



Ajuntament de Granollers

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ
DEL SERVEI DE CÒPIES DE SEGURETAT DELS SISTEMES
D'INFORMACIÓ DE L'AJUNTAMENT DE GRANOLLERS



Contingut

1	Objecte del contracte.....	1
2	Descripció de la situació actual	1
3	Especificacions tècniques i funcionals dels requeriments	3
3.1	Requeriments mínims del sistema de còpies de seguretat	3
3.1.1	Característiques de l'equip d'emmagatzematge pel segon CPD	4
3.1.2	Característiques del servidor físic i la llibreria de Cintes.....	6
3.1.3	Característiques del programari de backup	7
3.1.4	Projecte de Migració de infraestructura de backup	11
3.1.5	Bossa d'hores	11
4	Accions per a una contractació pública responsable	12

Confidencialitat

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



1 Objecte del contracte

L'objecte del contracte és mantenir, i ampliar la capacitat si escau, el servei integral de gestió, execució i suport de les còpies de seguretat de tots els sistemes d'informació corporatius per tal de garantir la continuïtat dels sistemes davant qualsevol incident físic o lògic. L'ajuntament de Granollers disposarà d'una consola de gestió que permeti la definició, planificació, execució - manual i automàtica - i recuperació de les còpies de seguretat.

2 Descripció de la situació actual

Actualment, l'Ajuntament de Granollers autogestiona un servei de còpies de seguretat amb recursos propis basat en tecnologia del fabricant Veritas.

Amb aquesta tecnologia, actualment s'estan fent salvaguardes dels següents elements:

- Tots els servidors virtuals corporatius que s'executen sobre plataformes de virtualització Vmware, mitjançant programari backup Exec versió 12, que aprofita la funcionalitat d'SnapShot de la pròpia plataforma de virtualització Vmware. És important ressaltar que aquesta tecnologia ens permet la recuperació amb els següents nivells de granularitat:
 - Arxius o carpetes específiques dins els diferents discs de les màquines virtuals, tant per hostes amb sistemes operatius Microsoft com Linux (CentOS, Ubuntu...etc). La recuperació pot fer-se a la ubicació original o en ubicacions alternatives.
 - Màquines virtuals completes, a punt per a la seva execució completa
 - Arxius de configuració i VMDK d'una màquina virtual.
 - Un arxiu VMDK específic, assignat a una altra màquina virtual ja existent.
 - Màquines virtuals completes en entorn de laboratori.
- De servidors físics (mitjançant agent instal·lat localment, salvaguardant tot o part del contingut de la màquina).
- De servidors físics i de base de dades Oracle 12.1.0.2.0 Standard Edition que s'estan executant en mode RAC sobre un Oracle Linux (mitjançant agent instal·lat localment, salvaguardant tot o part del contingut de la màquina).
- D'instàncies de bases de dades SQL server versions 2012, 2014, 2016, (mitjançant agent específic per a SQLserver instal·lat localment en el servidor SQLserver).
- D'instàncies de bases de dades MySQL (mitjançant agent específic per a MySQL instal·lat localment en el servidor MySQL).
- De Directoris Actius de Microsoft, actualment basat en Microsoft 2016 Server (mitjançant agent específic per a MSAD instal·lat localment als servidors de Directori Actiu).
- D'arxius ubicats en una carpeta compartida des d'una NAS Windows Storage Server.

Amb aquesta tecnologia, actualment s'estan efectuant còpies de seguretat diàries per un total de 40 TB d'espai en origen (espai en origen del conjunt d'objectes salvaguardats: màquines virtuals, còpies de les diferents instàncies de bases de dades MySQL, SQLserver i Oracle, arxius en la NAS...) amb aquestes persistències i ubicacions:



Per fitxers d'us diari i BBDD:

- Persistències. Com a mínim, estem conservant:
 - Còpies conservades dels darrers 7 dies.
 - Còpies full conservades de les darreres 4 setmanes.
 - Còpies full conservades de les darreres 4 mesos
 - Una còpia full mensual conservada dels darrers 12 mesos (darrer dia del mes).

