

PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

1. Objecte del contracte

El present document té per objecte establir les prescripcions tècniques que han de regir la licitació per a la contractació del servei de subscripció, posada en funcionament, manteniment i suport integral en modalitat núvol (cloud) de la plataforma NEXT, incloent-hi l'accés a les seves aplicacions associades, en particular el sistema de comptabilitat CGAP.

La plataforma NEXT forma part de les solucions tecnològiques de l'empresa BL España Software SLU (Berger-Levrault), configurant-se com una solució informàtica específica per a la gestió econòmica i financera en l'àmbit de l'administració pública.

El servei es presta en modalitat SaaS (Software as a Service), i inclou, a més de les corresponents llicències d'ús per als usuaris, la gestió integral de la infraestructura tecnològica, el manteniment del sistema, les actualitzacions, el suport tècnic i la resta de serveis necessaris per garantir el correcte funcionament, disponibilitat i seguretat de la plataforma durant tota la vigència del contracte.

2. Abast funcional i dimensionament d'usuaris

Durant el període de vigència del contracte, l'entitat comptarà una llicència per als següents usuaris.

Cgap +, 5 usuaris nominals.

3. Activació i Configuració al Núvol

3.1. Informació Preliminar

Les solucions al núvol s'ofereixen en un model SaaS (Software as a Service), la qual cosa permet el seu accés des d'un entorn web o mitjançant un programari client, segons l'acordat amb l'entitat. Aquest model garanteix una gestió integral en la qual BL España Software SLU assumeix les següents responsabilitats, eliminant la necessitat que l'entitat inverteixi recursos en Manteniment de la infraestructura que suporten les aplicacions.

- Manteniment de la infraestructura que suporta les solucions.
- Monitoratge i optimització del rendiment dels entorns tecnològics.
- Gestió i aprovisionament de servidors físics i virtuals.
- Subministrament i manteniment de llicències de programari associades, com Microsoft Windows Server, Microsoft RDS CAL, SQL Server, Oracle o Microsoft Office 365 (opcional).
- Manteniment dels centres de dades, incloent-hi mesures de seguretat física i energètica.
- Administració de bases de dades, amb actualitzacions, còpies de seguretat i restauracions.
- Aplicació de pegats de seguretat en sistemes operatius i infraestructura tecnològica.
- Implementació de seguretat perimetral, amb protecció enfront d'atacs DDoS i detecció d'intrusions.
- Gestió de còpies de seguretat per a bases de dades, sistemes operatius i solucions contractades.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

- Aprovisionament de programari addicional per a assistència remota (opció disponible si s'acorda amb l'entitat).
- Desplegament de millores i actualitzacions de les solucions al núvol.

3.2. Característiques del Cloud

3.2.1. Ubicació del Centre de Processament de Dades

La infraestructura i plataformes tecnològiques necessàries per a la prestació del servei estaran allotjades a la Regió Espanya d'AWS, distribuïdes entre els seus tres centres de dades, tots ells dins de la Península Ibèrica. A més, els sistemes de còpia de seguretat que contenen dades s'externalitzaran a altres regions dins de la Unió Europea, essent la Regió d'Irlanda d'AWS la ubicació per defecte per a aquesta redundància.

3.2.2. Exclusivitat i dedicació de recursos

Tota la infraestructura virtual estarà dedicada exclusivament a l'execució d'aplicacions comercialitzades per Berger-Levrault. Les bases de dades seran dedicades, garantint que cap altra entitat ni organisme hi tindrà accés compartit, reforçant així la seguretat i confidencialitat de la informació.

3.2.3. Plataforma Tecnològica i Seguretat

La plataforma tecnològica es desplegarà en alta disponibilitat, garantint continuïtat operativa davant incidències. Inclourà un nucli comú que incorporarà funcionalitats d'Autenticació, Autorització i Auditoria, permetent el compliment dels requisits establerts per la LOPDGDD en matèria de protecció de dades. S'integraran controls d'accés i mecanismes d'autenticació, així com eines de monitoratge, registre d'activitat, bloqueig de sessions i control de qualitat del codi font en compliment de l'Esquema Nacional de Seguretat.

El sistema assegurarà un rendiment eficient i estable, optimitzant l'ús de recursos per garantir una experiència d'usuari adequada. S'estableix el compromís que totes les transaccions s'executaran en temps compatibles amb una correcta usabilitat, excloent-se de l'esmentada mesura els retards atribuïbles a serveis externs al sistema.

3.2.4. Mesures de Seguretat

La implementació de mesures de seguretat resulta essencial per garantir la integritat, confidencialitat i disponibilitat de les dades, així com per prevenir accessos no autoritzats i assegurar la recuperació de la informació davant de possibles incidents. Per a això, s'aplicaran les mesures tècniques i organitzatives necessàries, en funció de l'estat de la tecnologia, la sensibilitat de les dades tractades i els riscos als quals puguin estar exposats, ja siguin derivats d'accions humanes o de causes físiques o naturals. Aquestes mesures tenen com a objectiu evitar l'alteració, pèrdua, accés o tractament no autoritzat de les dades, i s'alinearan amb els estàndards internacionals aplicables, com la ISO/IEC 27001 i l'Esquema Nacional de Seguretat (ENS), garantint així un enfocament integral i conforme a les millors pràctiques de seguretat.

Berger-Levrault presta els serveis de manera segura per a la qual cosa disposa de mesures de seguretat conforme al Reial decret 311/2022.

