CSUC E22/18: Sistema Dinàmic d'Adquisició pel subministrament de programari i els serveis associats que l'acompanyen per a les Entitats que integren el grup de compra

Categoria 2: Subministrament de programari per la gestió de la infraestructura TIC, seguretat inform…

Contractació específica Fundació Universitat Oberta de Catalunya (UOC)

Títol: Subscripció llicències Nessus Pro.

A	OBJECTE DEL CONTRACTE ESPECÍFIC

Títol: Subscripció llicències Nessus Pro.

Número d'expedient: ESP33/CSUC2218/C2

Òrgan de contractació: Sr. Antoni Cahner Monzó, Gerent de la Fundació Universitat Oberta de Catalunya (UOC)

Codi CPV: 48000000 Paquets de software i sistemes d'informació.

Divisió en Lots:

☑ NO, atès que l'objecte del contracte està configurat com una única unitat funcional. Atenent el considerant 78 de la Directiva 2014/24/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, sobre contractació pública, i l'article 99 de la LCSP, el fet de dividir la licitació en lots podria comportar que l'execució del contracte esdevingui excessivament difícil i onerosa des d'un punt de vista tècnic.

Data aprovació: Data signatura Gerent UOC, com a Òrgan de contractació.

B	NECESSITATS A SATISFER I IDONEÏTAT DEL CONTRACTE ESPECÍFIC

Justificació de la Necessitat

La universitat gestiona una infraestructura tecnològica extensa i complexa que dona servei a milers d'estudiants, personal docent i investigador, i personal de gestió. Aquesta infraestructura emmagatzema i processa un volum considerable de dades sensibles, incloent-hi:

- **Dades Personals**: Informació identificativa i acadèmica d'estudiants i empleats.
- **Dades de Recerca**: Propietat intel·lectual i resultats d'investigacions, sovint de gran valor estratègic i econòmic.
- **Dades Administratives**: Informació financera, de recursos humans i de gestió operativa.

La manca d'un sistema d'auditoria de seguretat continu i automatitzat exposa la institució a riscos significatius:

- **Risc de Seguretat i Operatiu**: Les vulnerabilitats en sistemes operatius, aplicacions o configuracions de xarxa són la principal porta d'entrada per a ciberatacs. Un

incident de seguretat podria resultar en la interrupció de serveis crítics (campus virtual, correu electrònic, sistemes de gestió), afectant directament l'activitat docent, investigadora i administrativa.

- **Risc Legal i de Compliment**: El Reglament General de Protecció de Dades (GDPR) exigeix que la universitat implementi "mesures tècniques i organitzatives apropiades" per garantir la seguretat de les dades personals. La incapacitat de demostrar una diligència deguda en la gestió de vulnerabilitats ens exposa a sancions econòmiques severes i a un greu dany reputacional. Nessus ens permet generar l'evidència documentada de les auditories de seguretat que exigeix la normativa.
- **Risc Financer i Reputacional**: Una bretxa de seguretat comporta costos directes (recuperació de sistemes, notificacions legals) i indirectes (pèrdua de confiança per part d'alumnes, institucions col·laboradores i organismes finançadors).

Solució Adoptada

Nessus és l'estàndard de la indústria per a l'escaneig i la gestió de vulnerabilitats. La seva funció principal és identificar, classificar i reportar de manera sistemàtica les febleses de seguretat en tots els actius tecnològics de la universitat. A més a més, aquesta solució ja es troba actualment en funcionament a la Universitat.

La seva implementació ha permès a la UOC:

- **Automatitzar la detecció**: Realitzar auditories completes de la infraestructura de manera regular i automàtica, una tasca inviable de fer manualment a la nostra escala.
- **Prioritzar la resposta**: Els informes de Nessus classifiquen les vulnerabilitats segons la seva criticitat, permetent-nos enfocar els recursos tècnics en la resolució dels problemes més urgents i de major impacte.
- **Garantir la diligència deguda**: Disposar d'un registre auditable de les anàlisis de seguretat i les accions de remediació, fonamental per al compliment normatiu (GDPR).

