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.

AB OBJECTE I MODALITAT DEL CONTRACTE DERIVAT

Títol: **Subministrament de llicències de SalesForce**

Número d'expedient: **DER15/CSUC2125/L1**

Codi CPV: 48000000-8 Paquets de programari i sistemes d'informació

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 a convidar i els descomptes pels que es van homologar són les següents:

Lot 1:

Empresa	Descompte catàleg plataforma Salesforce	Descompte resta de productes fora de la plataforma Salesforce
Navarra Tecnologia De Software SL	75 %	55 %
Omega CRM Consulting S.L.	30 %	5 %
VASS Consultoría de Sistemas SL	40 %	40 %

B VALOR ESTIMAT DEL CONTRACTE

Set-cents quaranta-nou mil vint-i-nou euros amb deu cèntims IVA exclòs (749.029,10 €), IVA exclòs

L'adjudicatària haurà de proporcionar el conjunt de llicències següent:

Grup 1: Marketing

Quantitat	Producte	Número d'unitats
1	Marketing Cloud Engagement - Enterprise Edition	12
700	Additional Contacts - Enterprise Edition (1000)	12
20	SSL Certificate	12
4	Sender Authentication Package	12
1	Marketing Cloud Advertising Professional	12
1	Marketing Cloud Advertising Professional - Contacts (1000)	12
35	Marketing Cloud Advertising - Additional Audiences	12
1	SMS/MMS Mobile Messages (1000)	12
1	SMS/MMS Code Lease - No charge with Edition	12
1	Marketing Cloud Personalization - Premium (EMEA)	12
5	Marketing Cloud Personalization - Unique Visitors	12

Grup 2: Core

Quantitat	Producte	Número d'unitats
300	Education Cloud - Unlimited Edition	12
250	Education Cloud Intelligence - Unlimited Edition	12
250	Slack Enterprise Grid	12
2.000	Customer Community Plus for Education Cloud - UE - Members	12
3.000	Customer Community Plus for Education Cloud - UE - Logins (Per Month)	12
90	Education Cloud Limited Staff Access - Unlimited Edition	12

Grup 3: Datacloud

Quantitat	Producte	Número d'unitats
1.500	Customer Data Cloud for Marketing - Data Services Card (100k Credits)	1
10	Customer Data Cloud - Segmentation & Activation (100k Credits)	1
1	Force.com - Unlimited Edition (Administrator) - Cross Product	12
1	Customer Data Cloud Starter for Marketing - Unlimited Edition	12

Universitat Oberta de Catalunya

Grup 4: Digital Engagement

Quantitat	Producte	Número d'unitats
667	Salesforce Message Credits - WhatsApp for Marketing (1,000)	1
100	Digital Engagement - Unlimited Edition	12

Grup 5: Mulesoft

Quantitat	Producte	Número d'unitats
10	MuleSoft - Anypoint API Manager Pre-Production - Platinum Edition	4
10	MuleSoft - Anypoint API Governance - Platinum Edition	4
3	MuleSoft - Additional vCore Pre-Production - Platinum Edition	4
1	MuleSoft - Anypoint Flex Gateway (100M API Calls) - Platinum Edition	4
10	MuleSoft - Anypoint API Manager Production - Platinum Edition	4
1	MuleSoft - Anypoint Platform Base Subscription - Titanium Edition	8
2	MuleSoft - Included vCore - Production	8
4	MuleSoft - Included vCore - Pre-Production	8
6	MuleSoft - Additional vCore Production - Titanium Edition	8
4	MuleSoft - Additional vCore Pre-Production - Titanium Edition	8
30	MuleSoft - Anypoint API Manager Production - Titanium Edition	8
30	MuleSoft - Anypoint API Manager Pre-Production - Titanium Edition	8
30	MuleSoft - Anypoint API Governance - Titanium Edition	8
20	MuleSoft - Anypoint Flex Gateway (100M API Calls) - Titanium Edition	8

Grup 5: Agentforce

Quantitat	Producte	Número d'unitats
10.500	Agentforce Service Agent Conversations - Unlimited Edition	12
1	Salesforce Foundations - Agentforce Service Agent	12
1	Salesforce Foundations - Data Cloud Segmentation & Activation	12
1	Salesforce Foundations	12
1	Einstein for Sales Add-on - Unlimited Edition	12
10.500	Additional Einstein Requests for Agentforce (200)	12

El valor estimat del contracte s'ha calculat tenint en compte els càlculs del procediment basat amb número d'expedient DER13/CSUC2125/L1, el qual s'ha declarat desert per no haver-se rebut ofertes vàlides.