3.2.4.1. Mesures de Seguretat Física



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

Disseny segur

- Selecció d'emplaçaments

Els emplaçaments dels centres de dades s'elegeixen amb summa cura per mitigar els riscos mediambientals, com inundacions, condicions climàtiques extremes i activitat sísmica. Les zones de disponibilitat estan construïdes de manera que siguin independents i estiguin físicament separades entre si.

- Redundància

Els centres de dades estan dissenyats per preveure i tolerar errors mentre es mantenen els nivells de servei. En cas d'error, els processos automatitzats desvien el trànsit de la zona afectada. Les aplicacions principals s'implementen en un estàndard N + 1, de manera que en cas que es produeixi un error en un centre de dades, hi hagi capacitat suficient per poder equilibrar la càrrega del trànsit entre els altres llocs.

- Disponibilitat

Cada zona de disponibilitat s'ha dissenyat perquè funcioni de forma independent amb una alta fiabilitat. Les zones de disponibilitat estan connectades, la qual cosa li permet dissenyar aplicacions amb facilitat que commutin per error entre les zones de disponibilitat sense interrupcions. Els sistemes d'alta resistència i, per tant, la disponibilitat dels serveis, són una funció del disseny del sistema.

- Planificació de capacitat

AWS monitora en tot moment l'ús dels serveis per implementar infraestructura per tal de donar suport als nostres compromisos i requisits de disponibilitat.

Continuïtat del negoci i recuperació de desastres

- Pla de continuïtat del negoci

El pla de continuïtat del negoci d'AWS descriu les mesures que s'han d'implementar per evitar i reduir les interrupcions mediambientals. Inclou detalls operatius sobre els passos que s'han de realitzar abans, durant i després d'un succés. El pla de continuïtat del negoci està recolzat per proves que inclouen simulacions de diferents situacions.

Accés físic

- Accés dels empleats al centre de dades

AWS proporciona accés físic al centre de dades només als empleats autoritzats. Tots els empleats que necessitin tenir accés al centre de dades primer han de demanar l'accés i proporcionar una justificació empresarial vàlida. Aquestes sol·licituds es concedeixen en funció del principi de privilegis mínims.

- Accés de tercers al centre de dades

L'accés de tercers el sol·liciten empleats d'AWS autoritzats, que han d'omplir una sol·licitud d'accés de tercers i proporcionar una justificació empresarial vàlida. Aquestes sol·licituds es concedeixen en funció del principi de privilegis mínims.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

Monitoratge i registre

- Registres d'accés als centres de dades
L'accés físic als centres de dades d'AWS es registra, es monitoritza i es manté.
- Monitoratge de l'accés als centres de dades
Monitoritzem els centres de dades mitjançant centres globals d'operacions de seguretat, que són responsables de monitoritzar, provar i executar programes de seguretat.

Vigilància i detecció

- CCTV
Els punts d'accés físic a les sales de servidors es graven amb càmeres de televisió de circuit tancat (CCTV). Les imatges es conserven d'acord amb els requisits legals i de conformitat.
- Punts d'entrada al centre de dades
L'accés físic està controlat en els punts d'accés de l'edifici per personal de seguretat professional mitjançant videovigilància, sistemes de detecció d'intrusions i altres recursos electrònics.
- Detecció d'intrusions
S'han instal·lat sistemes de detecció d'intrusions electrònics a la capa de dades per monitorar, detectar i alertar automàticament el personal sobre els incidents de seguretat.

Administració de dispositius

- Administració de recursos
Els actius d'AWS s'administren centralment a través d'un sistema d'administració de l'inventari que emmagatzema i realitza un seguiment del propietari, la ubicació, l'estat, el manteniment i informació descriptiva dels recursos propietat d'AWS.
- Reordenació de contingut multimèdia
AWS classifica com a Crítics els dispositius d'emmagatzematge de contingut multimèdia usats per emmagatzemar les dades dels clients i, per això, les tracta com d'alt impacte al llarg del seu cicle de vida. AWS té normes estrictes sobre com instal·lar, mantenir i, finalment, destruir els dispositius quan ja no són útils. Quan un dispositiu d'emmagatzematge arriba al final de la seva vida útil, AWS el dona de baixa mitjançant les tècniques detallades en NIST 800-88. Els mitjans que emmagatzemaven dades dels clients continuen estant sota el control d'AWS fins que es donen de baixa de forma segura.

Sistemes d'ajuda a les operacions

- Energia
Els sistemes de subministrament elèctric dels nostres centres de dades estan dissenyats perquè puguin duplicar-se i mantenir-se per complet sense que això repercuteixi en les operacions, 24 hores al dia. AWS garanteix que els centres de dades estiguin equipats amb sistemes de subministrament elèctric de reserva per garantir el subministrament a les operacions en casos de talls elèctrics per cobrir les càrregues més importants i essencials de la instal·lació.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

- Condicions climàtiques i temperatura

Els centres de dades d'AWS fan servir mecanismes per controlar les condicions climàtiques i mantenir una temperatura de funcionament constant per als servidors i un altre maquinari i, així, impedir el sobreescalfament i reduir la possibilitat que es produeixin interrupcions del servei

- Detecció i extinció d'incendis

Els centres de dades d'AWS estan equipats amb sistemes de detecció i d'extinció d'incendis. Els sistemes de detecció d'incendis utilitzen sensors de detecció de fum en els espais de xarxes, mecànics i d'infraestructura.