Per fitxers d'us històric:

- Persistències. Com a mínim, estem conservant:
 - Còpia incremental setmanal conservada 4 setmanes.
 - Còpies full mensual conservada 12 mesos
 - Una còpia full mensual conservada dels darrers 12 mesos (darrer dia del mes).

Per màquines virtual:

- Persistències. Com a mínim, estem conservant:
 - Còpia diària incremental conservada 15 dies
 - Còpia setmanal full conservada 4 setmanes
 - Còpia mensual full conservada 4 mesos

La volumetria actual a la que es pot considerar un creixement anual de un 5% en recursos es l'actual:

Hosts vmware	8
Maquines Virtuals.	165 unitats, aprox 14TB
Oracle	2 servidors físics, aprox 2,5TB
Fitxers usuaris	aprox 4TB
Fitxers històrics	aprox 18TB

Les còpies de seguretat acaben residint en dues ubicacions:

- En una cabina StoreOnce local al CPD de Sant Josep per tenir sempre còpies properes. En aquesta ubicació tenim una còpia complerta de tota la rotació.
- En una servidor NAS i un DataDomain que permeten, dividint manualment la càrrega en ambdós tenir una copia duplicada de la StoreOnce principal. Aquest dos elements estan ubicats a un CPD secundari a uns 3Kms connectat per F.O.



3 Especificacions tècniques i funcionals dels requeriments

L'exploració actual del sistema de còpies de seguretat considerem que no es ni prou òptim ni prou segur ni amb els programari s prou actualitzats del mercat i per tant es vol canviar de situació actual de servei per un servei integral de gestió, execució i suport de les còpies de seguretat de tots els sistemes d'informació corporatius per tal de garantir la continuïtat dels sistemes de davant qualsevol incident físic o lògic, que ha de tenir, com a mínim, les mateixes capacitats i funcionalitats del sistema actual afegint tots els requisits i característiques que es s'indiquen en aquest apartat.

El sistema de backup es contractarà en dues modalitats. Tot el maquinari que es demanarà en aquesta solució s'adquirirà al inici del contracte i serà propietat de l'Ajuntament de Granollers, mentre el programari i serveis s'englobaran en mode servei amb una quota de pagament únic que inclogui tots els components necessaris per complir amb els requeriments mínims exigits i les millors proposades. L'únic element que ha de mantenir-se a la proposta i que el seu manteniment no estarà subjecte a aquest contracte serà la cabina de còpies StoreOnce, que això si, estarà dedicada en exclusiva a la solució actual un cop les còpies existents deixin de tenir vigència.

L'adjudicatari serà l'encarregat de configurar i posar a punt el sistema de còpies de seguretat en mode «claus en mà» per la explotació dels sistemes d'Informació de l'Ajuntament de Granollers. És a dir, haurà d'aportar el programari necessari i gestionar el maquinari existent o adquirit per implementar el subsistema de còpies de seguretat; oferir una consola de gestió, definició, planificació, execució - manual i automàtica - i recuperació de les còpies de seguretat, amb les característiques ja esmentades en l'apartat anterior.

Qualsevol ampliació en el servei i el seu cost serà mesurada d'acord amb els costos d'ampliació d'espai contractat i especificats a l'oferta.

No es considerarà com a cost d'ampliació la incorporació de nous elements de programari necessaris per realitzar el backup de noves versions o nous elements incorporats als sistemes d'informació de l'Ajuntament: Sistemes Operatius, Hypervisors, SGBDs i MSAD.

Qualsevol element de maquinari necessari per interconnectar la nova infraestructura a la infraestructura actual ha d'estar inclosa en el contracte i no ha de suposar en cap cas un cost addicional.

3.1 Requeriments mínims del sistema de còpies de seguretat

La proposta mínima que es demana i requereix a l'adjudicatari passa per la renovació completa de dos de les peces actuals del sistema de còpies de seguretat de l'Ajuntament de Granollers.

1- La substitució de les cabines d'emmagatzemament de backups del segon CPD per una nova de característiques equivalents o superiors a la actual i que puguin treballar en sincronia per millorar al màxim el rendiment.