En aquell procediment es va tenir en compte el descompte mig que el fabricant es va comprometre a ofertar igualitàriament a tots els distribuïdors dels productes objecte del contracte i inclús un marge als efectes de que les empreses disposessin d'un benefici industrial adequat i als efectes de donar compliment a l'article 101.2 de la LCSP, segons el qual en el càlcul del valor estimat s'han de tenir en compte, a més dels costos que es derivin de l'execució material dels serveis, les despeses generals d'estructura i el benefici industrial.

No obstant això, amb posterioritat s'ha detectat que els imports previstos no estaven ajustats al principi d'onerositat. Aquesta situació ha impedit que les empreses homologades puguin obtenir cap benefici industrial, ja que el pressupost de licitació ha estat pràcticament igual al preu de cost i el marge de benefici ha resultat ser pràcticament inexistent. Això ha provocat que el contracte resulti antieconòmic per a les empreses interessades, fent que no es presenti cap oferta. Aquesta manca d'interès no només ha estat evidenciada per l'absència d'ofertes, sinó també per les comunicacions rebudes de diversos proveïdors homologats que han manifestat la inviabilitat econòmica del contracte.

En aquest context, cal reforçar la justificació del nou càlcul del valor estimat del contracte per garantir que s'ajusta plenament al principi d'onerositat. Segons aquest principi, els contractes han de permetre una relació econòmica justa entre les parts, assegurant que els licitadors puguin cobrir els costos d'execució, incloent-hi les despeses generals, i obtenir un benefici industrial raonable. Això és essencial per fomentar la participació de les empreses i garantir la competència en els procediments de contractació pública.

A la llum d'aquestes consideracions, en el recàlcul del pressupost de licitació cal tenir en compte:

1. **Adequació als costos reals del mercat: Identificar els costos reals de producció i distribució dels productes objecte del contracte, assegurant que el preu base reflecteixi fidelment la realitat econòmica del sector.**
2. **Inclusió d'un benefici industrial raonable: Garantir que el marge de benefici industrial sigui suficient per fer atractiu el contracte per a les empreses licitadores, evitant que el pressupost de licitació quedi igualat al preu de cost.**
3. **Promoció de la competència efectiva: establir unes condicions econòmiques que incentivin la participació activa d'un nombre significatiu de proveïdors, afavorint la lliure competència i obtenint millors condicions per a la UOC.**

Doncs bé, tenint en compte això, s'ha configurat el pressupost en els termes anteriorment exposats, però afegint-hi un import addicional de 9.000 euros, equivalent a un 1,2% del pressupost. I això amb la finalitat que les empreses disposin d'un marge més adequat al mercat i que d'aquesta manera puguin participar al present procediment confeccionant les seves ofertes d'acord amb l'estratègia que decideixin seguir basant-se en el principi de risc i ventura. Cal tenir en compte que, malgrat el % mig de benefici industrial en el sector corresponent al CNAE J62 és del 8,21%, en aquest cas s'ha considerat convenient reduir-lo atesa la naturalesa del contracte i les prestacions a dur a terme per part del contractista (subministrament de les llicències sense prestació de serveis addicionals com serveis d'implantació, consultoria, desenvolupament, manteniment, etc.).

I tot això sense perjudici que les empreses homologades hagin de respectar els descomptes que van oferir en el procediment d'homologació segons s'especifica a la resolució d'homologació de l'acord marc, i que consten transcrits a l'apartat A de la present fitxa de contractació basada.

D'altra banda, i addicionalment a tot l'exposat anteriorment, es deixa constància que el valor estimat del present contracte és inferior a l'import romanent a l'Acord Marc de referència, segons confirmació del Consorci de Serveis Universitaris de Catalunya (CSUC).

Dins d'aquesta xifra

☒ No hi ha inclòs cap import destinat a modificacions contractuals.

C	PRESSUPOST BÀSIC DE LICITACIÓ I PREUS APLICABLES

Nou-cents sis mil tres-cents vint-i-cinc euros amb vint-i-un cèntims (906.325,21 €), IVA inclòs.

- 749.029,10 euros import net
- 157.296,11 euros import IVA (21%)

D	DURADA, PRÒRROGUES I CONDICIONS DE SUBMINISTRAMENT

Durada: **Dotze (12) mesos a comptar des de l'01 de febrer 2025.**

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

Termini de la pròrroga: **N/A**
Nombre màxim de pròrrogues: **N/A**

Es preveuen preus unitaris?: SÍ☐ NO☒

Facturació d'imports per part del contractista:

Una sola factura per l'import total de cada comanda realitzada. Facturació a 30 dies.

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.

Lloc del subministrament: Els serveis es presten de forma remota i són proporcionats pel propi fabricant Salesforce sobre la seva infraestructura.

Veure annex 3.