- Detecció de fuites

Per detectar la presència de fuites d'aigua, AWS equipa els centres de dades amb funcionalitat per detectar la presència d'aigua.

3.2.4.2. Mesures de Seguretat Lògica

El servei NEXT incorpora els controls de seguretat lògica que garanteixen la seguretat de les dades emmagatzemades i proporcionen un accés segur i controlat a les aplicacions publicades.

Cloudfront

La publicació de les aplicacions NEXT es realitza mitjançant el servei AWS Cloudfront. Cloudfront és un servei de xarxa de distribució de contingut (CDN) d'AWS que entrega dades i aplicacions a usuaris de manera ràpida i segura mitjançant una xarxa global d'ubicacions perimetrals. Pel que fa a seguretat, Cloudfront ofereix múltiples capes de protecció integrades, incloent xifrat d'extrem a extrem (TLS), compatibilitat amb AWS WAF per definir regles personalitzades de firewall. A més, permet restringir l'accés al contingut mitjançant firmes i tokens, així com usar polítiques de control d'accés basades en identitat. Tot això permet protegir tant el contingut com la infraestructura backend contra accessos no autoritzats i amenaces comunes a la xarxa

WAF (Tallafocs d'aplicacions web)

AWS WAF (Web Application Firewall), s'integra a Cloudfront i està configurat en totes les distribucions de les aplicacions NEXT. WAF és un servei de firewall d'aplicacions web que protegeix les aplicacions web i APIs enfront d'amenaces comunes com injeccions SQL, scripts entre llocs (XSS) i altres atacs a la capa 7. Funciona mitjançant l'ús de regles personalitzables que permeten inspeccionar i filtrar el trànsit HTTP i HTTPS en funció de condicions com adreces IP, encapçalats, URI, cadenes de consulta i més. AWS WAF s'integra fàcilment amb serveis com Amazon Cloudfront, Application Load Balancer i API Gateway, proporcionant una defensa escalable i en temps real sense afectar el rendiment. A més, permet automatitzar respostes a patrons d'atac mitjançant regles gestionades o personalitzades, la qual cosa millora significativament la postura de seguretat de les aplicacions desplegades en AWS.

Antivirus (EDR i EPP)

Tots els servidors que conformen la plataforma NEXT incorporen un antivirus que combina protecció EDR i EPP en un únic agent lleuger per a endpoints, oferint una defensa avançada i automatitzada.

El mòdul EDR proporciona detecció i resposta en temps real davant amenaces com ransomware i moviments laterals, utilitzant intel·ligència artificial, anàlisi de comportament i automatització SOAR sense necessitat de codi.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

El mòdul EPP, per la seva banda, actua com un antivirus de nova generació que combina anàlisis per firmes, heurística i protecció contra phishing, malware i ransomware.

Junts, ofereixen una solució sòlida, certificada i adaptada a entorns exigents, complint estàndards com l'Esquema Nacional Seguretat i garantint una protecció contínua i eficaç

Accés segur als servidors

L'accés als servidors es realitza de forma segura mitjançant la funcionalitat Sessions Manager d'AWS Systems Manager, L'accés segur amb AWS Systems Manager, que permet connectar-se als servidors sense usar claus SSH ni obrir ports com el 22 o 3389, la qual cosa redueix la superfície d'atac. Les sessions s'estableixen a través de l'agent SSM usant HTTPS, i es poden auditar completament amb registres a CloudTrail, S3 o CloudWatch Logs. El control d'accés es gestiona amb IAM, la qual cosa permet definir qui pot accedir i amb quins permisos. A més, tot el trànsit està xifrat d'extrem a extrem i és compatible amb instàncies Linux i Windows.

Parxís de sistemes

Els sistemes operatius que conformen la plataforma NEXT estan actualitzats segons les recomanacions del fabricant. La gestió de pegats es realitza mitjançant AWS Patch Manager que automatitza el procés d'aplicar la seguretat i actualitzacions. Permet mantenir els sistemes actualitzats sense intervenció manual, reduint el risc de vulnerabilitats.

Patch Manager permet garantir que els sistemes es mantenen protegits davant vulnerabilitats conegudes.

Les actualitzacions s'instal·len en entorns controlats de validació i un cop certificats s'instal·len als entorns de Producció.

Monitoratge

El monitoratge en sistemes aporta visibilitat, control i capacitat de reacció davant el comportament dels recursos de TI. Permet supervisar en temps real l'estat, rendiment i disponibilitat de servidors, aplicacions, xarxes i serveis, detectant fallades o anomalies abans que afectin l'usuari final.

Els seus principals beneficis inclouen:

- Detecció primerenca de problemes: permet anticipar-se a errors, caigudes o sobrecàrregues.
- Optimització del rendiment: identifica colls d'ampolla o ús ineficient de recursos.
- Seguretat: ajuda a detectar comportaments inusuals que podrien indicar incidents de seguretat.
- Compliment i auditoria: registra esdeveniments clau i facilita el seguiment per a normatives i estàndards.
- Presa de decisions informada: proporciona dades concretes per planificar capacitats, actualitzacions o inversions.

La plataforma NEXT està controlada per una solució integral de monitoratge disponible en tot moment (24x7x365). Aquest sistema de control serà operat per un equip dedicat i especialista en el monitoratge de les aplicacions Berger-Levrault.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

Adicionalment, un equip especialista en infraestructures cloud, monitoritzarà contínuament la infraestructura per garantir el bon funcionament per si el potencial origen d'una incidència estigués relacionat amb components del Sistema i no amb els aplicatius.

