Ajuntament de Calella

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PEL CONTRACTE DE SUBMINISTRAMENT DEL LLICENCIAMENT DELS EQUIPS DE SEGURETAT PERIMETRAL I ELS SERVEIS ASSOCIATS I EL SERVEI DE SISTEMES DE CÒPIES DE SEGURETAT AL NÚVOL DE L'AJUNTAMENT DE CALELLA

Contingut

Confidencialitat

La informació continguda en aquest Plec només pot ser utilitzada per a elaborar les ofertes del present procediment. Queda expressament prohibida qualsevol altre utilització. La prerrogativa de confidencialitat s'estendrà a l'empresa adjudicatària en l'execució de les activitats objecte d'aquest procediment.

1 Introducció

El present Plec de Prescripcions Tècniques conté les especificacions i requeriments tècnics de l'Ajuntament de Calella, en endavant l'Ajuntament, pel subministrament de les llicències dels sistemes de seguretat perimetral i els serveis associats i els serveis de sistemes de còpies de seguretat al núvol.

Atenent a les necessitats i requeriments de l'Ajuntament i als sistemes existents al mercat i per tal de facilitar al màxim la concurrència dels diferents proveïdors, s'ha diferenciat en 2 lots:

- Lot 1 – Subministrament de llicències dels sistemes de seguretat perimetral i serveis associats.
- Lot 2 – Serveis de sistemes de còpies de seguretat al núvol i serveis associats.

Els capítols a continuació inclouen una descripció dels sistemes actuals així com els requeriments tècnics de cadascun dels lots de la present contractació.

2 Objectius i abast del contracte

2.1 Objectius

Els objectius principals del procediment són els següents:

- Llicenciar els equips de seguretat perimetral de l'Ajuntament per garantir la protecció de la infraestructura informàtica davant amenaces externes.
- Disposar dels serveis de còpies de seguretat al núvol de Veeam Cloud per les còpies de seguretat, assegurant la correcta protecció i recuperació de dades dels sistemes de l'Ajuntament.
- Garantir l'evolució tecnològica, manteniment i suport dels sistemes de seguretat perimetral i de còpies de seguretat, adaptant-se a les noves amenaces i necessitats de l'Ajuntament.

2.2 Abast

L'abast del contracte contempla:

- Lot 1 – Subministrament de llicències dels sistemes de seguretat perimetral i serveis associats:
  - Subministrament
    - Llicenciament dels equips de seguretat perimetral.
  - Serveis
    - Auditoria anual de seguretat.
    - Vigilància proactiva de bugs de seguretat publicats per el fabricant i recomanacions del "Centro Criptológico Nacional" i de l'Agència de Ciberseguretat de Catalunya.
    - Actualització i configuració del servidor a on resideix el sistema de logs Forti Analyzer.
    - Actualització i manteniment dels sistemes de seguretat perimetral per garantir la seguretat perimetral de la xarxa.

- Lot 2 - Serveis de sistemes de còpies de seguretat al núvol i serveis associats:
  - Serveis
    - Servei de còpies de seguretat al núvol per poder emmagatzemar 10 TB d'informació amb backups diaris i amb 2 mesos de retenció.
    - Configuració del servei de còpies de seguretat al núvol per tota la infraestructura de servidors de l'Ajuntament.
    - Revisió de les còpies per comprovar que es fan correctament.

3 Descripció de la situació actual

A continuació es descriu la situació actual dels sistemes de seguretat perimetral i de còpies de seguretat de l'Ajuntament, objecte de renovació en el present Plec de Prescripcions Tècniques.

3.1 Equips de seguretat perimetral

Actualment, es disposa de tres equips de seguretat perimetral del fabricant Fortinet que actuen com a equips de seguretat perimetral per a les connexions a Internet de l'Ajuntament i la Comissaria de Policia, i el sistema centralitzat d'anàlisi i gestió de logs de seguretat de Fortinet, Forti Analyzer. La taula a continuació indica els models dels que es disposa:

Seu	Model	Unitats
Ajuntament	Fortigate 100 F	2
Policia	Fortigate 40 F	1
Ajuntament	Forti Analyzer	1
TOTAL		4

3.2 Sistemes de còpies de seguretat

Actualment, l'Ajuntament disposa del sistema de còpies de seguretat Veaam Backup en local per tota la infraestructura de servidors de l'Ajuntament. Aquesta consta de 22 servidors virtualitzats amb un volum aproximat de 7 TB.