2- La incorporació d'un nou servidor físic que permeti fer les còpies més eficients a màxim rendiment juntament amb un sistema de llibreria de cintes per poder tenir una tercera còpia offline.



3- La incorporació d'un nou programa de còpies de seguretat amb les millors prestacions a nivell de funcionalitats, velocitat i adaptació a les tecnologies existents als CPDs de l'Ajuntament de Granollers.

4- El projecte de reconfiguració, optimització i millora de la situació actual, que permeti el compliment del ENS i protegeixi els sistemes informàtics de l'ajuntament de Granollers davant de atacs, desastres o altres elements que provoquessin la caiguda irrecuperable del sistema actiu.

5- Una bossa d'hores de suport addicional per futures reconfiguracions, dubtes o solucionar problemes tant de l'entorn de còpies com de de tota la infraestructura de servidors i cabines actuals de l'Ajuntament de Granollers.

3.1.1 Característiques de l'equip d'emmagatzematge pel segon CPD

Es requereix un sistema d'emmagatzematge de backup empresarial (Purpose-Built Backup Appliance, PBBA), específicament dissenyat per a la funcionalitat de contenir còpies de seguretat.

El detall de les característiques tècniques que s'han de satisfer segueixen a continuació:

- El sistema proposat ha d'oferir una controladora base amb les següents característiques:
 - Mínim de dos (2) CPU cadascun
 - Mínim de 512GB RAM, de tipus DDR4-3200
 - Mínim de dos (2) ports de 10GBase-T Ethernet (PCIe)
 - Mínim de dos (2) ports de 1/10GBase-T Ethernet (integrades en placa)
 - Mínim de dos (2) discs dedicats per contenir el sistema operatiu
 - Ha de d'admetre l'etiquetatge de VLAN. Els ports IP que s'ofereixen del mateix tipus també admetran agregacions de ports (port bonding).
 - El sistema proposat ha d'oferir un mínim de 80TB d'espai local brut (RAW), distribuït en discs de 8TB.
 - Tres (3) anys de suport del fabricant 24x7
 - Ha de poder escalar fins a com a mínim 200TB d'espai local brut (RAW).
 - Ha de ser escalable també fins com a mínim 200TB de capacitat neta local, i uns 400TB addicionals de capacitat neta usant emmagatzematge en el núvol com AWS, Azure o sobre un object storage S3.

Es considera la capacitat neta local com: el resultat de restar la capacitat bruta local del sistema (RAW) l'espai necessari per a la implementació de la protecció de la informació (grups de RAID, discs de hot spare) sense aplicar cap tècnica d'estalvi en disc com deduplicació, i/o compressió. Tampoc es considerarà pel càlcul d'espai local la capacitat externa que es pugui consumir en el núvol públic o privat.

- Ha de tenir una única capa d'emmagatzematge local activa per operar amb les dades. No es permetran configuracions amb moviment intern o arxivat de la informació a una capa secundària de disc dins de l'emmagatzematge local del mateix repositori.
- Ha de poder oferir un rendiment sostingut d'escriptura de com a mínim 25TB/hr.a d'incorporar totes les llicències necessàries per implementar les funcionalitats de deduplicació/compressió i rèplica optimitzada (permetent la transmissió de blocs únics no duplicats).