La solució integral està basada en Zabbix, Prometheus, AWS CloudWatch, AWS Cloud Trail, una solució SIEM, PowerAutomate, i WAF. L'eina principal (Zabbix) actualment està monitoritzant més de 500 paràmetres per segon, i implementa més de 50 mètriques de monitoratge per a cadascun dels servidors.

A continuació, es mostren algunes de les mètriques monitoritzades de cadascun dels servidors:

- **Rendiment i ús de CPU:** Ús de CPU, temps d'usuari, privilegiat, interrupcions, DPC, cues.
- **Memòria:** Memòria lliure, total i usada, espai en PSARU, fallades de pàgina, pàgines per segon, ús de memòria, bytes en caixet
- **Xarxa:** Adreces IP, interfícies de xarxa.
- **Sistema Operatiu i Recursos del Sistema:** Nom de host, uptime, descripció del sistema, arquitectura, nombre de processos, nombre de fils.
- **Emmagatzematge:** Espai lliure i usat en Yarp, memòria de sistema, arxius del sistema.
- **RDS (Remote Desktop Services):** Sessions actives, inactives, i totals de RDS.
- **Disponibilitat i Salut:** Disponibilitat de l'agent, ping del servidor i latència

Còpies de Seguretat

La política de Backup de les dades emmagatzemades en NEXT s'estableix segons la criticitat del recurs i les dades emmagatzemades.

- **Backup complet dels últims 7 dies:** S'aplica a Servidors d'Aplicacions que no contenen dades tan sols binaris de les aplicacions i són fàcilment recreables des d'una plantilla.
- **Backup complet dels últims 14 dies més una foto setmanal amb rotació de 4 setmanes:** Servidors d'infraestructura que contenen configuració, però no contenen dades
- **Backup complet dels últims 14 dies més una foto setmanal amb rotació de 54 setmanes (1 any):** Servidors i repositoris que contenen dades. S'externalitzen diàriament a una segona regió geogràfica (Irlanda) amb una retenció de 14 dies en aquesta segona regió.

Adicionalment, per a les bases de dades, es realitza una còpia mitjançant un pla de manteniment de SQL Server cap a un Bucket S3 la política del qual és la següent:

- Backup Full Semanal
- Backup Diferencial Diari
- Backup del Log de Transaccions cada 10 minuts
- Retenció 15 dies en disc
- Retenció de 14 dies i 52 setmanes en còpia de seguretat en repositori de còpia.

El RTO (Recovery Time Objective) compromès serà de 2 hores, mentre que el RPO (Recovery Point Objective) serà d'1 hora.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

Requeriments de connectivitat

La connexió a les aplicacions NEXT està optimitzada per usar el mínim ample de banda necessari mitjançant la compressió de dades i optimització del trànsit.

L'ample de banda necessari per connexió varia segons el tipus d'activitat de l'usuari i la configuració de l'entorn.

A continuació, es detallen estimacions basades en el consum d'un usuari segons el tipus d'activitat que realitzi en les aplicacions NEXT.

Activitat de l'Usuari	Ample de Banda Aproximat
Sessió inactiva	~0.3 Kbps
Ús d'aplicacions d'Escriptori	100–150 Kbps
Ús d'Aplicacions Web amb intercanvi de documents	6–6.5 Mbps

Nombre d'Usuaris per connexió	Ample de banda recomanat
1 – 10 Usuari	10 Mbps
10 – 30 Usuaris	30 Mbps
30 – 50 Usuaris	50 Mbps
50 - 100 Usuaris	100 Mbps
+ 100 Usuaris	150 Mbps

Amb l'objectiu de reforçar la seguretat i reduir el risc de patir un ciberatac, l'accés a les aplicacions NEXT es limitarà exclusivament a adreces IP ubicades en territori espanyol. Per accedir des de l'estranger, caldrà establir una connexió VPN amb la infraestructura on-premise del client ubicat a Espanya, assegurant que tot el trànsit es redirigeixi a través del túnel VPN perquè l'accés a NEXT es realitzi amb una IP declarada a Espanya. La provisió, manteniment i configuració d'aquesta VPN no forma part d'aquesta proposta.

4. Continuïtat del servei

4.1. Pla de Recuperació davant Desastres Berger-Levrault

Berger-Levrault garanteix la continuïtat del servei davant una caiguda crítica del sistema mitjançant el seu Pla de Recuperació davant Desastres. Aquest pla contempla diversos escenaris avaluats i el seu objectiu és el de garantir la continuïtat operativa del servei NEXT en cas d'un incident greu que afecti la seva infraestructura tecnològica o els seus serveis crítics. Això inclou esdeveniments com fallades de maquinari, ciberatacs, desastres naturals, errors humans o altres esdeveniments imprevistos.

- Minimitzar el temps d'inactivitat (downtime).
- Recuperar sistemes, dades i serveis essencials el més ràpid possible.
- Reduir la pèrdua de dades mitjançant còpies de seguretat i rèpliques.
- Protegir la integritat i confidencialitat de la informació.
- Mantenir la continuïtat del negoci mentre es restauren els serveis.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

- Assignar rols i responsabilitats clares en situacions de crisi.
- Complir amb normatives legals o contractuals sobre continuïtat del negoci.