4 Divisió en lots

Atenent a les necessitats i sistemes requerits per l'Ajuntament, a les solucions existents al mercat i per tal de facilitar al màxim la concurrència de diferents proveïdors, s'han definit els següents lots:

- Lot 1 – Subministrament de llicències dels sistemes de seguretat perimetral i serveis associats
- Lot 2 – Serveis de sistemes de còpies de seguretat al núvol i serveis associats

El Lot 1 contempla:

- Subministrament
  - Llicenciament dels equips de seguretat perimetral.
- Serveis
  - Auditoria anual de seguretat.
  - Vigilància proactiva de bugs de seguretat publicats per el fabricant i recomanacions del "Centro Criptológico Nacional" i de l'Agència de Ciberseguretat de Catalunya.
  - Actualització i configuració del servidor a on resideix el sistema de logs Forti Analyzer.
  - Actualització i manteniment dels sistemes de seguretat perimetral per garantir la seguretat perimetral de la xarxa.

El Lot 2 contempla:

- Serveis
  - Servei de còpies de seguretat al núvol per poder emmagatzemar 10 TB d'informació amb backups diaris i amb 2 mesos de retenció.
  - Configuració del servei de còpies de seguretat al núvol per tota la infraestructura de servidors de l'Ajuntament.
  - Revisió de les còpies per comprovar que es fan correctament.
-

5 Requeriments generals

5.1 Model d'atenció

El model d'atenció entre l'adjudicatari i l'Ajuntament ha de garantir un punt únic de contacte. Aquesta gestió es podrà realitzar per telèfon i correu electrònic. Totes les sol·licituds realitzades han de quedar reflectides mitjançant correu electrònic, de manera que l'Ajuntament les pugui consultar en qualsevol moment.

El suport tècnic s'ha de prestar durant l'horari laboral habitual, que serà de 8:00 a 18:00 hores, de dilluns a divendres, excloent festius.

5.2 Legalitat vigent

Totes les propostes s'ajustaran a la legalitat vigent en matèria de seguretat de la informació i protecció de dades, així com la resta de normatives, instruccions i recomanacions vigents d'aplicació en cadascun dels àmbits de l'abast del present contracte.

L'Ajuntament no assumirà cap responsabilitat derivada de l'incompliment dels marcs legals vigents durant la durada del contracte per part dels adjudicataris, que hauran d'assumir qualsevol cost o responsabilitat en aquest àmbit.

5.3 Model de devolució

Les propostes dels licitadors han de garantir la possible devolució del servei a un altre proveïdor un cop finalitzat el contracte objecte del present procediment.

Es requereix que durant tota la vigència del contracte es garanteixi que, a la seva finalització, es podrà dur a terme una devolució del servei amb el menor impacte per l'Ajuntament tenint en compte que les llicències i els sistemes proporcionats per l'adjudicatari seran propietat de l'Ajuntament.

En aquest sentit, per garantir el baix risc i el menor temps de transició en la devolució del servei, es requereix que a la finalització del contracte, l'adjudicatari estarà obligat a proporcionar a l'Ajuntament tota la informació relativa al contracte, ja sigui tècnica o administrativa, així com tots els suports electrònics que puguin estar en possessió de l'adjudicatari per tal de garantir el traspàs al nou proveïdor en un termini màxim de 4 setmanes.

6 Lot 1 – Subministrament de llicències dels sistemes de seguretat perimetral i serveis associats

6.1 Requeriments generals

A continuació es detallen els requisits tècnics mínims que els licitadors han de considerar pel llicenciament dels equips de seguretat perimetral.

