Diputació, 355
08009 Barcelona
112.gencat.cat

PLEC DE PRESCRIPCIONS TÈCNIQUES PER LA CONTRACTACIÓ DEL SERVEI DE MANTENIMENT DELS NIVELLS 1 I 2 DE SISTEMES DE LA PLATAFORMA DE SERVIDORS I DEL SERVEI DE MANTENIMENT EN CIBERSEGURETAT DEL CENTRE D'ATENCIÓ I GESTIÓ DE TRUCADES D'URGÈNCIA 112 CATALUNYA.

Generalitat de Catalunya

Diputació, 355
08009 Barcelona
112.gencat.cat

ÍNDEX

Diputació, 355
08009 Barcelona
112.gencat.cat

Diputació, 355
08009 Barcelona
112.gencat.cat

1. INTRODUCCIÓ

El Centre d'Atenció i Gestió de Trucades 112 de Catalunya (CAT112) centralitza totes les trucades d'urgència de Catalunya, per a que els ciutadans i ciutadanes puguin sol·licitar els serveis públics d'urgències sanitàries, d'extinció d'incendis i salvaments, de seguretat ciutadana, de protecció civil i d'altres quan es trobin davant d'una situació d'emergència.

El CAT112 disposa de dos centres redundants operativa i tecnològicament ubicats a Gran Via (L'Hospitalet de Llobregat) i a Reus. Cada centre té instal·lats els equipaments tecnològics adients per poder atendre el cent per cent de les trucades que es puguin produir en qualsevol moment. La plataforma tecnològica que facilita l'atenció a les emergències està formada per l'aplicació de despatx d'emergències, sistema de Telefonia, sistema d'emmagatzematge de dades, Sistema d'Enregistrament i consolidació de trucades que han de donar servei ininterromput 24 hores al dia els 365 dies de l'any. Així mateix CAT112 té en servei una sèrie d'eines TIC administratives que faciliten el funcionament de la organització.

El bon funcionament d'aquests sistemes i la seva seguretat és d'importància cabdal atesa la criticitat del servei que ofereix el CAT112 vers el ciutadà. En aquest sentit, disposar d'un bon servei de manteniment que garanteixi no tant sols el correcte funcionament dels sistemes i la seva seguretat, si no també previngui possibles avaries i en faciliti la evolució tecnològica per adaptar-se a noves necessitats i prevenció en Ciberseguretat, és essencial.

2. OBJECTE DEL PLEC

L'objecte d'aquest plec és la contractació del servei de manteniment de nivells 1 o primera atenció i nivell 2 o atenció especialitzada i l'escalat i coordinació amb el manteniment del nivell 3 o manteniment del fabricant (fora de l'abast d'aquest servei) dels sistemes TIC del CAT112 així com el servei de manteniment i assessorament en Ciberseguretat dels sistemes TIC del CAT112. S'inclouen en el servei les tasques administratives, organitzatives, d'operació i gestió necessàries per tenir els sistemes en un funcionament òptim. La finalitat del servei és:

- Maximitzar la disponibilitat de les aplicacions informàtiques de gestió d'emergències, el sistema de telefonia, el sistema d'explotació de dades i d'altres sistemes auxiliars, minimitzant el temps de resolució d'incidències i realitzant tasques preventives que minorin l'aparició d'aquestes.

- Tenir la màxima traçabilitat davant l'escalat d'incidències que permeti seguir la resolució de les mateixes i per tant poder gestionar més eficientment l'impacte en els processos del servei del CAT112.

Diputació, 355
08009 Barcelona
112.gencat.cat

- Disposar d'uns sistemes tecnològics en un funcionament òptim tant pel que fa a la utilització de recursos, la usabilitat i la seguretat informàtica. Per això el servei de manteniment especialitzat haurà de proposar de manera proactiva els canvis en el funcionament i configuracions, les actualitzacions a aplicar i, en general totes les actuacions necessàries per tal d'optimitzar el funcionament del sistemes.

- Disposar d'un manteniment que inclogui l'àmbit de la Ciberseguretat que garanteixi la seguretat, disponibilitat i integritat dels sistemes d'informació i la xarxa de l'organització, així com l'adequació a estàndards i bones pràctiques reconegudes com l'Esquema Nacional de Seguretat (ENS), la norma ISO/IEC 27001, la política de ciberseguretat de la Generalitat de Catalunya i les recomanacions de l'Agència de Ciberseguretat de Catalunya o equivalents a nivell estatal i europeu.

- Actuar de forma proactiva amb la detecció de vulnerabilitats, resposta a incidents, monitorització contínua, realització d'anàlisis i auditories tècniques, realització d'informes i plans d'acció, implantació de mesures, tot el seguiment associat, etc.

3. ABAST

La contractació descrita en aquest plec inclou els serveis de gestió, operació, administració, manteniment de ciberseguretat i manteniment de nivells 1 i 2 de la infraestructura tecnològica que suporten el programari de gestió d'emergències Séneca i les seves integracions, el maquinari de la centraleta de telefonia, les eines administratives (intranet, altres), i màquines auxiliars del Cat112:

- Maquinari: servidors, plataforma d'hiperconvergència i components associats.
- Electrònica de xarxa de la plataforma d'hiperconvergència i equips de comunicacions relacionats.
- Plataforma de virtualització VMWARE, incloent administració, actualitzacions i optimització del rendiment.
- Programari base: sistemes operatius Windows i Linux, incloent configuració i manteniment de tallafocs del sistema, paràmetres de seguretat, SNMP i altres serveis essencials.
- Sistemes de còpies de seguretat i replicació: gestió, supervisió i manteniment de les còpies i de la replicació de dades entre centres.
- Gestió i administració de la seguretat: Antivirus, aplicació de pegats de seguretat, resolució de vulnerabilitats i millores contínues de seguretat.
- Monitorització de sistemes i serveis crítics.

Diputació, 355
08009 Barcelona
112.gencat.cat

- Manteniment de servidors generals: Serveis de domini (Active Directory), Serveis de DHCP i DNS, Servidors de fitxes, Sistemes de Proxy, etc.
- Altres serveis core de la infraestructura.
- Suport en el manteniment de les estacions de treball: Suport en incidències complexes, problemes de programari base i ciberseguretat
- Monitorització de sistemes.

En l'àmbit de la Ciberseguretat aquest plec inclou:

- Anàlisi i auditoria tècnica inicial detallada dels sistemes, infraestructura TIC, arquitectura de xarxa, vulnerabilitats, procediments i controls existents.
- Informe d'auditoria i pla d'acció.
- Implantació de mesures i manteniment.
- Resultats i seguiment.
- Monitorització ciberseguretat

4. DESCRIPCIÓ DE SERVEIS

El plec inclou el manteniment de nivell 1 (primera assistència) i nivell 2 (assistència especialitzada) i la prestació de serveis de gestió i administració de sistemes en general, per la resolució d'incidències o canvis i configuracions sota petició del CAT112. A part tot el manteniment de Ciberseguretat (anàlisi i auditoria tècnica inicial detallada, informe d'auditoria i pla d'acció, implantació de mesures i manteniment, resultats i seguiment).