El RTO (Recovery Time Objective) compromès en els escenaris avaluats serà de 2 hores, mentre que el RPO (Recovery Point Objective) serà d'1 hora.

Berger-Levrault es compromet a realitzar una prova anual del pla per comprovar la seva funcionalitat. Un cop completada la prova, Berger-Levrault proporcionarà al CLIENT una evidència de l'execució de les proves de continuïtat i contingència.

4.2. Pla de Recuperació davant Desastres Amazon Web Services

AWS garanteix la continuïtat dels seus serveis mitjançant un sòlid Pla de Recuperació davant Desastres (DRP) integrat en el disseny de la seva infraestructura global. La seva arquitectura està distribuïda en múltiples regions i zones de disponibilitat físicament independents, la qual cosa permet aïllar fallades i mantenir la disponibilitat del servei fins i tot davant d'esdeveniments crítics.

La plataforma incorpora mecanismes automatitzats de detecció, commutació i recuperació, així com replicació de dades i proves regulars de resiliència. A més, tots els serveis clau han estat dissenyats per tolerar fallades, amb objectius de disponibilitat i durabilitat molt alts. Gràcies a aquesta estratègia, AWS assegura una infraestructura resilient que sustenta la continuïtat operativa fins i tot davant incidents a gran escala.

Adicionalment, AWS incorpora polítiques i procediments de resposta pandèmica en la seva planificació de recuperació de desastres per tal de preparar-se per respondre ràpidament a amenaces de brots de malalties infeccioses. Entre les estratègies de mitigació s'inclouen models de contractació de personal alternatiu per transferir els processos crítics a recursos fora de la regió i l'activació d'un pla d'administració de crisi per donar suport a les operacions empresarials crítiques. Els plans pandèmics estan lligats a agències i normatives sanitàries internacionals, inclosos punts de contacte per a les agències internacionals.

5. Protecció de Dades i Confidencialitat

5.1. RGDP

En compliment del Reglament (UE) 2016/679, de 27 d'abril (RGPD), i de la Llei Orgànica 3/2018, de 5 de desembre (LOPDGDD), l'entitat disposa d'un Sistema de Gestió de Protecció de Dades auditat per una entitat independent, que garanteix l'adequat compliment dels requisits legals vigents. En aquest marc, s'han desenvolupat accions de revisió i auditoria orientades a verificar el compliment íntegre de les obligacions aplicables, incloent-hi l'avaluació periòdica de les mesures tècniques i organitzatives implantades, la revisió del Registre d'Activitats de Tractament, la comprovació de la correcta gestió de consentiments i bases jurídiques, la supervisió dels procediments de resposta davant incidents de seguretat i la verificació dels acords formalitzats amb encarregats del tractament. Així mateix, el Sistema contempla l'adequada gestió i atenció dels drets dels interessats —accés, rectificació, supressió, oposició, limitació, portabilitat i altres drets reconeguts— garantint la seva tramitació en els terminis i condicions previstos per la normativa. Tot això permet assegurar un marc de compliment sòlid,



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

actualitzat i alineat amb els principis de responsabilitat proactiva i millora contínua establerts per la normativa vigent.

5.2. Confidencialitat

Berger-Levrault estarà obligat a mantenir la plena confidencialitat i secret, pel que fa a la informació manejada durant l'execució del contracte. Aquesta obligació tindrà una durada de 5 anys des del coneixement d'aquesta informació, llevat que en el present plec o en el contracte corresponent, es determini un termini major.

Berger-Levrault tractarà amb la màxima reserva tots i cadascun dels aspectes de la informació implicada, no podent comunicar-los o cedir-los a tercers llevat que aquest prèviament autoritzat per CLIENT.

Totes les persones que intervinguin en qualsevol fase del procés de contractació estaran subjectes al deure de confidencialitat a què es refereix l'article 5.1.f) del Reglament (UE) 2016/679.

Berger-Levrault disposa d'acords amb tots els proveïdors implicats, i específicament manté encàrrecs i contractes de confidencialitat, i exigeix que els seus usuaris amb accés a les dades, formalitzi contractes de confidencialitat, els quals són requerits i revisats.

Tots els processos associats a l'obligació de confidencialitat són revisats, en base al procés de verificació de mesures de seguretat de l'Esquema Nacional de Seguretat – Reial Decret 311/2022.

Berger-Levrault no copiarà, ni reproduirà, ni comunicarà o exhibirà, cap element, informació, document i anàlegs, que li hagi estat lliurats per a la prestació o que hagués de generar per a l'execució del servei.

A tots els efectes queden sotmeses a confidencialitat, les dades personals de les quals és responsable CLIENT i tota la informació institucional i de caràcter intern i organitzatiu, no sotmesa a publicitat activitat, es vegi implicada.

S'exceptua qualsevol submissió al deure de secret o confidencialitat o reserva, a aquella informació afectada per la Llei 19/2013, llevat que, de la mateixa, i específicament pel contingut en l'Art. 14 i Art 15, es determini un límit a la seva necessària transparència –en les seves dues modalitats; accés o publicitat activa-.

El compromís de confidencialitat s'estén a CLIENT i els seus usuaris respecte a la informació confidencial, associada a la plataforma i saber fer de Berger-Levrault.