Aquest contractació té com a objectiu la subscripció de llicències del programari NESSUS Pro del fabricant TENABLE Inc. Aquest programari està dins del catàleg electrònic del SDA 22/18, a la categoria 2.

Contracte subjecte a co-finançament:

☑ NO

C	VALOR ESTIMAT DEL CONTRACTE ESPECÍFIC

Valor estimat del Contracte específic: 4.800,00 €, IVA exclòs

Concepte	Total contracte específic (IVA exclòs)
Llicència Nessus Pro	4.800,00 €
TOTAL	**4.800,00 €**

Mètode aplicat per al seu càlcul: D'acord amb l'article 101 de la LCSP, aquest valor estimat inclou l'import del pressupost màxim (IVA exclòs) i l'import de les eventuals modificacions del contracte.

El valor estimat del contracte s'ha calculat partint de la seva durada màxima, dels preus unitaris previstos a l'Apartat E del present Quadre-resum. El càlcul s'ha efectuat de manera estimativa, no trobant-se la UOC obligada a contractar un determinat número de serveis objecte del contracte, sinó únicament aquells que consideri necessaris. Per aquest motiu, la UOC no es troba obligada a esgotar els imports indicats més amunt, que són imports màxims, i l'empresari seleccionat no tindrà dret a rebre una compensació o indemnització.

Per a calcular el Valor Estimat del Contracte específic:

☑ No s'ha inclòs cap import destinat a modificacions contractuals.

D PRESSUPOST BASE DE LICITACIÓ, PREUS I FACTURACIÓ

Pressupost base de licitació: 5.808,00 €, IVA inclòs

Concepte	Import durada inicial (IVA exclòs)	Import IVA (21%)	Import durada inicial (IVA inclòs)
Llicència Nessus Pro	4.800,00 €	1.008,00 €	5.808,00 €
TOTAL	**4.800,00 €**	**1.008,00 €**	**5.808,00 €**

Sistema de determinació del preu: Tant alçat.

Facturació:

Una sola factura en el moment de donar d'alta la subscripció.

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 en el termini de seixanta (60) dies, mitjançant una transferència bancària al número de compte que el contractista hagi indicat.

En qualsevol cas, cadascuna de les factures emeses contindrà la següent informació:

- Període de realització del servei que s'està facturant
- Identificació del nombre d'unitats en què es mesuri el producte (o prestacions) que seran objecte de facturació en el període esmentat.
- Imports incorreguts en desenvolupament de les tasques, hores o unitats en què es mesuri el producte (o prestacions) contractual, així com el seu desglossament en cas que existeixin diverses prestacions o que regeixin diversos tipus de preus unitaris.
- IVA correctament desglossat aplicable a cada base imposable.

- Codi de centre de responsabilitat i número de comanda. Aquesta informació serà indicada per la UOC.

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	DURADA DEL CONTRACTE ESPECÍFIC I PRÒRROGUES

Durada: un (1) any, comptats a partir de la data de signatura del contracte.

Possibilitat de pròrrogues: No

Durada màxima del Contracte específic, pròrrogues incloses: Un (1) any

F	TRAMITACIÓ DE L'EXPEDIENT I PROCEDIMENT D'ADJUDICACIÓ DEL CONTRACTE ESPECÍFIC

Forma de tramitació de l'expedient de contractació: Ordinària

Procediment d'adjudicació del contracte específic:

Procediment: Contractació específica Sistema Dinàmic d'Adquisició 22/18 CSUC.

Procediment inferior a 50.000,00 euros IVA excl.

Tramitació electrònica: SI

Inscripció al RELI: No obligatori per a participar en el procediment

Mesa de contractació: NO

En cas de fallida tècnica que impossibiliti l'ús de l'eina de Sobre Digital el darrer dia de presentació de les proposicions, l'Òrgan de contractació admetrà les proposicions presentades fora del termini sempre hi quan l'AOC hagi comunicat la incidència i la proposició hagi estat presentada dins d'un període de temps equivalent al comunicat per la pròpia AOC.