4.1. MANTENIMENT

L'adjudicatari proveirà els serveis de manteniment de nivells 1 i 2 dels sistemes detallats en l'apartat 5 d'aquest document i el manteniment de Ciberseguretat detallat en l'apartat 6 d'aquest document. Així mateix, s'inclouen els serveis de gestió, administració i configuració dels sistemes mantinguts.

L'adjudicatari haurà de garantir la disponibilitat d'un únic número de telèfon de contacte per a la comunicació d'incidències crítiques, tant per Sistemes com Ciberseguretat, operatiu les 24 hores del dia, els 365 dies de l'any. Aquest canal haurà d'assegurar l'atenció immediata i la correcta escalada de les incidències d'alta criticitat que puguin afectar la continuïtat del servei.

Addicionalment, l'adjudicatari haurà de posar a disposició un canal únic per a la gestió d'incidències no crítiques i per a la tramitació de sol·licituds de servei. Aquest canal podrà consistir en una adreça de correu electrònic específica o bé en una plataforma o

Diputació, 355
08009 Barcelona
112.gencat.cat

eina de ticketing que permeti l'obertura, seguiment i traçabilitat de les incidències i sol·licituds.

En tots els casos, els canals habilitats hauran de garantir la correcta identificació, registre, classificació, priorització i seguiment de les peticions, així com la seva resolució dins dels nivells de servei establerts.

4.1.1. NIVELLS.

L'oferta inclourà els següents nivell de manteniment:

- Nivell 1 o primera assistència : Corresponen a aquest nivell la detecció, registre (helpdesk com a únic punt d'entrada d'incidències), assistència tècnica en la diagnosi d'errors i la elaboració i aplicació de solucions per a incidències i avaries; resolució de la incidència si és possible i escalat a nivells superiors si és necessari.

- Nivell 2 o manteniment especialitzat: S'encarregarà de solucionar les incidències amb una complexitat més elevada o d'escalar-les a nivell 3 si és necessari i fer-ne el seguiment mentre no estiguin resoltes.

CAT112 té establerts els contractes de manteniment de nivell 3 de tots els sistemes inclosos en aquest plec. Així doncs l'abast del contracte es limita al manteniment de nivells 1 i 2 i l'obertura, coordinació, suport i seguiment de casos amb el nivell 3 de fabricant si la incidència ho requereix.
Així mateix, CAT112 disposa d'un servei de manteniment informàtic in situ que realitzarà la primera atenció a les incidències i en farà el traspàs si és necessari al servei de manteniment objecte d'aquest plec. L'empresa adjudicatària podrà fer ús del servei de manteniment informàtic in situ del CAT112 per a utilitzar com a "mans remotes", ajuts puntuals i consultes.
L'accés a les màquines serà compartit per l'adjudicatària del servei, els tècnics in-situ i l'empresa mantenidora de les aplicacions.
El servei el realitzarà l'adjudicatari amb mitjans propis: equipament adequat (ordinadors, telèfons, eines de diagnosi i resolució i, en general, tot el que requereixi la seva feina) i tècnics amb la formació i experiència necessàries d'acord amb el punt 3 de la memòria justificativa.

4.1.2. TIPOLOGIA

L'oferta inclourà les següents tipologies de manteniment:

Diputació, 355
08009 Barcelona
112.gencat.cat

- **Administració de sistemes i ciberseguretat**: correspon a les tasques de configuració, operació i administració dels sistemes inclosos en plec bé com a tasques habituals o sota demanda del CAT112 dutes a terme per a que el sistema funcioni correctament (manteniment de sistemes i manteniment de Ciberseguretat).

- **Preventiu**: totes aquelles activitats a realitzar de forma programada, com a mesures de prevenció per l'aparició d'incidències com per exemple auditories i revisions periòdiques, manteniment físic dels equips, proves, monitorització, anàlisis.

L'adjudicatari presentarà en un període de trenta dies des de l'inici del servei:

- Un **pla de manteniment preventiu** amb el detall de les actuacions que durà a terme durant el període de vigència del contracte separat any a any.

- Un calendari, durant el període de vigència del contracte, de suport del fabricant de tots els elements mantinguts, incloent-hi els períodes d'**End of Service**, **End of Maintenance** i **End of Support**.

- Un **pla de manteniment en Ciberseguretat** amb el detall de les actuacions que durà a terme durant el període de vigència de contracte separat any a any.

- **Evolutiu**: aplicació de pegats i actualitzacions. El servei inclou de manera ordinària:
  - Aplicacions de pegats de seguretat i actualitzacions per als servidors Windows cada 2 mesos.
  - Aplicacions de pegats de seguretat i actualitzacions per als servidors RedHat cada 4 mesos.
  - 1 actualització de versió de VMWARE i la plataforma d'hiperconvergència cada any.

- **Correctiu**: compren les activitats necessàries per solucionar errors lògics o físics en qualsevol dels sistemes objecte del contracte. Inclou per exemple la reparació o canvi d'equipament, configuracions, evolutius, la mà d'obra requerida i les actuacions necessàries que se'n derivin. El manteniment correctiu es desenvoluparà de diferent manera segons la incidència a tractar siguin:

  - Incidències amb afectació directa en el servei d'atenció a les emergències: es donen en els entorns productius i afecten a la operativa ordinària del servei.

Diputació, 355
08009 Barcelona
112.gencat.cat

- Incidències sense afectació directa en el servei d'atenció a les emergències: es donen en entorns no productius (pre – producció, formació), o en els que suporten les eines administratives.

4.1.3. RESOLUCIÓ D'INCIDÈNCIES AMB AFECTACIÓ DIRECTA EN LA GESTIÓ DE LES EMERGÈNCIES (Manteniment correctiu).

S'estableixen per al manteniment correctiu d'incidències amb afectació en la gestió de les emergències uns nivells de compliment en funció de la naturalesa, afectació i tipologia d'incidències que s'hauran de complir en tot moment.

4.1.3.1. CLASSIFICACIÓ D'INCIDÈNCIES

Les avaries o incidències es classificaran en **crítiques, greus o lleus** segons la seva afectació a l'operativa del servei d'atenció de trucades d'emergència.

Crítica: Provoca la no disponibilitat o degradació molt greu en el funcionament de les màquines que donen suport a:

- Plataforma Séneca.
- Integració amb telefonia.
- Sistema de telefonia
- Integració telemàtica amb agències.
- Servidors d'aplicacions.

En general, es considerarà avaria crítica la que origina una aturada i/o degradació en el funcionament normal de les sales operatives (degradació en el servei d'atenció major o igual al 40%), la que provoqui l'activació de protocols de contingència operatius, la repetició de la mateixa avaria greu. En qualsevol cas es considerarà avaria crítica si es produeix una davallada dels nivells de servei o increment en el temps mig d'operació.