6.1.1 Equip de treball tècnic i certificacions

L'equip tècnic responsable de la gestió, implementació i manteniment de les llicències ha de comptar amb un conjunt de competències i certificacions professionals que garanteixin l'adequada gestió de la infraestructura de seguretat, així com el compliment dels estàndards de seguretat i operatius establerts.

L'equip tècnic haurà d'estar format per professionals amb una àmplia experiència en la gestió d'equips de seguretat perimetral i sistemes de seguretat de xarxa. L'equip haurà de disposar de les següents capacitats:

- Gestió d'equips de seguretat perimetral FortiGate: Experiència en la configuració, administració i manteniment de firewalls FortiGate, incloent-hi l'optimització de les llicències associades.
- Gestió de sistemes de logs FortiAnalyzer: Coneixement en la gestió de logs i la configuració de sistemes FortiAnalyzer, així com la seva integració amb la infraestructura existent.
- Administració de seguretat de xarxa: Capacitat per gestionar, diagnosticar i resoldre problemes relacionats amb la seguretat de xarxa, aplicant les millors pràctiques i normatives del sector.
-

6.1.2 Documentació

6.1.2.1 Informes de canvis i millores

El licitador es compromet a lliurar informes trimestrals amb propostes concretes de canvis i millores. Els informes hauran d'incloure:

- Anàlisis de la utilització i estat de les llicències.
- Anàlisis de les possibles incidències identificades.
- Propostes concretes de canvis i millores..

6.1.2.2 Documentació de les llicències

El licitador haurà de proporcionar una documentació detallada i actualitzada semestralment sobre les condicions i estat de les llicències relacionades amb els equips de seguretat perimetral. Els documents hauran de contenir, com a mínim, els següents elements:

- Resum de les llicències adquirides i en ús, incloent-hi les dates d'inici i caducitat de les mateixes.
- Possibles canvis en la tipologia de llicències.
- Detalls sobre l'adquisició de llicències addicionals per ampliar la capacitat del sistema, en cas que sigui necessari.
- Informació sobre l'estat de les renovacions de llicències per garantir que no hi hagi interrupcions en el servei de seguretat.
- Recomanacions sobre l'optimització dels plans de llicenciament en funció de l'evolució de les necessitats de seguretat i trànsit de la xarxa.

6.2 Requeriments tècnics

6.2.1 Subministrament de llicències

Es requereix del subministrament de llicències per als següents equips de seguretat FortiGate i sistema de logs FortiAnalyzer, per tal de garantir la protecció i el rendiment adequat dels sistemes de seguretat perimetral dels CPD de l'Ajuntament de Calella i la comissaria de policia de Calella. El dimensionament d'aquestes llicències es troba a l'apartat 6.3.

Es requereix el subministrament de les següents llicències per als firewalls FortiGate 100F, destinats al CPD principal de l'Ajuntament de Calella:

- Llicència FortiGate 100F - Unified Threat Protection (UTP), que inclou les següents funcionalitats:
    - Intrusion Prevention System (IPS): Protecció avançada contra intrusions a la xarxa.
    - Advanced Malware Protection (AMP): Protecció contra malware avançat.
    - Application Control: Control d'aplicacions per gestionar l'ús de software a la xarxa.

- URL, DNS i Video Filtering: Filtrat de trànsit web i control d'accés a vídeos en línia.
- Antispam Service: Servei de detecció i bloqueig de correus electrònics de spam.
- FortiCare Premium: Suport tècnic i serveis de manteniment Premium per a l'equip, amb accés a actualitzacions de programari i assistència especialitzada.

Es requereix el subministrament de les següents llicències per al firewall FortiGate 40F, que inclou les següents funcionalitats:

- Llicència FortiGate 40F - Unified Threat Protection (UTP), que ha d'incloure les mateixes funcionalitats especificades per al FortiGate 100F, incloent:
  - Intrusion Prevention System (IPS): Protecció avançada contra intrusions a la xarxa.
  - Advanced Malware Protection (AMP): Protecció contra malware avançat.
  - Application Control: Control d'aplicacions per gestionar l'ús de software a la xarxa.
  - URL, DNS i Video Filtering: Filtrat de trànsit web i control d'accés a vídeos en línia.
  - Antispam Service: Servei de detecció i bloqueig de correus electrònics de spam.
  - FortiCare Premium: Suport tècnic i serveis de manteniment Premium per a l'equip, amb accés a actualitzacions de programari i assistència especialitzada.