G	LICITADORS CONVIDATS A PARTICIPAR

Es convida a presentar oferta al licitador adherit a la categoria *Categoria 2: Subministrament de programari per la gestió de la infraestructura TIC, se…* **del Sistema Dinàmic d'Adquisició CSUC 22/18:**

- SERVICIOS MICROINFORMÁTICA, S.A.

Es convida a SERVICIOS MICROINFORMÁTICA, S.A en mèrits d'allò previst al Plec de Clàusules Particulars del procediment de referència, i en tant que aquesta empresa és l'única adherida per la contractació de llicències Nessus dins d'aquest Sistema Dinàmic d'Adquisició.

H	DATA MÀXIMA DE PRESENTACIÓ D'OFERTA I INSTRUCCIONS DE PRESENTACIÓ

DIA I HORA MÀXIM DE PRESENTACIÓ DE L'OFERTA:

La data que s'estableixi a l'anunci de licitació a la Plataforma de Contractes.

INSTRUCCIONS DE PRESENTACIÓ:

Enviament de l'oferta: a través del Sobre digital mitjançant enllaç a la publicació al perfil del contractant.

Formats de documents electrònics admissibles: Format .pdf o formats equivalents que admetin signatura electrònica incorporada.

I	CONTINGUT DEL SOBRE ÚNIC

☒Sobre únic, amb l'aportació de la següent documentació:

- Annex I. Model d'oferta econòmica i declaració responsable.

L'oferta econòmica que presenti el licitador convidat s'ha d'ajustar al model d'oferta que s'adjunta com a Annex I d'aquesta fitxa d'invitació.

En l'oferta econòmica s'entendran inclosos a tots els efectes els altres impostos (diferents de l'IVA), tributs, taxes i cànons de qualsevol índole que siguin d'aplicació, així com totes les despeses que s'originin per a l'adjudicatari, a conseqüència de l'acompliment de les obligacions previstes en la licitació específica.

Cada licitador només podrà presentar una oferta econòmica, no sent admeses les proposicions econòmiques per import superior al pressupost prèviament aprovat.

En cas de discordança entre la quantitat consignada en xifres i la consignada en lletres, prevaldrà la consignada en lletres.

No s'acceptaran aquelles proposicions que tinguin omissions o errors que impedeixin conèixer clarament tot allò que l'Òrgan de Contractació estimi fonamental per a l'oferta.

Tot el contingut d'aquest apartat és d'acord amb el Plec de Clàusules Particulars.

J	CRITERIS DE VALORACIÓ DEL SOBRE ÚNIC

En la present contractació específica NO es fixen criteris de valoració de l'oferta perquè només s'ha convidat a una empresa en mèrits del que disposa el *Plec de clàusules administratives per a la licitació del sistema dinàmic d'adquisició pel subministrament de programari i els serveis associats que l'acompanyen per les entitats que integren el grup de compra* "PCP".

K	OBERTURA DE PLIQUES

L'obertura dels sobres es durà a terme en sessió privada.

L	DOCUMENTACIÓ INFORMATIVA ADDICIONAL

La documentació informativa addicional que acompanya aquesta fitxa és la següent:

- Annex I. Model d'oferta econòmica i declaració responsable.
- Annex II. Condicions del subministrament i/o servei associat.
- Annex III. Mesures de seguretat

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 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.

Visita recomanada a les instal·lacions: NO

M	UNITAT ENCARREGADA DEL SEGUIMENT I EXECUCIÓ DEL CONTRACTE ESPECÍFIC I RESPONSABLE DEL CONTRACTE

Unitat encarregada del seguiment i execució del Contracte Específic:

Unitat d'Arquitectura i seguretat tecnològiques de l'Àrea de Tecnologia.

Responsable del Contracte Específic:

Jose Torre Adell, responsable de la unitat d'Arquitectura i seguretat tecnològiques de l'Àrea de Tecnologia.

N	CONDICIONS ESPECIALS DE COMPATIBILITAT

Han participat empreses en l'elaboració de les especificacions tècniques o dels documents preparatoris del Contracte Específic o dites empreses han assessorat a l'òrgan de contractació?