- El sistema ha d'integrar un motor de deduplicació obligatòriament in-line, fent l'optimització d'espai abans de l'escriptura als discos físics. No es permetran dispositius que utilitzin deduplicació post procés.
- L'algoritme de la deduplicació ha de poder treballar obligatòriament mides de bloc variable sobre les dades de backup, per reconèixer un major nombre de patrons repetits i garantir la màxima eficiència en l'enviament i l'emmagatzematge de dades al mateix repositori.
- Addicionalment a la deduplicació, ha d'integrar obligatòriament la compressió in-line de les dades, és a dir, abans de l'escriptura sobre els discs físics. No es permetran dispositius que utilitzin compressió post procés.
- El sistema proposat ha de protegir les dades mitjançant un RAID 6 hardware, que vindrà configurat de fàbrica i no requerirà manipulacions addicionals durant fase d'instal·lació. En cas d'haver d'escalar el tamany, s'incorporarien discs en grups RAID 6 addicionals.
- Addicionalment, ha d'incorporar com a mínim un (1) disc en rol de hot spare per cada RAID grup.
- Ha de disposar de mecanismes de revisió i verificació continus durant la ingesta de la informació, i periòdicament, sobre les dades ja emmagatzemades per assegurar la consistència de la informació.
- Ha de suportar la funcionalitat d'encriptació data-at-rest, que compleixin la validació FIPS140-2. El xifrat de les dades s'ha de realitzar després del procediment de deduplicació, podent-se executar sobre la totalitat del repositori així com sobre volums parcials.
- Addicionalment, també haurà de suportar la funcionalitat de Secure Erase, per tal de garantir que no es puguin recuperar dades de forma no autoritzada. Cal que compleixi NIST SP800-88, realitzant un mínim de set (7) sobre escriptures aleatòries.
- Ha d'incloure mecanismes de seguretat per tal de garantir la protecció total davant d'atacs de ransomware i altres malware.
 - Autorització dual: el sistema requerirà d'un sistema d'autorització dual mitjançant un usuari específic de seguretat per tal de validar l'execució o no de les operacions crítiques sobre el sistema (modificar i/o esborrar un volum/tot l'emmagatzematge, canvi en la data/hora, desactivació de la funcionalitat d'autorització dual).
 - Immutabilitat: el sistema podrà configurar un període d'immutabilitat com a mínim a nivell de volum.
- El sistema proposat ha de suportar accés VTL FC, VTL ISCSI, NFS exports i SMB shares com repositori de backup, amb accés concurrent per a cadascun d'ells.
- Haurà de poder emular, com a mínim, els formats de cintes LTO-5, LTO-6 i LTO-7.
- Ha de tenir la capacitat de configurar com a mínim una combinació de 64 biblioteques de cintes i objectius NAS juntament amb 100.000 o més ranures de cartutxos en un únic dispositiu.
- Ha de tenir intel·ligència per entendre tant la deduplicació basada en origen com en destí i s'ha d'integrar amb el software de backup proposat.
- El dispositiu proposat serà capaç d'oferir el seu emmagatzematge de forma directa i integrada a les aplicacions de backup, de manera que s'optimitzin les transferències de dades i no sigui necessari utilitzar els modes VTL ni NAS. Es requereix integració d'aquesta funcionalitat pel software de backup actualment en producció a l'Ajuntament, com a mínim. Aquesta capacitat permet realitzar les tasques de deduplicació en origen utilitzant el mateix algorisme que implementa el dispositiu de disc.



- Ha d'admetre també, mitjançant el motor de deduplicació natiu del sistema d'emmagatzematge, la recepció i/o enviament de forma optimitzada de dades de i/o cap a l'entorn de backup ja en producció, ubicat en el CPD Principal de l'Ajuntament:
 - Aplicació de deduplicació en la transmissió des de l'origen.
 - Alliberant de cicles de còmput dels servidors de medis de l'eina de backup, ja que les dades es transmeten d'Appliance a Appliance. Els servidors de backup passen a gestionar i monitoritzar el procés.
 - Ha de garantir la replicació nativa entre appliances de backup per a mantenir la capacitat de deduplicació i compressió aplicada per el sistema actual cap al nou sistema. A més es requereix que des de la mateixa eina de backup hi hagi control de les dades replicades en el sistema secundari per accedir en cas de necessitat.
- Disposar de la designació de producte "Cyber CatalystSM" segons el programa "Cyber CatalystSM by Marsh" (<https://www.marsh.com/us/campaigns/cyber-catalyst-by-marsh.html>).
- Ha de ser integrable a una plataforma de monitorització basada en protocol SNMP.
- Ha de poder gestionar de forma còmoda mitjançant una interfase gràfica (GUI), que també tindrà la possibilitat de gestionar de forma centralitzada la resta de PBBA ja existents en l'entorn de l'Ajuntament.