Es requereix el subministrament de la següent llicència per al sistema de gestió de logs FortiAnalyzer, destinat al CPD de l'Ajuntament de Calella:

- FortiCare Premium Support 1 Year per al FortiAnalyzer (per a una capacitat de 1-6 GB diaris de logs), que ha d'incloure:
  - Suport tècnic Premium: Accés a assistència especialitzada durant un any per garantir el correcte funcionament del sistema.
  - Suport per a la gestió de logs: Manteniment del sistema de logs FortiAnalyzer amb una capacitat de processament de logs de fins a 6 GB per dia.

6.2.2 Serveis associats

A continuació es detallen els serveis d'oferta obligatòria i els serveis addicionals que es valoraran.

6.2.2.1 *Serveis d'oferta obligatòria*

6.2.2.1.1 *Auditoria bianual*

Es prestarà una auditoria bianual integral de la infraestructura de seguretat perimetral, per avaluar el rendiment, la configuració i la seguretat dels equips, detectar vulnerabilitats i proposar millores. Inclourà la revisió de llicències, el compliment de polítiques i la coherència de configuracions, finalitzant amb un informe amb recomanacions per optimitzar el sistema segons les millors pràctiques de seguretat. En el cas d'executar les dues pròrrogues, durant la segona s'haurà de prestar aquesta auditoria.

6.2.2.1.2 *Vigilància proactiva*

Es prestarà un servei de vigilància proactiva contínua en relació amb les possibles amenaces a la seguretat. Aquest servei comprèn el seguiment d'errors detectats pels fabricants i d'alertes del CCN i l'Agència de Ciberseguretat de Catalunya. Es monitoritzaran noves vulnerabilitats i s'aplicaran mesures com actualitzacions, ajustos de configuració i noves normes per protegir els sistemes perimetrals.

6.2.2.1.3 *Actualització i configuració del servidor*

Es prestarà un servei d'actualització i configuració del servidor del sistema de logs FortiAnalyzer. Aquest servei inclou la instal·lació d'actualitzacions, l'optimització del rendiment i la seguretat, la revisió de la configuració actual i la millora de la gestió i anàlisi dels logs.

6.2.2.1.4 *Manteniment*

L'adjudicatari actuarà com a intermediari directe amb el fabricant per gestionar qualsevol incidència tècnica relacionada amb el llicenciament dels equips de seguretat perimetral. Això inclou la gestió de les sol·licituds de suport tècnic, coordinant la comunicació entre l'Ajuntament i el fabricant per tal d'assegurar la correcta resolució dels problemes, així com el seguiment i actualització de l'estat de les incidències fins a la seva resolució final.

Quant al manteniment, l'adjudicatari serà el responsable de les següents tasques de manteniment:

- Suport per resolució d'incidències en horari d'oficina de 8:00 a 18:00.
- Assistència tècnica per la configuració dels sistemes:
    - Suport i resolució d'incidències: El servei de suport tècnic inclourà la resolució d'incidències sense límit de casos. Això vol dir que, en cas d'incidència, el licitador haurà d'oferir suport de manera continuada i sense restriccions en el nombre d'incidències, amb un compromís de resolució en els temps establerts. El suport tècnic haurà de ser accessible a través de diversos canals especificats a l'apartat 5.1.
    - Gestió de RMA amb el fabricant: El licitador es compromet a gestionar totes les sol·licituds de RMA directament amb el fabricant en cas de fallades dels equips. El licitador serà responsable de garantir que tots els tràmits es facin de

manera eficaç i que els equips defectuosos siguin substituïts dins del termini pactat.