Es consideraran avaries crítiques aquelles que provoquin la no disponibilitat de l'aplicació o degradació en el funcionament de Séneca, la no disponibilitat de la integració amb agències, la pèrdua de la integració amb telefonia, la pèrdua de telefonia, la pèrdua de dades si aquestes no són recuperables, i qualsevol altra de característiques similars a aquestes.

Greu: Es considerarà com avaria greu, aquella que provoqui una degradació en el servei d'atenció d'entre el 20% i el 39% i afecti a:

- Plataforma Séneca i GIS
- Integració amb telefonia.
- Sistema de telefonia

Diputació, 355
08009 Barcelona
112.gencat.cat

- Integració telemàtica amb agències, Terminals d'avisos.
- Servidors d'aplicacions.

Es considerarà també avaria greu la repetició de la mateixa avaria lleu o aquella que impedeixi la operativa normal del servei, si no es produeix una davallada dels nivells de servei ni increment en el temps mig d'operació (en aquest cas es considerarà crítica).

Es consideraran avaries greus aquelles que provoquin la degradació en el funcionament de Séneca (tant el de sales operatives 112 com les aplicacions web de Séneca), o de la integració entre Séneca i Centraleta, la degradació de la telefonia, i demés incidències amb afectacions a la operativa normal de les sales no considerades com a critiques.

Lleu: Es considerarà com avaria lleu d'un sistema aquella que provoqui una degradació del servei entre el 1% i el 19 % de les seves prestacions, o les que afectin al sistema d'explotació de dades DataWareHouse i BI, intranet, eines administratives, aplicacions web de séneca d'informes.

Avaria o episodi crític.

Si la incidència és conseqüència d'un conjunt d'averies relacionades ho denominem episodi i cal considerar el temps des de l'inici de la primera averia que en forma part, independentment de les seves conseqüències immediates per al càlcul dels temps de resposta i resolució. Respecte a l'ANS i les penalitzacions, els criteris a seguir pels episodis seran els mateixos que els de les avaries.

Es considerarà resolta una incidència quan totes les funcionalitats afectades per aquesta estiguin totalment normalitzades.

Nota: les actuacions realitzades sense previ avís al CAT112 que tinguin afectació al servei, seran considerades com a incidència a tots els efectes d'acord amb les afectacions que causin.

4.1.3.2. DEFINICIONS DE TEMPS

Es defineixen uns temps màxims d'actuacions que s'hauran de complir en tots els casos. Es tindran en compte les definicions següents:

- Cobertura horària: franja horària en la qual són d'aplicació els serveis i en la qual s'han de complir els nivells de qualitat definits en el present plec.

- Temps de resposta: Temps des de que el CAT112 intenta comunicar amb el servei de nivell 1 de l'adjudicatari i aquest respon per a poder comunicar la incidència i coordinar següents passos.

Diputació, 355
08009 Barcelona
112.gencat.cat

- Temps de resolució: temps des de que la incidència arriba al nivell 1 de l'adjudicatari i aquesta es resol.

Per les avaries no detectades en una revisió de sistemes o manteniment preventiu es consideraran l'inici dels temps de nivell de servei (ANS) des del moment en que es realitza la revisió o manteniment corresponent.

4.1.3.3. ACORDS DE NIVELL DE SERVEI

La següent taula presenta els temps establerts per al servei:

Tipus d'incidència	Cobertura horària	Temps de resposta	Temps de resolució
Crítica	24 x 7	½ h	2h
Greu	24 x 7	½ h	4h
Lleu	24 x 7	4h	24h

4.1.3.4. PROTOCOL D'ACTUACIÓ DAVANT INCIDÈNCIES

CAT112 notificarà la incidència a l'adjudicatari. Un cop avisat, el Nivell 2 procedirà a resoldre la incidència dins del temps de resposta estipulat en el acord de nivell de servei. Durant el temps que duri l'actuació, el nivell 1 de CAT112 supervisarà i donarà el suport necessari. En cas que la incidència no es pugui resoldre des del Nivell 2, aquest l'escalarà al Nivell 3 de fabricant/desenvolupador (el nivell 3 està fora de l'abast d'aquesta contractació) i s'encarregarà de la coordinació amb aquest nivell per a solucionar la incidència. La incidència no estarà tancada fins que el nivell 1 del CAT112 i el Nivell 2 ó 3 així ho acordin.

En el cas de les actuacions a nivell de manteniment preventiu, es seguiran les pautes definides i planificades en el "Pla de manteniment preventiu". Com en el cas del manteniment correctiu, aquestes tasques es faran sota la supervisió i col·laboració del nivell 1 de manteniment del CAT112.

En el cas de les actuacions a nivell evolutiu, aquestes es realitzaran en funció de les necessitats evolutives dels sistemes. L'activació i planificació d'aquestes actuacions necessiten el vistiplau del Responsable del Servei del CAT112. Com en els casos anteriors, aquestes actuacions es faran sota la supervisió i col·laboració del Nivell 1 de manteniment.

Diputació, 355
08009 Barcelona
112.gencat.cat

4.1.4. RESOLUCIÓ D'INCIDÈNCIES SENSE AFECTACIÓ DIRECTA EN LA GESTIÓ DE LES EMERGÈNCIES I SOL·LICITUDS.

Es defineix aquí el procediment que se seguirà en la resolució de les incidències que tot i dificultar el funcionament del servei d'atenció a les emergències no tenen un impacte directe en la seva eficiència.

Quan es produeixi una incidència, CAT112 la notificarà a l'empresa adjudicatària i la registrarà.

La incidència s'atendrà com a màxim el següent dia laborable i se solucionarà en 1 dia com a màxim. Si per alguna raó justificada, no és possible acomplir amb el temps de resolució, l'empresa adjudicatària proposarà una solució associada a un calendari d'implementació que haurà de ser validada pel CAT112. En qualsevol cas, totes les incidències i sol·licituds s'hauran de solucionar abans de 15 dies excepte per causes suficientment justificades.

4.1.5. GESTIÓ DE SOL·LICITUDS DE CANVI I MILLORA EN ELS SISTEMES

L'adjudicatari haurà de prestar el servei de gestió de **sol·licituds de canvi**, enteses com aquelles actuacions que, no tenint la consideració d'incidència, comportin **ajustos menors de configuració, millores funcionals limitades o adaptacions puntuals** dels sistemes inclosos en l'abast del contracte.

Aquestes actuacions tindran caràcter **no evolutiu** i **no projectual**. En cap cas podran incloure treballs que impliquin:

- Desenvolupaments nous o ampliacions de funcionalitat que excedeixin l'ajust o millora puntual.
- Implantació de productes, plataformes o mòduls addicionals no previstos en el contracte.
- Reenginyeria d'arquitectura, migracions, moviments a altres infraestructures o ampliacions de capacitat estructural.
- Tasques que requereixin dedicacions superiors al màxim establert en aquest apartat.

