CSUC Exp. 21/25 l'acord marc d'homologació de proveïdors per al subministrament de llicències de programari de Salesforce i de solucions especialitzades de backup per Salesforce i els seus serveis associats per a les entitats que integren el grup de compra LOT 1

UNIVERSITAT OBERTA DE CATALUNYA

CONTRACTACIÓ DERIVADA

FITXA D'INVITACIÓ

ÒRGAN DE CONTRACTACIÓ

L'òrgan de contractació que adjudicarà i formalitzarà el contracte serà el Sr. Antoni Cahner Monzó, Gerent de la Universitat Oberta de Catalunya.

A OBJECTE I MODALITAT DEL CONTRACTE DERIVAT

Títol: **Serveis per la implantació d'EducationCloud**

Número d'expedient: **DER17/CSUC2125/L1**

Codi CPV: 72000000-5 Serveis TI: consultoria, desenvolupament de programari, Internet i suport.

Empreses a convidar:

Segons la clàusula 23.1.3., l'òrgan de contractació de l'entitat iniciarà la licitació de cadascun dels contractes basats, mitjançant l'enviament, per correu electrònic o e-notum, d'una invitació a les empreses que correspongui segons el rang econòmic de la licitació (mínim de tres licitadors per contractes de 50.000 € fins a 221.000 € i tots els licitadors als contractes superiors a 221.000 €), i hagin estat seleccionades en l'acord marc, a fi i efecte que presentin, en un termini no superior a deu (10) dies naturals, la documentació següent: una oferta econòmica, igual o inferior a la presentada a l'acord marc i la declaració responsable de vigència dels requisits de capacitat i aptitud per contractar.

Les empreses homologades a convidar són les següents:

Lot 1:

Empresa
Navarra Tecnologia De Software SL
Omega CRM Consulting S.L.
VASS Consultoría de Sistemas SL

Les empreses homologades resten vinculades pel seu preu màxim d'homologació, pel que individualment hauran d'ofertar un preu igual o inferior a aquest.

Els preus màxims presentats pels proveïdors en l'homologació són els següents:

Perfils	OMEGA CRM	NTS SEIDOR	VASS
Tarifa màxima Consultor sènior (per hora).	55,00 €	49,00 €	45,00 €
Tarifa màxima Arquitecte (per hora).	60,00 €	49,00 €	50,00 €
Tarifa màxima	55,00 €	49,00 €	42,00 €

B VALOR ESTIMAT DEL CONTRACTE

Tres-cents setanta-vuit mil cinc-cents vuitanta-cinc euros **(399.300,00 €), IVA exclòs**

D'acord amb la següent estimació:

Perfils	Preu/hora màxim (IVA exclòs)	Hores estimades	Import per perfil (IVA exclòs)
Consultor sènior	55,00€	1.800	99.000,00 €
Arquitecte	60,00€	880	52.800,00 €
Analista Programador (Platform developer II)	55,00€	4.500	247.500,00 €
			399.300,00 €

El valor estimat del contracte s'ha calculat partint dels preus unitaris màxims que van oferir les empreses en la seva homologació pels perfils demanats i l'estimació d'hores necessàries per a cada perfil.

Dins d'aquesta xifra NO hi ha inclòs cap import destinat a modificacions contractuals.

Platform developer II (per hora).			

C PRESSUPOST BÀSIC DE LICITACIÓ I PREUS APLICABLES

Quatre-cents cinquanta-set mil tres-cents vuitanta (483.153,00 €), IVA inclòs.

- 399.300,00 euros import net
- 83.853,00 euros import IVA (21%)

Sistema de determinació del preu: **Tant alçat**

El preu de la licitació (i el que serà objecte de valoració) és un preu tancat a tant alçat pel total de les tasques a realitzar. El total de l'oferta i l'adjudicació serà el resultant de sumar les hores proposades pel preu hora proposat dels diferents perfils demanats:

Perfils	Preu/hora màxim (IVA exclòs)	Hores estimades	Total IVA exclòs	Total IVA inclòs
Consultor sènior	55,00€	1.800	99.000,00 €	119.790,00 €
Arquitecte	60,00€	880	52.800,00 €	63.888,00 €
Analista Programador (Platform developer II)	55,00€	4.500	247.500,00 €	299.475,00 €
TOTAL (IVA inclòs)				**483.153,00 €**

El pressupost de licitació contracte basat pels Serveis s'ha calculat partint dels preus màxims per perfil oferts a l'homologació). No obstant, cadascuna de les empreses homologades tindrà com a preu màxim aquell corresponent al que va oferir a la seva pròpia homologació.

Facturació d'imports per part del contractista:

Fita de meritació	% sobre import d'adjudicació
FM-1 **Aprovació de l'estructura de projecte, equips i fases de preparació i validació del pla de govern del risc i del pla de govern del projecte**, i el contingut de tots els entregables que forma part del projecte, el primer mes després de l'inici del contracte. Evidència: Acta de reunió amb la validació per part del comitè de direcció.	5%
FM-2 Aprovació per part del comitè de direcció de tots els **plans vinculats al projecte**, segons s'ha descrit en	10%

D DURADA, PRÒRROGUES I CONDICIONS DE SUBMINISTRAMENT

Durada: Vint-i-quatre (24) mesos des de la signatura del contracte basat.

Es preveu la possibilitat de pròrroga (pròrrogues): SÍ ☐ NO☒

Lloc del subministrament: Els serveis es presten de forma remota.

Veure annex 2.

l'apartat d'objectius, (als 3 mesos després de la data d'inici del projecte). Pla de desplegament Pla d'adopció i govern del producte Pla de proves i qualitat Pla de posta en marxa Pla de Transició i gestió del canvi Pla de monitoratge i observabilitat Pla de contingència Pla de govern del risc Pla de govern del projecte Pla de projecte Pla de disponibilització (dades) Pla de revisió/definició dels dominis (dades) Pla de seguretat Pla de compliment normatiu Pla de post implantació Pla de migració Mapa d'integracions Document d'Arquitectura Manual d'operació Principis de disseny Evidència: Acta de reunió amb la validació per part del comitè de direcció.	
FM-3 Aprovació explícita pel comitè de direcció del **plantejament global de parametrització i configuració** al cap de 4 mesos després de la data d'inici del projecte). Evidència: Acta de reunió amb la validació per part del comitè de direcció.	10%
FM-4 Aprovació explícita pel comitè de direcció de la suficiència del **grau d'avenç de tots els plans vinculats** a la posada del servei d'atenció segons s'ha aprovat en el pla de projecte (al cap de 6 mesos des de l'inici del projecte). Evidència: Acta de reunió amb la validació per part del comitè de direcció.	15%
FM-5 Acceptació per part del Comitè de direcció del r**esultat de les proves d'acceptació (UATs) per al servei d'atenció**, al cap de 8 mesos des de l'inici del projecte. Evidència: Acta de reunió amb la validació per part del comitè de direcció.	15%
FM-6 Aprovació explícita de l'inici del suport post-implantació complint els ANS definits en el marc del contracte, 1 més després de la posada en marxa del **servei d'atenció** Evidència: Acta de reunió amb la validació per part del comitè de direcció.	10%
FM-7 Acceptació per part del Comitè de direcció del r**esultat de les proves d'acceptació (UATs) pel servei de tutoria**, al cap de 16 mesos des de l'inici del projecte. Evidència: Acta de reunió amb la validació per part del	15%

comitè de direcció.	
FM-8 Aprovació explícita de l'inici del suport post-implantació complint els ANS definits en el marc del contracte, 1 més després de la posada en marxa del **servei de tutoria** Evidència: Acta de reunió amb la validació per part del comitè de direcció.	10%
FM-9 Tancament del projecte. Evidència: Acta de reunió amb la validació per part del comitè de direcció.	10%

Criteris de facturació:

Des del moment de meritació de cada pagament que pertoqui i, en rebre la factura corresponent, si no es detecta cap incidència o error es procedirà a abonar l'import que pertoqui mitjançant una transferència bancària al número de compte que el contractista hagi indicat.

L'enviament de les factures s'ha de fer per un dels dos canals següents a l'atenció de l'Àrea d'Economia i Finances:

- En format digital, a la bústia de correu electrònic factures@uoc.edu
- En format electrònic, al web https://seu-electronica.uoc.edu, des del qual es pot accedir a l'espai https://efact.eacat.cat/bustia/?emisorId=16

Per a la cessió o endós de qualsevol factura emesa en relació amb els subministraments i serveis objecte de contractació caldrà la conformitat prèvia de la UOC.

E DATA MÀXIMA DE PRESENTACIÓ D'OFERTES I INSTRUCCIONS DE PRESENTACIÓ

LLOC, DIA I HORA MÀXIMS DE PRESENTACIÓ DE LES OFERTES:

Mitjans electrònics a través de:

https://contractaciopublica.gencat.cat

Formats de documents electrònics admissibles:

Format .PDF o formats similars que admetin signatura electrònica

DATA I HORA MÀXIMES: **5 de maig de 2025** HORA:**12.00:00h**

INSTRUCCIONS DE PRESENTACIÓ:

☒ Les ofertes s'han de presentar en **1 SOBRE,** denominat "3 – Oferta econòmica".

F MESA DE CONTRACTACIÓ

President: Alexandre Hernández Ossó, Director Grup Operatiu Jurídic-Contractual i Advocat l'Àrea d'Assessoria Jurídica de la UOC.

Secretari: Jordi Vidiella Curto, Advocat especialitzat en Contractació Pública de l'Assessoria Jurídica de la UOC.

Vocal 1: Pedro Mingueza de la Vila, Tècnic especialitzat de l'Àrea de Tecnologia o persona que el substitueixi.

Vocal 2: Manel Nofuentes Ramos, Tècnic especialitzat/da en Contractació Pública de l'Assessoria Jurídica de la UOC

G CONTINGUT DEL SOBRE 2 I OBERTURA

Extensió màxima del contingut? SÍ☒ NO☐

1 Solució proposada (màx. 30 planes)

1.1 Education Cloud com a resposta al repte (màx. 18 planes)

El licitador presentarà la proposta de solució a les prescripcions descrites a l'annex 2. Farà una descripció detallada de com es donarà resposta a la necessitat des de les prestacions de la plataforma i de quina és la proposta per maximitzar el valor de la mateixa.
Per a la valoració d'aquest criteri d'adjudicació es prendran en consideració els següents aspectes:

H CRITERIS DE VALORACIÓ DEL SOBRE 2

☒ **Hi ha Sobre 2.**

TOTAL DE PUNTS **(a adjudicar mitjançant els criteris d'aquest apartat)**		**49**
1	**Solució proposada**	**20**
1.1	Education Cloud com a resposta al repte	**12**

- La proposta de cobertura de les necessitats en base a l'aprofitament de les capacitats de la plataforma.
- La proposta de valor addicional en l'aprofitament de les capacitats de la plataforma més enllà de la necessitat base.
- La proposta per a la gestió del cicle de vida de la solució en un context de plataforma compartida amb altres solucions i equips de treball.

Criteri de valoració apartat 1.1 (Fins a 12 punts)

- **12 punts.** La proposta aporta elements complementaris que donen una visió innovadora i diferencial amb relació a les necessitats (annex 2) que asseguren l'assoliment dels objectius.
- **6 punts.** La proposta aporta elements complementaris que donen una visió innovadora i diferencial amb relació a les necessitats (annex 2), però no incrementen de forma substancial les probabilitats d'assoliment dels objectius.
- **3 punts.** La proposta presenta ambigüitats que només permeten assegurar l'assoliment dels objectius parcialment.
- **0 punts**. La proposta és incompleta o no permet assegurar l'assoliment dels objectius.

1.2 Equip de treball (màx 10 planes)

Es presentaran els perfils indicats anteriorment amb el volum i distribució que es consideri oportú.

Es valorarà el grau d'adequació i la coherència de l'equip proposat atenent les necessitats del servei a executar.

El grau d'adequació dels perfils a les activitats dels serveis. Les evidències presentades en relació a l'experiència dels perfils que confirmin l'adequació de l'equip, tot a partir de:

- Experiència prèvia en la implantació d'Education Cloud
- Encaix de cada perfil amb els diferents rols necessaris per a la implantació
- Relació de treballs fets prèviament per cada perfil proposat amb relació a les tecnologies requerides a l'annex 2.

Criteri de valoració apartat 1.2 (Fins a 8 punts)

- **8 punts.** La proposta aporta un equip de treball ajustat a les necessitats que assegura l'assoliment dels objectius.
- **3 punts.** La proposta presenta ambigüitats que només permeten assegurar l'assoliment dels objectius parcialment.
- **0 punts**. La proposta és incompleta o no permet assegurar l'assoliment dels objectius.

2 Model de transformació (màx. 20 planes)

2.1 Proposta de transformació (màx. 10 planes)

Per tal de valorar el nivell de comprensió del licitador del repte, el licitador presentarà la proposta de transformació del model dels serveis d'atenció i tutoria al voltant d'Education Cloud.

Criteri de valoració apartat 2.1 (Fins a 8 punts)

- **8 punts.** La proposta aporta elements complementaris que donen una visió innovadora i diferencial de la transformació que assegura l'assoliment dels objectius.
- **4 punts.** La proposta aporta elements complementaris que donen una visió innovadora i diferencial de la transformació, però no incrementen de forma substancial les probabilitats d'assoliment dels objectius.
- **2 punts.** La proposta presenta ambigüitats que només permeten assegurar l'assoliment dels objectius parcialment.
- **0 punts**. La proposta és incompleta o no permet assegurar l'assoliment dels objectius.

1.2	Equip de treball	**8**
2	**Model de transformació**	**15**
2.1	Proposta de transformació	**8**
2.2	Proposta de desplegament	**7**
3	**Arquitectura i integracions**	**8**
4	**Gestió del canvi i formació**	**6**
4.1	Gestió del canvi	**3**
4.2	Formació	**3**

Normalització

Per a cadascun dels criteris subjectius, una vegada determinada la puntuació tècnica de l'apartat per a totes les ofertes, s'aplicarà la següent fórmula lineal i proporcional on l'oferta tècnica amb la millor valoració obtindrà la màxima puntuació de l'apartat, la resta d'ofertes obtindran una puntuació proporcional i l'oferta que obté valoració zero mantindrà els zero punts:

$$Pop = P * \frac{VTop}{VTmv}$$

On:

- Pop és la puntuació de l'apartat per a l'oferta a valorar.
- P és la puntuació màxima de l'apartat.
- VTop és la valoració tècnica de l'apartat per a l'oferta que es puntua. VTmv és la valoració tècnica de l'apartat amb millor valoració.

2.2 Proposta de desplegament (màx. 5 planes)

El licitador presentarà la descripció de les diferents fases del servei que cobriran tot el període de durada del contracte en base a les prescripcions tècniques descrites al l'annex 2. Farà una descripció detallada de la seva temporalitat, les activitats, l'equip i dedicacions previstes.

Per a la valoració d'aquest criteri d'adjudicació es prendran en consideració els següents aspectes:

- Que sigui específic per l'objecte del contracte, pels serveis descrits a l'annex 2 així com pel context de treball detallat (eines i procediments) El grau d'adequació de les fases del servei a les prescripcions tècniques.
- Assegurant el traspàs de la implantació a l'equip de servei de la UOC.
- Definició i planificació de les activitats de governança i seguiment del projecte.

Criteri de valoració apartat 2.2 (Fins a 7 punts)

- **7 punts.** La proposta aporta una proposta de desplegament diferencial i realista, ajustat a les necessitats.
- **4 punts.** La proposta aporta una proposta de desplegament correcte.
- **1 punt.** La proposta presenta ambigüitats que només permeten assegurar l'assoliment dels objectius parcialment.
- **0 punts**. La proposta és incompleta o no permet assegurar l'assoliment dels objectius.

4. Arquitectura i integracions (màx. 5 planes)

El licitador presentarà la descripció dels mecanismes per garantir l'aplicació dels principis i normativa d'arquitectura descrits a l'Annex - Principis de Tecnologia.

Per a la valoració d'aquest criteri d'adjudicació es prendran en consideració els següents aspectes:

- Concreció en la definició de les activitats i instruments per a una correcta definició, desplegament i manteniment de l'arquitectura de la plataforma Education Cloud i dels sistemes afectats.
- El plantejament d'arquitectura tècnica de la solució.
- Detall i model d'intregració amb les resta d'eines de la UOC necessàries.

Criteri de valoració apartat 4 (Fins a 8 punts)

- **8 punts.** La proposta aporta elements complementaris que donen una visió innovadora i diferencial de l'arquitectura del projecte, i incrementen de forma substancial les probabilitats d'assoliment dels objectius.
- **4 punts.** La proposta aporta elements complementaris que donen una visió de l'arquitectura, però no incrementen de forma substancial les probabilitats d'assoliment dels objectius.
- **2 punts.** La proposta presenta ambigüitats que només permeten assegurar l'assoliment dels objectius parcialment.
- **0 punts**. La proposta és incompleta o no permet assegurar l'assoliment dels objectius.

5 Gestió del canvi i formació (màx. 10 planes)

5.1 Gestió del canvi (màx. 5 planes)

El licitador haurà de proposar les línies mestres del pla de gestió del canvi i d'acompanyament que se'n derivin de la implementació de nous processos.

S'ha de detallar les accions proposades per tal d'assolir èxit en el coneixement i ús de l'aplicació per part dels usuaris finals. Com a mínim ha d'incloure:

- Pla global de gestió del canvi
- Pla de comunicació, amb una descripció de les sessions de comunicació previstes
- Pla de suport en el període de gestió del canvi proposat.

Criteri de valoració apartat 5.1 (Fins a 3 punts)
- **3 punts.** La proposta dona una visió clara i entenedora sobre el pla de gestió del canvi previst.
- **1 punts.** La proposta presenta ambigüitats que només permeten assegurar l'assoliment dels objectius parcialment.
- **0 punts**. La proposta és incompleta o no permet assegurar l'assoliment dels objectius.

5.2 Formació (màx. 5 planes)

El licitador haurà de proposar les línies mestres del pla de formació on es descriguin la metodologia, els recursos i la dedicació prevista per poder instruir a tots els usuaris clau, gestors i mantenidors de les aplicacions incloses dins l'àmbit de subministrament.

Posteriorment i abans de la fase d'implantació, l'Adjudicatari haurà de desenvolupar el pla de formació, que també haurà de ser revisat i aprovat per la Direcció del Projecte.

Criteri de valoració apartat 5.2 (Fins a 3 punts)
- **3 punts.** La proposta dona una visió clara i entenedora sobre el pla de formació previst.
- **1 punts.** La proposta presenta ambigüitats que només permeten assegurar l'assoliment dels objectius parcialment.
- **0 punts**. La proposta és incompleta o no permet assegurar l'assoliment dels objectius.

Obertura Sobre 2 en acte públic: No

I CONTINGUT DEL SOBRE 3 I OBERTURA

OFERTA ECONÒMICA aportada mitjançant l'annex 1 d'aquesta fitxa d'invitació, i amb l'annex I i en format PDF.

Els preus oferts pels licitadors hauran de ser iguals o inferiors als que van oferir respectivament en el procediment d'adjudicació de l'Acord Marc, sense superar els preus unitaris màxims establerts al quadre C.

D'acord amb la clàusula 23.1 Encàrrecs del Plec de clàusules administratives particulars que regulen l'Acord Marc d'homologació de proveïdors per al subministrament de llicències de programari de Salesforce i de solucions especialitzades de backup per Salesforce i els seus serveis associats per a les entitats que integren el grup de compra LOT 1 (exp. 21/25 de CSUC), les empreses han de presentar, a més de l'oferta econòmica, la següent documentació:

- Declaració responsable de vigència dels requisits de capacitat i aptitud per contractar. Veure annex 2
- Si s'escau, declaració responsable relativa a la constitució de garantia definitiva mitjançant la modalitat de retenció en preu. Veure annex 4.

Obertura Sobre 3 en acte públic: Si

Es notificarà als participants la data i hora de l'obertura del sobre 3 que es farà de forma telemàtica.

J CRITERIS DE VALORACIÓ DEL SOBRE 3

Criteris de valoració del sobre 3 **Descompte a aplicar per a cada ítem**	**51 punts**
Oferta econòmica	**51 punts**
Les ofertes presentades pels licitadors es valoraran per la Mesa de contractació d'acord amb el criteri del preu més baix.	

$$Puntuació = 51\ x\ \frac{Preu\ oferta\ menor\ (\%)}{Preu\ oferta\ a\ valorar\ (\%)}$$

On 51 és el nombre de punts màxim que s'atorga en funció de cada producte.