- Substitució i configuració d'equips en cas d'avaria: En cas d'avaria d'un dels equips de seguretat perimetral, el licitador haurà d'oferir un servei de substitució immediata per un equip equivalent o superior, així com la configuració i posada en marxa de l'equip substituït. Aquest servei haurà d'incloure tant la substitució del maquinari com la seva configuració per garantir la mínima interrupció en els serveis de seguretat.
- Copia de seguretat de la configuració del equips: El licitador es compromet a realitzar còpies de seguretat regulars de la configuració dels equips de seguretat perimetral, de manera que en cas d'incidència o fallada del sistema, es pugui restaurar la configuració original de forma ràpida i sense perdre cap dada crítica. Les còpies de seguretat s'hauran de realitzar de forma automàtica o segons un pla de manteniment acordat, amb garanties de seguretat i protecció de les dades emmagatzemades.

6.2.2.2 Serveis d'oferta addicional

Addicionalment, els licitadors podran oferir altres serveis d'oferta opcional que seran valorats:

- Auditoria de hacking ètic: Avaluació controlada de la seguretat dels sistemes i xarxes municipals mitjançant tècniques d'intrusió simulada per identificar vulnerabilitats contemplant, com a mínim, una campanya durant els dos anys de contracte.
- Campanyes de conscienciació per al personal de l'Ajuntament de Calella mitjançant eines de phishing ètic contemplant, com a mínim, una campanya anual.
- Servei d'assessorament tècnic en ciberseguretat. Servei CISO: Bossa d'hores de 10 hores de suport expert per a la definició, implementació i seguiment de polítiques i estratègies de seguretat de la informació.

6.3 Dimensionament

Les taules a continuació detallen el dimensionament mínim requerit quant a llicències:

Elements	Dimensionament
Llicenciament FortiGate 100F	2
Llicenciament FortiGate 40F	1
Llicenciament FortiAnalyzer	1

6.4 Termini de posada en marxa del servei

El termini d'implantació dels serveis contemplats en la present contractació ha de ser com a màxim de 30 dies naturals a comptar a partir de la data de signatura del contracte.

6.5 Pla de qualitat

Els licitadors inclouran al pla de qualitat la metodologia que serà d'aplicació per a garantir el compliment dels SLA requerits, que a tots els efectes es consideraran compromisos de qualitat.

A continuació es detallen els SLA requerits:

Paràmetre	SLA requerit	Penalització requerida
Termini d'implantació		
Termini màxim d'implantació	Igual o inferior a 30 dies naturals	1% de l'import del subministrament per cada setmana d'endarreriment.
Serveis		
Entrega de l'informe d'auditoria anual, el primer informe 6 mesos respecte la signatura del contracte. El següents informes amb periodicitat anual des de l'entrega del primer.	Igual o inferior a 30 dies naturals	0,5% de la quota mensual total per cada setmana de desviació
Temps de resposta		
Temps de resposta a sol·licituds.	Igual o inferior a 2 hores laborables	0,5% de la quota mensual total per cada hora de desviació
Resolució de consultes		
Resolució de consultes i sol·licituds.	Igual o inferior a 16 hores laborables	2% de la quota mensual total per cada hora de desviació
Resolució d'incidències		
Resolució d'incidències lleus.	Igual o inferior a 16 hores laborables	0,5% de la quota mensual total per cada 4 hora de desviació
Resolució d'incidències greus.	Igual o inferior a 8 hores laborables	1% de la quota mensual total per cada hora de desviació

Paràmetre	SLA requerit	Penalització requerida
Resolució d'incidències molt greus.	Igual o inferior a 4 hores laborables	2% de la quota mensual total per cada hora de desviació

Els SLA anteriors contemplen els següents tipus d'avaries:

- Incidència molt greu
  - Incidències que impedeixen l'operativa dels equips de seguretat perimetral.
- Incidència greu
  - Incidències que permetin l'operativa dels equips de seguretat perimetral de manera degradada o que afectin a l'operativa del Forti Analyzer.
- Incidència lleu
  - Qualsevol incidència no inclosa en els casos anteriors.

6.6 Model de proposta

Informació tècnica que incloure al sobre de criteris de judici de valor:

Segons el detall dels criteris de judici de valor que es detallen al plec de clàusules administratives particulars.