El contractista estarà obligat a informar immediatament el responsable del contracte quan una sol·licitud excedeixi aquests límits, indicant-ne els motius i proposant, si escau, la seva tramitació com a projecte o actuació extraordinària.

Diputació, 355
08009 Barcelona
112.gencat.cat

4.1.5.1. TIPOLOGIA DE SOL·LICITUDS INCLOSES

Es consideren dins l'abast exclusivament:

- **Ajustos menors de configuració** en servidors, sistemes operatius, eines de virtualització, serveis de xarxa o aplicacions.
- **Modificacions de paràmetres** per optimització, adaptació de comportaments o millora d'eficiència.
- **Actualitzacions o modificacions no crítiques** que no requereixin intervencions fora d'horari ni processos complexos de validació.
- **Petites ampliacions de funcionalitat** dins dels mòduls o capacitats ja existents i sense alteració de dependències tècniques.

En general, no podran comportar més de **8 hores de dedicació estimada** per part de l'empresa adjudicatària.

4.1.5.2. TERMINIS DE RESPOSTA I RESOLUCIÓ

Per tal de garantir l'adequada prestació del servei, el contractista haurà de complir els següents terminis màxims:

Temps màxim de resposta

El contractista haurà de facilitar una **resposta inicial en un termini màxim d'1 dia laborable** des de la recepció de la sol·licitud.
Aquesta resposta haurà d'incloure:

- Confirmació de recepció
- Validació de l'abast i admissibilitat de la sol·licitud
- Estimació preliminar de termini i recursos necessaris
- En cas necessari, petició d'informació addicional

Temps ordinari de resolució

Les sol·licituds admeses hauran de ser **resoltes en un termini màxim de 3 dies laborables** des de la seva acceptació.

Sol·licituds que no es puguin resoldre en el termini ordinari

En els casos en què la naturalesa de la sol·licitud impedeixi el compliment del termini ordinari, el contractista haurà d'emetre, **abans del venciment del termini**, un **calendari justificat**, que inclourà:

Diputació, 355
08009 Barcelona
112.gencat.cat

- Descripció detallada de les tasques pendents
- Fonament tècnic de la impossibilitat de resolució en el termini
- Planificació de treball amb dates parcials i data prevista de finalització
- Dependències o riscos associats

Aquest calendari haurà de ser validat pel responsable del contracte per considerar-se acceptat.

4.1.6. TRACTAMENT D'INCIDÈNCIES I SOL·LICITUDS JA EXISTENTS

Per a les sol·licituds i incidències existents en el moment d'inici del servei, s'estableix un període màxim de 10 dies des de la data en que el CAT112 en faci el traspàs de la relació d'incidències i sol·licituds pendents a l'empresa adjudicatària per a que aquesta doni solució o presenti una planificació per a donar solució.

4.2. MONITORITZACIÓ

L'Adjudicatari haurà de monitoritzar els sistemes inclosos en l'abast del plec de manera contínua (24 x 7). La contractació inclou el muntatge d'una plataforma (maquinari i llicències si és necessari) de monitorització amb capacitat suficient per monitoritzar tots els sistemes de CAT112, la configuració de les alarmes necessàries, així com la configuració en els elements a monitoritzar.

A part, CAT112 disposa d'una eina de monitorització dels seus sistemes d'informació i infraestructures tecnològiques (el detall de l'eina s'haurà de sol·licitar demanant l'"Annex 1 - Característiques del Maquinari", mitjançant una notificació electrònica a través de la Plataforma de serveis de contractació pública (PSCP)). En aquest sentit, es requereix que l'adjudicatari realitzi una anàlisi exhaustiva de la configuració actual de la plataforma, incloent-hi l'arquitectura desplegada, els paràmetres de configuració, els mecanismes d'alerta, el rendiment, la seguretat i les integracions existents.

A partir d'aquesta anàlisi, l'adjudicatari haurà de presentar un informe tècnic amb propostes de millora i optimització de la plataforma, que podran incloure, entre d'altres, l'actualització a noves versions, la implementació d'arquitectures d'alta disponibilitat o en clúster, la millora de l'escalabilitat, l'optimització del rendiment, el reforç de la seguretat i qualsevol altra acció que contribueixi a garantir la robustesa, eficiència i evolució futura del sistema de monitorització.

En qualsevol cas queda inclòs en la licitació els serveis professionals pel desplegament del clúster de la plataforma de monitorització.

Diputació, 355
08009 Barcelona
112.gencat.cat

4.3. BOSSA D'HORES

S'inclou en aquest plec una bossa de 100 hores de tècnic especialista per any en els sistemes inclosos en el plec. Aquesta bossa podrà correspondre a un o diversos tècnics que podran realitzar les seves tasques de manera seqüencial o simultània. La bossa d'hores s'executarà per a dur a terme aquelles actuacions sobre els sistemes inclosos en el plec que no estan incloses inicialment en l'abast del servei.

4.4. SEGURETAT I PRIVACITAT.

El servei inclou la gestió i administració dels antivirus, l'aplicació de pegats de seguretat, la gestió i implementació de polítiques d'accés i, anàlisi i definició de polítiques se segmentació de xarxa i tallafocs, en general totes les actuacions necessàries per garantir la seguretat dels sistemes i prevenció en l'àmbit de la ciberseguretat. El servei s'haurà d'adaptar i seguir les recomanacions del CESICAT pel que fa a mesures de seguretat, privacitat i accés als sistemes.

4.5. IMPLANTACIÓ D'UN SISTEMA MFA PELS LLOCS DE TREBALL

Aquest apartat té per objecte la implantació d'un sistema d'autenticació multifactor (MFA) o mecanisme equivalent de reforç de la seguretat en l'accés als PCs de lloc de treball d'ús compartit de l'organització (la relació dels PCs s'haurà de sol·licitar demanant l'"Annex 1 - Característiques del Maquinari", mitjançant una notificació electrònica a través de la Plataforma de serveis de contractació pública (PSCP)).

La solució haurà de tenir en compte que els usuaris no disposen de lloc de treball fix, ni es pot assumir la disponibilitat de telèfon mòbil (corporatiu o personal), ni és viable l'ús de sistemes biomètrics. En conseqüència, el sistema proposat no podrà dependre de dispositius personals ni de mecanismes biomètrics.

La solució haurà de garantir un nivell de seguretat superior a l'autenticació basada exclusivament en usuari i contrasenya, ser compatible amb entorns multiusuari d'alta rotació, permetre la gestió centralitzada d'identitats i credencials, assegurar la traçabilitat dels accessos i integrar-se amb els sistemes corporatius existents. El contracte inclourà el disseny, la implantació, les proves, integració, documentació, posada en servei i suport de la solució proposada.

La solució podrà ser estar basada en funcionalitats natives de Windows o qualsevol altra solució de mercat. En aquest últim cas les llicències i demes despeses associades al projecte aniran a càrrec de la empresa adjudicatària.