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: **30 de desembre de 2024** HORA:**12.00h**
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, o persona que el substitueixi.

Secretari: Jordi Vidiella Curto, Advocat especialitzat en Contractació Pública de l'Assessoria Jurídica de la UOC, o persona que el substitueixi.

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, o persona que el substitueixi.

G CONTINGUT DEL SOBRE 2 I OBERTURA

☒ **No hi ha Sobre 2.**
Procediment d'adjudicació: Licitació mitjançant preu més baix

H CRITERIS DE VALORACIO DEL SOBRE 2

☒ **No hi ha Sobre 2.**

I CONTINGUT DEL SOBRE 3 I OBERTURA

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

☒ **Compra directa**
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.

Extensió màxima del contingut? NO☐ SÍ☒ Nombre màx. de pàg: 1

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 seleccionades han de presentar l'annex 1 degudament complimentat i signat.

J CRITERIS DE VALORACIÓ DEL SOBRE 3

Criteris de valoració del sobre 3	100
Subministrament de llicències de SalesForce	100

Les ofertes presentades pels licitadors es valoraran per la Mesa de contractació d'acord amb el criteri del preu més baix.

$$Puntuació = 100\ x\ \frac{Menor\ proposta\ econòmica\ (€)}{Proposta\ econòmica\ a\ valorar\ (€)}$$

Obertura Sobre 3 en acte públic: Mitjans telemàtics **L'obertura es farà en data 07 de gener de 2025 a les 12:30. L'enllaç per accedir a la convocatòria és el següent:** meet.google.com/qhp -wpne-tnp	
K GARANTIA DEFINITIVA	**L CONSULTES I DUBTES**
Ha de constituir-se garantia definitiva? ☒ **Sí** **5%, sobre el pressupost base de licitació, exclòs l'IVA, segons allò disposat a la clàusula 23.1.3 del Plec clàusules administratives 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 (exp. CSUC 21/25).**	Les empreses convidades tenen a la seva disposició la bústia **contractacio@uoc.edu** com a mitjà únic on formular les consultes i els dubtes que puguin sorgir durant l'elaboració de la seva proposta. Per tal de facilitar la identificació del procediment objecte de la consulta, en l'assumpte del correu electrònic ha de constar la paraula "**EXPEDIENT**" seguida del "**NÚMERO D'EXPEDIENT**" de referència que s'indica en el quadre A. La UOC recollirà tots els dubtes i consultes formulades a l'esmentada bústia i en donarà resposta. 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. Data de resposta general de dubtes per correu electrònic per part de la UOC a totes les empreses seleccionades: 20 de desembre de 2024
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 D'OFERTA 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 LOT 1 (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 preus unitaris màxims indicats en els annexos indicats a continuació, més l'import de l'Impost sobre el Valor Afegit que correspongui;

Producte	**Preu màxim de licitació (IVA exclòs)**	**Preu total ofert (IVA exclòs)**	**Import IVA**	**Preu total ofert (IVA inclòs)**
Subministrament de llicències de SalesForce	**749.029,10 €**	.- €	.- €	.- €

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

Signatura del/de la declarant

ANNEX 2
CARACTERÍSTIQUES TÈCNIQUES DEL PROGRAMARI A SUBMINISTRAR

Justificació:

La Fundació per a la Universitat Oberta de Catalunya ("UOC") té l'objectiu de transformar els serveis d'atenció i tutorització desplegant un nou sistema d'informació sobre la plataforma Salesforce Education Cloud.

En concret, 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, que la Universitat pretén aproximar a les expectatives que aquest col·lectiu té. Per a poder-ho fer i aplicar el model desitjat, és imprescindible que tots els agents de contacte amb l'estudiantat treballin sobre una mateixa plataforma que els permeti tenir una visió integral de totes les interaccions amb la Universitat, així com assegurar que es pot passar el testimoni entre els diferents agents de contacte d'una forma òptima i transparent per a l'estudiantat.

Actualment, la UOC compta amb Salesforce per interactuar amb l'estudiantat a la primera etapa del seu *journey*, que correspon als processos comercials. Els equips comercials utilitzen Salesforce per dur a terme la seva activitat principal.

En canvi, un cop l'estudiantat fa la seva primera matrícula, els serveis que la Universitat posa a disposició per a acompanyar-lo es produeixen sobre diferents plataformes incompatibles entre elles. Això impedeix una correcta coordinació entre els equips i que aquests tinguin la informació necessària per poder tenir una conversa amb l'estudiant que permeti una comprensió integral del seu cas, repercutint en una creixent insatisfacció de l'estudiantat. Per a poder resoldre aquest conjunt d'obstacles, és necessari que els agents d'acompanyament a l'estudiant treballin sobre la mateixa plataforma sobre la qual avui es disposa en les primeres fases del seu journey fins a completar totes les fases. En l'actualitat la UOC es concentra en les fases relacionades amb l'aprenentatge i, en concret, en els següents elements del model d'acompanyament de la UOC:

- Servei d'atenció.
- Servei de tutoria.
- Servei d'informació.