Informació tècnica que incloure al sobre corresponent als criteris automàtics, juntament amb l'oferta econòmica.¡:

Segons el detall dels criteris automàtics que es detallen al plec de clàusules administratives particulars.

INFORMACIÓ IMPORTANT: Els licitadors hauran de tenir en compte que la informació continguda al sobre de criteris de judici de valor no pot permetre pressuposar o anticipar la continguda al sobre de criteris automàtics. Si no, aquest fet comporta l'exclusió directa de la proposta en qüestió.

7 Lot 2 – Serveis de sistemes de còpies de seguretat al núvol i serveis associats

7.1 Requeriments generals

7.1.1 Equip de treball tècnic i certificacions

Els tècnics que treballin en la implementació, manteniment i suport dels sistemes de còpies de seguretat al núvol han de disposar d'un conjunt de competències i certificacions professionals que garanteixin l'adequada gestió del serveis de sistema de còpies de seguretat al núvol.

7.1.2 Documentació

7.1.2.1 Informe diari

El licitador haurà de proporcionar un informe diari que documenti els resultats de les còpies de seguretat realitzades durant el dia. Aquest informe haurà d'incloure, com a mínim, la següent informació:

- Estat de la còpia de seguretat.
- Detalls de l'error: En cas d'incidència, el missatge d'error detallat i el motiu de la fallada, per tal de permetre una resolució ràpida.
- Quantitat de dades processades/copiades.
- Temps de durada de la còpia: Temps utilitzat per completar la tasca de còpia de seguretat.
- Recursos afectats: Detalls sobre els sistemes o màquines virtuals específiques que han estat incloses o afectades per la còpia de seguretat.
- Comentaris generals: Qualsevol altre comentari o alerta generada pel sistema.

7.1.2.2 Documentació Actualitzada del Sistema

El licitador haurà de proporcionar anualment una documentació completa i actualitzada del sistema de còpies de seguretat. Aquesta documentació ha de reflectir qualsevol canvi realitzat al llarg de l'any, incloent-hi:

- Descripció de l'arquitectura de la solució: Diagrames i descripcions detallades de la infraestructura de còpies de seguretat, incloent-hi la ubicació de les còpies (locals i remotes), les màquines virtuals i físicament protegides, i el flux de dades.
- Configuració dels sistemes de còpies de seguretat: Inclou els procediments específics per a la configuració del sistema, les polítiques de còpia, les tasques de retenció i les programacions.

- Eines i software utilitzats: Documentació sobre el programari i les eines de suport utilitzades per gestionar les còpies de seguretat.
- Estratègia de recuperació davant de desastres: Procediments per recuperar les dades en cas de fallada crítica, incloent temps estimats per a la restauració, tipus de dades afectats i les eines utilitzades en el procés de recuperació.
- Polítiques de seguretat: Mesures adoptades per garantir la seguretat de les còpies de seguretat (encriptació, protecció contra ransomware, accés controlat, etc.).
- Procediments d'auditoria i control: Mètodes de control per a la verificació periòdica de les còpies de seguretat i processos de supervisió.
- Registre de modificacions i actualitzacions: Historial de canvis realitzats a la configuració i l'estructura del sistema, incloent actualitzacions de llicències, canvis en la infraestructura o nous requisits de seguretat implementats.

7.2 Requeriments tècnics

A continuació, es detallen els requeriments tècnics referents als sistemes de còpies de seguretat.

7.2.1 Requeriments del servei

El licitador s'encarregarà de la configuració i posada en marxa del servei Veeam Cloud per a tota la infraestructura de servidors de l'Ajuntament de Calella, que actualment consta de 22 servidors virtualitzats amb un volum aproximat de 7 TB. A més, haurà de realitzar la compra de qualsevol llicència associada necessària per al correcte funcionament del sistema de còpies de seguretat, sense cap cost addicional per a l'Ajuntament. El licitador també haurà de dur a terme la revisió periòdica de les còpies de seguretat per garantir que aquestes es realitzen correctament i que es poden restaurar en cas necessari.