Diputació, 355
08009 Barcelona
112.gencat.cat

Si la solució està basada en elements físics que s'hagin d'adquirir pel correcte funcionament de la solució quedaran fora de l'abast d'aquest plec. En qualsevol cas el cost dels dispositius físics proposats no podran superar els 20€ per unitat.

L'oferta ha d'incloure la proposta de solució MFA descrita.

4.6. REVISIÓ, NETEJA I OPTIMITZACIÓ DE CONFIGURACIONS I DE L'ESPAI EN DISC DEL SISTEMA D'HIPERCONVERGÈNCIA

L'adjudicatari haurà d'incloure dins l'abast del servei de manteniment una revisió, neteja i optimització de les configuracions existents, així com l'optimització de l'espai en disc del sistema d'hiperconvergència basat en tecnologia VMware. Aquesta revisió s'haurà de realitzar durant els primers tres mesos del servei.

En concret, les tasques inclouran, com a mínim:

1. Revisió de configuracions:
    a. Anàlisi de la configuració actual dels clústers, hosts, màquines virtuals i polítiques d'emmagatzematge.
    b. Verificació de coherència amb les bones pràctiques del fabricant i amb els requeriments de rendiment i disponibilitat del servei.
    c. Detecció de configuracions obsoletes, duplicades o ineficients.
    d. Proposta de millores tècniques degudament justificades.

2. Neteja i racionalització:
    a. Eliminació controlada de màquines virtuals obsoletes, snapshots antics o no justificats i fitxers residuals.
    b. Revisió i depuració de polítiques d'emmagatzematge no utilitzades.
    c. Consolidació d'espais i recursos infrautilitzats.

3. Optimització de l'espai en disc
    a. Monitoratge de la capacitat utilitzada i disponible.
    b. Aplicació de mecanismes d'optimització disponibles a la plataforma (deduplicació, compressió, reclamació d'espai, etc., si escau).
    c. Reequilibri de dades entre nodes per garantir una distribució òptima.
    d. Planificació preventiva de creixement de capacitat.

4. Informes:
    a. Elaboració d'un informe tècnic detallat amb les actuacions realitzades, incidències detectades, recomanacions i estat de capacitat.

Diputació, 355
08009 Barcelona
112.gencat.cat

Totes les actuacions hauran de realitzar-se minimitzant l'impacte en el servei, preferentment en finestres de manteniment acordades prèviament, i seguint els procediments de control de canvis establerts per l'organització.

4.7. SERVEI DE MANTENIMENT DE LA CIBERSEGURETAT

S'inclou la realització, com a mínim, de les següents accions:

4.7.1. ANÀLISI I AUDITORIA TÈCNICA

S'haurà d'executar una auditoria de seguretat detallada que inclou com a mínim:

- Sistemes i infraestructures TIC (incloent arquitectura):
  - Servidors físics i virtuals.
  - Plataformes d'hiperconvergència i entorns de virtualització.
  - Sistemes operatius i aplicacions crítiques.
  - Sistemes de so i comunicació interna (VoIP, etc.).
  - Solucions antivirus, antimalware i EDR existents.
  - Solució actual de SIEM (revisió de casos d'ús, fonts integrades, configuració, etc.).
  - Sistemes de còpies de seguretat (estratègia, xifratge, prova de restauració, etc.).
  - Sistemes balancejats.

- Arquitectura de xarxa:
  - Segmentació de la xarxa i segregació de serveis.
  - Dispositius de seguretat perimetral (firewalls, proxies, etc.).
  - Sistemes de detecció i prevenció d'intrusions (IDS/IPS).
  - Punts d'accés, VLANs i configuracions de seguretat Wifi.
  - Accés remot, VPNs i controls d'accés.

- Procediments i controls existents:
  - Gestió d'identitats i privilegis i vulnerabilitats derivades (Controlados de domini, Active Directory, etc.).
  - Control de registres (logs) i esdeveniments.
  - Política de contrasenyes i autenticació multifactor (MFA).
  - Procediments de resposta a incidents.

- Anàlisi de riscs:
  - Identificació d'actius crítics.
  - Amenaces i vectors d'atac.
  - Impacte (confidencialitat, integritat, disponibilitat).

Diputació, 355
08009 Barcelona
112.gencat.cat

  - Matriu de risc.
  - Controls existents i controls recomanats.
  - Pla d'acció.

- Pentest:
  - Anàlisi de l'arquitectura de seguretat.
  - Consultoria de l'estat de ciberseguretat del CPD realitzada mitjançant entrevistes i recollida d'informació i basada en una matriu de controls del framework de ciberseguretat NIST que s'han considerat necessaris per poder reduir el grau d'exposició a les 5 principals amenaces de l'àmbit Generalitat.
  - Anàlisi tècnica de febleses i riscos de ciberseguretat.
  - Auditoria tècnica interna en modalitat caixa gris seguint metodologies reconegudes i el sistema de puntuació CVSS. Identificarà les principals vulnerabilitats detectades en la infraestructura del Centre de Processament de Dades.
  - Anàlisi a nivell de infraestructura crítica.
  - Consultoria sobre la conformitat de la Llei de Protecció de les Infraestructures Critiques (LPIC), per valorar el nivell de seguretat física i l'estat de ciberseguretat de la infraestructura crítica, en base a la resposta del formulari proporcionat i entrevistes per part dels consultors.
  - Anàlisi de compliment de l'Esquema Nacional de Seguretat en base al perfil de compliment dels CPDs.
  - Estat de compliment del perfil de l'Esquema Nacional de Seguretat que s'ha definit pels CPDs en base a la resposta del formulari de subscripció a serveis de ciberseguretat del SOC de l'Agència de Ciberseguretat de Catalunya.

L'auditoria s'haurà de dur a terme durant els tres primers mesos del servei.

4.7.2. INFORME D'AUDITORIA I PLA D'ACCIÓ

A partir dels resultats de l'anàlisi, s'haurà de redactar un informe d'auditoria que identifiqui, com a mínim:

- Actius crítics.
- Vulnerabilitats detectades i riscos associats.
- Compliment amb els controls bàsics i reforçats de l'ENS i els controls de l'Annex A de la ISO/IEC 27001.

S'haurà de proposar un pla d'acció amb mesures correctores i preventives, classificades segons prioritat, impacte i complexitat d'implantació. Aquest pla inclourà, com a mínim:

Diputació, 355
08009 Barcelona
112.gencat.cat

- Canvis de configuració o reorganització dels sistemes i la xarxa amb recursos interns.
- Proposta d'arquitectura de sistemes o millores en l'arquitectura existent.
- Incorporació de nous sistemes, serveis o llicències (com sistemes SIEM, solucions MFA, gestors de vulnerabilitats, etc.).
- Estimació econòmica dels costos de llicenciament i desplegament dels elements externs proposats.
- Implicacions, afectacions i estimacions de durada d'aquesta implementació dintre el funcionament continu que ha de garantir el servei del CAT112.