K GARANTIA DEFINITIVA

Ha de constituir-se garantia definitiva?

L CONSULTES I DUBTES

Sol·licituds d'informació addicional. Les empreses licitadores poden dirigir-se a l'òrgan de contractació per sol·licitar els aclariments relatius a l'establert a la fitxa o la resta de documentació que puguin sorgir durant l'elaboració de la seva proposta, a

☒ **Sí. 5%, sobre el preu màxim d'adjudicació, exclòs l'IVA. És a dir, la garantia definitiva es constituirà en relació al preu màxim resultant del càlcul del descompte ofertat pel licitador proposat per l'adjudicació i els consums màxims indicats a l'apartat C.**

La garantia definitiva es podrà constituir mitjançant les modalitats admeses legalment, inclosa la retenció en preu. Els licitadors que optin per aquesta modalitat hauran d'aportar la corresponent declaració responsable conforme a l'Annex 4 de la present fitxa de contractació derivada.

En aquest sentit, dita declaració conforme l'Annex 4 podrà ser inclosa juntament amb la documentació de l'oferta.

través de l'apartat de preguntes i respostes del tauler d'avisos de l'espai virtual de la licitació:

La UOC recollirà tots els dubtes i consultes formulats a l'apartat de preguntes i respostes de l'espai virtual de la licitació i publicarà un anunci al tauler d'avisos del Perfil del contractant de l'entitat, amb el document que recull els aclariments i la informació addicional sol·licitats per les empreses licitadores.

La data màxima per poder enviar les consultes finalitzarà dos dies abans de la data màxima de presentació de propostes. Posteriorment, la UOC no atendrà consultes addicionals.

M PROTECCIÓ DE DADES PERSONALS

Encarregat del tractament de dades de caràcter personal:

El contractista és encarregat de tractament de dades LOPDGDD:
☐ NO. ☒ SÍ.
En cas que sigui encarregat del tractament: Veure annex relatiu a les mesures de seguretat.

Comunicació de dades de caràcter personal:
L'execució del Contracte requereix la comunicació de dades per part de l'entitat contractant:
☒ NO. ☐ SÍ.
L'execució del Contracte requereix la comunicació de dades per part de l'entitat contractista:
☒ NO. ☐ SÍ.

K RECURS ESPECIAL EN MATÈRIA DE CONTRACTACIÓ

En la mesura en què aquest contracte té un valor estimat superior a 100.000 euros, els actes qualificats indicats en l'article 44 de la LCSP poden ser objecte de:

☒ Recurs especial en matèria de contractació davant del Tribunal Català de Contractes del Sector Públic, d'acord amb la regulació d'aquest recurs que es conté a la LCSP i en el termini de quinze (15) dies hàbils a comptar segons allò disposat a l'article 50 de la LCSP o, alternativament, Recurs contenciós administratiu davant del Jutjat contenciós administratiu de Barcelona en el termini màxim de dos (2) mesos a comptar des del dia següent al de la seva notificació, de conformitat amb allò previst a l'article 46 de la Llei 29/1998, de 13 de juliol, Reguladora de la Jurisdicció contenciosa administrativa.

ANNEX 1

MODEL DE PROPOSICIÓ ECONÒMICA I DECLARACIÓ RESPONSABLE

En/Na ....., amb domicili a l'efecte de notificacions a ..... c/ ..... , Núm. ..... amb DNI ..... en representació de ..... amb NIF ..... assabentat/da de les condicions i requisits que s'exigeixen per a l'adjudicació, per procediment derivat de l'Acord Marc d'homologació de proveïdors per al subministrament de llicències de programari de Salesforce i de solucions especialitzades de backup per Salesforce i els seus serveis associats per a les entitats que integren el grup de compra (exp. 21/25 de CSUC), faig constar que:

1. DECLARO sota la meva responsabilitat, que concorren en l'empresa ..... els mateixos requisits de capacitat i aptitud per contractar que van servir per a l'adjudicació del Lot 1 de l'Acord Marc de referència.

2. Em comprometo a portar a terme l'objecte del contracte amb els descomptes sobre preu de catàleg indicats a continuació, més l'import de l'Impost sobre el Valor Afegit que correspongui;

Serveis professionals presentats per la realització del projecte en modalitat claus en ma.					
Perfil	**Nombre Hores**	**Preu hora ofertat (IVA exclòs)**	**Import /IVA exclòs)**	**Import IVA (21%)**	**Import (IVA inclòs)**
Consultor sènior					
Arquitecte					
Analista Programador					
		Total*			

*Cal indicar el preu total de l'oferta, i serà sobre aquest total que es farà la valoració del preu, i en resultarà el preu d'adjudicació.

I perquè consti, signo a ....., ... de ..... de .....

Signatura del/de la declarant

Segell de l'empresa licitadora

ANNEX 2

CARACTERÍSTIQUES TÈCNIQUES DE LA PRESTACIÓ

Justificació

La UOC està immersa en un procés de profunda transformació digital. Una de les línies estratègiques de la mateixa passa per la transformació de l'experiència de l'estudiantat. Aquesta transformació focalitza en primera instància en els serveis d'acompanyament a l'estudiantat i en els processos comercials com a instruments per a garantir la sostenibilitat de la institució i per a aproximar-la a les expectatives que tenen d'ella el seu estudiantat.

Per una altra banda, la UOC està impulsant una altra línia estratègica orientada a la transformació de tots els sistemes que donen suport a la gestió acadèmica (el que es coneix per Student Information System). L'estratègia tecnològica de la Universitat passa per una estratègia SaaS en tots aquells àmbits on existeixi un mercat de productes madur i complet. En aquest sentit, a través de diferents processos, s'ha determinat que l'ecosistema Salesforce, que ja és base en sistemes clau de la UOC, proporciona totes les funcionalitats que donen cobertura als àmbits anteriorment descrits sota una plataforma sòlida, madura i robusta.

En el marc d'aquest projecte es fa necessari disposar d'un **servei** que permeti implementar l'estratègia de desplegament de tot el conjunt de processos a través dels quals es desplega l'acompanyament a l'estudiant a la UOC, sobre el nou vertical Salesforce Education Cloud.

Education Cloud és la proposta específica de servei del fabricant per al sector de l'educació superior.

Per a l'execució de les tasques d'implementació, es requereixen els serveis per garantir una solució sòlida i global sobre la plataforma Education Cloud.

Context

L'acompanyament a la UOC ha de contribuir a una millor experiència de l'estudiantat durant totes les etapes de la seva relació amb la universitat. Ha de respondre a les seves necessitats acadèmiques, socials, emocionals i professionals, afavorint el seu èxit formatiu. A més, l'estudiantat ha de percebre aquest acompanyament com un servei personalitzat i proactiu, que li faciliti els tràmits i li ofereixi respostes àgils, garantint alhora l'eficiència i la sostenibilitat del servei.

Servei d'Atenció

Introducció

El Servei d'Atenció de la UOC té la missió d'oferir un servei excepcional que respongui a les necessitats dels nostres usuaris (estudiantat, professorat col·laborador i públic en general) a través d'una atenció personalitzada i eficient, alineada amb els valors i objectius de la Universitat. El nostre compromís és proporcionar informació, solucions, recursos, acompanyament i oportunitats de forma immediata i accessible, amb l'objectiu de facilitar l'experiència de tots els usuaris que es posen en contacte amb nosaltres. Aquest servei busca un acompanyament que fomenti la vinculació amb la UOC, adaptant-nos a la diversitat de realitats i necessitats de cada persona. A més, treballem per garantir que el desenvolupament de les nostres tasques estigui en sintonia amb els estàndards d'excel·lència de la Universitat, amb l'objectiu de proporcionar respostes completes, optimitzar els temps de resposta i evitar la reiteració de consultes, tot garantint una experiència d'usuari de qualitat i en constant millora.

Situació actual

Equip d'atenció

Actualment, el Servei d'Atenció està format per un volum d'uns 400 agents que s'organitzen de la següent manera:

- 1r nivell / Front Office (FO) format per 50 agents externalitzats
- 2n nivell / Back Office (BO) format per 350 agents entre equip intern UOC (equip de gestió i TGPs (Tècnics Gestió de Programes))

Els quals han de donar resposta a volums d'unes 350K consultes/any (amb una distribució aproximada de 78% FO i 22% BO).

Canals de comunicació

Els usuaris poden interactuar amb el servei d'atenció a través de diversos canals dels que no tots estan integrats a les plataformes UOC.

Com a canals integrats tenim els formularis d'atenció del portal web o l'espai d'atenció dins del Campus Virtual. Les consultes que arriben per aquesta via generen una entrada a l'eina de atenció actual.

Existeixen altres canals d'atenció als usuaris no integrats directament amb les plataformes UOC, com per exemple, correus que arriben a diferents bústies genèriques, missatges en comptes de xarxes socials com X, o atenció síncrona mitjançant trucades en remot per resoldre problemàtiques concretes. En períodes concrets d'activitat també s'habiliten canals específics d'atenció com és el cas del xat integrat, actiu durant els processos d'avaluació final.

Actualment no existeix un canal obert per atendre telefonicament (sí que hi ha un telèfon específic per problemes de recuperació de contrasenya i 2FA (Doble Factor d'autenticació), o en moments concrets de suport a l'activitat com durant les proves finals).

L'atenció per els canals no integrats s'ha de registrar a l'eina d'atenció de manera manual pels agents que atenen la consulta.

Resolució de consultes

Cadascuna de les consultes adreçades pels usuaris, independentment del seu perfil (estudiant, professor, alumni o extern), des dels formularis indicats com a canals integrats, genera una petició en l'eina actual de gestió de casos. Aquestes consultes queden també reflectides a la fitxa única de l'usuari.

En contrapartida, les interaccions dels usuaris que no arriben pels canals integrats (trucades, twitter, comunicació amb un tutor, etc) no queden reflectides de manera específica com una interacció amb l'usuari, ha de ser el gestor qui, manualment, afegeixi aquesta informació a mode de notes/comentaris sobre una consulta existent que pugui estar relacionada amb la consulta realitzada.

A l'entrada de consultes integrada, el sistema assigna una primera classificació de les peticions tenint en compte el perfil de l'usuari i la tipologia de la consulta per assignar-les a un nivell de suport (N1 o N2). Aquest enfocament permet oferir una atenció personalitzada i garantir que cada sol·licitud es gestioni de manera coherent.

Recepció i Classificació de Sol·licituds

Les peticions dels usuaris que arriben a través de canals identificats com integrats (formularis en espais de Campus i portal públic) es vinculen automàticament a la fitxa de l'usuari, mantenint la traçabilitat completa de la seva història d'interaccions amb la UOC. No obstant això, les diferents consultas rebudes d'usuari es visualitzen com a casos individuals no relacionats, cosa que dificulta el seguiment de consultes relacionades (mode conversa). Aquestes consultes entrades pels canals integrats, es classifiquen i assignen automàticament al nivell de suport segons la tipificació seleccionada per l'usuari en el formulari d'entrada a partir de desplegables. Aquesta classificació no és completa ni massa precisa, per la qual cosa els agents han de fer una feina prèvia d'anàlisi del contingut textual de la consulta rebuda per realitzar manualment la correcta classificació i assignació en cas de que sigui necessari.

Pel que fa a les consultes que arriben des de els canals no integrats, la feina d'introducció de la consulta al sistema l'ha de fer el gestor de manera manual: ja sigui creant una consulta nova associant-la a l'usuari (per exemple quan l'usuari truca per problemes amb la contrasenya), ja sigui completant alguna de les consultes obertes i relacionades amb el cas amb la informació addicional rebuda (per exemple quan es fa una trucada a l'estudiant per a recabar més informació respecte a la consulta oberta),

Gestió i Escalat de Casos

Els agents de Nivell 1 tenen accés a l'historial complet de l'usuari i a la descripció detallada de la seva consulta, fet que els permet oferir una resposta eficient i personalitzada. Quan la consulta requereix un coneixement més especialitzat o un grau de personalització més alt, el cas es deriva a Nivell 2, on un equip especialitzat proporciona una solució més detallada. Si la resolució requereix la intervenció d'un especialista d'una àrea específica de la universitat, el cas s'escala a Nivell 3. En aquest nivell, la gestió es duu a terme per un equip que no forma part del Servei d'Atenció mitjançant un sistema d'informació diferent. En aquests casos, és fonamental garantir la traçabilitat, assegurant que la informació necessària es transmeti als agents de Nivell 1 o 2 per proporcionar la resposta adequada.

Assistència i Resolució

Les limitacions generades per l'antiguitat tecnològica de l'eina dificulten la integració de nous canals virtuals, l'atenció integral de l'usuari i impedeixen tenir immediatesa i lògica omnicanal.

Les eines actuals tenen carències que dificulten la gestió eficient de la resolució de les consultes que es supleixen amb accions manuals. Alguns exemples d'aquestes carències:

- Haver d'anotar les trucades telefòniques com a observacions textuals dintre d'una consulta.
- No poder relacionar inputs que un mateix usuari ha fet per diferents canals (bústies d'atenció, canal @UOCrespon de X, telèfon,...).
- No poder fer resolució massiva de casos quan hi ha pics d'entrada de consultas per un mateix motiu.
- Limitació a l'hora d'aplicar filtres de cerca dins de la propia eina per agilitzar l'anàlisi i resolució de casos.
- Mancança de funcionalitats que permetin fer un anàlisi de les dades i seguiment del servei.

Els usuaris són informats sobre l'estat de la seva sol·licitud a través de notificacions (correus electrònics). També poden consultar consultes pendents de respondre i històric de consultes des del seu espai personal de Campus. Quan el cas es resol, l'usuari rep una notificació (email) amb la resposta a la seva consulta.

Com a punts febles del sistema actual:

- De les consultes obertes un usuari només pot conèixer el seu estat (si està pendent de resposta o ja s'ha tancat).
- Un usuari no té cap manera de preguntar/reclamar l'estat d'una consulta oberta no resolta. Això implica que hagi d'obrir una nova petició fent referència el cas original. Això provoca overhead al gestor que al rebre la segona consulta ha de fer la relació amb l'original de manera manual.
- En casos concrets els serveis d'atenció donen respostes parcials per tranquilitzar i/o donar feedback als usuaris però això no es pot fer en tots els casos perquè a més és una tasca manual que a més s'ha de fer de manera individual (consulta a consulta).

Anàlisi i Millora Contínua

L'eina d'atenció no disposa de cap mecanisme que permeti fer un seguiment de l'activitat. A partir de la informació històrica de les consultes s'han generat informes analítics que es generen amb una certa periodicitat però no en temps real. Els indicadors recollits estan relacionats amb volums i tipologies de consultes, temps de resolució. No existeixes indicadors per mesurar la qualitat de les respostes proporcionades.

Conclusions

La situació actual del Servei d'Atenció és la següent:

- Equip format per uns 400 agents dividits entre equip N1 (50 agents externalitzats) i N2 (350 agents gestió/TGPs) no especialitzats.
- Canals digitals d'atenció aïllats i no interrelacionats.
- Es tracten alts volums de consultes (400K a l'any)
- Eina de resolució amb limitacions funcionals que dificulten que els gestors puguin donar un servei de manera eficient i eficaç.
- L'eina actual no té cap funcionalitat que permeti fer un seguiment del servei

Resultats esperats en l'àmbit d'acompanyament per part del Servei d'Atenció

La UOC vol transformar l'experiència de l'estudiantat respecte del Servei d'atenció, per a que aquest sigui ràpid, eficient i omnicanal gràcies a un ecosistema tecnològic enterprise integrat que permeti a l'equip d'atenció millorar en eficiència i productivitat a més de ser proactius i donar una atenció personalitzada. Aquest canvi ens permetrà:

- **Reorganitzar** el servei i impulsar un nou model de **coordinació** interna orientat a resoldre les necessitats de l'estudiant i qualsevol altre usuari que s'adreci als serveis d'atenció.
- Baixar el **temps de resposta** als estudiants prop del 80% en 24h i prop 30% en 1r contacte.

- **Incrementar el nombre de canals** i que estiguin integrats per a una experiencia **omnicanal** i incrementar l'ús de **canals síncrons** (20% de les consultes).
- Escolta de la conversa amb l'estudiant definint patrons per a detectar la **criticitat** de les situacions expressades. Oferir de **forma proactiva trobades síncrones (**trucades, videoconferències, xats…) per a gestionar la situació de la millor manera.
- Disposar de mecanismes que permetin poder fer un **seguiment del servei en temps real** de cara a poder aplicar accions correctives de manera àgil i proactiva.
- Disposar d'una **visió global e integrada de les interaccions** dels usuaris amb els serveis d'atenció i tutoria independentment del canal d'entrada que aquest hagi fet servir per establir el contacte que permeti eficientar el treball dels gestors.
- **Millorar l'experiència dels estudiants versus els serveis d'atenció de la UOC**, per exemple, donant més transparència sobre l'estat de les consultes obertes de manera que es pugui consultar el seu estat i progrés en qualsevol moment, o que aquests rebin notificacions personalitzades.

A continuació es descriu amb més nivell de detall l'aspiracional de Servei d'Atenció al que es vol arribar.

Equip d'atenció

El Servei d'Atenció es vol reorganitzar cap a un model d'equips més especialitzats:

- 1r nivell format per agents externalitzats (encara per determinar la dimensió final d'aquest equip). Licitacions especialitzades
- 2n nivell especialitzat: format per persones del grup operatiu de Serveis d'Atenció amb capacitat de decisió. També són els responsables de sistematizar els processos i continguts que 1r nivell fa servir com a font de coneixement per atendre les consultes.
- 3r nivel de gestió: equip intern UOC (equip de gestió i TGPs (Tècnics Gestió de Programes)) que no forma part del Servei d'Atenció i que dona el seu servei en eines pròpies. La seva resposta mai es fa directa a l'usuari sino que es retorna a un dels altres nivells (1 o 2) per a que ho facin.

Canals de comunicació

Un dels objectius del Servei d'Atenció és garantir que cada usuari pugui contactar amb nosaltres de manera àgil, accessible i eficaç, independentment del canal que utilitzi. La plataforma d'atenció omnicanal ha de permetre als usuaris interactuar amb nosaltres a través de diversos canals integrats, com el portal web, l'espai d'atenció del Campus Virtual, correu electrònic, videotrucades, xarxes socials com X i Instagram, i xat integrat durant els processos d'avaluació.

A més, es vol anar incorporant progressivament nous canals com un xatbot per a consultes recurrents i WhatsApp per a comunicacions instantànies.

Cada interacció ha de mantenir-se fluida i coherent, assegurant que l'atenció sigui ràpida, personalitzada, a través del canal més adequat en cada cas i alineada amb les expectatives dels usuaris.

Resolució de consultes

La gestió de consultes (casos) a dissenyar ha de garantir que cada usuari, independentment del seu perfil (estudiant, professor, alumni o extern), rebi un acompanyament adequat, eficient, personalitzat i a temps. Cada sol·licitud ha de quedar vinculada a l'usuari de manera que es pugui assegurar la traçabilitat de totes les interaccions evitant duplicats.

El sistema ha de ser capaç d'organitzar i classificar automàticament les peticions, tenint en compte el perfil de l'usuari, la tipologia de la consulta i la seva prioritat, per assignar-les al nivell de suport més adequat (N1 o N2), també ha de tindre en compte les disponibilitats dels agents en cada moment per fer una assignació eficient dels casos. Aquest enfocament permetrà oferir una atenció personalitzada i garantir que cada sol·licitud es gestioni de manera estructurada i eficient.

Recepció i Classificació de Sol·licituds

Les peticions dels usuaris podran arribar a través de diversos canals i es vinculen automàticament a la fitxa de l'usuari, mantenint la traçabilitat completa de la seva història d'interaccions amb la UOC. El sistema classificarà i assignarà automàticament cada cas al nivell de suport adequat, garantint una

resposta ràpida i eficaç segons la disponibilitat dels agents i la complexitat del cas. Aquesta assignació ha de tindre em compte tant la disponibilitat dels agents com a criteris de priorització que es puguin establir (aquestes prioritzacions haurien de ser idealment configurables per l'equip intern de Serveis d'Atenció i servirien per adaptar el servei a moments concrets d'activitat, situacions sobrevingudes, etc…).

Gestió i Escalat de Casos

Els agents de Nivell 1 tindran accés a l'historial complet de l'usuari i a la descripció detallada de la seva consulta, fet que, juntament amb el seu coneixement sistematitzat dels processos, els permetrà oferir una resposta ràpida i personalitzada. Quan la consulta requereix un coneixement més especialitzat o no es pugui resoldre immediatament, el cas es derivarà a Nivell 2, on un equip especialitzat proporciona una solució més detallada.