Les parts declaren a tots els efectes, el caràcter confidencial d'aquella informació a la qual tinguin accés en ocasió de l'execució del contracte, que se li hagués donat el referit caràcter en els plecs o en el contracte, o que per la seva pròpia naturalesa hagi de ser tractada com a tal. S' inclou expressament tota la informació associada a mesures de seguretat i de protecció, configuracions desenvolupades, proteccions del servei i aplicacions, elements i descripcions d'infraestructura i arquitectura, processos d'autenticació i protocols de seguretat, comunicacions, incidències, informes de tercers, controls de capacitat i avaluacions de les



PLEC PRESCRIPCIONS TÈCNiques DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

disponibilitats implicades, anàlisis automàtiques, xarxes i proteccions del perímetre, elements adscrits a la continuïtat, registres d'activitat i proteccions associades, protocols de còpies i restauracions, elements de manteniment i garanties implicades, i quants altres elements puguin considerar-se un risc als efectes del servei contractat o la informació vinculada al mateix.

6. Garantia d'accés a la informació

Quan CLIENT ho requereixi, Berger-Levrault quedarà obligat a garantir l'exercici dels drets d'accés per part dels ciutadans o empreses, mitjançant l'ús de formats estandarditzats de dades que compleixin els requisits establerts a l'Esquema Nacional d'Interoperabilitat:

- Els documents i serveis d'administració electrònica que es posin a disposició dels ciutadans o d'altres administracions públiques han de ser visualitzables, accessibles i funcionalment operables en condicions que permetin satisfer el principi de neutralitat tecnològica i evitin la discriminació als ciutadans o empreses per raó de la seva elecció Tecnològica
- S'adoptaran les mesures organitzatives i tècniques necessàries per tal de garantir la interoperabilitat en relació amb la recuperació i conservació dels documents electrònics al llarg del seu cicle de vida.
- Els documents electrònics es conservaran en el format en què hagin estat elaborats, tramesos o rebuts, i preferentment en un format corresponent a un estàndard obert que preservi al llarg del temps la integritat del contingut dels documents, de la signatura electrònica i de les metadades que l'acompanyen. Així mateix, Berger-Levrault garantirà la capacitat d'integració del sistema objecte del present contracte sobre aquells altres sistemes de gestió i producció administrativa amb els quals el CLIENT pugui operar, com ara la seu electrònica o el Gestor Documental, per a la qual cosa tindrà en consideració els webservices (propis i aliens) que permetin aquesta integració de forma coherent, senzilla i transparent, garantint aquesta integració.

7. Portabilitat de la informació. Reversió del sistema

Berger-Levrault disposa d'una política alineada amb l'Esquema Nacional de Seguretat i la normativa vigent en matèria de protecció de dades, que regula la devolució, transferència i/o eliminació de la informació gestionada en els seus sistemes.

Les dades emmagatzemades a la plataforma Next són i continuaran sent en tot moment propietat exclusiva del CLIENT. En el moment de la resolució del contracte o finalització del Servei, Berger-Levrault lliurarà al CLIENT, o a la persona o entitat que aquest designi, la totalitat de les dades, juntament amb la informació tècnica i de configuració del Sistema, en un format exportable i estructurat, que permeti al CLIENT la seva conservació en els seus propis sistemes o, si s'escau, la migració a un nou proveïdor sense pèrdua d'informació.

Berger-Levrault garantirà que la transferència de les dades i el control del Sistema es realitzin en un termini màxim d'un mes des de la sol·licitud del CLIENT. El cost d'aquests serveis no està inclòs en l'abast econòmic actual del present plec i, en cas de ser requerit, serà objecte de contractació específica posterior conforme als termes establerts en la memòria corresponent.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

Així mateix, el CLIENT es reserva el dret a exigir la transferència dels serveis a un nou proveïdor quan consideri que la prestació no compleix els nivells de servei (SLA) o condicions funcionals i operatives acordades, basant-se en els informes o incidències comunicades durant l'execució del Servei.

8. Gestió i Optimització dels Serveis

La subscripció inclou una sèrie de serveis mensuals dissenyats per garantir l'estabilitat i l'òptim rendiment de les solucions al núvol:

- **Gestió de còpies de seguretat**, seguint el Pla de Backup establert.
- **Supervisió contínua de servidors (24/7)**, amb un sistema d'alertes en cas d'incidències o degradació del servei.
- Actualització de versions dels nostres productes.
- **Ajust dinàmic d'infraestructura**, permetent ampliacions o reduccions segons les necessitats de l'entitat.
- **Anàlisi preventiu**, amb revisió de registres (logs) per optimitzar el rendiment.
- **Auditories semestrals** per avaluar i millorar l'acompliment de les solucions.
- **Plans de contingència**, dissenyats per activar-se en cas d'incidències greus.
- **Restauració de còpies de seguretat**, disponible sota sol·licitud de l'entitat.

8.1. Serveis d'activació i onboarding

L'activació de mòduls i l'onboarding al núvol està dissenyat per ser un procés àgil i sense friccions per als usuaris. Com a part d'aquesta transició, es durà a terme:

- **Unificació d'administradors**, assegurant una gestió centralitzada.
- Actualització a l'última versió disponible dels productes.
- **Migració de dades**, incloent-hi l'exportació de bases de dades i la seva transformació per adaptar-les a l'entorn al núvol.

A més, els usuaris finals podran accedir anticipadament per realitzar proves abans de la posada en producció, garantint una transició sense interrupcions.

No es requereix formació específica per als mòduls ja en funcionament, ja que les solucions mantenen la mateixa experiència d'ús que en versions anteriors.