4.7.3. IMPLANTACIÓ DE MESURES I MANTENIMENT

Segons l'abast pactat amb el CAT112, es poden aplicar directament les accions proposades o bé fer-ne el seguiment tècnic. El servei ha d'incloure, com a mínim:

- Implementació dels canvis a nivell de sistemes, xarxa i configuració.
- Monitorització contínua dels sistemes amb focus en la ciberseguretat (mitjançant eines pròpies o sistemes SIEM si es contracten).
- Supervisió de logs, detecció d'anomalies i alertes de seguretat.
- Revisió periòdica de l'estat de la ciberseguretat i ajustos del pla d'acció.
- Suport en la gestió d'incidents i resposta davant amenaces.
- Assistència en el procediment de resposta a incidents i prevenció o en el desenvolupament de Playbook.
- Assistència en la creació i manteniment d'un sistema de reserva aïllat de la xarxa per a suplir un centre en cas de necessitat (totes les màquines necessàries per poder arrancar de forma bàsica el servei d'atenció de les trucades d'emergència 112).

4.7.4. RESULTATS I SEGUIMENT

S'inclou reunions periòdiques amb informes de seguiment que mostrin, com a mínim:

- Estat de les mesures implantades.
- Incidents o alertes detectades.
- Recomanacions contínues de millora.
- Evolució del nivell de maduresa en ciberseguretat.

4.8. SERVEI PROACTIU

L'empresa adjudicatària haurà de prestar el servei de manera proactiva havent de de proposar millores en el funcionament establert per:

- Garantir el funcionament i la continuïtat dels sistemes TIC.

Diputació, 355
08009 Barcelona
112.gencat.cat

- Optimitzar els recursos del sistema facilitar la informació d'ús i ocupació dels sistemes.
- Disposar d'un sistema segur tant pel que fa a possibles vulnerabilitats dels propis equips com a protecció de dades, d'acord amb les directrius de CESICAT.
- Establir estratègies i polítiques de còpies de seguretat per donar compliment a l'estàndard de continuïtat del CAT112 optimitzant les finestres de còpia.
- Assessorar al CAT112 en l'ús de les TIC pròpies i noves informar de tecnologies que puguin millorar les existents.
- Establir estratègies de Ciberseguretat que garanteixi la seguretat, disponibilitat i integritat dels sistemes d'informació i la xarxa de l'organització, així com l'adequació a estàndards i bones pràctiques reconegudes com l'Esquema Nacional de Seguretat (ENS), la norma ISO/IEC 27001 i les recomanacions de l'Agència de Ciberseguretat de Catalunya o equivalents a nivell estatal i europeu.

5. SISTEMES I APLICACIONS INCLOSOS.

El plec inclou el manteniment de nivells 1 i 2 dels equipaments dels CPDs de Gran Via i Reus.
Tot i que el manteniment de nivell 3 queda fora de l'àmbit d'aquesta contractació, l'empresa licitadora haurà de dur a terme totes les gestions necessàries amb els mantenidors de nivell 3 per resoldre la incidència o petició: obertura de ticket, seguiment, enviament d'informació, mans remotes, proves, en general tot el que sigui necessari per la resolució de la incidència.

5.1. MAQUINARI, HIPERCONVERGÈNCIA, VIRTUALITZACIÓ I SISTEMES.

- Servidors físics i sistemes d'hiperconvergència(HC) HP Simplivity.
- Electrònica de xarxa del sistema d'hiperconvergència HP.
- Plataforma de virtualització VMWARE.
- Programari base com per exemple sistemes operatius Windows, Linux, UNIX, bases de dades, servidors d'aplicacions (excepte els de les centraletes AVAYA).
- S'inclou també la plataforma d'HC de les centraletes de telefonia.
- Futurs elements (servidors, electrònica de xarxa o similars) relacionats amb la Ciberseguretat que es puguin afegir a tot el maquinari del CAT112.

La present licitació fa referència a la plataforma hardware actualment instal·lada i en servei al CAT112, les característiques de la qual es descriuen en els apartats corresponents del present plec.

Diputació, 355
08009 Barcelona
112.gencat.cat

No obstant això, durant el període d'execució del contracte, el CAT112 es reserva el dret de renovar, substituir o evolucionar la plataforma tecnològica, ja sigui mitjançant el canvi de fabricant, de model o de tipologia de solució hardware, d'acord amb les seves necessitats organitzatives i tecnològiques.

En aquest supòsit, l'adjudicatari restarà obligat a prestar els serveis objecte del contracte sobre la nova plataforma que s'implanti, en les mateixes condicions, nivells de servei i obligacions establertes en el present plec, sempre que la nova solució sigui equivalent en funcionalitat i abast a la substituïda. L'adjudicatari haurà d'adaptar els seus procediments, coneixements i recursos tècnics per garantir la continuïtat i qualitat del servei, sense que això comporti cap cost addicional per al CAT112, llevat que s'estableixi expressament el contrari en el contracte.

5.2. SISTEMA DE CÒPIES DE SEGURETAT I RÈPLIQUES DE DADES

S'inclou la gestió complerta i el manteniment del sistema de còpies de seguretat (Veeam Backup i Rman): Gestió, configuració i administració del sistema, desplegament i configuració dels clients de còpies de seguretat, restauracions. En general, totes les configuracions i actuacions necessàries per implementar les còpies i restauracions (incloent proves) d'acord amb les indicacions del CAT112.
Així mateix, també inclou l'establiment, l'administració i manteniment de la rèplica de dades entre els centres de Reus i Gran Via.

Detall del maquinari dels sistemes inclosos en el plec.
Les empreses licitadores interessades a rebre el detall i característiques del maquinari i programari a mantenir, ho hauran de sol·licitar demanant l'"Annex 1 - Característiques del Maquinari", mitjançant una notificació electrònica a través de la Plataforma de serveis de contractació pública (PSCP).
Els elements que es detallen són els que conformen els sistemes a dia de la redacció dels plecs segons l'inventari actualitzat. Qualsevol element addicional de cada un dels subsistemes detallats, o que s'adquireixi per l'ampliació del funcionament global del servei, passarà a formar part dels elements a mantenir.

6. GESTIÓ DEL SERVEI

6.1. RESPONSABLES

L'adjudicatari designarà un o dos responsables (un per la part de Sistemes i l'altre per la part de Ciberseguretat) que actuarà com a interlocutor per a qualsevol qüestió relacionada amb l'execució de les prestacions.

Diputació, 355
08009 Barcelona
112.gencat.cat

CAT112 designarà un o dos responsables (un per la part de Sistemes i l'altre per la part de Ciberseguretat) per a supervisar i coordinar els treballs fets, exigir els mitjans necessaris per garantir el nivell de servei compromès i solucionar qualsevol dubte que pugui sorgir durant la prestació de serveis objecte d'aquest plec.

Es realitzarà un seguiment del servei coordinat amb CAT112, mitjançant reunions periòdiques mensuals. El prestador del servei haurà de generar mensualment un informe d'activitats i de seguiment de les incidències, el format del qual serà consensuat entre el proveïdor i CAT112.