Si la resolució requereix la intervenció d'un especialista d'una àrea específica de la universitat, el cas s'escalarà a Nivell 3 que estarà fora de l'eina del Servei d'Atenció. En aquests casos, és fonamental garantir la traçabilitat, assegurant que la informació necessària es transmeti als agents de Nivell 1 o 2 per proporcionar la resposta adequada.

Assistència i Resolució

Els usuaris reben atenció personalitzada a través de diversos canals de comunicació, amb l'objectiu d'oferir respostes precises, eficients i en el menor temps possible. La incorporació de la intel·ligència artificial i eines de supervisió avançades optimitza el procés de resolució, millorant l'eficiència i la qualitat del servei. Els usuaris estan informats en tot moment sobre l'estat de la seva sol·licitud a través de notificacions i des del seu espai personal. Quan el cas es resol, l'usuari rep una notificació amb la solució proporcionada. El sistema, a més, permet aplicar polítiques proactives per anticipar possibles incidències i resoldre-les abans que l'usuari les sol·liciti, millorant l'experiència d'usuari i garantint una atenció eficient.

Anàlisi i Millora Contínua

Per garantir la millora contínua, es generen informes analítics en temps real amb indicadors clau com el temps mitjà de resolució, el compliment dels Acords de Nivell de Servei (ANS) i la qualitat de les respostes proporcionades pels agents. Aquesta informació facilita la presa de decisions informades i la detecció de possibles àrees de millora, ajudant a optimitzar els recursos i processos del servei. Les eines de supervisió avançades permeten als responsables del servei realitzar un seguiment detallat de cada cas i identificar tendències o anomalies que requereixen atenció immediata. Això garanteix que el servei sigui adaptatiu i que els estàndards d'excel·lència siguin mantinguts de manera constant, millorant així la satisfacció de l'usuari i maximitzant l'eficiència operativa.

El sistema permet realitzar un seguiment proactiu, oferint solucions abans que l'usuari les sol·liciti, reduint la necessitat de noves consultes i millorant l'experiència global de l'usuari. Aquest enfocament no només assegura una atenció de qualitat, sinó que també fomenta una adaptació constant a les necessitats dels usuaris, garantint una millora contínua del servei.

Acció Tutorial

Introducció

Acció Tutorial és un servei de suport continuat a l'estudiant al llarg de tota la seva trajectòria acadèmica a la UOC. El tutor té la responsabilitat d'acompanyar i orientar l'estudiant en tots els àmbits relacionats amb el seu aprenentatge, des de la matrícula fins al seguiment de l'activitat acadèmica, avaluacions digitals i qualsevol altra interacció amb la universitat fora de l'àmbit docent, amb l'objectiu de garantir el seu èxit i prevenir possibles situacions d'abandonament.

Tots els estudiants i tutors disposen d'un espai específic dins del sistema de la UOC, on mantenen una relació propera i compartixen informació sobre l'evolució de l'estudiant, els tràmits acadèmics i altres aspectes relacionats amb el seu procés educatiu.

Els cinc punts clau de l'acció tutorial actualment són:

1. **Incorporació de l'estudiant a la universitat i a l'acció tutorial:** En començar els seus estudis, l'estudiant és acompanyat pel tutor per entendre el funcionament del campus virtual, conèixer el model educatiu de la UOC i familiaritzar-se amb els tràmits i serveis disponibles a través de les diverses eines de la universitat.
2. **Tutorització de la matrícula:** Els estudiants poden enviar al seu tutor una proposta de matrícula que serà validada pel seu tutor, assegurant-se que l'estudiant esculli correctament els crèdits i matèries d'acord amb els requisits acadèmics i personals.
3. **Acompanyament durant el desenvolupament del curs**: Els tutors acompanyen l'estudiant en moments clau del semestre, com la connexió a les aules docents, el seguiment de l'avaluació continuada, la tria de torns per a les proves finals i altres aspectes acadèmics importants. Utilitzen indicadors i eines per detectar possibles riscos d'abandonament i oferir el suport necessari.
4. **Orientació professional**: A mesura que l'estudiant s'apropa al final dels seus estudis, el tutor li proporciona orientació sobre les possibles especialitzacions dins del pla d'estudis, les pràctiques externes i les sortides laborals relacionades amb la seva titulació.
5. **Acompanyament per àmbit de coneixement**: En determinades iniciatives, el tutor acompanya l'estudiant dins d'un àmbit d'estudis concret, proporcionant suport especialitzat en funció de l'àrea de coneixement a la qual pertany el seu pla d'estudis.

La UOC té la voluntat d'ampliar i millorar constantment els serveis d'acompanyament per oferir una atenció integral a l'estudiant, revisant i ampliant les funcions del tutor per assegurar que es doni un suport personalitzat, eficient i alineat amb les necessitats dels estudiants al llarg del seu recorregut acadèmic

La UOC actualment disposa dels següents tipus de tutors per a les diferents iniciatives d'oferta formativa que ofereix:

Iniciativa	Número programes	Tipus de tutor	Número tutors
Graus	**27**	**D'inici - personal propi UOC (2 primers semestres)**	**53**
Graus	27	De seguiment - col·laborador extern (a partir del 3r semestre)	185
Màsters universitaris oficials	53	Únic - col·laborador extern	235
Màsters i postgraus propis	254	Únic - col·laborador extern	50
Cicles Formatius de grau superior (FP)	8	Únic - col·laborador extern	31
CP(Cursos professionalitzadors)	25	Únic - col·laborador extern	6

Escola d'idiomes (CIM) **Majors de 25 anys** **Assignatures lliures**	**4** **4** **+150**	**Únic - personal propi UOC**	**4**
Escola de programació UOC Skills Microcredencials Seminaris Doctorat	2 1 34 2 10	Únic - col·laborador extern	15

L'abast d'aquest plec es limita a la implantació d'una solució per transformar l'acció tutorial per a totes les iniciatives en les que participa un tutor que sigui personal propi de la UOC.

Cal tenir en compte que hi ha 3 iniciatives (Graus, Màsters universitaris oficials i FP) que requereixen una sol·licitud d'accés per part de l'estudiant abans de formalitzar la primera matrícula i en aquest període entre la sol·licitud d'accés i la primera matrícula també hi ha una acompanyament per part d'un tutor.

Situació actual

L'assessorament del tutor actualment requereix d'una configuració i parametrització específica en funció de la campanya, oferta planificada i model d'assessorament.

El tutor actualment s'assigna quan es formalitza la sol·licitud d'accés en aquelles iniciatives en les que es requereix (Graus, Màsters Universitaris i FP) o en el moment de finalitzar la matrícula directa en les iniciatives en les que no es requereix la sol·licitud d'acces.

El procés actual de tutorització per a Graus és el següent:

L'estudiantat de nou accés està assignat a la tutor d'inici durant els seus dos primers semestres a la UOC. Un cop formalitza la tercera matrícula, és reassignat a la tutoria de seguiment de forma manual per l'equip de gestors d'Acció Tutorial per mitjà d'una funcionalitat que ofereix el SIS (Student Information System) actual GAT (Actual plataforma corporativa per la gestió docent). Aquesta acció es fa de forma massiva per a tots els tutors i tots els Graus de la UOC.

Actualment, l'eina principal de treball del tutor d'inici és el **Full de Seguiment**, un full de càlcul a Google Drive on s'hi anota tota la informació rellevant de l'estudiantat per fer-ne un bon seguiment. Es considera poc eficient i intuitiu, utilitzant codis de colors per tal de diferenciar els que estan en diferents situacions (proposta de matrícula realitzada, matrícula formatlizada, etc.) Les dades que s'utilitzen per emplenar aquests Excels s'extreuen de diferents sistemes de la UOC.

Altres eines que fa servir actualment el tutor d'inici per la seva gestió són:

- Espai Virtual d'Acollida (EVA): Accessible des del Campus Virtual per a estudiants que han sol·licitat accés. És l'espai d'interacció estudiant - tutor abans de la primera matrícula. Permet publicar informació i recursos per tal que els estudiants assignats a aquest espai la puguin consultar.
- Aula de tutoria del LMS CANVAS: És l'espai d'interacció estudiant - tutor un cop l'estudiant ha fet una primera matrícula. Disposa d'un fòrum, un tauler per publicar informació per a tots els estudiants de l'aula i un espai per oferir recursos per tal que els estudiants assignats els puguin consultar.
- Qüestionari d'Ampliació de Dades: Espai on l'estudiant registra informació rellevant per a l'acompanyament per part del seu tutor, com per exemple les hores que pot dedicar als estudis.
- Tutorització de matrícula: Permet al tutor donar resposta, recomanant o no, a la proposta de matrícula realitzada per l'estudiant. S'analitza la situació personal i acadèmica de l'estudiant i es planifica la seva matrícula tenint en compte l'estat actual del seu expedient, la dificultat de les assignatures candidates a matricular i la dedicació que requeriran, assegurant que les assignatures escollides siguin compatibles amb les seves responsabilitats personals i professionals. Aquest diàleg entre el tutor i l'estudiant pot tenir diverses iteracions, on es fan diferents simulacions de possibles escenaris acadèmics. Això permet valorar opcions alternatives i ajustar la matrícula segons l'evolució de les necessitats i expectatives de l'estudiant.
- Eina de prevenció d'abandonament: Permet als tutors enviar missatges individuals o massius als estudiants en funció de 9 indicadors de risc d'abandonament que obtenen les dades del LMS

Canvas i el SIS actual GAT. Les dades recullen l'activitat de l'estudiant a CANVAS i accés a diferents espais de les aules així com les qualificacions obtingudes, tan parcials com finals.

- Fitxa de l'Estudiant (visualitzador de dades de l'estudiant procedents de diferents sistemes UOC)
- Informes i consultes basades en diferents criteris de filtre per segmentar els estudiants tutoritzats i poder fer accions amb ells.

Dues vegades l'any, els tutors d'inici emplenen un informe final de tutoria per a cada estudiant que finalitza el seu segon semestre a la UOC. Aquest informe serveix per a traspassar informació rellevant de l'estudiant al tutor de seguiment.

Cal tenir en compte que un estudiant pot estar cursant simultàniament més d'un estudi i per tant tindrà un tutor assignat per a cada estudi que estigui cursant.

Els gestors d'Acció Tutorial poden configurar al SIS actual GAT els tutors disponibles per a cada estudi, diferents criteris per fer l'assignació automàtica del tutor a l'estudiant segons les necessitats de cada esutdi així com fer reassignacions de tutors a estudiants individuals i massives.

Els informes del tutor (Dashboards i reports) inclouen dades sobre propostes, matrícules, conversions, motius de no matriculació, accions per incentivar la matrícula, estat de correus electrònics, tipologia d'estudiants, observacions d'accés i de matrícula, tasques realitzades pel tutor, consultes i segmentacions (demogràfiques, acadèmiques, etc.).

Els informes de coordinació (Dashboards i reports) analitzen dades referents a total de matrícules i rematrícules, conversió, accessos, crèdits/ingressos, fidelització, motius d'abandonament/no matrícula, temps de resposta, volum d'interaccions (individuals i col·lectives), trucades del tutor, control de campanyes i tipologia de consultes.

A tots els informes es poden aplicar filtres per estudi, programa, tutor/a, idioma, semestre, dates i cohort.

Resultats esperats en l'àmbit d'acompanyament per part dels tutors

La UOC vol transformar l'experiència de l'estudiant per a que sigui propera i escalable al llarg de tot el seu cicle de vida maximizant l'eficiència dels recursos mitjançant un ecosistema tecnològic enterprise integrat que optimitzi els processos d'acompanyament i que impulsi l'èxit académic, la fidelització i l'engagement de l'estudiant.

Algunes de les iniciatives que es volen executar per millorar l'experiència dels estudiants en l'àmbit d'acompanyament per part dels tutors són:

- Personalització de l'experiència en base a les necessitats de l'estudiant a cada moment així com la tipologia de persona a la qual pertany
- Acompanyament integral optimitzant la comunicació i les recomanacions sobre la base del perfil de l'estudiant
- Maximitzar capacitats de "digital engagement" per respondre a les necessitats dels estudiants
- Omnicanalitat: consistència en les interaccions amb l'estudiant a través de qualsevol canal
- Focus en l'experiència, personalització i acompanyament durant els primers 6 mesos
- Potenciar les capacitats d'autoservei/autogestió de l'estudiant
- Segmentació de l'estudiant en base a les característiques, les preferències, la fase del cicle de vida, el nivell de satisfacció…
- Traçabilitat de l'experiència completa de l'estudiant incloent interaccions, comunicacions i documentació
- Identificació i acompanyament d´estudiants amb diversitat funcional
- Increment de la proactivitat dels tutors fent ús de l'automatització de processos i Agents IA de suport (copilots)

- Optimització de les comunicacions amb els tutors, reduïnt el número d'interaccions 1:1 de baix valor
- Definició de models de propensió i recomanacions segons l'històric
- Racionalització i optimització en l'assignació de tutors
- Seguiment de l'experiència de l'estudiant a les fases d'aprenentatge i gestió acadèmica

Aquestes iniciatives han de permetre obtenir els següents resultats

Més	Menys
Satisfacció de l'estudiant Qualitat en el servei d'assessorament Personalització en l'assessorament Número de matriculacions "Engagement" de l'estudiant Retenció (> 6 mesos) Ratio alumnes / tutor (eficiència) Proactivitat i atenció per part dels tutors	Abandonament primerenc (< 6 mesos) Volum de consultes als tutors Temps de resposta a l'estudiant en les consultes als tutors

La nova solució a implantar ha d'oferir les següents capacitats:

- **Gestió de cites amb el tutor:** Garantir que l'estudiant pugui sol·licitar cites amb el seu tutor i altres membres de l'equip d'assessorament.
- **Engagement consistent omnicanal:** Oferir una experiència fluida i coherent de l'estudiant mitjançant múltiples canals de comunicació (email, SMS, Whatsapp, webs, telefonía, Slack...), en cada punt de contacte.
- **Canals d'autoservei:** Proporcionar als estudiants eines d'autoservei accessibles i fàcils d'utilitzar, que els hi permetin gestionar de manera autònoma aspectes clau de la seva experiencia acadèmica. Inclouen accés a bases de dades de coneixement amb recomanacions contingut a l'estudiant que resolen la cerca d'informació o la resolució de problemes així com xatbots, tots dots alimentats per IA basada en dades.
- **Experiència de l'estudiant personalitzada:** Oferir als estudiants una experiència adaptada a les seves necessitats, interessos i objectius, mitjançant la recomanació d'itineraris d'aprenentatge (Learner Pathways) i l'ús de dades emmagatzemades a Salesforce o a sistemes UOC externs per per a proporcionar contingut, recursos i suport personalitzat al llarg de la seva trajectòria acadèmica.
- **Col·laboració:** Facilitar espais i eines que fomentin la interacció i el treball en equip entre estudiants i altres actors acadèmics, promovent la resolució de dubtes i l'intercanvi de coneixement.
- **Planificació dels objectius de l'estudiant:** Gestionar plans d'acció personalitzats (Care Plans) en base als seus objectius acadèmics, amb una monitorització continua de l'estudiant facilitant intervencions del tutor i permetent ajustos i millores continues durant la trajectòria acadèmica..
- **Gestió i enviament de sol·licituds:** Enviament i gestió per part de l'estudiant de consultes emeses mijançant els diferents canals, proporcionant experiències i respostes personalitzades.
- **Assignació d'assessors experts:** Dessignar de forma automatitzada, a partir de pools d'experts predefinits, profesionals especialitzats segons les necessitats i árees d'estudi, garantint el millor suport possible al llarg del cicle de vida de l'estudiant.
- **Registre de documents**: Permetre la recepció i organització d'informació rellevant, facilitant la gestió i l'accés a la documentació quan sigui necessari.
- **Alertes de documentació pendent:** Generar alertes automàtiques sobre documents dels estudiants necessaris, assegurant que compleixin amb tots els requisits administratius i

acadèmics a temps.

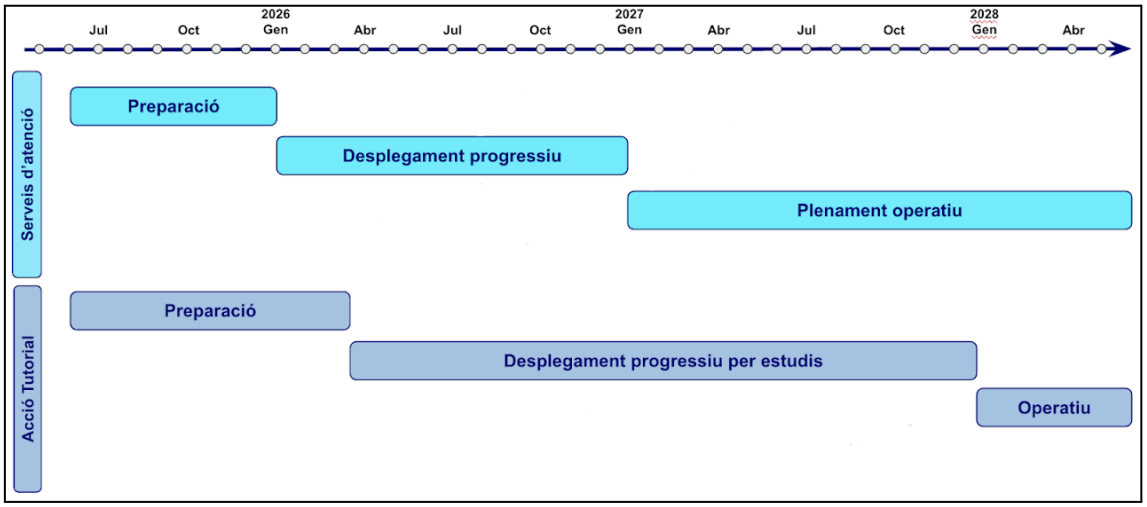
- **Analítica i informes**: Permetre millorar la qualitat del servei i prendre decisions basades en dades de suport i/o acadèmiques que per analitzar tendències i desenvolupar estratègies per millorar els resultats dels estudiants i l'eficiència dels tutors.

i ha de permetre optimitzar els processos actuals

- Incrementant substancialment la productivitat dels tutors degut a la unificació d'eines de tutorització (tutorització de matrícula, seguiment, prevenció d'abandonament, comunicacions..) i de la desaparició de sistemes manuals de suport a la gestió (Excel i informes de traspàs a tutors de seguiment).
- Incrementant la qualitat de la dada impactarà positivament en la capacitat de personalitzar la comunicació amb l'estudiant de manera precisa (historial d'interaccions, informació del perfil actualitzada, preferències d'idioma o canals de comunicació,...).
- Millorant d'experiència de l'estudiant a la navegació i accés a la informació derivada de la unificació de portals d'informació i col·laboració amb el tutor.
- Reduint les taxes d'abandonament mitjançant scoring i alertes sobre mètriques calculades per IA predictiva sobre la base d'històric de dades.
- Agilitzant les comunicacions suprimint la pèrdua d'informació i reduint els temps d'assessorament amb la introducció d'espais de col·laboració avançats persona a persona i grups.
- Millorant en indicadors d'eficiència i escalabilitat a través de la capacitat d'automatitzar altres processos de tutorització a l'estudiant.
- Facilitant als gestors d'Acció Tutorial l'anàlisi del seguiment de l'activitat i la productivitat dels tutors individualment i per altres criteris com per exemple, estudis. També es podrà controlar l'impacte dels tutors en el rendiment dels estudiants.