☑ NO

O	COMPROMÍS D'ADSCRIURE O DESTINAR A L'EXECUCIÓ DEL CONTRACTE ESPECÍFIC ELS MITJANS PERSONALS O MATERIALS SUFICIENTS

Compromís d'adscriure o destinar a l'execució del Contracte específic els mitjans personals o materials suficients.

☑ NO

P	CAUSES DE MODIFICACIÓ ADDICIONALS A LES PREVISTES A L'ARTICLE 205 DE LA LCSP

Causes de modificació contractuals:

☑ No es preveuen causes de modificació diferents a les previstes a l'article 205 de la LCSP.

Q	GARANTIA DEFINITIVA CONTRACTE ESPECÍFIC

Garantia definitiva contracte específic: NO

R	CRITERIS PER A DECLARAR QUE UNA OFERTA CONTÉ VALORS ANORMALS O DESPROPORCIONATS

Criteri per a declarar que una oferta conté valors anormals o desproporcionats

En convidar-se només a una sola empresa, no procedeix la fixació de criteris per a declarar que una oferta conté valors anormals o desproporcionats.

S	PREVENCIÓ DE RISCOS LABORALS I PROTECCIÓ DE DADES PERSONALS

Encarregat de tractament de dades de caràcter personal

El contractista és encarregat del tractament de dades LOPDGDD: NO

Comunicació de dades de caràcter personal

L'execució del contracte requereix la comunicació de dades per part de l'entitat contractant:

NO

L'execució del contracte requereix la comunicació de dades per part del contractista: NO

T	MECANISMES D'IMPUGNACIÓ

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

☑ Recurs d'alçada impropi en el termini màxim d'un (1) mes a comptar des del dia següent al de la notificació de l'acte que s'impugni, d'acord amb allò establerts als articles 44.6 i 47 de la LCSP i als articles 121 i 122 de la Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.

Signatura Adjudicatari	Signatura Òrgan de Contractació

ANNEX I

OFERTA ECONÒMICA (SOBRE ÚNIC)

El sotasignat _____, amb DNI _____, actuant en nom [indiqueu "propi" o la denominació de l'empresa a qui representa i el seu NIF], assabentat/ada de l'anunci publicat al *Perfil del contractant* de la UOC i de les condicions i requisits que s'exigeixen per a l'adjudicació del **contracte "**Subscripció llicències Nessus"**. (expedient número** ESP30/CSUC2218/C2**)**, faig constar que:

- DECLARA sota la seva responsabilitat, que concorren en l'empresa ..... els mateixos requisits de capacitat i aptitud per contractar que van servir per a l'adhesió al Sistema Dinàmic d'Adquisició pel subministrament de programari i els serveis associats que l'acompanyen per a les Entitats que integren el grup de compra (exp. CSUC 22/18).

- Es compromet (en nom propi o de l'empresa que representa) a executar-lo amb estricta subjecció als requisits i condicions esmentats, d'acord amb el preu global i els preus unitaris (segons que correspongui) següents:

Oferta econòmica	**Preu màxim (IVA exclòs)**	**Import IVA**	**Preu ofertat (IVA inclòs)**
Llicència Nessus Pro	€	€	€

_____, a ____ de _____ de 20___.

Signatura:

(S'ha de fer oferta per a tots i cadascun dels preus que s'indiquen en l'Apartat D del Quadre de Característiques. Queden automàticament excloses del procediment de licitació les ofertes que presentin qualsevol valor superior al pressupost base de licitació —o, si n'hi ha, als preus unitaris màxims— indicats en l'Apartat D del Quadre de Característiques)

ANNEX II

CONDICIONS DEL SUBMINISTRAMENT

L'adjudicatari estarà obligat a subministrar les llicències del programari objecte d'aquest contracte en un màxim de 7 dies naturals des de la data de signatura del contracte.

Les condicions del servei de manteniment de les llicències són les estàndards que apareixen al següent enllaç de la web oficial del fabricant Tenable Inc.:
https://static.tenable.com/prod_docs/tenable_slas.html.

ANNEX III MESURES DE SEGURETAT

1. Introducció

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)?	NO
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 dóna 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.

2.5.5.4. 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.