6.2. COORDINACIÓ.

L'adjudicatari haurà de coordinar tots els serveis inclosos en el plec involucrats en la resolució d'una incidència i a la vegada coordinar les actuacions amb mantenidors d'altres sistemes que estiguin o puguin estar implicats en la mateixa. Així mateix informarà al CAT112 dels avenços que es produeixin en el transcurs d'una incidència.

6.3. SEGUIMENT DEL SERVEI

A banda dels contactes propis per les necessitats del servei, es realitzaran reunions setmanals de seguiment del servei, en les que es tractarà l'estat del sistemes, incidències detectades, propostes de millora, evolutius i estat dels sistemes a nivell de ciberseguretat. Així mateix es realitzarà una reunió mensual per avaluar el servei prestat en el període, revisar les actuacions dutes a terme i planificar les actuacions pendents. Extraordinàriament es podran realitzar reunions per tractar temes puntuals que afectin el funcionament dels sistemes, la ciberseguretat o del servei.

6.4. INFORMES

- **INFORME MENSUAL**:
  L'adjudicatari presentarà un informe de seguiment **mensual** de caràcter ordinari que inclourà com a mínim:
  - Les actuacions tant ordinàries com extraordinàries realitzades durant el període amb les propostes de millora que es considerin adients.
  - Resultats i recomanacions resultat de l'execució de tasques de manteniment preventiu.
  - Consum de la bossa d'hores.
  - Resum de l'estat en matèria de Ciberseguretat.
  - Qualsevol altre tema que sigui d'interès per al servei.

- **INFORME DIARI (Checklist):** Es presentarà un informe diari de l'estat dels sistemes amb els paràmetres bàsics dels sistemes mantinguts:
  - Estat general de la plataforma.

Diputació, 355
08009 Barcelona
112.gencat.cat

- Events de sistema.
- Processos crítics en servei.
- Ocupació de memòria, cpu, espai en disc, ocupació de memòria i demés paràmetres dels sistemes.
- Estat de connectivitat.
- Còpies de seguretat.
- Qualsevol altre paràmetre o indicador que pugui ser d'interès per al servei.

** L'informe diari no serà necessari quan la plataforma de monitorització estigui totalment operativa i garanteixi que qualsevol incidència en els sistemes és notificada de manera immediata.

- **INFORME D'INCIDÈNCIES:** Per les averies critiques i greus caldrà realitzar informes específics, detallant com a mínim quin tipus d'averia s'ha produït, la seva afectació al servei, quina ha estat la solució i l'evolució del procés de resolució. Finalment, el informe indicarà les actuacions de millora recomanades.

- **LLISTAT DE PERSONES I USUARIS AMB ACCÉS ALS SISTEMES DEL CAT112**: L'adjudicatari, cada 2 mesos, haurà d'enviar al CAT112 un llistat amb la relació dels usuaris actius i les baixes de la VPN que CAT112 li haurà donat accés.

7. CONDICIONS DE PRESTACIÓ DEL SERVEI

7.1. ÀMBIT D'ACTUACIÓ

El servei s'haurà de prestar al Centre d'Atenció i Gestió de Trucades d'Urgència 112 (CAT112) de Catalunya de Reus i Gran Via:

- CAT112 Gran Via (Avinguda de la Granvia de l'Hospitalet, 195, 08908 L'Hospitalet de Llobregat).
- CAT112 Reus (C. dels Pagesos, 2, 43204 Reus).

7.2. DURADA DE L'EXPLOTACIÓ DEL SERVEI

La prestació dels serveis previstos en aquest plec serà per 1 any i 6 mesos (de l'1 de juliol de 2026 o data d'adjudicació del contracte fins al 31 de desembre de 2027, ambdós inclosos), més 2 anys prorrogables (de l'1 de gener de 2028 al 31 de desembre de 2029, ambdós inclosos).

Diputació, 355
08009 Barcelona
112.gencat.cat

7.3. TIPOLOGIA I HORARI DEL SERVEI

Pel que fa al manteniment, el servei en general serà en remot fent ús dels mecanismes de connexió que el CAT112 posarà a disposició del licitador d'acord amb les recomanacions de CESICAT, amb cobertura 24 hores x 7 dies durant els 365 dies de l'any. Quan la resolució d'una incidència ho requereixi, el servei serà a més presencial.

7.4. PROCEDIMENTS PER ACCEDIR ALS SISTEMES

CAT112 disposa d'un procediment on estableix les normes i mesures per garantir un accés segur i controlat als sistemes, protegint la integritat, confidencialitat i disponibilitat de les dades. Les empreses licitadores hauran de sol·licitar aquest procediment demanant l'"Annex2 - Procediment accés sistemes 112 extern", mitjançant una notificació electrònica a través de la Plataforma de serveis de contractació pública (PSCP).

7.5. NORMATIVA DE PREVENCIÓ DE RISCOS LABORALS.

L'empresa adjudicatària serà responsable que el seu personal compleixi les normatives legals de seguretat i higiene en el treball i de prevenció de riscos laborals que siguin d'aplicació durant la prestació dels seus serveis i serà igualment responsable dels accidents o malalties que en l'exercici de la seva feina puguin incórrer.

7.6. ADAPTACIÓ DEL SERVEI A ISO 22301

CAT112 disposa de la certificació de la ISO de continuïtat 22301. Aquesta certificació implica canvis en els protocols i processos d'actuació del CAT112 del seu pla de continuïtat i com a conseqüència canvis en la interacció i operativa dels proveïdors. L'adjudicatari s'adaptarà a aquests canvis i els incorporarà en els seus processos d'actuació en el servei CAT112.
Així mateix l'empresa adjudicatària participarà en els test i proves que es duran a terme en el marc de la ISO i que requereixen dels seus serveis segons indicacions del CAT112.

7.7. ACORD DE CONFIDENCIALITAT I COMPLIMENT DE LA NORMATIVA DE PROTECCIÓ DE DADES.

Per al personal de l'empresa adjudicatària del concurs, que durant la prestació dels seus serveis tingui accés a espais, serveis, instal·lacions o suports que continguin dades de caràcter personal responsabilitat de la Generalitat de Catalunya o de les seves entitats

Diputació, 355
08009 Barcelona
112.gencat.cat

dependents, els serà d'aplicació allò que estableix el Reglament (UE) 2016/679, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades i pel que es deroga la Directiva 95/46/CE, ostentant la condició d'encarregat de tractament i a la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

L'empresa adjudicatària adaptarà el seu servei a allò que s'estableix els protocols de seguretat i en especial, el compliment de les mesures tècniques i organitzatives que aplica el CAT112.

Així mateix, l'empresa adjudicatària es compromet a no divulgar a tercers la informació confidencial que se li faciliti o a la que hagi pogut tenir accés en el desenvolupament del servei contractat.