No obstant això, en un futur s'arribarà fins i tot a abastar al moment en que l'estudiant esdevé Alumni. Per tant, en l'actualitat es fa necessari complementar el parc de llicències de què es disposa per permetre desplegar sobre la mateixa plataforma els serveis indicats, donat que és la manera idònia de disposar d'una visió consolidada del journey de l'estudiantat al llarg de tota la seva relació amb la UOC.

La satisfacció de la necessitat descrita ha de passar necessàriament per la convocatòria de la present contractació derivada, per part de la UOC, així com d'una licitació mitjançant la qual s'adjudiqui el contracte relatiu al subministrament de les llicències Salesforce que es descriuen als plecs rectors de dita licitació.

I és que l'adquisició de totes les llicències requerides no pot fer-se exclusivament a través de l'Acord Marc d'homologació de proveïdors per al subministrament de llicències del programari Salesforce, de solucions especialitzades de backup i serveis associats per a les entitats que formen part del grup de compra, convocat pel Consorci de Serveis Universitaris de Catalunya (CSUC), amb número d'expedient 21/25, del qual la UOC és entitat adherida.

L'anunci de la licitació de l'acord marc esmentat es va publicar al perfil de contractant del CSUC en data 10 de desembre de 2021, el seu pressupost es va dimensionar fa tres anys i no contempla els volums necessaris per donar resposta a la necessitat que s'ha previst tenir en els propers anys si es té en compte el pressupost compromès per les diverses entitats contractants adherides mitjançant els contractes derivats adjudicats. Essent això així, i tenint en compte que és una necessitat recurrent a la institució, cal, addicionalment a la tramitació de la present contractació específica, convocar un procediment de licitació

obert per a l'adjudicació d'un contracte que tingui un pressupost adequat a les necessitats previstes per la Universitat i que permeti donar cobertura a la totalitat de les necessitats de la UOC.

Objectiu:

Atès l'objectiu anteriorment esmentat, en l'actualitat es fa necessari complementar el parc de llicències de què es disposa per permetre desplegar sobre la mateixa plataforma els serveis indicats, donat que és la manera idònia de disposar d'una visió consolidada del journey de l'estudiantat al llarg de tota la seva relació amb la UOC.

En concret, per a assolir aquest objectiu, es fa necessària l'adquisició de llicències salesforce. En concret, les llicències que previsiblement es requeriran durant la vigència del Contracte són les que s'indiquen a les taules de l'apartat B de la present fitxa de contractació basada.

Productes a subministrar: Els indicats a l'apartat B de la present fitxa de contractació basada.

Lloc de subministrament: El subministrament es presta de forma remota pel propi fabricant Salesforce sobre la seva infraestructura.

ANNEX 3
MESURES DE SEGURETAT PER PROVEÏDORS

En el cas: Es treballa total o parcialment en les instal.lacions del proveïdor però amb eines/infraestructures de la UOC. No s'envien emails en nom de la UOC

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?	NO
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?	Sí

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.

a) 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.

b) 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

c) 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.

d) 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.

e) 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

f) 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.

g) 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.

h) 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.

i) 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.

j) 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

k) 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.

l) 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

m) 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.

n) **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.

o) **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

p) **2.5.1. Control d'accés**

a) **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.

b) 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.

c) 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.

q) 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.

r) **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.

a) **2.5.3.1. Seguretat en l'ús del correu electrònic**

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

- Les direccions web (URL) incloses en els correus electrònics i els continguts dels mateixos han de ser supervisats prèviament pel departament de Prevenció Tecnològica del Frau.

- El departament de Prevenció Tecnològica del Frau ha de conèixer les Dades de la UOC que seran incloses en els correus. Aquestes no han de ser confidencials ni secretes, i aquest departament determinarà si han de ser emmascarades i de quina manera.

- La UOC ha de rebre:

    a. L'avís previ de l'enviament dels correus electrònics.

    b. Una breu explicació del contingut del correu electrònic.

    c. Un exemple del correu electrònic/SMS que rebran els clients.

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

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

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

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

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

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

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

s) **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.

t) 2.5.5. Gestió de les operacions

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

u) 2.5.6. Revisió

a) 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.

b) 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.

c) 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.

d) 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.

v) 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.

a) 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.

b) 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.

w) **2.5.8. Monitorització**

a) **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.

b) **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.

x) **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.