gestió de versions de DB	Flyway (Java)		< 7.5.x	>= 7.5.x	9.x	Suportades versions que han tingut alguna release durant els últims 2 anys
	Liquibase (Java)		< 4.8	>= 4.8.x	4.19.x	Suportades versions que han tingut alguna release durant els últims 2 anys
	SQLAlchemy Alembic (Python)		< 1.6	>= 1.6.x	1.9.x	Suportades versions que han tingut alguna release durant els últims 2 anys
	migrate (Golang)		< 4.15	>= 4.15.x	4.15.x	Suportades versions que han tingut alguna release durant els últims 2 anys
	Sequelize (NodeJS)		< 5.22	>= 5.22.x	6.28.x	Suportades versions que han tingut alguna release durant els últims 2 anys

LowCode Application Platform	OutSystems		-	-	-	És el mètode preferent de desenvolupament d'aplicacions a la UOC. S'han d'analitzar les característiques del sistema abans de decidir anar a lowcode o desenvolupament tradicional. La plataforma lowcode té limitacions relatives al llicenciament (volum d'usuaris, nivell de suport, ...).
Infraestructura com a Codi	Terraform		< 1.1.x	>= 1.1.x	1.3.x	Suportades versions minor per les quals la data d'alliberament de la última release tingui una antiguitat inferior a 1 any
Bases de Dades (Relacional)	Oracle	Només manteniment	<=11g	12c		Només per manteniment d'aplicacions legacy
	MySQL		<=5.6	>=5.7	8.0	A AWS recomanem Aurora

	PostgreSQL	Opció recomanada	<11.x	>=11.x	14	A AWS recomanem Aurora
Bases de Dades (Documental)	MongoDB		<=4.2	>=4.4	5.0	
	AWS DynamoDB					AWS
	AWS DocumentDB					AWS
Bases de Dades (Clau-Valor)	Redis		< 6.0	>=6.0	7	A AWS recomanem Elasticache
CMS i Portals	Liferay	Només manteni	<= 7.2.x	7.3.x	7.4.x	Es consideren com a suportades les versions de Liferay dins "Premium Support Phase"

		ment				
	OpenCMS	Només manteniment	< 12.x	12.x, 13.x	14.x	
	WordPress	Només manteniment	<= 4.x	>= 5.x	>= 6.x	No es poden desenvolupar sistemes d'informació amb WP, només per a serveis existents que ja es basen en aquest producte
	DXP					SaaS
CRM	Salesforce					SaaS
Runtimes Docker	Java		eclipse-temurin:8-jre-alpine	eclipse-temurin:11-jre-alpine	eclipse-temurin:17-jre-alpine	Alpine com a distribució recomanada. En cas de problemes (incompatibilitats) en fase de projecte es decidirà quina altre utilitzar.

	NodeJS		node:8.16.0-alpine node:10-alpine node:12-alpine node:14-alpine	node:16-alpine	node:18-alpine	Alpine com a distribució recomanada. En cas de problemes (incompatibilitats) en fase de projecte es decidirà quina altre utilitzar.
	Golang		golang:1.11-alpine golang:1.12-alpine golang:1.13-alpine golang:1.14-alpine golang:1.15-alpine golang:1.16-alpine golang:1.17-alpine	golang:1.18-alpine	golang:1.19-alpine	Alpine com a distribució recomanada. En cas de problemes (incompatibilitats) en fase de projecte es decidirà quina altre utilitzar.

	Python		python:2.7-slim-buster python:3.6-slim-buster python:3.7-slim-buster	python:3.8-slim-buster python:3.9-slim-buster python:3.10-slim-buster	python:3.11-slim-buster	Debian com a distribució recomanada. En cas de problemes (incompatibilitats) en fase de projecte es decidirà quina altre utilitzar.
Servidor web	Apache	Només manteniment	<= 2.2	2017-04-01T22:00:00.000Z	2017-04-01T22:00:00.000Z	
	NGinx		< 1.21.x	1.21.x	1.22.x	
Servidor d'aplicacions	WildFly	Només manteniment	<= 20.x	>= 21.x	27.x	Es recomana anar a runtime Docker de Java i Spring Boot
	JBoss EAP	Només manteni	<= 7.3.x	7.4.x	7.4.x	Es recomana anar a runtime Docker de Java i Spring Boot

		ment				
	Tomcat	No recomanat	<= 7.x,8.0, 10.0.x	8.5, 9.0	10.1.x	Es recomana anar a runtime Docker de Java i Spring Boot
	Jetty	No recomanat	<= 9.x	10.x	11.x	Es recomana anar a runtime Docker de Java i Spring Boot
Sistemes operatius	Ubuntu	Només manteniment	< 17.x			
	RHEL/CentOS	Només manteniment	< 7	7.x	8.x	
	Amazon Linux 2	Opción recomanda				Utilitzar la AMI corporativa "TEMPLATE_UOC"

		AWS				
	Suse	Només manteniment	< 12.x			
	Windows Server		<= 2012 R2	2016	2019	Nomes per a servidors de Xarxa Interna, no per a serveis en producció
	Windows Desktop		< 10	10	11	Nomes per a equips d'usuari, no per a serveis en producció
	Solaris	Només manteniment	< 10	11		