8.2. Serveis no inclosos

Aquesta oferta no contempla els serveis següents:

- Adquisició de llicències Microsoft Office 365.
- Client VPN o línies punt a punt
- Entorns de proves, que s'hauran de contractar de forma addicional si l'entitat els necessita

◇ Nota: En cas que l'entitat requereixi algun d'aquests serveis caldrà realitzar una valoració personalitzada i seran objecte de proposta econòmica addicional.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

8.3. Actualització Contínua i Compliment Normatiu

La subscripció al núvol garanteix que la plataforma estigui sempre actualitzada i en òptimes condicions de funcionament, sense necessitat d'intervenció per part de l'entitat.

Funcional: La plataforma s'actualitza de forma contínua i automàtica per millorar el seu rendiment, eficiència i usabilitat. Aquestes millores s'implementen directament en l'entorn de producció de manera transparent, assegurant sempre l'accés a la versió més avançada de la solució.

Legal: Davant de qualsevol canvi en normatives d'obligat compliment, la plataforma s'adapta de forma automàtica, garantint que sempre estigui alineada amb la legislació vigent sense requerir instal·lacions addicionals ni intervencions manuals.

Correctiu: Qualsevol incidència o error detectat es corregeix amb prioritat segons el seu impacte. Gràcies a l'arquitectura al núvol, les correccions s'apliquen de forma remota, minimitzant l'impacte en el servei i assegurant la seva disponibilitat constant.

8.4. Optimització i Supervisió Constant

Es realitzen revisions contínues per detectar i corregir possibles inconsistències en les dades, ja siguin fallades en el funcionament dels mòduls del producte o errors derivats de la migració de dades al núvol.

Aquest procés és completament automatitzat, la qual cosa permet una supervisió proactiva sense afectar l'operativitat del sistema. D'aquesta manera, es garanteix un servei sempre optimitzat i lliure d'interrupcions.

8.5. Serveis no inclosos

Els serveis següents queden exclosos de la present proposta per a l'ús de les solucions en el núvol:

- **Errors per manipulació no autoritzada.** No s'inclou la correcció d'errors derivats de modificacions realitzades per personal no autoritzat per BL España Software SLU.
- **Adaptacions personalitzades.** No es contemplen desenvolupaments a mida, canvis en la configuració del sistema de l'entitat ni modificacions per atendre noves necessitats operatives sorgides de l'ús.
- **Correcció d'anomalies externes.** No es cobreixen incidències atribuïbles exclusivament a l'equip informàtic de l'entitat, fallades a la xarxa o deficiències en l'entorn de treball que no guardin relació directa amb les solucions al núvol.
- **Reparacions per virus o programari extern.** No s'inclouen intervencions per resoldre problemes causats per malware, virus o programari aliè a les solucions contractades.
- **Actualització a versions superiors (upgrades).** No es contempla la substitució del programari per una versió que impliqui canvis en la tecnologia base, com llenguatge de programació, sistema operatiu o base de dades.



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

- **Adaptacions a necessitats específiques.** No es preveuen modificacions per cobrir circumstàncies excepcionals de l'entitat ni canvis en la seva infraestructura local.
- **Consultes legals.** No s'inclouen assessoraments sobre normativa legal, llevat d'aquells relacionats amb les actualitzacions de les solucions.
- **Consultes sobre configuracions externes.** No es presta suport per a configuracions d'equips, instal·lacions de l'entitat o incidències derivades de maquinari, condicions ambientals o fallades en el subministrament elèctric aliens a les solucions contractades.

9. Suport Integral

9.1. Espai de clients i suport a l'usuari al núvol

A través de l'Espai de Clients <http://espacioclientes.berger-levrault.es>, l'Entitat tindrà a la seva disposició els següents serveis:

Registre i seguiment de sol·licituds a través de tiquets

Permet registrar consultes o incidències aportant la màxima informació per poder solucionar les peticions.

Aquest model permet un suport disponible les 24 hores.

Qualsevol consulta o incidència es registrarà a través de l'obertura d'un tiquet en el sistema que permetrà fer seguiment i traçabilitat.

Qualsevol canvi en la gestió dels assumptes reportats es comunicarà via correu electrònic i en cas de ser necessari, es contactarà amb l'entitat per telèfon.

L'equip especialitzat gestiona cada petició garantint una experiència àgil, coherent i transparent, d'acord amb l'estàndard de servei al núvol.

Tipus de sol·licituds:

Consultes i incidències: atenció prioritzades segons la seva criticitat.

Sol·licituds de millora o adaptació funcional: analitzades per l'equip de producte per avaluar la seva viabilitat a l'entorn al núvol. Les aprovades s'incorporen al roadmap d'actualitzacions.

El model al núvol permet que el nostre equip tècnic especialitzat accedeixi de forma segura, immediata i controlada a l'entorn de l'entitat per analitzar i resoldre incidències. Aquest nou enfocament ofereix:

- Assistència més ràpida i amb traçabilitat completa de cada intervenció.
- Orientació pràctica sobre funcionalitats i millors pràctiques d'ús.
- Resolució directa d'incidències, amb menor necessitat d'intercanviar arxius o coordinar sessions remotes.

Gestió de les dades de contacte



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

Els usuaris que comptin amb accés a aquest Espai de Clients podran modificar i actualitzar les seves dades en qualsevol moment. Només el/s Administrador/es de l'Entitat podran canviar o eliminar dades de tots els usuaris registrats per a la seva organització, a més de gestionar les altes i baixes d'usuaris.