7.8. FACTURACIÓ

La facturació del servei objecte del contracte tindrà caràcter mensual i es realitzarà a mes vençut. Cada factura corresponent a un període mensual haurà d'incloure el conjunt de serveis ordinaris efectivament prestats durant el mes natural immediatament anterior, d'acord amb les condicions i l'abast definits en aquest plec.

El contractista haurà d'emetre i trametre la factura corresponent al CAT112 dins dels set (7) primers dies naturals del mes següent al període facturat. La factura s'haurà de presentar pels mitjans formalment establerts per l'òrgan de contractació i haurà de complir tots els requisits legals, fiscals i administratius aplicables.

La manca d'emissió de la factura dins del termini indicat no eximirà el contractista del compliment de les obligacions del servei ni comportarà, per si mateixa, dret a cap modificació dels terminis de pagament previstos en el contracte.

Les factures es desglossaran en els següents conceptes i imports:

1. Manteniment, monitorització, i gestió del servei (tots els mesos per un import corresponent a la sisena part de l'import semestral dels serveis).

2. Bossa d'hores: es facturaran les executades durant el període de facturació (mes en curs).

Limitacions d'ús i facturació de la bossa anual d'hores

El contracte inclou una bossa d'hores anuals destinada exclusivament a la prestació dels serveis definits en aquest Plec. Aquesta bossa constitueix el màxim d'hores que el

Diputació, 355
08009 Barcelona
112.gencat.cat

contractista podrà destinar i facturar durant els períodes anuals de vigència del contracte.

En conseqüència:

- No es podran facturar, en cap cas, més hores de les assignades per a cada any natural.
- Qualsevol dedicació que superi el límit anual establert quedarà expressament exclosa de facturació i requerirà, si s'escau, contractació o autorització independent fora d'aquesta bossa.
- Les hores no utilitzades no seran acumulables, traslladables ni compensables en exercicis posteriors, i es consideraran extingides a efectes econòmics en finalitzar cadascun dels períodes anuals del contracte.
- La gestió i control del consum de la bossa d'hores serà responsabilitat del contractista, que haurà d'aportar mensualment el detall d'hores executades i l'estat del consum acumulat, als efectes de verificació per part del CAT112.

En cas d'incórrer en penalitzacions, els imports de les penalitzacions es descomptaran en la factura del mes corresponent.

La facturació anual no podrà excedir en cap cas l'import de la oferta.

8. PENALITZACIONS

CAT112 tindrà dret a aplicar les següents penalitzacions econòmiques sempre i quan la causa origen del no compliment en les condicions i terminis establerts en aquest plec sigui atribuïble a l'empresa adjudicatària.

8.1. INCIDÈNCIES AMB AFECTACIÓ DIRECTA EN LA GESTIÓ DE LES EMERGÈNCIES

D'acord amb les definicions d'incidències descrites en el punt 4.1.3.1., les penalitzacions seran:

- **Incidència Crítica**:

  En cas d'incompliment dels ANS, s'executarà una penalització del 15 % del import mensual del servei de manteniment per a cada incompliment.

- **Incidència Greu**:

Diputació, 355
08009 Barcelona
112.gencat.cat

En aquest cas, d'incompliment dels l'ANS comportarà una penalització del 10 % de l'import mensual del servei de manteniment per a cada incompliment.

- **Incidència Lleu**:

  En cas d'incompliment dels l'ANS, es podrà executar una penalització del 5 % de l'import mensual del servei de manteniment per a cada incompliment.

8.2. INCIDÈNCIES SENSE AFECTACIÓ DIRECTA EN LA GESTIÓ DE LES EMERGÈNCIES I SOL·LICITUDS.

S'aplicarà una penalització de l'1% de l'import facturació ordinari mensual si hi ha un retard en el període que l'adjudicatari té per solucionar la incidència o per presentar calendari per la resolució més un 0,2% de l'import de facturació ordinari mensual addicional per cada setmana de retard en l'entrega de la solució o calendari.

Si no s'ha pogut solucionar la incidència en el període establert, s'ha presentat calendari de resolució i aquest no s'acompleix, s'aplicarà una penalització de l'1% de l'import facturació ordinari mensual més un 0,2% de l'import de facturació ordinari mensual addicional per cada setmana de retard en l'entrega de la solució.

8.3. SOL·LICITUDS

En cas d'incompliment en els temps de resposta i resolució de sol·licituds, CAT112 podrà aplicar penalitzacions per un import de l'1% de l'import facturació ordinari mensual més un 0,2% de l'import de facturació ordinari mensual addicional per cada setmana de retard en l'entrega de la solució.

8.4. PÈRDUA DE DADES

Es penalitzarà fins un 10% de l'import de facturació ordinari mensual si es produeix una pèrdua total o parcial de dades del servei d'emergències atribuïble a l'empresa adjudicatària. S'entenen com a dades tant les informàtiques com els enregistraments de veu.

8.5. ENTREGA D'INFORMES

Es penalitzarà amb un 2% de de facturació ordinari mensual per cada 5 dies de retard en l'entrega dels informes i plans detallats en aquest plec.

8.6. IMPORT MÀXIM DE PENALITZACIONS

El límit màxim del total de penalitzacions a aplicar es fixa en un 10 % del preu del contracte.

Diputació, 355
08009 Barcelona
112.gencat.cat

9. DEVOLUCIÓ DEL SERVEI

S'estableix un període de transició d'un mes a la finalització del contracte per minimitzar l'impacte de la possible transició a un nou adjudicatari. Es realitzarà un pla de devolució del servei que inclourà en qualsevol cas: traspàs de coneixement, traspàs de documentació, traspàs del servei.

Traspàs del Coneixement

Es realitzaran sessions de traspàs de coneixement amb el nou adjudicatari amb l'objectiu d'explicar el funcionament actual i exposar tot el coneixement necessari per dur a terme el manteniment de les centraletes. Aquestes sessions poden ser del tipus que es decideixi com el més adequat en cada moment i en funció de l'evolució del mateix traspàs (conferències, workshops, treball en paral·lel, formació d'equips mixtes,...).

Traspàs de Documentació

A l'inici de la fase de traspàs del coneixement, l'adjudicatari lliurarà al nou adjudicatari tota la documentació disponible pel que fa als sistemes dels que passi a responsabilitzar-se. En cas que sigui necessari, es podran realitzar les sessions oportunes per explicar el contingut de la documentació.

Traspàs de Servei

S'estableix una setmana per a la fase d'execució de la transició. Durant aquest període, es coordinaran les actuacions per a que el nou adjudicatari estigui en condicions d'emprendre el servei amb garanties suficients.

10. ESTRUCTURA I CONTINGUT DE LES PROPOSTES

Les propostes han d'incloure, com a mínim, el següent:

- Descripció detallada del servei ofert.
- Processos i metodologia del servei.
- Proposta de pla de manteniment.
- Model organitzatiu i gestió del servei.

Signat electrònicament

Responsable de sistemes i integracions

Diputació, 355
08009 Barcelona
112.gencat.cat

Generalitat de Catalunya