Planificació orientativa

De forma orientativa i sense condicionar la proposta que els licitadors han de presentar, aquesta és una planificació a molt alt nivell del projecte:



Integracions

El proveïdor haurà de realitzar les integracions de la nova eina amb els següents sistemes UOC:

- Obtenció de dades acadèmiques del SIS actual GAT per tal que tant els tutors com el servei d'atenció les puguin consultar
- Obtenció de dades personals dels estudiants de TERCERS (base de dades de les persones amb les que interacciona la universitat i que no són personal UOC) per tal que tant els tutors com el servei d'atenció les puguin consultar

- Obtenció de dades del SIS en actualment en construcció, basat en RIO Education sobre la mateixa instància de Salesforce Education Cloud, per tal que tant els tutors com el servei d'atenció les puguin consultar
- Obtenció de dades de la instància de Salesforce EDA (predecessora d'Education Cloud) amb Sales Cloud actual que s'utilitza per als processos comercials per tal que tant els tutors com el servei d'atenció les puguin consultar.
- Obtenció de dades de BART (sistema d'avauació d'estudis previs) per tal que tant els tutors com el servei d'atenció les puguin consultar.
- Obtenció de dades de RAEP (sistema de reconeixement de l'experiència professional) per tal que tant els tutors com el servei d'atenció les puguin consultar
- Enllaç a la Fitxa de l'Estudiant actual per tal que tant els tutors com el servei d'atenció les puguin consultar.
- Obtenció de dades de LMS Canvas per al seguiment de la docència per tal que tant els tutors com el servei d'atenció les puguin consultar.
- El portal de la UOC per poder demanar suport al servei d'atenció
- El Campus virtual de la UOC tant per al servei d'atenció com per a l'acció tutorial.
- Importació de dades de la plataforma de dades de la UOC basada en Snowflake cap a Salesforce tant pel servei d'atenció com per l'acció tutorial.
- Exportació de dades de l'activitat dels tutors a Salesforce cap a la plataforma de dades de la UOC basada en Snowflake en la implantació de l'acció tutorial.
- Escalats a les eines d'atenció del Nivel 3: CAU (Eina de gestió de peticions dels estudiants) , JIRA (Aplicació corporativa per la gestió de peticions) en la implantació del servei d'atenció
- Exportació de dades cap al sistema de captació de la percepció: Qualtrics (aplicació corporativa per la gestió d'enquestes) en la implantació del servei d'atenció

Aspectes a considerar

La nova solució per als serveis d'Atenció i Tutoria compartirà instància de Salesforce Education Cloud amb el projecte de transformació de la gestió acadèmica GAUDÍ, que ja es troba executant-se la seva primera fase amb la implatació del nou SIS anomenat SISCO basat en el producte RIO Education. Aquesta primera fase inclou la implantació de dues iniciatives: Cursos Professionalitzadors (finals de 2025) i Màsters Universitaris oficials (finals de 2026). Cal tenir en compte les decisions preses en aquest projecte que tinguin impacte en l'acompanyament per part dels tutors, principalment en la part d'estructura acadèmica dels plans d'estudis, idiomes de docència, etc.

També s'ha de tenir en compte que actualment la UOC disposa d'una altra instància de Salesforce amb Sales Cloud amb l'arquitectura EDA (predecessora d'Education Cloud). És utilitzada únicament per als processos comercials i recull l'oferta acadèmica i comercial de la UOC, amb integracions amb el SIS actual GAT i el portal de la UOC "Oferta formativa" amb la DXP d'Adobe.

Annex - Serveis de fabricant disponibles

Per a la correcta execució d'aquest projecte, la UOC contractarà al fabricant el servei "Signature Success Plan". Aquest servei només estarà disponible per a l'organització Education cloud.

Els serveis inclosos en el "Signature Success Plan" per a la UOC són els següents:

- Gestió d'Èxit del Client:
  - Customer Success Manager: Un punt de contacte dedicat que ofereix experiència proactiva, recomanacions personalitzades i coordinació de recursos tècnics.
  - Customer Success Score: Una avaluació integral de l'èxit, que mostra l'ús de productes i funcions, la salut de les implementacions i la participació amb els recursos d'aprenentatge.
  - Success Path: Un camí d'èxit personalitzat creat conjuntament amb el CSM per establir objectius i seguir el progrés.
  - Success Reviews: Revisions periòdiques per mesurar el progrés i l'èxit.
- Technical Health:
  - Revisions Especialitzades en Arquitectes: Treball amb arquitectes de Salesforce per revisar, mantenir i millorar la solució.
  - Gestió d'esdeveniments clau: preparació per a esdeveniments d'alta demanda i moments crítics.
  - Monitorització Proactiva: Monitorització 24/7 i Smart Alerts personalitzats.
  - Revisió Anual de Salut Tècnica: Anàlisi completa de l'entorn Signature de Salesforce.
- Adopció de Productes:
  - Guia d'Adopció Personalitzada: Orientació adaptada a les necessitats de la UOC.
  - Programes de Coaching Dirigits per Experts: Millors pràctiques i configuració.
- Experiència del Client:
  - Classes Virtuals Guiades per Instructors: Formació en profunditat organitzada per producte, rol i nivell.
  - Descomptes a Certificacions: Vouchers de certificació en grup per validar les habilitats de l'equip.
  - Comunitat Trailblazer: Accés a la comunitat de Salesforce.
- Resolució de Problemes:
  - Suport tècnic: Accés 24/7/365 a l'equip de suport tècnic amb diferents nivells de resposta segons la gravetat.
  - Suport per a Desenvolupadors: Optimització de codi personalitzat i guia d'implementació.
  - Línia directa d'emergència: resposta ràpida per a problemes crítics.

A més, el pla inclou serveis d'onboarding per assegurar una col·laboració efectiva amb Signature Success.

Annex - Estàndards metodològics

S'indiquen a continuació els mínims metodològics que demana la UOC als seus proveïdors per al desenvolupament i evolució d'aplicacions. Cal tenir en compte que aquesta documentació es troba en revisió i ampliació contínua, per la qual cosa és important consultar-la habitualment en el lloc de publicació.

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 proveïdor, només els logos corporatius vigents de la UOC.
- La UOC és la propietària de tots els lliurables elaborats pels diferents proveïdors
- 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.
- Els proveïdors tindran accés a les aplicacions corporatives sempre amb el seu correu UOC

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 de DCU, Qualitat, Seguretat o Arquitectura, que caldrà afegir al registre de lliurables 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.

Lliurables Existents

A continuació es mostra la relació completa de lliurables existents associats a cada fase i la fita de projecte a la qual està associats.

1. Fase Maduració

Fites: La fita inicial d'aquesta fase és: "Inici de Projecte", la fita resultant de l'acceptació dels lliurables i activitats que corresponen a aquesta fase és: "KickOff del projecte"

Lliurable	**Detall**
Fitxa Iniciativa	Una Iniciativa és una agrupació d'un o més Projectes. Una Iniciativa pertany a un Programa, que al seu torn és una agrupació d'una o diverses Iniciatives.
Comanda	Les comandes són bàsiques per poder començar un projecte i serveixen per vehicular els pagaments als proveïdors.

Contracte	El contracte és el marc legal sota el qual es pot dur a terme un projecte. Ens servirà com a referència per a consultar les condicions pactades amb el proveïdor. Contractació de serveis o adquisició de llicències que requereixen tramitació o concurs: contractes menors, negociats, oberts, harmonitzats i derivades en concursos d'homologació. Modificació de contractes ja existents
Fitxa de Programa	Des d'un punt de vista operatiu, un Programa és una agrupació de diverses Iniciatives (1,N).
Gestió de Canvi	Una Gestió de Canvi és un tipus de issue que s'utilitza quan el pressupost inicial es veu afectat per un canvi d'abast en el projecte o l'aparició d'un nou requeriment.
Objectiu	La issue de tipus "Objectiu" reflecteix el motiu pel qual emprenem una acció (Programa o Iniciativa), i defineix que pretenem aconseguir amb aquesta acció. Ens diu on estem i on volem arribar amb la implantació.
Document de Necessitats	El document de Necessitats defineix les necessitats del projecte, els aspectes metodològics que ha de satisfer el proveïdor i les condicions de contractació i prestació del servei. Per validar la Proposta de solució, i per elaborar el plec de necessitats, existeix com a recurs la **checklist de verificació de la proposta de solució** (la plantilla es troba a l'apartat de plantilles i repositori del lliurable")
Proposta de Solució	La proposta de solució és el document que presenta el proveïdor com a resposta a la petició de projecte que els lliurem amb el Plec de Necessitats.

2. Fase Inici

Fites: La fita inicial d'aquesta fase és: "Inici de Projecte", la fita resultant de l'acceptació dels lliurables i activitats que corresponen a aquesta fase és: "KickOff del projecte"

Lliurable	**Detall**

Presentació kickoff	Utilitzar la plantilla que facilita la UOC. En cap cas, es pot utilitzar logo, imatges, etc... del proveïdor. Per més detalls normatius, veure Normativa de Lliurables El contingut mínim correspon a: o Objectius o Abast o Planificació o **Organització** (modificada matriu RACI) o Òrgans de seguiment o Riscos o Lliurables + Calculadora de lliurables **(Novetat)** o **Pressupost i costos** (Pressupost inicial, possibles rangs de costos, ...) o Eines La Planificació indicada ha d'estar pactada per tots els implicats del projecte (Tant siguin de caràcter extern com qualsevol unitat operativa de caràcter intern)
Històries d'usuari	Les històries d'usuari són una descripció breu d'una funcionalitat del producte tal com la percep l'usuari. Una definició d'alt nivell d'un requisit, que conté només la informació suficient perquè els desenvolupadors puguin produir una estimació raonable de l'esforç per implementar-lo. Ha de aportar un valor clar a l'usuari Els requeriments d'un projecte cal transformar-los en històries d'usuari i èpiques. Aquests requisits s'elaboren sobre la base de necessitats recollides a l'Avantprojecte i al plec de necessitats.
Planificació	Realitzar una planificació estimada en setmanes, considerant el Calendari de Distribucions i les possibles de dependències del projecte amb altres projectes en curs.
Document d'Arquitectura (DA) (conté DAC)	El Document de Descripció d'Arquitectura (DA) és una declaració d'intencions envers la construcció d'un sistema d'informació, que es converteixen en acords un cop aprovat. En aquest lliurable s'ha de descriure: ● La relació del nou sistema amb altres ● Com es construirà el nou sistema (amb quines tecnologies i perquè) ● Com es desplegarà el nou sistema ● Quines entitats de dades utilitzarà ● Justificació de decisions que fan que certs aspectes es realitzin d'una manera concreta El DA l'ha d'elaborar l'integrador i es pot iterar fins que s'arriba a l'acord abans de començar a implementar. L'aprovació del DA és responsabilitat de l'equip d'arquitectura.

3. Fase Disseny i Implementació

Fites: En aquesta fase existeixen varies fites, cada una d'elles és obligatòria per tal que es pugui iniciar el Desplegament a PRO. La fita final d'aquesta fase és "Desplegament a PRO"

Lliurable	**Detall**
Disseny Funcional	El disseny funcional conté una descripció detallada de les necessitats del sistema, establint què farà i com s'espera que ho faci. Els casos d'ús, els requisits funcionals i requisits no funcionals completen conjuntament la descripció del sistema.
Disseny Tècnic	El disseny tècnic descriu el disseny del sistema, generat a partir de la documentació de l'anàlisi i disseny funcional, considerant el conjunt de posibilitats i restriccions específiques de la plataforma.
Codi Aplicació - Codi Font	El codi font d'una aplicació són tots els fitxers necessaris que es requereixen per a què una aplicació funcioni correctament. Es divideix en Components Tècnics. Es considera codi font: ● Codi que generarà l'executable de l'aplicació i tots els fitxers associats necessaris (fitxers de configuració, …) ● Codi de cada un dels components tècnics ● Codi de proves unitàries i proves d'integració, codi de proves automatitzades ● Scripts de base de dades ● Infraestructura com a codi ● Els artefactes que genera una aplicació
Recepta desplegament al núvol	La recepta Cloud és un document en forma de formulari que te dues parts. La primera fa referència al desplegament dels serveis de infraestructura i en ella es recullen detalls específics per poder fer l'aprovisionament d'aquests serveis. La segona fa referència a la informació necessària per poder incorporar l'aplicació en el sistema de CI/CD de la UOC.

Estratègia de Proves	El document d'estratègia de proves té com a propòsit descriure l'enfocament amb el qual s'abordaran les proves d'un projecte. Descriu els objectius perseguits amb les proves a realitzar durant el projecte, l'abast d'aquestes proves, quins elements seran provats i quins elements no, les necessitats que s'han de cobrir per a realitzar unes proves amb èxit, quins equips participaran en les proves, quina estratègia de disseny i execució de proves se seguirà en el projecte, així com una planificació de totes aquestes activitats. El contingut mínim que ha de tenir és: ● Plantejament general ● Referències a la documentació funcional ● Planificació de les proves ● Inclòs en l'abast de les proves ● No inclòs en l'abast de les proves ● Riscos segons característiques de qualitat ● Riscos segons Funcionalitats / Històries d'usuari ● Riscos del procés de proves ● Estratègia d'execució de proves ● Criteris d'entrada, de sortida, de suspensió i de represa de proves ● Entorn ● Infraestructura i Dades ● Informe de resultats ● Catàleg de proves Els criteris d'acceptació del document d'estratègia de proves són: ● L'estratègia de proves està consensuada amb tots els membres de l'equip: (proveïdor, equip projecte AT i usuaris) ● L'estratègia de proves és realista i realitzable ● L'estratègia de proves defineix les proves que realitzaran cada un dels equips en quant a funcionalitats, tècniques i temporalitat
Manual d'Operacions	Aquest document recull la informació necessària per tal de que AiS Operacions mantingui el servei ala nivell requerit. El Contingut Principal és informació relativa als elements de configuració del servei, monitoratge, backup, operatives de resposta a incidents, continuitat, ... El responsable de Operacions assignat al projecte acceptarà el Manual d'Operacions.
Terraform	Este documento especifica las **normativa y como desarrollar código HCL dentro de UOC para que sea aceptado.** Terraform es una herramienta de código abierto de "Infraestructura como código (IaC)", creada por HashiCorp, que permite crear, cambiar y versionar infraestructura de forma eficiente. Es una herramienta de codificación declarativa (ANSIBLE en contraste combina la configuración declarativa y la procedimental) que usando el lenguaje de alto nivel llamado HCL (Hashicorp Configuration Language) describir el estado final de una infraestructura para ejecutar una aplicació.

Wireframe	L'objectiu d'aquest lliurable és definir i decidir sobre: o L'estructura bàsica de la interfície (layout) o El disseny d'interacció en escriptori i responsive o Arquitectura de la informació, sistemes de navegació i flux de pantalles o Elements d'interacció per a usuaris de lector de pantalla o Com les funcionalitats queden representades en la interfície i reflecteixen els objectius de negoci contemplats en l'abats del projecte
Disseny gràfic	L'objectiu d'aquest lliurable és definir i decidir sobre la aplicació dels estils gràfics UOC en la interfície. Si no s'ha elaborat un wireframe previ, també permet definir: o L'estructura bàsica de la interfície (layout) o El disseny d'interacció en escriptori o Arquitectura de la informació, sistemes de navegació i flux de pantalles o Elements d'interacció per a usuaris de lector de pantalla o Com les funcionalitats queden representades en la interfície
Funcional d'interacció (UX)	L'objectiu d'aquest lliurable és descriure les interaccions i funcionalitats de la interfície amb detall suficient per a què l'equip de desenvolupament pugui: o Valorar l'esforç econòmic o Desenvolupar la solució
Anotacions d'accessibilitat sobre wireframe i disseny	L'objectiu d'aquest lliurables és definir i decidir sobre certs elements de la interfície a nivell semàntic i d'equitatge que condiciona la UX d'usuaris amb lector de pantalla i el compliment de la doble A.
Anotacions dels colors emprats en el disseny	Les anotacions dels colors emprats en el disseny conté una llista de la combinació de colors que hem emprat i la seva relació de contrast a l'hora de crear els dissenys gràfics de l'eina.
Front-end	Aquest lliurable permet consolidar: o Elements d'interacció i navegació o Disseny gràfic o Compliment de l'accessibilitat o Estàndards i bones pràctiques html
Producte en PRE (UX)	Tenir un producte/aplicació/funcionalitat plenament funcional per consolidar: o Elements d'interacció i navegació o Disseny gràfic o Compliment de l'accessibilitat o Estàndards i bones pràctiques html

	o Contingut real o simulat que repliqui les casuístiques de visualització
Service Blueprint	L'objectiu d'aquest lliurable és mapejar els Servei digitals per dissenyar-los i/o millorar-los, identificant: o Les accions de l'usuari i els seus touchpoints o Els fluxos de tasques informació o Les tasques i persones del Negoci o Eines i processos interns
Estratègia de Proves	El document d'estratègia de proves té com a propòsit descriure l'enfocament amb el qual s'abordaran les proves d'un projecte. Descriu els objectius perseguits amb les proves a realitzar durant el projecte, l'abast d'aquestes proves, quins elements seran provats i quins elements no, les necessitats que s'han de cobrir per a realitzar unes proves amb èxit, quins equips participaran en les proves, quina estratègia de disseny i execució de proves se seguirà en el projecte, així com una planificació de totes aquestes activitats. El contingut mínim que ha de tenir és: o Plantejament general o Referències a la documentació funcional o Planificació de les proves o Inclòs en l'abast de les proves o No inclòs en l'abast de les proves o Riscos segons característiques de qualitat o Riscos segons Funcionalitats / Històries d'usuari o Riscos del procés de proves o Estratègia d'execució de proves o Criteris d'entrada, de sortida, de suspensió i de represa de proves o Entorn o Infraestructura i Dades o Informe de resultats o Catàleg de proves Els criteris d'acceptació del document d'estratègia de proves són: o L'estratègia de proves està consensuada amb tots els membres de l'equip: (proveïdor, equip projecte AT i usuaris) o L'estratègia de proves és realista i realitzable o L'estratègia de proves defineix les proves que realitzaran cada un dels equips en quant a funcionalitats, tècniques i temporalitat

Pla de Proves (Test Plan)	Els casos de prova es desenvolupen per definir els elements que són necessaris validar a fi d'assegurar que l'aplicació funciona correctament, suporta la càrrega esperada i està construïda amb un alt nivell de qualitat. La definició dels casos i del test plan cal que respongui al definit a l'Estratègia de Proves Un cas de prova ha de contenir bàsicament: ○ § Precondicions § Dades de prova § Pas a Pas § Resultat Esperat Cal definir tants tests plans com es defineixi a l'estratègia de proves i cal que siguin coherents i complets. Al pla de proves s'han d'incloure les proves de càrrega (veure Proves de Rendiment) El Pla de proves d'accessibilitat a confluence és obligatori
Informe de Resultats de Proves	L'Informe de resultat de les proves (per qualsevol tipus de pla de proves) esdevé el conjunt de resultats sorgits de l'execució del pla de proves. Ha d'existir la traçabilitat entre el que es defineix a l'estratègia de proves, les fites del projecte, els milestones a Testrail i els informes de resultats.
Informe resultats proves accessibilitat	El informe de proves d'accessibilitat conté una descripció detallada de les proves que s'han portat a terme en la maqueta i a PRE per tal de garantir l'assoliment del nivell d'accessibilitat indicat en els requeriments. Cal referenciar les eines emprades (com lectors de pantalla, eines automàtiques, etc). Completa l'informe la taula on s'indica si passa o no cada un dels criteris .

4. Fase Implantació

Fites: És obligatori tenir els lliurables d'aquesta fase acceptats per tal d'assolir la fita "Inici Desplegament a PROD". Una vegada assolida, les següents fites que s'han d'indicar son: "Desplegament a PROD Finalitzat" i "GO LIVE". En alguns casos, aquestes dues fites poden tenir el mateix End Date, però s'han de diferenciar tal com s'indica.

Lliurable	**Detall**
Manual d'Operacions	Aquest document recull la informació necessària per tal de que AiS Operacions mantingui el servei ala nivell requerit. El contingut principal és informació relativa als elements de configuració del servei, monitoratge, backup, operatives de resposta a incidents, continuïtat, etc. El responsable d'Operacions assignat al projecte acceptarà el Manual d'Operacions.
Document d'Acords de Ciberseguretat (DAC)	Aquest document estableix un acord de compromís vinculant entre la UOC i el desenvolupador pel què s'acorda maximitzar la seguretat del programari desenvolupat i de les aplicacions adquirides, d'acord amb una sèrie de termes que

	s'hauran de pactar abans de començar qualsevol activitat del desenvolupament. Al més alt nivell la UOC i el desenvolupador acorden que: • Les decisions de seguretat compromeses en aquest acord estan basades en la comprensió del risc inherent a l'aplicació desenvolupada i les dades tractades. • Que les activitats dedicades a incrementar la seguretat de l'aplicació estaran balancejades i fortament distribuïdes al llarg del cicle de vida del desenvolupament. • Les activitats i la documentació generada caldrà que s'integrin en el cicle de vida del desenvolupament del programari i en cap cas estaran separades de la resta del projecte. • Tota la informació relativa a la seguretat de l'aplicació serà revelada, informada i compartida per part del proveïdor i la UOC. Si es donés el cas, el proveïdor especificarà de forma argumentada quins aspectes de la seguretat de l'aplicació i del desenvolupament pensa no complir.
Manual d'Usuari	El manual o guia d'usuari recull l'especificació per l'ús del programari.
Pla de formació	El Pla de formació defineix les accions de formació per als usuaris i actors relacionats.