Formació digital i contínua

La subscripció inclou accés permanent a un programa de formació digital orientat a mantenir actualitzats els usuaris i optimitzar l'ús de la plataforma. S'ofereixen sessions periòdiques online (webinars), complementades amb materials de suport —gravacions, manuals, FAQs, vídeos, microcàpsules i tutorials— accessibles en tot moment.

Finalitat de la formació:

- Garantir que els usuaris coneguin les darreres novetats funcionals i millores de l'aplicació.
- Difondre les millors pràctiques identificades des del servei de Relació Client.
- Fomentar la col·laboració i l'intercanvi d'experiències entre entitats i equips.
- Consolidar un ús més eficient i homogeni de les solucions.

La formació digital elimina desplaçaments, aporta flexibilitat i assegura l'accés universal a continguts de valor, facilitant l'adopció i l'aprofitament ple de la plataforma.

Centre de Recursos i documentació

L'Espai de Clients integra un Centre de Recursos amb informació actualitzada i autogestionable, que complementa la formació contínua i la comunicació amb les entitats.

Conté:

- Comunicacions oficials sobre el servei i les actualitzacions.
- FAQs, manuals d'usuari i butlletins informatius.
- Materials formatius i documentació tècnica de referència.

Aquest entorn centralitza la informació essencial i permet a cada usuari accedir fàcilment als recursos necessaris per operar amb autonomia i mantenir-se al dia.

Sol·licitud de modificacions funcionals

L'Entitat podrà fer arribar les seves propostes de millora o modificacions funcionals a través del servei de suport. Totes elles quedaran registrades en els nostres sistemes perquè puguin ser analitzades en les futures evolucions que es plantegin. Ens comprometem a informar sobre les millores incorporades en cada nova versió del programari.

Alta i baixa d'usuaris

L'Entitat serà el responsable de demanar les altes i baixes d'usuaris a través de l'Espai de Clients, seguint els procediments i canals establerts per a tal fi.

Es fa èmfasi en la correcta gestió de les baixes d'usuaris, ja que resulta un aspecte crític des del punt de vista de la seguretat de la informació i el control d'accessos. La comunicació immediata de les baixes permet garantir que aquells usuaris que ja no hagin de disposar d'accés al servei no



PLEC PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEIS DE SUBSCRIPCIÓ, POSADA EN FUNCIONAMENT, MANTENIMENT I SUPORT INTEGRAL EN MODALITAT NÚVOL (CLOUD) DE LA PLATAFORMA NEXT (SISTEMA DE COMPTABILITAT CGAP), MITJANÇANT PROCEDIMENT NEGOCIAT SENSE PUBLICITAT (Article 168 de la LCSP)

puguin seguir accedint als sistemes, evitant així possibles accessos no autoritzats, fuites d'informació o incompliments de la normativa vigent en matèria de seguretat.

L'adjudicatari executarà les altes i baixes sol·licitades una vegada rebuda la petició formal per part del Client, assegurant la traçabilitat de les sol·licituds i la correcta aplicació de les mesures de control d'accés definides.

10. Serveis no inclosos

Queden exclosos de la present proposta els serveis següents:

- La correcció d'errors imputables a la manipulació del programa o migració de dades per personal no autoritzat expressament per BL España Software SLU.
- La correcció d'anomalies imputables exclusivament a l'equip informàtic utilitzat, així com avaries per causes de la xarxa general o deficiències de l'ambient de treball i que no guardin cap relació de causalitat amb l'aplicació.
- La reparació causada per l'acció de virus o altres agents infecciosos, o per instal·lació de nous programes per part del client i que siguin alienes a BL España Software SLU.
- Substitució del programa original per un de nou que sigui objecte d'una millora de nivell que impliqui up-grade o canvi de plataforma (llenguatge, sistema operatiu o base de dades).
- L'adaptació dels productes a les circumstàncies excepcionals del client, a noves necessitats derivades de l'ús dels seus productes o al canvi del seu sistema informàtic, entenent com a tal el sistema operatiu del seu servidor o clients, el sistema de gestió de bases de dades, la topologia i infraestructura de la seva xarxa o la incorporació de nous dispositius perifèrics no contemplats en el projecte inicial.
- Les consultes de tipus legal o d'interpretació de la legislació o de la seva normativa.
- Les consultes d'operacions alienes a les derivades de l'operatòria del producte.
- Les consultes sobre configuració d'instal·lacions informàtiques o els problemes derivats d'anomalies imputables exclusivament a l'equip informàtic utilitzat, a deficiències en les condicions ambientals de treball, així com a avaries de la xarxa general de corrent altern, o variacions de la mateixa, que no guardin cap relació amb la qualitat dels productes.
- Activitats que ha de realitzar un usuari administrador que es proporciona a cada entitat.
- Configuració aplicacions després de la implantació.
- Manteniment entorns preproducció.
- Formació a nous usuaris que s'incorporen a l'entitat o a usuaris ja existents.
- La realització de serveis fora de l'horari establert a l'apartat anterior.
- Configuracions noves, creacions de noves entitats.
- Gestió i manteniments de bases de dades.
- Manteniment, actualització i instal·lació de nous certificats.
- Gestió de Firewall, antivirus i proxys.

(Document signat electrònicament)