Les tasques a realitzar i els requeriments del servei seran els següents:

- Integració amb la infraestructura existent: Els servidors de l'Ajuntament de Calella ja compten amb còpies de seguretat locals que compleixen els requisits de seguretat. La implantació del servei Veeam Cloud es farà de forma complementària, evitant interferències amb les còpies locals i programant-les en horaris diferenciats per garantir el rendiment dels sistemes.
- Configuració del Veeam Cloud: Es configurarà el servei Veeam Cloud com a complement a les còpies locals, per reforçar la protecció i recuperació de dades. El procés inclourà una anàlisi prèvia de les dades emmagatzemades i de la capacitat de la infraestructura actual. Es requereix la capacitat necessària al Veeam Cloud per emmagatzemar les còpies de seguretat durant dos mesos on el volum de dades d'origen pot arribar fins als 10 TB.
- Revisió de les còpies de seguretat: Es durà a terme una revisió completa de les còpies de seguretat per assegurar la seva eficàcia, integritat i capacitat de restauració per garantir la protecció contínua de les dades. També s'avaluarà la programació i l'ús de

recursos per optimitzar els temps de còpia sense afectar el rendiment de la infraestructura.

- Compatibilitat entre còpies locals i còpies al núvol: Els backups al núvol s'han de configurar de forma independent i eficient, sense interferir amb els locals, amb un límit de 10 hores per operació per evitar afectacions al rendiment.
- Backups diaris: Els backups s'han de realitzar de manera automàtica en una base diària, amb possibilitat de configurar períodes i horaris específics per a la seva execució.
- Retenció de dades de 2 mesos: Es mantindran còpies de seguretat durant un període mínim de 2 mesos per complir amb les polítiques de retenció i garantir la recuperació de dades en cas de pèrdues o incidències.
- Escalabilitat: La llicència ha de permetre l'escala del servei en cas de necessitat futura, de manera que es pugui augmentar l'emmagatzematge de forma senzilla si es requereix més espai o més temps de retenció.
- Còpies de seguretat immutables: Els arxius de còpies de seguretat hauran de ser emmagatzemats en un mode immutable, garantint que no puguin ser modificats ni eliminats fins que finalitzi el període de retenció establert (2 mesos).
- Protecció davant de ransomware: Els serveis de còpies de seguretat immutables han de garantir la seguretat de les dades enfront de qualsevol atac de ransomware, evitant que els arxius de còpies de seguretat siguin xifrats o esborrats per atacs externs. El sistema ha de ser compatible amb les funcionalitats de Veeam per la creació de còpies de seguretat immutables, aprofitant les seves funcionalitats avançades de protecció.
- Retenció i recuperació: El sistema ha de permetre la configuració de períodes de retenció que impedeixin la modificació de les còpies de seguretat durant aquest temps, permetent la seva recuperació en qualsevol moment en cas d'incidència de seguretat.
- Funcionalitat de configuració fàcil: Ha de ser fàcil de configurar, amb l'opció d'activar i gestionar còpies de seguretat immutables mitjançant un sistema centralitzat de gestió.

Els backups al núvol hauran de conviure amb els backups locals existents, s'haurà de garantir que no es produeixen conflictes de manera que no s'interfereixi ni afectar el rendiment. El procés complet de còpia de seguretat cap al núvol haurà de dissenyar-se i optimitzar-se perquè no superi en cap cas les 10 hores de durada en el cas dels backups incrementals i de 2 dies en el cas dels backups complets. Aquesta limitació temporal és essencial per assegurar que el procés de backup no interfereixi amb les operacions habituals del sistema ni amb altres tasques de manteniment.

7.2.2 Manteniment

El servei de manteniment i suport tècnic per a la solució de còpies de seguretat ha de garantir la resolució eficient de qualsevol incidència que pugui sorgir durant el seu funcionament. El suport s'ha de proporcionar en horari d'oficina, incloent les següents condicions:

El suport tècnic s'ha de prestar durant l'horari laboral habitual, que serà de 8:00 a 18:00 hores, de dilluns a divendres, excloent festius. Això inclou la resolució d'incidències relacionades amb

els sistemes de còpies de seguretat Veeam i la gestió de possibles fallades o problemes operatius.