5. Fase Tancament

Fites: La fita resultant d'aquesta fase és "Tancament". S'ha d'assegurar que totes les fites indicades tipus "Fites claus de NEGOCI" hagin estat assolides.

Lliurable	**Detall**
Informe de Tancament	L'informe de tancament detalla tots els aspectes del tancament del projecte com administratius i de relació amb els proveïdors, assoliment d'objectius, etc. L'informe de tancament inclou una avaluació global del desenvolupament del projecte, amb l'objectiu de reflectir la qualitat i grau de satisfacció dels productes obtinguts, evolució del projecte en temps, abast, alineament amb els objectius inicials, etc. A més , es recolliran les experiències positives i negatives per que serveixin d'ajuda en situacions futures. Criteris d'acceptació o L'aplicació està a disposició de l'usuari. o S'han lliurat tots els lliurables mínims Normatius seguint la Normativa de Lliurables o S'ha fet planificació de traspàs a manteniment o S'ha fet una reunió de tancament del projecte amb els actors interessats.

Traspàs a Manteniment	L'objectiu d'aquest procediment, és assegurar que un desenvolupament, un cop superat el període de garantia, estigui suportat per un servei de manteniment que disposi de tot el coneixement necessari per tal de poder assolir els ANS definits. Aquest procediment és normatiu, independentment que el proveïdor desenvolupador del projecte sigui el mateix o no que el proveïdor que assumeix el manteniment del producte resultant. Aquest procés s'inicia juntament amb la fase de Garantia del projecte. Al finalitzar el període de garantia, s'ha d'assegurar que el traspàs ja té l'acceptació per part del Responsable del Servei de la UOC. Per tal d'assegurar un procés de traspàs satisfactori i sense impactes en el servei, és indispensable: o Identificació dels interlocutors claus del procés o Identificació de les necessitats de manteniment o Entrega de la documentació requerida tant a nivell funcional com tècnic o Sessions de formació / resolució de dubtes del proveïdor destí o Acceptació per part del responsable del servei de la UOC
Informe declaració accessibilitat	L'objectiu de la declaració d'accessibilitat és obtenir la declaració del proveïdor respecte al compliment de la doble A. La qual conté una declaració del nivell d'accessibilitat que s'ha assolit al final del projecte. Aquesta declaració d'accessibilitat s'hauria de mostrar en 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.

6. Artefactes Seguiment i Control

Artefactes Bàsics de Projecte	**Detall**
Aquests artefactes són els bàsics per al seguiment i control d'un projecte. Apliquen a qualsevol tipología de projecte	
Acta de Reunió	L'acte de la reunió és un artefacte de seguiment que conté un resum de tots els temes tractats en les diferents tipus de reunions i seguiments que es realitzen en el decurs del projecte. Cal crear una acta de cada reunió que es faci durant l'execució del projecte. Totes aquestes actes de reunions s'agrupen en el registre de reunions que es troba a l'espai Confluence del projecte de forma que ens permet conèixer en tot moment l'historial de les decisions que s'han pres en les diferents reunions. Per generar la llista de actes de reunió es pot fer servir la plantilla CLAU_Registre de Reunions Criteris d'acceptació: o Les actes es donaran per aprovades automàticament si en el termini de 3 dies laborables si no es rep cap esmena. o Les esmenes, en cas de rebre's, seran introduïdes en l'acta i aquesta serà novament distribuïda, considerant-se com a definitiva. Qualsevol apreciació sobre les esmenes s'haurà de tractar en la sessió següent

Registre de Reunions	El registre de reunions és un artefacte (pàgina de confluence) que conté un índex de totes les actes realitzades durant el projecte. Cal configurar-lo a l'inici del projecte. S'actualitza dinàmicament a mesura que es creen actes de reunió a l'espai del projecte tal i com indica Acta de Reunió.Cal revisar que sempre contingui totes les actes de reunió del projecte.
Informe de Direcció	Informe pel Comitè de Direcció. Continguts mínims: Informacions rellevants i balanç de l'execució, Planificació, Fites i dependències, Riscos
Informe de Seguiment	Informe de Segiment del Projecte. Continguts mínims: Tasques en curs, Tasques pendents, Planificació, Fites i dependències, Fets rellevants, Riscos.
Fitxa de Projecte	La fitxa de projecte és l'artefacte de seguiment que conté informació de l'estat del projecte, els participants, la planificació, i els costos del projecte Cal mantenir-la actualitzada amb una periodicitat màxima d'una setmana.
Seguiment de fites	Totes les fites consensuades en el kick off han d'estar registrades a JIRA. Es indispensable que el cap de projecte UOC revisi l'estat i la planificació de les fites un cop a la setmana durant el projecte per tal que en qualsevol moment es pugui coneixer l'avanç del projecte revisant la planificació de les fites. Les fites les registrem a JIRA amb l'issuetype anomenat "Fita". Tots els projectes tenen unes fites bàsiques comunes. Hi ha un mecanisme de creació massiva que les genera, ajudant d'aquesta manera al cap de projecte amb la creació de fites. Caldrà que reviseu les fites creades i les adapteu al vostre projecte.
Seguiment de riscos	Tots els riscos consensuats en el kick off, i qualsevol risc que es detecti durant l'execució del projecte, han d'estar registrats a JIRA. Els riscos han d'estar ben informats indicant: o Tipus Risc o Responsable o Plà de mitigació o Data possible mitigació És indispensable que el cap de projecte UOC actualitzi aquesta informació un cop per setmana. En cas de ser necessari, des de la issue Type Risc del JIRA, es pot escalar a la CDA marcant el camp "flagged" = impediment
Registre de lliurables	El registre de lliurables és un artefacte que conté un índex del projecte que serveix per fer el seguiment del lliurament i l'acceptació dels lliurables de cada fase del projecte. Al inici del projecte o de cada fase cal definir el conjunt de lliurables que s'han de generar durant l'execució del projecte. Tots aquests lliurables s'agrupen en el registre de lliurables que esta dintre de la home del projecte de forma que ens permet coneixer en tot moment l'estat dels lliurables de cada fase. Per generar la llista de lliurables es pot fer servir la plantilla CLAU_Registre de lliurables Criteris d'acceptació o Apareix una entrada per a cada lliurable específic del projecte (lliurables que es van definir al kickoff) o Tots els lliurables específics del projecte es troben en estat Aprovat o N/A

Home dels Projectes	La home del projecte es la porta d'entrada a la documentació del projecte a confluence. Al donar d'alta el projecte es crea transparentment per l'equip aquesta portada. Quan l'espai del projecte està creat a Confluence, l'equip de projecte ha de configurar l'espai del projecte: adaptar les macros i pàgines de tot l'espai,al context del projecte. Cal mantenir actualitzades i en funcionament, totes les macros i pàgines de Confluence així com les capçaleres de registre d'acceptació de cada una de les pàgines que pertanyen a l'espai
Artefactes de projectes d'implantació o evolució d'aplicacions	**Detall**
Aquests artefactes cal afegir-los quan el projecte implica la implantació o evolució d'una o més aplicacions	
Fitxa d'Aplicació i Component Tècnic	La fitxa d'aplicació conté tota la informació relativa a una aplicació i és un issuetype de Jira. Normalment, només existeix una per aplicació. Les aplicacions es divideixen tècnicament en components tècnics. La fitxa d'aplicació i la dels seus components tècnics ha d'estar sempre actualitzada. És obligació del servei de manteniment mantenir-la actualitzada però quan un projecte la implanta o l'evoluciona, és responsabilitat del projecte mantenir-la actualitzada
Panell de Qualitat	El panell de Qualitat és un Board que permet fer el seguiment de la qualitat del projecte en temps real. Cal configurar-lo a l'inici del projecte i vetllar perquè sempre mostri com a mínim: o Incidències / Bugs pendents de resoldre o Deploys o Qualitat del codi (SonarQube) § Qualitat de codi inicial § Qualitat del codi actual o Checklist de lliurables
Artefactes Agrupadors de documents d'aplicacions	**Detall**
Aquests artefactes cal configurar-los a l'espai del Projecte per a poder mostrar la documentació que es genera als espais de les aplicacions en el marc del projecte. El seu propi nom indica els documents de les aplicacions que conté.	
Documents d'Arquitectura (agrupador)	Conté referències a tots els documents d'arquitectura de les aplicacions implicades en un projecte.
Document d'acords de ciberseguretat	Conté referències a tots els documents d'acords de ciberseguretat de les aplicacions implicades en un projecte.

(Agrupador)	
Manuals d'Operacions (Agrupador)	Conté referències a tots els manuals d'operacions de les aplicacions implicades en un projecte.
Dissenys Tècnics (Agrupador)	Conté referències a tots els dissenys tècnics de les aplicacions implicades en un projecte.
Dissenys Funcionals (Agrupador)	Conté referències a tots els dissenys funcionals de les aplicacions implicades en un projecte.
Manuals d'usuari (Agrupador)	Conté referències a tots els manuals d'usuari de les aplicacions implicades en un projecte.
Traspassos a Manteniment (Agrupador)	Conté referències a tots els document de traspàs a manteniment de les aplicacions implicades en un projecte.
Receptes de desplegament al núvol (Agrupador)	Conté referències a totes les receptes de desplegament al núvol de les aplicacions implicades en un projecte.

Documentació i lliurables dels petits Evolutius

- Els evolutius, de la mateixa manera que evolucionen l'aplicació, també han d'evolucionar la seva Suite de Proves, creant o eliminant tants Casos de Prova i Plans de Proves com sigui necessari i sempre vinculats a un Milestone que identifiqui l'evolutiu (amb la Clau)

  L'espai Confluence de l'aplicació també cal mantenir-lo actualitzat ja sigui per fer les modificacions pertinents o si no hi ha contingut, caldrà afegir-lo només de les parts afectades per l'evolutiu. Aquests són els documents que normalment cal revisar de l'espai de l'aplicació pertinent:

  - Disseny Tècnic
  - Disseny Funcional
  - Test Suite
  - Manual d'Usuari
  - Document d'Arquitectura
  - Manual d'Operacions
  - Full de Ruta: Cal actualitzar els canvis que es fan a l'aplicació en una línia temporal.

Documentació i lliurables durant el manteniment d'aplicacions

- Durant el període de manteniment de les aplicacions, cal mantenir actualitzada la documentació de les aplicacions a Confluence i també la seva fitxa d'aplicació. Els principals documents que cal mantenir actualitzats són:

- Disseny Tècnic
- Disseny Funcional
- Test Suite
- Manual d'Usuari
- Document d'Arquitectura
- Manual d'Operacions
- Full de Ruta: Cal actualitzar els canvis que es fan a l'aplicació en una línia temporal.
- Errors Documentats

- Tota la documentació referent a una aplicació ha de mantenir-se dins de l'espai Confluence de l'aplicació. (No a l'espai del servei de manteniment o l'espai dedicat a altres equips o projectes). En tot cas, pot referenciar-se des d'altres espais.

Revisió i acceptació dels lliurables

La revisió i acceptació dels lliurables es fa mitjançant el registre de lliurables dels projectes que romandrà a Confluence.

- Es considera la data de lliurament quan el proveïdor fa un comentari a peu de pàgina del lliurable de Confluence informant al responsable UOC del seu lliurament i actualitzarà la capçalera del document.
- Per defecte es disposaran d'un màxim de 10 dies laborables per l'acceptació dels documents. Per les actes de reunió aquest termini és de 3 dies laborables. Passats aquests terminis, el proveïdor pot donar el document per acceptat automàticament i modificar la capçalera del lliurable a Confluence.
- En cas d'esmenes, s'afegirà un comentari a peu de pàgina del document i es pot complementar amb comentaris inline en el propi document.
- Les no conformitats s'hauran de resoldre per defecte en una màxim de 2 dies laborables. En aquest cas, les revisions posteriors per part de la UOC diposaran, per defecte 5 dies laborables.

Nomenclatura

- És obligatori mantenir la nomenclatura de les aplicacions de forma coherent a totes les eines per a poder garantir la traçabilitat entre elles.
- Quan parlem de "CLAU" (KEY), estem parlant de la CLAU que ve derivada de l'aplicació a JIRA.

Nomenclatura a les eines de desenvolupament

Eines de desenvolupament	**Aplicació "DEMO"**	**Components Tècnics " DEMO_front, DEMO_back..."**
JIRA	Cada aplicació té un projecte JIRA associat. Veure [Tipus de projectes ji La clau (CLAU) d'aquest projecte de JIRA és l'identificador principal de l'aplicació (que es propaga a la resta d'eines) La informació bàsica de l'aplicació es troba a la Fitxa d'Aplicació	Moltes aplicacions es divideixen en components, a JIRA es defineixen amb un issuetype "component" que penja de la Fitxa d'Aplicació Al camp "component tècnic" de les issues de tipus "deploy" es mostren tots els components de l'aplicació.

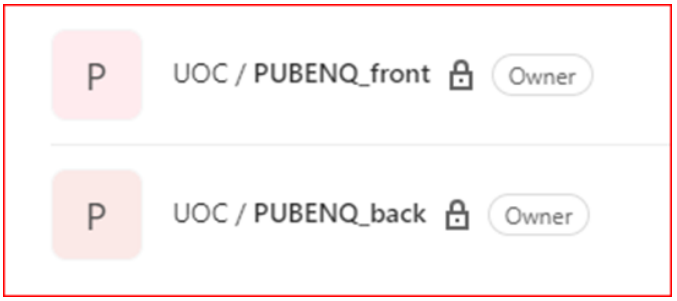
<table>
<tr><td>Confluence</td><td>Hi ha un espai de documentació a Confluence per a cada aplicació. La relació amb els projectes a JIRA és 1projecte jira=1espai confluence.</td><td>La documentació dels components queda dins de l'espai de Confluence de l'aplicació. S'organitza en pàgines i subpàgines</td></tr>
<tr><td>Gitlab</td><td colspan="2">Tots els repositoris d'aplicacions pengen sota el grup principal /UOC. Els repositoris dels components tècnics han d'estar anidats sobre una carpeta amb la KEY de l'aplicació.

Aplicacions o components tècnics nous
Dins de la carpeta de l'aplicació es creen els diferents repositoris, un per a cada component tècnic que requereixi repositori de codi. El nom del Component Tècnic segueix la Normativa de Nomenclatura

Exemple d'organització correcta d'aplicació i components tècnics a gitlab

Nous Components tècnics d'aplicacions legacy
En aplicacions legacy, a vegades no hi ha anidació de components tècnics sota la carpeta de l'aplicació. En el moment de crear un nou component tècnics, si no hi és la carpeta, caldrà demanar la seva creació i organitzar correctament la jerarquia com a mínim del nou component tècnic. És recomanable depenent de la dedicació, aprofitar i recol·locar també els altres components tècnics sota la nova carpeta de l'aplicació.

Exemple d'organització incorrecta d'aplicació i components tècnics a gitlab. Els components tècnics pengen directament de /UOC enlloc de /UOC/PUBENQ, que no existeix.

 
</td></tr>
<tr><td>Outsystems</td><td colspan="2">Per cada component (Application dins OutSystems) s'haurà d'especificar el següent:

Nom: <PROGRAMA> <APLICACIO> <COMPONENT> (Ex. GAUDI GDD Backoffice, GAUDI GDD Core, ...)
Tipus: Reactive WebApp, Tablet App, Phone App, External Web Portal, Traditional Web, Service
Capa (calculat): End User, Core, Foundation
I per cada mòdul dins una Application:
Nom: <APLICACIO>_<COMPONENT>_<SUFFIX>
Tipus: Reactive WebApp, Tablet App, Phone App, External Web Portal,</td></tr>
</table>

	Traditional Web, Service, Library, Extension *Capa (calculat)*: End User, Core, Foundation	
Jenkins	Es crea una carpeta per aplicació anomenant-la CLAU FOLDER Dins de la carpeta de l'aplicació es creen les pipes o jobs necessaris per a cada component tècnic. El nom del component tècnic és el prefix de la pipe o job de jenkins. El nom del component tècnic coincideix amb el summary de la issue component a JIRA i amb els valors que té el camp "Component tècnic" definit per a aquella aplicació a Jira. Els noms han de coincidir per a què CI/CD funcioni correctament	
SonarQube	L'aplicació (CLAU) es defineix a nivell de projecte **Normatiu 2020/01:** el paràmetre "key" de Sonarqube, ha de coincidir amb el nom del component tècnic. Amb el procediment de CICD, les branques no productives s'identifiquen amb un sufix automàticament. exemple no correcte: key (Sonarqube): edu.uoc.demo:demo_back exemple correcte: key (Sonarqube): DEMO_back Exemple de branca: DEMO_back_staging	
TestRail	Existeix un repositori general de casos de prova que es troba al projecte TestRail anomenat "_APLICACIONS" Per cada aplicació (coincident amb CLAU JIRA) es crearà **un test suite** dins del projecte "_APLICACIONS" Es defineix un Milestone per a cada projecte, el seu nom és la CLAU del projecte.	La definició dels casos de prova normalment es fa en termes funcionals o per històries d'usuari, no es separa per component tècnic però en cas de fer-se, es faria fent servir el concepte de TestRail de "sections" dins del test suite.

CMDB	CI (Aplicacions) equivalent a la CLAU de jira.	CI (Aplicacions) afegint la relació de "consists of" amb l'aplicació i l'entorn com a sufix (excepte a PRO) L'exemple quedaria així: DEMO_front_pre DEMO_front_test DEMO_front DEMO_infra
AWS	Política de nomenclatura del serveis cloud públics	Política de nomenclatura del serveis cloud públics
Azure	Política de nomenclatura del serveis cloud públics	Política de nomenclatura del serveis cloud públics

Control d'aplicació del Normatiu

El registre de lliurables és l'indicador de salut sobre l'estat dels lliurables i també l'indicador de compliment de la Normativa.

Cal que tots els lliurables d'una fase del projecte esdevinguin acceptats abans de poder passar a la següent fase del projecte.

Es realitzaran auditories Internes del control d'aplicació del Normatiu sense avís previ.

L'incompliment d'aquesta Normativa generarà No conformitats en els projectes o els manteniments de les aplicacions.

Annex - Principis de Tecnologia

Principis estratègics

Els **nous sistemes i aplicacions** es regiran pels principis de **Business first**, **cloud first i cloud Native** , **mobile first** (en el sentit de **multidispositiu**), **Data-driven** (la dada com a actiu més important de l'organització) i finalment el principi **d'aportació de Valor**

Principi de Business First

La tecnologia desplegada a la UOC ha de respondre a les necessitats i els objectius de negoci de la institució en cada moment. Per tant, ha de ser flexible i adaptable, per a ajustar-se de manera gradual als canvis del negoci de la institució o en tot cas, ser fàcilment reemplaçable per nova tecnologia que si que s'hi ajustin.

Per tant, cal tenir en compte que:

- Els sistemes d'informació estan en **constant transformació**.
- Quan es desplega una nova solució cal tenir en compte tant els processos d'actualització que un sistema patirà al llarg del temps com els processos de substitució del producte una vegada finalitzat el seu temps de vida.
- Així doncs, molts productes tenen una **obsolescència programada**, que coincideix amb la finalització del seu contracte o amb l'estratègia de millora tecnològica de la institució (vegeu ROI First i proposta de valor).
- A vegades, un producte no desapareix de l'ecosistema, però una part de la seva funcionalitat és assumida per un altre sistema (*strangler application*).
- La transformació digital en un ecosistema complex, només és possible sota un bon govern. La millora dels processos de govern de la tecnologia i de les dades és un factor clau que cal no descuidar mai.

Principi de Cloud first i cloud Native

- **Desplegament** d'aplicacions i sistemes **al núvol** de manera preferent i pensant en les propietats i els avantatge del núvol.
- La computació al núvol **converteix el hardware en software**. L'ús de components soft en comptes de hard, fa que les propietats del software siguin aplicables a les infraestructures tecnològiques de manera que és possible administrar-les i automatitzar-les.
- **Cloud native** vol dir contractar o desenvolupar una aplicació o un sistema pensant des de l'inici en aquestes propietats i avantatges del cloud.
- Els proveïdors de computació al núvol permeten **gestionar el hardware com a servei** (vegeu SaaS), de manera que moltes d'aquestes propietats del software aplicades a les infraestructures estan disponibles com a servei (usar cloud avui és usar un servei SaaS).

La UOC prioritza l'elecció de solucions **SaaS** (Software as a Service):

- El SaaS és un model de distribució del software on la lògica (codi en execució) i les dades les gestiona un (o més d'un) proveïdor que **ofereix la funcionalitat del software a través del núvol**.
- El SaaS normalment es consumeix sota un **model de 1** (el software) a **N** (els clients), en qualsevol moment i amb una **política de pagament per ús o de subscripció** basada en **mètriques de consum**.

- El SaaS permet **models de desplegament de noves funcionalitats de manera automàtica i continuada (versionless)**, de forma que el servei contractat no es cenyeix a unes funcionalitats fixes sinó variables al llarg del temps. Per aquest motiu, la contractació del SaaS està sempre lligada a la capacitat del proveïdor per a fer avançar i evolucionar el producte contractat (inclosa la solvència del proveïdor per a oferir el servei durant tot el contracte i mitigar així el risc de lock-in).

Per poder maximitzar l'ús de SaaS, cap pensar la solució aplicant el Principi de **Market fit**:

- **Adequació** d'un producte tecnològic **a les necessitats del mercat**.
- Quan es desenvolupa un producte a mida, és habitual demanar els requisits i les necessitats als futurs usuaris d'aquest. Aquest procés, sovint no és aplicable quan es contracta un producte de mercat.
- Per seleccionar correctament un producte de mercat, és imprescindible analitzar primer els nostres processos per tal d'**adequar-los a la manera d'operar estàndard o més utilitzada** en la majoria d'organitzacions del nostre sector.

Les **metodologies Lean** ofereixen un bon marc de referència sobre com afrontar aquesta adequació a les necessitats del mercat.

Tenint en compte tots aquests factors, la recepta a utilitzar és:

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

2. Si no existeix un SaaS, probablemente en el futur, ja sigui perquè has pogut aplicar Market fit o perquè el mercat ha evolucionat, segurament existirà. Mentrestant, pots cobrir aquest GAP funcional desenvolupant una aplicación en LowCode o Cloud Native.

   Les eines de desenvolupament ràpid o **Low Code**, permeten crear aplicacions i sistemes tecnològics de manera **visual i ràpida**, reduint la complexitat associada al desenvolupament de software.

   Quan un producte de mercat no cobreix totes les prestacions esperades, es recomana desenvolupar aquest **gap** de manera ràpida i dins la fase d'implantació del producte **mitjançant eines Low Code**.

   Les **eines Low Code**, també permeten l'experimentació i el prototipatge per a la **realització de pilots o proves de concepte**.

3. 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.

4. Aquest desenvolupament (Low Code o Cloud Native) i les integracions que amb altres solucions que requereixi, es faran sempre 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

Principi Data-Driven

- La **Interoperabilitat** és la capacitat de dos o més sistemes, de compartir dades amb l'objectiu de **facilitar l'intercanvi d'informació** entre ells.

- Els sistemes d'informació d'una organització són cada vegada més complexes i es comporten cada cop més com a un **ecosistema**.
- En un ecosistema digital, les dades són allò que s'intercanvien els sistemes i, per tant, són un dels principals drivers per la presa de decisions a diversos nivells (**Data-driven**). De fet, conèixer i governar aquestes dades, és essencial i necessari tant per als processos d'analítica de dades com per a la interoperabilitat entre aplicacions i sistemes.
- Per cada nou sistema o aplicació a introduir a un ecosistema, és imprescindible valorar tant les dades que aquest nou sistema proveeix i consumeix com els mecanismes tecnològics que aporta per a fer-ho (Integrabilitat).

Principi d'aportació de Valor

- Quan es contracta, desenvolupa o integra un producte, cal **calcular el retorn de la inversió (ROI)**.
- El càlcul del retorn de la inversió permet una **planificació empresarial i financera** dels costos i beneficis tecnològics.
- Quan aquest producte no té unes funcionalitats fixes sinó variables (SaaS) cal gestionar al llarg del contracte el seu ROI, que dependrà de les **capacitats de la institució per adoptar** lo abans possible **aquestes noves funcionalitats** disponibles.
- Una **proposta de valor** és una estratègia empresarial que maximiza la demanda a través de configurar de manera òptima l'oferta. Així doncs, en la gestió del **portafoli** (oferta), cal considerar tant l'**homogeneïtzació** (maximització del ROI) com el **risc de dispersió tecnològica** (que satisfà la demada però sense optimitzar l'oferta).
- En definitiva estem dient que cal 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.**

Principis sobre el disseny d'aplicacions

S'apliquen al re-disseny d'aplicacions ja existents, noves aplicacions *cloud native* i aplicacions en *LowCode.*

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:
    a. 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**.

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 a l'**API Gateway**, 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**:
    a. **Proves** per a verificar la qualitat del codi, el suport de càrrega o requisits no funcionals del sistema.
    b. **Documentació detallada** del projecte (descripció d'arquitectura, document funcional, manual de desplegament, manual d'explotació, …).
    c. **Control de versions**. El sistema en el seu conjunt ha de ser tractat com un producte amb les seves versions majors, menors, etc
    d. **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...).

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.

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

Els principis tecnològics que acabem de veure indiquen el camí per a disposar d'un catàleg d'aplicacions i tecnologies que s'ajusten a l'arquitectura tecnològica proposada (la piràmide).

Els principis són doncs un posicionament tàctic per arribar a un dels nostres objectius estratègics principals que no és altre que transicionar (aplicant els principis) de la situació actual fins a assolir l'arquitectura objectiu (la piràmide) a la vegada que no descuidem el servei i la governança tecnològica.

Però com podem aplicar aquests principis a la pràctica? No sempre és fàcil interpretar un principi, saber quan aplicar-lo ni com. És per això que disposem de dos elements principals que ens permeten aplicar els principis d'una manera operativa:

- Els Semàfors de Salut de la tecnologia de la UOC. Vegeu-los a l'apartat Vista d'Aplicacions/Semàfors de Salut.
- La Taula de Criteris tecnològics segons tipologies d'aplicacions. Vegeu-la al final de l'apartat Vista d'Aplicacions/Tipologia d'Aplicacions.

Tractament de dades

Publicació de les dades

- L'estratègia de dades adoptada per la UOC es basa en un model de publicació de Productes de Dades per part dels orígens de dades. Per tant, el sistema de l'adjudicatari hauria de tenir la capacitat de publicar les seves dades de qualsevol àmbit o mòdul que contingui, en el format i temps que requereixin els usuaris UOC, tot a través de la Plataforma d'Interoperabilitat (o integració) UOC.

- En cas de no poder publicar Productes de Dades directament, hauria de ser possible la publicació de tot el model de dades intern a partir de la Plataforma d'Interoperabilitat UOC per tal d'integrar-se amb la Plataforma Informacional.

- En cas de no complir cap dels anteriors, s'ha d'indicar el detall de la cobertura del model de dades sencer que es podria publicar.

Consum de les dades

- Les dades publicades, siguin Productes de Dades directament o el model sencer, seran integrades amb la Plataforma Informacional a través de la Plataforma d'Interoperabilitat.La Plataforma d'Interoperabilitat (o d'Integració) és l'eina que integra els diferents serveis web i infraestructures de dades de la UOC, tant legacy com cloud.

Latència de les publicacions de dades

- La latència mínima requerida és el més pròxim possible al real time, amb l'objectiu de disposar de la informació en el mínim de temps possible des que es genera la dada fins que es publica.

- Tot i així, per valorar les diferents possibilitats de latència de dades, s'haurien de detallar quines opcions proporciona el sistema.

- En cas de no poder mantenir internament un històric de dades i versions, el sistema juntament amb la Plataforma d'Interoperabilitat, han d'assegurar que no hi hagin pèrdues en la publicació de versions i dades.

Full de Ruta de Programari

A data de redacció del present document hi ha definit el següent full de ruta de programari. Donat que s'actualitza semestralment, en el moment d'iniciar un desenvolupament caldrà consultar la última versió publicada.

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)

			Obsolet	Suportat	Recomanat UOC	Distribució / Observacions
Llenguatges i runtimes	Golang		<= 1.19	>= 1.20	1.23	
	Java		< 11	11, 17	21	Només s'accepten versions LTS
	NodeJS		<= 16	18, 20	22.9	Només s'accepten versions LTS
	Python		<= 3.8	>= 3.9	3.12	(AWS lambda soporta de la 3.9 hasta la 3.12 a 14/10/24)
	PHP		<= 8.0	>= 8.1	8.3	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		<= 16	17	18	Només s'accepten versions LTS
	React		<= 16	17	18.3.1	
	Vue		<= 2.6.x	>= 2.7.x	3.5.x	
Gestió de dependències	Maven (Java)		<= 3.6	>= 3.8	3.9	
	NPM (NodeJS)		< 7.24	>= 7.24	10.8.3	

	Go Modules (Golang)		<= 1.20	>= 1.21	1.23	
	PiP (Python)		<= 21.x	22.x	24.2	
Frameworks de Desenvolupament	Spring Framework (Java)		<= 4.3.x, <= 5.2.x	5.3.x	6.1	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	3.39.x	Es pren de referència la darrera minor version en data 25/9/2024. Existeix la v4 però no es contempla perquè incorpora un nou model de licensing
	Hugo (webs estàtiques)		< 0.91.x	>= 0.101.x	0.134.3	Es pren de referència la darrera minor version en data 25/09/2024
	Gatsby (webs estàtiques)		< 5.0.x	5.x.x	5.13	V4.x finaliza el soporte en q4 del 23
Gestió de versions de DB	Flyway (Java)		< 9.4.x	>= 9.4.x	10.18	Suportades versions que han tingut alguna release durant els últims 2 anys
	Liquibase (Java)		< 4.16	>= 4.16.x	4.29.2	Suportades versions que han tingut alguna release durant els últims 2 anys

	SQLAlchemy Alembic (Python)		< 1.8	>= 1.8.x	1.13.x	Suportades versions que han tingut alguna release durant els últims 2 anys
	migrate (Golang)		< 4.15	>= 4.15.x	4.18.x	Suportades versions que han tingut alguna release durant els últims 2 anys
	Sequelize (NodeJS)		< 6.24	>= 6.24.x	6.37.x	Suportades versions que han tingut alguna release durant els últims 2 anys
Acceleradors dev / Generadors de codi / Low Code	JHipster		< 7.5.x	>= 7.5.x	7.9.x	JHipster, a més del generador de codi, proporciona un entorn de desenvolupament i altres tools de suport (IDE Tools, JDL Studio). Per tal d'estar alineat amb el model de CI/CD de la UOC, cal que es generin frontend i backend per separat.
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		< 1.6.x	>= 1.6.x	1.9.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		<=11g	12c		Només per manteniment d'aplicacions legacy
	MySQL		<8.0.28	>=8.0.28	8.0.36	RDS end of standard support date 5.7 29 February 2024
	PostgreSQL		<13.8	>=13.8	16.3	A AWS recomanem Aurora

Bases de Dades (Documental)	MongoDB		<6.0	>=6.0	7.0	A AWS recomanem documentdb
	AWS DynamoDB		<=2017.11.29	2019.11.21	2019.11.21	AWS Global Tables. Engine version is internal manage by aws
	AWS Document DB				5.0	
Bases de Dades (Clau-Valor)	Redis		< 6.0	>=6.0	7.2	A AWS recomanem Elasticache
CMS i Portals	Liferay		<= 7.3.x	7.4.x	7.4.x	Es consideren com a suportades les versions de Liferay dins "Premium Support Phase"
	OpenCMS		< 12.x	12.x, 13.x, 14.x, 15.x	17.x	Només manteniment
	WordPress		<= 5.x	>= 6.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:18-jre-alpine eclipse-temurin:19-jre-alpine eclipse-temurin:20-jre-alpine	eclipse-temurin:8-jre-alpine eclipse-temurin:11-jre-alpine eclipse-temurin:17-jre-alpine	eclipse-temurin:21-jre-alpine	Alpine com a distribució recomanada. En cas de problemes (incompatibilitats) en fase de projecte es decidirà quina altre utilitzar.

				eclipse-temurin:21-jre-alpine		
	NodeJS		node:8.16.0-alpine node:10-alpine node:12-alpine node:14-alpine node:16-alpine	node:18-alpine node:20-alpine	node:20-alpine	Alpine com a distribució recomanada. En cas de problemes (incompatibilitats) en fase de projecte es decidirà quina altre utilitzar.
	Golang		golang:1.20-alpine	golang:1.21-alpine golang:1.22-alpine	golang:1.22-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 python:3.12-slim-buster	python:3.12-slim-buster	Debian com a distribució recomanada. En cas de problemes (incompatibilitats) en fase de projecte es decidirà quina altre utilitzar.
Servidor web	Apache		<= 2.2	2017-04-01T22:00:00.000Z	2017-04-01T22:00:00.000Z	Només manteniment
	NGinx		< 1.24.x	1.24.x	1.26.x	

Servidor d'aplicacions	WildFly		<= 22.x	>= 23.x	33.x	Només manteniment. Es recomana anar a runtime Docker de Java i Spring Boot
	JBoss EAP		<= 7.3.x	7.4.x	8.x	Només manteniment. Es recomana anar a runtime Docker de Java i Spring Boot
	Tomcat		<= 7.x,8.0,8.5,10.0.x	9.0	10.1.x	Només manteniment. Es recomana anar a runtime Docker de Java i Spring Boot
	Jetty		<= 11.x	12.x	12.x	Només manteniment. Es recomana anar a runtime Docker de Java i Spring Boot
Sistemes operatius	Ubuntu		< 17.x			Només manteniment.
	RHEL/CentOS		< 7	7.x	8.x	Només manteniment.
	Amazon Linux 2					Opció recomendada. Utilitzar la AMI corporativa "TEMPLATE_UOC"
	Suse		< 12.x			Només manteniment.
	Windows Server		<= 2012 R2	2016	2019	Només per a servidors de Xarxa Interna, no per a serveis en producció
	Windows Desktop		< 10	10	11	Només per a equips d'usuari, no per a serveis en producció
	Solaris		< 10	11		Només manteniment.

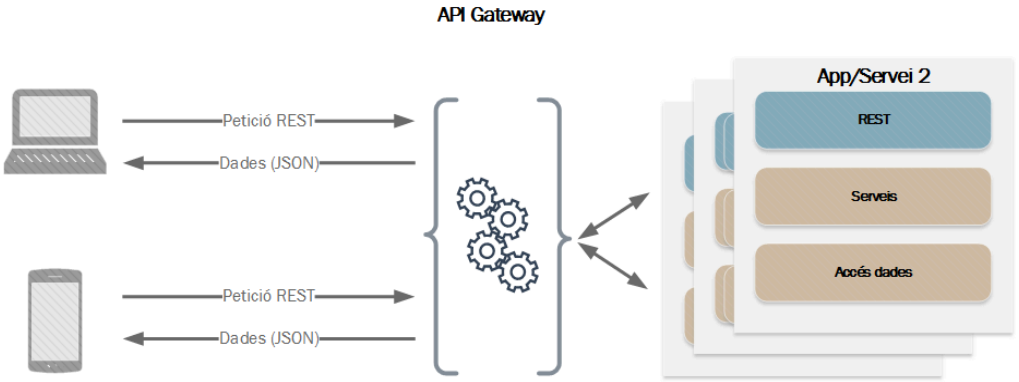
2. Preferiblement s'han d'utilitzar "versions recomanades": seleccionem l'última versió LTS i en cas que no existeixi el concepte en el programari en qüestió, última estable

Catàleg de Serveis tecnològics

	Tipus	OnPremise	AWS	Azure	Altres	Observacions
Servei de Contenidors	CaaS		x			AWS Fargate, AWS ECS
Servei de Cues	SaaS		x	x		AWS SQS, Azure Storage
Servei de Notificacions	SaaS		x	x		AWS SNS
Workflow	SaaS		x			AWS Step Functions (i express workflows)
Caché (aplicacions)	SaaS		x			AWS ElastiCache
CDN	SaaS		x			AWS Cloudfront
Object Storage	Storage		x	x		AWS = S3 Altres = Blob Storage
Big Data Storage	Big Data / BI			x		Azure Data Lake Store AWS Lake Formation
Anàlisi de Dades	Big Data / BI		x	x	PowerBI	Azure Data Lake Store AWS Lake Formation
Servei de Cerca	Search		x	x	GSS / GCE	- Crawler/Cerca GSS - pendent de substitució - Azure Search - AWS Cloud Search
SAML	Autenticació	x	x	x		Keycloak / Shibboleth
OAuth	Autenticació / Autorització	x	x	x		Keycloak

API Gateway UOC

Amb els canvis actuals en els patrons de desenvolupament, on les aplicacions s'orienten a serveis/apis, estan distribuïdes, i els consumidors d'aquests serveis poden ser diversos, apareix un problema de gestió d'aquestes comunicacions. Degut a això, ha sorgit un tipus d'eina que permet governar aquest escenari: l'API Gateway.



Un API Gateway el podem entendre com un firewall “de negoci”, un proxy, una eina de govern, on les regles que es configuren no són a nivell d’IP si no de URL, i que, a banda de permetre o denegar accessos, té moltes altres funcionalitats útils per al negoci.

Normalment, la suite de productes d’un API Gateway inclou tres de principals:

- API Manager: eina de gestió de les regles
- API Gateway: element físic o virtual que està punxat a la xarxa, normalment darrera dels balancejadors, i que interpreta les regles que li injecta el manager
- API Portal: web de comunicació on es representen les APIs que estan gestionades a l’eina i on s’ofereixen recursos per a desenvolupadors, com per exemple diferents SDKs per a connectar al servei, així com la possibilitat de registrar-se per a fer servir una API i obtenir el corresponent API Key

Com i quan utilitzar l'API Gateway?

Quan:

- es vol exposar un servei intern (no públic) de la UOC a internet
- es vol exposar un servei d'internet a aplicacions internes de la UOC (en principi, sense sortida a internet)
- es vol securitzar o canviar el mecanisme de seguretat que s'exposa, per a aïllar una aplicació d'un mecanisme de securització X
- es vol monitoritzar un servei
- es vol limitar l'ús d'un servei (quotes)
- es vol "cachejar" un servei
- es vol gestionar el cicle de vida d'un servei: versionat i obsolescència
- en temps de desenvolupament d'integracions per a crear "mock services" per a simular interfícies i respostes (https://en.wikipedia.org/wiki/Mock_object)

Com:

- en definir l'arquitectura de la solució han de quedar clares les interaccions i interfícies amb altres serveis, de manera que el cap de projecte o el cap de projecte d'integració puguin fer una petició al projecte PPSERVEIS

Quan no utilitzar l'API Gateway?

No utilitzar quan:

- el servei ja estigui exposat a internet

Excepcions:

- que es vulgui monitoritzar
- que es vulgui securitzar amb un altre mecanisme

- que es vulgui limitar l'accés
- que es vulgui cachejar
- no existeixi un servei exposat on aplicar la capa de govern (monitorització, securització, límits, caché, ...), és a dir, a l'API Gateway no es posarà lògica de negoci, només regles de govern.

Seguretat

La seguretat es tindrà en compte des de l'inici del desenvolupament d'una aplicació. Per tant, en tot desenvolupament es lliurarà un document que acrediti que s'han tingut en compte les consideracions relatives a la seguretat.

UX i Accessibilitat

Guia per a l'adquisició de productes de mercat

Introducció
Aquesta guia recull els criteris a tenir en compte a l'hora de seleccionar i/o valorar la compra d'un producte de mercat segons el punt de vista dels diferents àmbits de l'àrea de tecnologia.

Aquest criteris busquen establir una pauta que garanteixin uns mínims de qualitat del producte que es vulgui adquirir. Són uns criteris de caràcter general, per tant, depenent de les característiques del producte i de les necessitats de les àrees de gestió i/o docència, es podrien adaptar, sempre amb el vist i plau de l'àmbit de l'àrea de tecnologia responsable en cada cas.

Criteris d'UX, accessibilitat i front-end
Quan el producte a comprar mostra interfície a estudiant, potencial estudiant i/o docents, s'ha de tenir en compte el següent:

- **Estil gràfic:** l'eina permet personalitzar l'estil amb els mínims de tipografies UOC, colors de marca i logo.
- **Usabilitat**: el grau en que l'eina és usable i té una bona UX (en termes d'eficiència, eficàcia i satisfacció). Es pot mesurar per:
    - L'eina disposa de resultats d'enquestes de satisfacció i/o mètriques que mesuren la UX (NPS, etc)
    - L'eina ha passat un o varis tests d'usuaris.
    - Es disposa d'un informe heurístic que demostri la seva usabilitat
    - L'eina disposa d'un certificat ISO d'usabilitat o similar
- **Frontend**:
    - 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/)
- **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).
- **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)
        - 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%.
    - Optimització:
        - Icones en format font o svg, CSS optimitzades i minimitzades.
- **Multidioma**: La plataforma haurà de ser multi-idioma, i hauran d'estar disponibles en els idiomes: català (llengua vehicular de la Universitat i que ha de ser l'idioma per defecte), castellà i anglès. Així doncs, haurà de ser compatible amb caràcters llatins com pot ser el cas dels accents, la "ñ" i la "ç".
- **Accessibilitat**: grau en que l'eina de mercat compleix amb la doble AA, el mínim legal exigit a la UOC
    - 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 (demostrable amb validador automàtic. Sense errors i amb aspectes validats manualment), o estar en procés de compliment.
    - 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 "o equivalent, o estar en procés de compliment.