El servei de suport haurà de cobrir la resolució de qualsevol incidència tècnica que es pugui presentar durant el període de manteniment. Les incidències inclouen, però no es limiten a:

- Errors en les còpies de seguretat: Fallades en la creació, validació o recuperació de còpies.
- Problemes en la configuració: Errors de configuració en la infraestructura de còpies de seguretat.
- Incompatibilitats amb altres sistemes: Problemes d'integració amb altres solucions de seguretat o infraestructura de TI.

El servei de suport haurà de ser capaç de diagnosticar, identificar i resoldre qualsevol incidència en temps i forma adequats, per assegurar que el sistema de còpies de seguretat es mantingui operatiu.

7.3 Termini de posada en marxa del servei

El termini d'implantació dels serveis contemplats en la present contractació ha de ser com a màxim de 30 dies hàbils a comptar a partir de la data de signatura del contracte.

7.4 Pla de qualitat

Els licitadors inclouran al pla de qualitat la metodologia que serà d'aplicació per a garantir el compliment dels SLA requerits, que a tots els efectes es consideraran compromisos de qualitat.

A continuació es detallen els SLA requerits:

Paràmetre	SLA requerit	Penalització requerida
Termini d'implantació		
Termini màxim d'implantació	Igual o inferior a 30 dies naturals	1% de l'import del subministrament per cada setmana d'endarreriment.
Documentació		
Entrega de l'informe trimestral de canvis i millores.	Igual o inferior a 2 setmanes	0,5% de la quota mensual total per cada setmana de desviació
Entrega de la documentació semestral de l'estat de les llicències.	Igual o inferior a 30 dies naturals	0,5% de la quota mensual total per cada setmana de desviació

Paràmetre	SLA requerit	Penalització requerida
Temps de resposta		
Temps de resposta a sol·licituds.	Igual o inferior a 2 hores laborables	0,5% de la quota mensual total per cada dia de desviació
Resolució de consultes		
Resolució de consultes i sol·licituds.	Igual o inferior a 16 hores laborables	2% de la quota mensual total per cada hora de desviació
Resolució d'incidències		
Resolució d'incidències lleus.	Igual o inferior a 16 hores laborables	2% de la quota mensual total per cada 4 hora de desviació
Resolució d'incidències greus.	Igual o inferior a 8 hores laborables	3% de la quota mensual total per cada hora de desviació
Resolució d'incidències molt greus.	Igual o inferior a 4 hores laborables	5% de la quota mensual total per cada hora de desviació

Els SLA anteriors contemplen els següents tipus d'avaries:

- Incidència molt greu
  - Incidències que impedeixen l'operativa dels sistemes de còpia de seguretat.
- Incidència greu
  - Incidències que permetin l'operativa dels sistemes de còpia de seguretat de manera degradada.
- Incidència lleu
  - Qualsevol incidència no inclosa en els casos anteriors.

7.5 Model de proposta

Informació tècnica que incloure al sobre corresponent als criteris automàtics, segons el detall dels criteris automàtics que es detallen al plec de clàusules administratives particulars.

Addicionalment, els licitadors inclouran en el sobre corresponent a criteris automàtics una memòria amb el detall de la proposta tècnica. Aquesta haurà d'incloure els mitjans assignats al projecte, la metodologia i els esquemes necessaris per validar que la proposta dels licitadors s'adequa als requeriments del plec.

Aquesta memòria no serà objecte de valoració i puntuació però servirà per a la validació de que la proposta dels licitadors compleixen amb els requeriments mínims del plec de prescripcions tècniques i per a acreditar els aspectes que es valoren com a criteris automàtics. La memòria tindrà una extensió de com a màxim 10 pàgines sense comptar portada ni índex.

Calella a la data de la signatura

Reponsable de Digitalització i Smart City

Asensio Molina Montoya