Quan el producte a comprar mostra interfície únicament a equip de gestió i/o intern, s'apliquen els mateixos criteris anteriors exceptuant el següent:

- **Estil gràfic:**
    - L'aplicació haurà de permetre a l'usuari identificar en tot moment que es troba dins d'un "sistema UOC", mitjançant la visualització del logotip a totes les pantalles amb les que interactui.
    - Es valorarà objectivament que l'eina permeti personalitzar l'estil amb els mínims de tipografies UOC i colors de marca.
- **Accessibilitat i usabilitat**: si per necessitats de negoci, el producte de mercat en qüestió no compleix els criteris mínims d'usabilitat i accessibilitat, i davant les mateixes prestacions, s'ha de prioritzar aquell producte que sigui més accessible i usable.

UX

La normativa de UX estableix els requeriments, lliuraments i marc de treball a tenir en en compte en els projectes d'AT 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.

Aquesta normativa defineix, per tant,

- **Requeriments** en matèria de **UX**, **front-end** i **accessibilitat**
- Tipologia i caracteristicas dels **lliuraments UX d'Accessibilitat** demanats
- **Marc de treball** de les activitats UX en els projectes

Aquest requeriments, lliuraments i dinàmiques/models han de ser **tinguts en compte per part dels diferents proveïdors, i i han 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'ajustaran en funció de la naturalesa i objectius dels projectes, en consens amb el proveïdor.

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 cero.

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. Per exemple, hi haurà més flexibilitat en aplicació de la normativa en productes digitals UOC antics i destinats a usuaris gestió o en productes de mercat, i és serà més exigent en productes nous destinats a estudiants.

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.

Accessibilitat

Introducció

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.

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).

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.

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(Obre en finestra nova)", o en vigor.

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.

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 s'hi ha annexat documentació complementària que afegeix bibliografia per a ampliar coneixements.

Actualització sobre el govern i assegurament de l'accessibilitat (release normativa febrer 2023)
Degut a la jubilació del Llorenç Sabaté, el nostre expert en accessibilitat, cal actualitzar l'enfocament sobre el govern, l'execució i la verficció del compliment de l'accessibilitat.

A continuació es detallen les novetats respecte a això:

- La responsabilitat sobre l'àmbit d'accessibilitat en les iniciatives de Tecnologia passa a la comunitat UX, és a dir, a les 3 persones responsables de UX dels GOSD
- El nou model de gestió de l'accessibilitat es basa en
    - Govern:
        - L'eix estructural es disposar d'una política d'accessibilitat que serà d'obligat compliment per a tots els nostres proveïdors.
        - La comunitat UX serà la responsable de versionar aquesta política. La periodicitat d'aquesta renovació es decidirà en la comunitat UX.
        - La comunitat UX serà la responsable de comunicar la política als proveïdors i assegurar l'enteniment de la necessitat de compliment a través dels comités de govern de l'UX que ja existeixen.
        - Definir mecanismes que permetin avaluar el nivell de compliment de la política d'accessibilitat.
    - Execució:
        - Seran els proveïdors els responsables d'executar la política d'accessibilitat i presentar les corresponents evidències.
        - Els proveïdors han d'assegurar l'accessibilitat dels seus lliurables i execucions.
        - Per tant els proveïdors han de tenir el coneixement necessari per aplicar correctament la política d'accessibilitat, garantir-ne el seu compliment i donar solucions a problemàtiques devingudes.
    - Verificació del compliment:

- El proveïdor ha d'assegurar el compliment de la política d'accessibilitat en els projectes a través dels mecanismes definits en l'àmbit del govern
- Establir i mantenir els elements que permetin operativitzar la verificació, com ara
    - Un certificat d'accessibilitat
    - Un testrail executat amb èxit
    - Una verificació automàtica amb una eina especialitzada (caldrà indicar quina)
    - Una auditoria externa que realitza el propi proveïdor (si els hi hem indicat en l'encàrrec)
    - Una verificació externa encarregada des de la UOC
    - Etc.

Activitats

La Normativa d'accessibilitat la conformen les activitats que es descriuen a continuació:

- 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

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 accesible 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 (W3C Recommendation 06 Jun 2023)

- 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 podeu consultar la plana Requeriments d'accessibilitat.

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.

Executar el 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.

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. Veure cas a TestRail per més informació. 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. Es pot emprar entre altres els següents recursos

- Paleta de colors accessible
- Color Contrast Checker
- Altres recollits al apartat recursos d'accessibilitat

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 metodologia 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

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. la referència de la test suite és la: S176_ACCESSIBILITAT (Enllaç al TestSuite d'Accessibilitat dins de TestRail)

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 automàtica obtindrem un nivell aproximat de revisió d'accessibilitat del 32% (veure what we found when we tested tools on the worlds least accessible webpage), pel que es recomana una combinació de test manual i eines automàtiques. El W3C te una plana on recull les diferents eines per fer un test automatic (veure apartat bibliografia)

Creació informe resultat proves accessibilitat

Quan passem el test d'accessibilitat ja sigui via Pla de proves d'accessibilitat a confluence o seguint la nostra metodologia (del proveïdor) anirem recollint per cada criteri si passa, falla o no aplica. A més a més 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 manteniment cap eina si avanç no s'han solucionat els errors d'accessibilitat detectats en l'auditoria.

Declaració d'accessibilitat

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

Aquesta declaració d'accessibilitat s'hauria de mostrar en 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.

Eines i documents

El proveïdor ha de lliurar el Informe de Resultats de Proves conforme ha passat el pla de proves d'accessibilitat. Més concretament el (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, la qual es accessible des del link etiquetat com "accessibilitat" que es localitza en el peu del lloc web.

Annex - Normativa de Qualitat

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.

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.

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.

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.

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	**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").**

			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 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**

<table>
<tr>
<td>Rati de Seguretat</td>
<td>Seguretat</td>
<td>Anàlisi estàtic de codi font</td>
<td>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</td>
<td>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</td>
</tr>
<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><td colspan="5">TAULA RESUM COBERTURES DE CODI</td></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 productivity: lines should not be too long, "switch" statements should have at least 3 cases, ... 5. **INFO** Neither a bug	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

			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

Incompliment de la Normativa

L'incompliment d'aquesta Normativa generarà No conformitat en els projectes, les aplicacions, els serveis o els programes.

Annex - Normativa de Seguretat

Plataformes SaaS

Per a les plataformes SaaS es defineixen els criteris següents:

ÀMBIT SEGURETAT:

- Certificació ISO 27001 o ENS pel SaaS
- Garanteix la possibilitat de configuració de rols i permisos en funció d'usuaris i tasques.
- Registra les dades de cada intent d'accés, amb informació relativa a la identificació unívoca d'usuari, tipus d'accés, data i hora, informació accedida i les conserva un mínim de 12 mesos

- Permet tenir un registre actualitzat d'usuaris que reflecteixi 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 pot processar immediatament les baixes dels usuaris mitjançant les eines d'administració de les aplicacions, inhabilitant l'accés a les mateixes. La baixa d'un usuari implica el seu bloqueig temporal, abans de procedir a la seva eliminació definitiva.
- La solució ha de garantir que tota la informació viatja i s'emmagatzema xifrada (amb clau mínima 256 bits)
- Disposa de mesures de seguretat adequades en tots els entorns per garantir la confidencialitat, integritat i disponibilitat de les dades (i.e.: Firewall, Sistemes de Detecció i Prevenció de Intrusos (IDS/IDPS), Zona Desmilitaritzada (DMZ), Xarxes Privades Virtuals (VPN) i Proxy a la infraestructura.
- Disposen dels logs o registres de traçabilitat suficients per analitzar una intrusió o fuga d'informació en cas necessari.
- El prestador del servei 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.
- El Proveïdor 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.
- Possibilitat de definir IP Blacklist
- Caducitat de sessió en cas d'inactivitat (configurable)
- Disposar d'eines de revisió d'anàlisi forense
- Disposa 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, fent èmfasi en els administradors
- La solució haurà de garantir que s'empraran mecanismes d'eliminació segura d'informació. Aquests inclouen els casos de reciclatge de suports i de finalització del Servei.

ÀMBIT RGPD:

- Les dades han d'estar emmagatzemades en una ubicació de la UE
- Es tracten dades de categories especials?
- Permet definir criteris de conservació i eliminació periòdica de dades
- Dóna compliment a tota la normativa de protecció de dades personal RGPD, LOPDGDD
- Disposa d'un sistema d'atenció a l'exercici de drets en matèria de protecció de dades
- Disposa de Delegat de Protecció de Dades
- Disposa d'un protocol davant incidents i comunicació de bretxes de seguretat
- Tots els subcontractistes que utilitza el SaaS s'ubiquen a la UE (inclou els serveis cloud)

Desenvolupaments i configuracions

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

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 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

Seguretat Arquitectural
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
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 cada tipus de recurs protegit (incloses les llibreries que necessiten d'autorització de serveis externs

Seguretat Arquitectural
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
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

Seguretat Arquitectural
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 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 defecte i des del disseny per garantir ple compliment de totes les disposicions del RGPD i normativa adicional.
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)

Seguretat Arquitectural
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
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

Protecció de dades personals

L'adjudicatari haurà de donar compliment amb el que s'estableix en el Plec de Clàusules Pariculars, en matèria de Protecció de Dades Personals.

Annex – Desenvolupament segur del software.

Introducció

Aquest annex estableix el compromís d'acord entre el Client Universitat Oberta de Catalunya (d'ara en endavant UOC) i l'adjudicatari per tal de maximitzar la seguretat del software de l'aplicació (d'ara en endavant l'aplicació) d'acord amb els següents termes.

Filosofia

Aquest annex està destinat a clarificar els drets i obligacions relacionades amb la seguretat de les relacions comercials de les parts involucrades en el desenvolupament de l'aplicació. Al més alt nivell, aquestes parts acorden que:

Les decisions de seguretat estaran basades en el risc: Les decisions de seguretat es prendran conjuntament entre UOC i l'adjudicatari basant-se en una alta comprensió del risc que pot tenir l'aplicació.

Les activitats dedicades a la seguretat estaran balancejades: Els esforços dedicats a la seguretat de l'aplicació estaran fortament distribuïts durant tot el cicle de vida del seu desenvolupament.

S'integraran les activitats dedicades a la seguretat: Totes les activitats i la documentació generada aquí caldrà que s'integri en el cicle de vida de desenvolupament del software de l'aplicació i no podran en cap cas estar separades de la resta del projecte. Res en aquest annex implica un desenvolupament especial de software.

Podran aparèixer vulnerabilitats: Aquest annex assumeix que tot software pot tenir errors i que alguns d'aquests poden crear incidents de seguretat. Tant UOC com l'adjudicatari s'esforçaran en identificar les vulnerabilitats amb la major celeritat possible durant el cicle de vida de l'aplicació.

La seguretat de la informació serà completament revelada: Tota informació relacionada amb la seguretat de la informació de l'aplicació, serà compartida entre UOC i l'adjudicatari de forma immediata i completa. El proveïdor especificarà per escrit quins aspectes de la seguretat relacionada amb el desenvolupament pensa no complir.

Només es requereix aquella documentació que sigui útil en aspectes de seguretat: La documentació de seguretat no ha de ser extensa en excés en ordre a clarificar, descriure el disseny de la seguretat, el risc, l'anàlisi i els incidents.

Activitats del cicle de vida de l'aplicació

Comprensió del risc: UOC i l'adjudicatari acorden treballar de manera conjunta per comprendre i documentar els riscs que poden afectar a l'aplicació. Aquest esforç s'enfocarà a identificar possibles vulnerabilitats que afectin als actius i les funcionalitats de l'aplicació. Caldrà considerar cadascun dels punts, funcionalitats i casos d'ús definits en la part dels requeriments de l'aplicació.

Requeriments: Basant-se en el risc, UOC i l'adjudicatari acorden treballar de manera conjunta per definir uns requeriments de seguretat com a part de les especificacions del software a desenvolupar. Cadascun dels punts que s'hagin enumerat en la secció de requeriments caldrà que siguin discutits i avaluats conjuntament per UOC i l'adjudicatari. Aquests requeriments hauran de ser satisfets en la seva totalitat per l'aplicació.

Disseny: L'adjudicatari acorda proporcionar una documentació que expliqui de forma clara el disseny que s'implementa per assolir els requeriments de seguretat. Aquest disseny explicarà de forma clara si el suport als requeriments de seguretat provenen del software desenvolupat a l'aplicació, de software de terceres parts o de la plataforma en la que s'implementa el desenvolupament.

Implementació: L'adjudicatari acorda proporcionar i seguir un conjunt de bones pràctiques de programació. Aquestes guies indicaran com s'ha de formatar el codi, com s'ha d'estructurar i comentar.

Tanmateix el codi podrà ser revisat per alguna persona responsable de l'execució del projecte de la UOC que validarà els requeriments de seguretat i les guies de programació abans de que el codi de l'aplicació sigui considerat preparat per test.

Seguretat de l'anàlisi i proves: L'adjudicatari acorda proporcionar i seguir un pla de proves de seguretat el qual definirà la aproximació que s'hagi fet a cadascun dels requeriments de seguretat. El nivell del rigor d'aquesta activitat ha d'estar considerada i detallada en el pla del projecte. L'adjudicatari executarà el pla de proves de seguretat i proporcionarà els resultats a la UOC.

Desplegament segur: L'adjudicatari acorda proporcionar les guies per configurar l'aplicació de manera segura, ben documentades i de tal manera que cobreixin tots els requeriments especificats en el pla de projecte.

Àrees de seguretat

L'adjudicatari acorda que les següents àrees seran considerades durant la comprensió del risc i les activitats de definició dels requeriments de l'aplicació.

Validació i codificació: Tot el conjunt de requeriments que especifiquen les regles per canonicalitzar, validar i codificar cada entrada de l'aplicació, tant des dels usuaris, sistema de fitxers, directoris o sistemes externs. La regla per defecte serà que totes les entrades són invàlides a menys que compleixin una determinada especificació que ho permeti. Addicionalment, els requeriments de l'aplicació especificaran l'acció a emprendre quan es rebi una entrada no vàlida. Específicament, l'aplicació no serà susceptible a injecció, desbordament (overflow), manipulació (tampering) o d'altres atacs de corrupció d'entrada de dades.

Control d'accés: Els requeriments de l'aplicació inclouran una descripció detallada de tots els rols i perfils usats (grups, privilegis, autoritzacions) en l'aplicació. Els requeriments hauran també d'indicar tot el conjunt d'actius i funcionalitats proporcionades per l'aplicació. Els requeriments hauran d'explicar completa i exactament els drets d'accés a cadascun dels actius i funcions de l'aplicació per cadascun dels rols.

Registre (Logging): Dins dels requeriments caldrà que s'especifiquin quins esdeveniments són rellevants per la seguretat i les connexions de l'aplicació, com ara els atacs detectats, els intents fallits d'accés i els intents de guanyar privilegis. Els requeriments també especificaran quin tipus d'informació queda enregistrada para cadascun dels esdeveniments generats, incloent-hi la data, la descripció de l'esdeveniment, detalls de l'aplicació i d'altra informació forense d'utilitat.

Connexió a sistemes externs: Els requeriments especificaran com es tracta la autenticació cap a sistemes externs a l'aplicació, com ara les bases de dades i webservices. Totes les credencials necessàries per a la comunicació amb aquests sistemes que s'emmagatzemin en fitxers de configuració ho faran de forma protegida.

Encriptació: Els requeriments de l'aplicació especificaran quines dades han de ser xifrades, com s'han xifrat i com es manipularan els certificats y d'altres credencials. Les especificacions es referiran sempre a un algorisme estàndard d'alguna biblioteca abastament provada i utilitzada.

Personal i organització

Arquitecte de seguretat: L'adjudicatari assignarà responsabilitats en matèria de seguretat a un recurs, que passi a ser l'arquitecte de seguretat del projecte. Aquest certificarà la seguretat de cada lliurament.

Formació en seguretat: L'adjudicatari serà responsable d'assegurar que tots els seus membres de l'equip de desenvolupament estan capacitats en les tècniques de desenvolupament segur.

Biblioteques, frameworks d'aplicació i productes

Divulgació: L'adjudicatari farà públic el software de terceres parts usat en el desenvolupament de l'aplicació, incloent-hi les llibreries, frameworks, components i d'altres productes, siguin comercials, lliures, en codi obert o en codi tancat.

Avaluació: L'adjudicatari realitzarà els esforços raonables per assegurar que tot el software de terceres parts usat en l'aplicació, compleix els termes d'aquest annex. Si les llibreries tenen vulnerabilitats publicades en el moment de la signatura del contracte, l'adjudicatari es comprometrà a canviar-les per la versió que no presenti vulnerabilitats o per un altre producte que ofereixi majors garanties de seguretat sempre i quan sigui compatible amb el projecte.

Revisions de seguretat

Dret a la revisió: UOC té el dret a revisar el codi per fallades de seguretat. L'adjudicatari acorda proporcionar un suport raonable posteriorment a la data de lliurament i durant el període de garantia.

Cobertura de les revisions: Les revisions de seguretat inclouran tots els aspectes relacionats amb la distribució de l'aplicació, incloent-hi el codi desenvolupat, els components, productes i la configuració del sistema.

Àmbit de la revisió: Com a mínim, la revisió abastarà tots els requeriments de seguretat i cerca de d'altres vulnerabilitats. L'examen pot incloure una combinació d'escanejos de vulnerabilitats, tests de penetració, anàlisi del codi font, revisions per terceres parts i revisió del codi.

Problemes de seguretat descoberts: Seran reportats tant per UOC com l'adjudicatari. Totes aquestes qüestions seran rastrejades i solucionades tal i com s'especifica en la secció Gestió dels Problemes de Seguretat d'aquest annex.

Gestió dels problemes de seguretat

Identificació: L'adjudicatari farà un seguiment de tots els problemes de seguretat descoberts durant tot el cicle de vida de l'aplicació, disseny, execució, assajos, desplegament i garantia. El risc associat a cada problema de seguretat serà avaluat, documentat i informat a la UOC tan ràpid com sigui possible després del seu descobriment.

Protecció: L'adjudicatari protegirà adequadament la informació relativa a qüestions relacionades amb la seguretat i la documentació associada, per ajudar a que quedin exposades al mínim les possibles vulnerabilitats de l'aplicació.

Fiabilitat

Fiabilitat: L'adjudicatari oferirà un "paquet de certificació" que constarà de la documentació de seguretat creada al llarg del procés de desenvolupament. Aquest paquet de certificació establirà i descriurà com els requeriments de seguretat, disseny, implementació i els resultats de les proves van ser degudament complimentats i que totes les qüestions de seguretat es van resoldre adequadament.

Certificació: L'adjudicatari certifica que l'aplicació compleix amb els requeriments de seguretat, que en el desenvolupament s'han realitzat totes les activitats relacionades amb la seguretat i que tots els problemes de seguretat identificats s'han documentat i resolt. Qualsevol excepció a la Certificació de l'aplicació estarà plenament documentada en el lliurament. Aquesta Certificació estarà inclosa dins el "Paquet de Certificació".

Lliure de codi maliciós: L'adjudicatari garanteix que l'aplicació no conté cap codi que no sigui compatible amb els requeriments de l'aplicació i debiliti la seguretat de l'aplicació, inclosos els virus, cucs, bombes de temps, portes secretes, troians, ous de Pasqua i totes les demés formes conegudes de codi maliciós.

Acceptació de la seguretat i garantia

Acceptació: El software de l'aplicació no es considerarà acceptat fins que el "Paquet de Certificació" estigui complet i totes les qüestions de seguretat s'hagin resolt.

Investigació dels problemes de seguretat: Després de l'acceptació, si es descobreixen problemes de seguretat o existeix una sospita raonable, l'adjudicatari ajudarà a UOC a dur una investigació per determinar la naturalesa de la qüestió. Els fets es consideraran una novetat.

Qüestions de seguretat noves: L'adjudicatari i UOC acorden dins l'àmbit d'aplicació, que hi haurà un esforç necessari per a resoldre els nous problemes de seguretat i negociaran de bona fe un acord per a realitzar les tasques necessàries per corregir-los.

Annex - Integració Plataforma Informacional

Publicació de les dades:

- L'estratègia de dades adoptada per la UOC es basa en un model de publicació de Productes de Dades per part dels orígens de dades. Per tant, el nou sistema hauria de tenir la capacitat de publicar les seves dades de qualsevol àmbit o mòdul que contingui, en el format i temps que requereixin els consumidors finals, tot a través de la Plataforma d'Interoperabilitat UOC.
- En cas de no poder publicar Productes de Dades directament, hauria de ser possible la publicació de tot el model de dades intern a partir de la Plataforma d'Interoperabilitat UOC per tal d'integrar-se amb la Plataforma Informacional.
- En cas de no complir cap dels anteriors, s'ha d'indicar el detall de la cobertura del model de dades sencer que es podria publicar.

Consum de les dades:

- Les dades publicades, ja siguin Productes de Dades directament o el model sencer, seran integrades amb la Plataforma Informacional a través de la Plataforma d'Interoperabilitat.

Latència de les publicacions de dades:

- La latència mínima requerida és el més pròxim possible al real time, amb l'objectiu de disposar de la informació en el mínim de temps possible des que es genera la dada fins que es publica.
- Tot i així, per valorar les diferents possibilitats de latència de dades, s'haurien de detallar quines opcions proporciona el nou sistema.
- En cas de no poder mantenir internament un històric de dades i versions, el nou sistema juntament amb la Plataforma d'Interoperabilitat, han d'assegurar que no hi hagin pèrdues en la publicació de versions i dades.

ANNEX 3

MODEL DE SOL·LICITUD DE RETENCIÓ EN EL PREU

PER CONSTITUIR GARANTIA DEFINITIVA

El/la senyor/a _____, major d'edat, amb D.N.I. núm. _____, amb domicili a _____, en nom i representació de la Companyia Mercantil _____, domiciliada a _____, amb NIF _____ inscrita en el Registre Mercantil de _____ al Tom _____, Llibre ____, Foli _____ i full _____. El/la senyor/a _____ actua en la seva condició d'apoderat/da de la Companyia, i especialment facultat/da per aquest acte en virtut d'escriptura de poder autoritzada pel Notari/a de _____, Sr/a. _____, el dia ___ de _____ de _____, amb el núm. _____ del seu protocol,

EXPOSA

Que, en cas de resultar adjudicatari per la Universitat Oberta de Catalunya del contracte basat de "Serveis professionals de SalesForce" amb número d'expedient DER10/CSUC2125/L1,

SOL·LICITA

ia.

Nom i cognoms: _____

Data: _____

Signatura: _____

ANNEX 4

ACORD DE CONFIDENCIALITAT

Primer.- Mitjançant la signatura del present acord el proveïdor garanteix a la UOC que mantindrà la confidencialitat de tota aquella informació dades i documentació que li hagi estat comunicada per la UOC o a la qual hagi tingut accés, en format tangible o intangible i per qualsevol mitjà, amb ocasió de la realització de l'objecte del present procediment de contractació. A aquests efectes, s'obliga a mantenir-la en la més estricta confidencialitat i a no divulgar-la advertint, en el seu cas, d'aquest deure de confidencialitat i secret al seu personal i a qualsevol persona, que per la seva relació, hagi d'accedir a aquesta informació, així com a fer ús d'aquesta informació exclusivament per al desenvolupament de l'objecte del present procediment de contractació abstenint-se de qualsevol altra ús.

A efectes d'aquest acord, s'entén com a «Informació Confidencial» (en endavant, Informació Confidencial), amb caràcter enunciatiu i no limitatiu, especialment:

Qualsevol informació, reservada, confidencial o secreta relacionada, amb serveis, desenvolupaments informàtics, tecnològics, continguts objecte de drets d'autor, patents, tècniques, models, invencions, «know-how», processos, algoritmes, programes, executables, investigacions, detalls de disseny, informació financera, contractes de personal, proveïdors, llista de clients, bases de dades, inversionistes, relacions de negocis i contractuals, plans i estratègies de negoci i de mercadeig, mètodes d'administració, publicitat, màrqueting de formació i qualsevol altra informació revelada sobre els seus respectius negocis; així com qualssevol documents, apunts, documents de treball, notes, anàlisis, models, estudis o informes basats en o derivats de l'esmentada Informació confidencial.

Segon.- El proveïdor es compromet davant la UOC a adoptar les mesures oportunes i posar els mitjans necessaris per assegurar el tractament confidencial d'aquesta informació confidencial, mesures que no seran menors que les aplicades per ell/ella a la seva pròpia informació confidencial, assumint les següents obligacions:

1. Mantenir la confidencialitat de la informació confidencial i no desvelar ni revelar la informació de la UOC a terceres persones, excepte autorització prèvia escrita de la UOC.
2. Permetre l'accés a la informació confidencial únicament als partícips/socis, directors, empleats i assessors professionals de del proveïdor que necessitin la informació pel desenvolupament de les tasques en el marc del Contracte per a les quals l'ús d'aquesta informació sigui estrictament necessària i que estiguin subjectes a obligacions de confidencialitat no menys protectores que les establertes en el present Acord. Referent a això, el proveïdor advertirà a aquestes persones de les seves obligacions respecte a la confidencialitat, vetllant pel compliment de les mateixes.
3. Comunicar a la UOC tota la filtració de la informació de la que tingui o arribi a tenir coneixement, produïda per la vulneració de l'Acord de Confidencialitat o infidelitat de les persones que hagin accedit a la informació confidencial, amb el benentès que aquesta comunicació no eximeix al proveïdor de responsabilitat, però si la incompleix donarà lloc a les responsabilitats que es derivin d'aquesta omissió en particular.
4. Limitar l'ús de la informació confidencial a l'estrictament necessari per al compliment del Contracte, assumint la responsabilitat per tot ús diferent a aquest, realitzat per ella o per les persones físiques o jurídiques a les quals hagi permès l'accés a la informació confidencial.
5. Un cop finalitzat el Contracte, retornar o destruir qualsevol còpia de la informació confidencial de la UOC que pugui tenir en el seu poder.

Tercer.- Que, sens perjudici de les obligacions imposades per la normativa nacional i/o assumides per la part receptora de la informació confidencial, les obligacions de confidencialitat recollides en el present Acord no seran aplicables a la informació respecte de la qual el proveïdor pugui demostrar:

a) Que fos del domini públic en el moment d'haver-li estat revelada.

b) Que, després d'haver-li estat revelada, fora publicada o d'una altra forma passés a ser de domini públic, sense trencament de l'obligació de confidencialitat pel proveïdor.

c) Que en el moment d'haver-li estat revelada, la part que la va rebre ja la conegués o estigués en possessió de la mateixa per mitjans lícits o tingués dret legalment a accedir a la mateixa.

d) Que tingués consentiment escrit previ de la UOC.

e) Que hagi estat sol·licitada per les Autoritats Administratives o Judicials competents que hagin de pronunciar-se sobre aspectes totals o parcials del mateix, en aquest cas, el proveïdor haurà de comunicar-li a la UOC amb caràcter previ al fet que aquesta presentació tingui lloc, i l'assistirà en qualsevol eventual defensa contra la revelació de la informació sol·licitada.

Quart.- El present Acord no suposarà, en cap cas, la concessió de permís o dret exprés o implícit per a l'ús de patents, marques, drets d'autor o llicències, propietat de la UOC, llevat del que sigui estrictament necessari per complir amb el Contracte i aquesta autorització quedi manifestada expressament per escrit.

Cinquè.- La UOC no atorga cap garantia sobra l'exactitud o caràcter complet de la informació confidencial facilitada i no es compromet a informar dels canvis que es puguin produir en aquesta informació. Tot això s'entén sense perjudici que un acord definitiu entre les parts sobre el Contracte inclogui manifestacions i garanties quant a la informació subministrada, en aquest cas s'estarà al que es disposi en aquest acord.

Sisè.- En cas d'incompliment de qualssevol de les obligacions previstes en el present Acord, la UOC estarà facultada per reclamar al proveïdor el compliment específic de l'establert a l'Acord, fins i tot mitjançant l'adopció de mesures cautelars, juntament amb la indemnització que pels danys i perjudicis causats per l'incompliment li correspongui satisfer.

Setè.- El proveïdor està informat, consent i respectarà el compromís de protecció de dades de caràcter personal inclòs a la clàusula 38 d'aquest Plec. En tot cas, les parts es comprometen a donar compliment a totes les obligacions establertes al Reglament General de Protecció de Dades 679/2016, de 27 d'abril, de protecció de dades de caràcter personal.

La vulneració del deure de confidencialitat sobre la informació i/o les dades esmentades, i també de qualsevol obligació derivada de la legislació de protecció de dades de caràcter personal, serà causa de resolució d'aquest Contracte.

Vuitè.- Les parts es comprometen a mantenir vigent aquest Acord de Confidencialitat per un termini de cinc (5) anys des de la data de la signatura del mateix.

I, perquè així consti i produeixi efectes en el marc del procediment de contractació de referència, signo aquesta declaració a (localitat i data) [lloc], [dia] de [mes] de [any].

Signatura,

ANNEX 5

CONDICIONS PARTICULARS ENCARREGAT DEL TRACTAMENT

En compliment de l'expressament establert a l'article 122.2 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, donat que l'execució del contracte requereix el tractament per part del contractista de dades personals per compte del responsable del tractament, es fa constar la següent informació:

a. Categories de dades objecte de tractament:

1- Noms, cognoms, telèfons i correus electrònics de potencials estudiants.

2.- Noms, cognoms, número de document identificatiu (DNI,Passaport), telèfons i correus electrònics de estudiants matriculats.

b. Finalitat del tractament: Recollida, estructuració, modificació, conservació, extracció, consulta, interconnexió i conservació.

c. Mesures de seguretat aplicables, veure mesures de seguretat aplicables a proveïdors.

Així mateix, és obligació de l'entitat adjudicatària presentar abans de la formalització del contracte una declaració on posi de manifest on estaran ubicats els servidors i des de on es prestaran els serveis associats als mateixos segons el model adjunt.

Qualsevol canvi que es produeixi al llarg de la vida del contracte en relació a la informació declarada segons els paràgraf anterior, ha de ser comunicat pel contractista.

El licitador indicarà també a la seva oferta, si té previst subcontractar els servidors o serveis associats als mateixos, el nom o el perfil empresarial definit per referència a les condicions de solvència professional o tècnica dels subcontractistes als que s'hagi d'encarregar la seva realització.

Les obligacions anteriors es qualifiquen com essencials als efectes del que preveu la lletra f) de l'apartat 1 de l'article 211 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic.

Model Declaració de servidors i serveis associats

Procediment de contractació: CONTRACTE RELATIU A [veure títol indicat a APARTAT A] (EXPEDIENT [veure número expedient indicat a APARTAT A]).

Empresa: [nom de l'empresa]

[El Sr. / la Sra.] [nom i cognoms], amb el DNI número [núm. DNI], en representació de l'empresa [nom de l'empresa o "en representació pròpia" si s'escau],

DECLARO

1. Que els servidors des d'on es prestaran els serveis objecte del contracte que impliquen el tractament de les dades de caràcter personal detallades a les Condicions Particulars de l'Encarregat del Tractament estan ubicats a [localització del servidors]

2. Que els següents serveis associats als servidors [indicar serveis que siguin d'aplicació] es presten des de [indicar localització dels serveis associats]

3. Que els servidors i, en el seu cas, els serveis indicats a l'apartat anterior, estan subcontractats o es preveu la seva contractació a les següents entitats: [indicar proveïdors previstos d'aquest serveis o perfil empresarial definit per referència a les condicions de solvència professional o tècnica]

4. Que, segons s'estableix a la clàusula 38.2.C del Plec, garanteix que el tractament que porti a terme el subcontractista:

   a. S'ajusta a la legalitat vigent, al contemplat en aquest plec i a les instruccions de l'òrgan de contractació.

   b. Té formalitzat o formalitzarà en cas de resultar adjudicatari un contracte d'encàrrec de tractament de dades en termes no menys restrictives a les previstes en el present plec i amb sotmetiment exprés del subcontractista al RGPD i a la LOPDGDD, el qual serà posat a disposició de l'òrgan de contractació.

5. Que qualsevol canvi que es produeixi, al llarg de la vida del contracte, de la informació facilitada a la present declaració serà comunicat a la entitat contractant.

I, perquè així consti i produeixi efectes en el marc del procediment de contractació de referència, signo aquesta declaració a (localitat i data) [lloc], [dia] de [mes] de [any].

Signatura

Mesures de seguretat per a proveïdors

En el cas: Es treballa total o parcialment en les instal.lacions del proveïdor i amb aplicacions i/o infraestructura del Proveïdor. El proveïdor per proveir el servei ha d'emmagatzemar dades personals als seus sistemes. No s'envien emails en nom de la UOC

Index

Index 2

1. Introducció 4

2. Mesures de seguretat 4

2.1. Consideracions prèvies 4

2.1.1. Confidencialitat de les persones 5

2.1.2. Confidencialitat de la informació 5

2.2. Protecció de dades personals 5

2.2.1. Compliment de la legislació 5

2.2.2. Document de seguretat 7

2.2.3. Responsabilitat proactiva 7

2.3. Seguretat de la informació 8

2.3.1 Esquema de control 8

2.3.2 Accés a la informació 9

2.3.3. Gestió de canvis 9

2.3.4. Adquisició i desenvolupament d'aplicacions 9

2.3.5. Gestió d'operacions 10

2.4. Organització de la seguretat 10

2.4.1. Marc normatiu de seguretat TI 10

2.4.2. Identificació de responsabilitats 11

2.4.3. Anàlisi de riscos 12

2.4.4. Plans de formació/conscienciació 13

2.4.5. Notificació 13

2.5. Mesures tecnològiques 13

2.5.1. Control d'accés 13

2.5.1.1. Controlar l'accés a aplicacions i sistemes 14

2.5.1.2. Controls físics i ambientals 16

2.5.1.3. Autorització i autenticació 17

2.5.2. Desenvolupament i adquisició de sistemes de proveïdors amb accés a dades 17

2.5.3. Comunicacions 19

2.5.4. Incidències 19

2.5.5. Gestió de les operacions 21

2.5.5.1. Manteniment de sistemes 21

2.5.5.2. Ubicació de dades 22

2.5.5.3. Gestió de suports d'informació 22

2.5.5.4. Fitxers temporals 23

2.5.5.5. Servei compartit 24

2.5.6. Revisió 24

2.5.6.1. Revisions realitzades per la UOC 24

2.5.6.2. Control intern del Proveïdor 26

2.5.6.3. Controls coordinats amb la UOC 26

2.5.6.4. Devolució del Servei 27
2.5.7. Seguretat perimetral i d'infraestructura 27
2.5.7.1. Seguretat dels servidors 28
2.5.7.2. Seguretat perimetral 28
2.5.8. Monitorització 29
2.5.8.1. Monitorització de la seguretat dels sistemes 29
2.5.8.2. Custòdia i explotació dels logs de seguretat 29
2.5.9. Suport, continuïtat i contingència 29
2.6. Mesures específiques 30

1. Introducció

Les mesures de seguretat s'apliquen en casos en que hi ha tractament de dades personals per part del proveïdor.
Aquest model de mesures de seguretat s'aplica en el següent cas:

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

2. Mesures de seguretat

2.1. Consideracions prèvies

- S'autoritza expressament el tractament de dades personals en les instal·lacions del Proveïdor per les finalitats recollides en el contracte a que es refereixen el serveis del proveïdor. 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, el Proveïdor aplicarà en tot cas, les mesures de seguretat establertes per donar compliment al present document o a la normativa vigent.

- El Proveïdor emprarà 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.

2.1.1. Confidencialitat de les persones

- Tot el personal del Proveïdor 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. El Proveïdor 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 el Proveïdor 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.

2.1.2. Confidencialitat de la informació

- Amb caràcter general, el Proveïdor 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.

2.2. Protecció de dades personals

2.2.1. Compliment de la legislació

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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 del Proveïdor.

- El Proveïdor 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, el Proveïdor pugui conservar cap còpia de les Dades facilitades per la UOC.

- El Proveïdor 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 del Proveïdor 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.

2.2.2. Document de seguretat

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

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

2.2.3. Responsabilitat proactiva

- El Proveïdor 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.

2.3. Seguretat de la informació

2.3.1 Esquema de control

- El Proveïdor 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.

- El Proveïdor 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 el Proveïdor 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.

2.3.2 Accés a la informació

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

2.3.3. Gestió de canvis

- El Proveïdor 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.

2.3.4. Adquisició i desenvolupament d'aplicacions

- El Proveïdor 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.

2.3.5. Gestió d'operacions

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

2.4. Organització de la seguretat

2.4.1. Marc normatiu de seguretat TI

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

2.4.2. Identificació de responsabilitats

- El Proveïdor 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.

- El Proveïdor ha de designar un Coordinador encarregat de la gestió dels aspectes de seguretat amb la UOC. Aquest Coordinador del Proveïdor haurà d'assistir al Comitè de Coordinació mixt, entre el Proveïdor 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.

- El Proveïdor 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 del proveïdor	Indicar
Tipus de Mesures: ESTÀNDARS	Tipus de Tractament: MIXT

2.4.3. Anàlisi de riscos

- El Proveïdor 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.

- El Proveïdor 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.

2.4.4. Plans de formació/conscienciació

- El Proveïdor 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.

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

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

2.4.5. Notificació

- El Proveïdor ha de notificar a la UOC qualsevol succés que excedeixi del acord contractual assolit amb la UOC.

- El Proveïdor 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).

2.5. Mesures tecnològiques

2.5.1. Control d'accés

2.5.1.1. Controlar l'accés a aplicacions i sistemes

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

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor ha d'implantar els mecanismes necessaris que permetin tenir un registre actualitzat d'usuaris. El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

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

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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**.**

- El Proveïdor 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**.**

- El Proveïdor 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.

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

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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**.**

- El Proveïdor 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.

2.5.1.2. Controls físics i ambientals

- El Proveïdor 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.

- El Proveïdor 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.

2.5.1.3. Autorització i autenticació

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

- El Proveïdor 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.

- El Proveïdor 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, el Proveïdor 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.

2.5.2. 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 el Proveïdor 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, el Proveïdor 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.

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

2.5.3. Comunicacions

- El Proveïdor 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 del Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

2.5.4. Incidències

- El Proveïdor 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.

- El Proveïdor 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, el Proveïdor 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).

- El Proveïdor 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.

- El Proveïdor 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.

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

- El Proveïdor 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.

2.5.5. Gestió de les operacions

2.5.5.1. Manteniment de sistemes

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

2.5.5.2. Ubicació de dades

- El Proveïdor 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.

- El Proveïdor 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.

2.5.5.3. Gestió de suports d'informació

- El Proveïdor 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.

- El Proveïdor 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.

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

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

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

2.5.5.4. 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.

2.5.5.5. Servei compartit

- El Proveïdor ha d'implementar les mesures suficients per garantir la seguretat de la infraestructura tecnològica en cas de que sigui compartida amb altres clients del Proveïdor. La infraestructura tecnològica del Servei haurà de posseir canals de comunicació xifrats entre altres serveis que ofereixi el Proveïdor 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 del Proveïdor haurà de tenir la capacitat de xifrar la informació emmagatzemada, mitjançant algoritmes forts de xifrat, en cas de ser requerit.

2.5.6. Revisió

2.5.6.1. 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.

- El Proveïdor 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.

- El Proveïdor 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 del Proveïdor 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 del Proveïdor:
        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 el Proveïdor 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.

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

2.5.6.2. Control intern del Proveïdor

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

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

2.5.6.3. Controls coordinats amb la UOC

- La UOC i el Proveïdor 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 del Proveïdor, 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.

2.5.6.4. Devolució del Servei

- La UOC i el Proveïdor 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 pel Proveïdor durant la prestació del Servei.

- El Proveïdor 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**.**

2.5.7. Seguretat perimetral i d'infraestructura

- El Proveïdor 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.

- El Proveïdor 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.

2.5.7.1. 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.

2.5.7.2. 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.

2.5.8. Monitorització

2.5.8.1. Monitorització de la seguretat dels sistemes

- El Proveïdor 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.

2.5.8.2. 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. El Proveïdor 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.

2.5.9. Suport, continuïtat i contingència

- El Proveïdor 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. El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

- El Proveïdor 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.

2.6. Mesures específiques

- El Proveïdor 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, el Proveïdor haurà de presentar a la UOC les certificacions aplicables, quan així li ho requereixi.