3.1.2 Característiques del servidor físic i la llibreria de Cintes

Per tal de garantir una experiència de suport consolidada, es valorarà tant el servidor com l'autocarregador siguin del mateix fabricant i tinguin matrius de compatibilitat publicades conjuntes per tal d'assegurar-ne el funcionament.

La solució proposada per el servidor físic ha de complir les següents característiques mínimes:

- Un (1) equip de còmput arquitectura x86_64 estàndard
- L'ocupació en rack haurà de ser de 1U com a màxim
- Un (1) processador arquitectura x86_64, Intel Xeon-Silver 4310
- 128GB de memòria RAM tipus DDR4-3200 RDIMM, distribuïts en DIMMs de 16GB. El sistema de memòria ha de comptar amb correcció avançada d'errors i disposar de les següents opcions de configuració: online spare, mirrored memory i fast-fault tolerance
- Un total de dos (2) discs SSD SAS 24G 800GB, de categoria mínima Mixed Use (DWPD=3 o superior). El rendiment mínim de cada disc haurà de ser 135.000 IOPS en aleatori 50/50 W/R 4KB
- A nivell de connectivitat, es requereix:
 - 2 ports tipus 10/25Gb (Connexió SFP+/SFP28), distribuïts en una (1) placa de 2-port. Haurà d'incloure els cablejat DAC SFP+-SFP+ 10G per connectar a la infraestructura de xarxa actual.
 - 1 port tipus Fibre Channel (FC) 16Gbps, distribuït en una (1) placa de 1-port. Aquest port s'usarà per connectar en direct-attach la cinta LTO9, per tant s'han d'oferir garanties escrites de compatibilitat.
- Es requereix ventilació i alimentació redundada hot-plug (mínim 500W Platinum per PSU)
- Haurà d'incloure llicència per a la gestió remota de l'equip tipus (iLO, iDRAC o similar)
- Haurà de disposar de certificació per executar els principals sistemes operatius del mercat: Microsoft Windows Server, Red Hat Enterprise Linux, Suse Linux i especialment VMware ESXi 7.0/8.0
- Tres (3) anys de suport del fabricant 24x7



- Cada servidor ha d'oferir un sistema/controladora de gestió remota del sistema integrada a l'equip amb redirecció gràfica independent de les CPU de producció. S'haurà d'incloure el corresponent programari de consola de KVM virtual, amb les funcionalitats següents:
 - Gestió mitjançant interfície web
 - Possibilitat de compartir fins a 6 sessions simultànies per a la realització de tasques col·laboratives sobre el servidor
 - Seguretat basada en rols, proporcionant un accés d'usuaris que suporti two-factor authentication.
 - Llistat dels components del servidor i descripció de l'estat dels mateixos
 - Accés remot a l'estat i logs integrats del servidor
 - Regulació dinàmica d'energia de servidor
 - Gràfics 3D de temperatura de les parts del servidor
 - Apagar i encendre el servidor remotament, independentment del sistema operatiu.
 - Muntar remotament carpetes, CDs, DVDs, floppy, USBs, etc.
 - Càrrega d'imatges del sistema operatiu
 - Suportar monitorització SNMP sense necessitat d'agents al Sistema Operatiu
 - Enviament d'esdeveniments a servidor syslog
 - Sincronització NTP
 - Suportar automatització mitjançant una API Rest conforme amb Redfish
- La targeta de gestió (i SW associat) haurà de venir activada i totalment operativa per a cada node, tenint el servidor un port dedicat 1GbT RJ45 per a aquest fi.

La solució proposada per la llibreria de cintes ha de complir les següents característiques mínimes:

- Un (1) equip autocarregador de cintes que incorpori també una (1) unitat de cinta en tecnologia LTO9
- L'ocupació en rack haurà de ser de 1U com a màxim
- L'autocarregador haurà d'incorporar una unitat de cinta FC LTO9 i oferir espai per a vuit (8) slots
- L'autocarregador haurà de ser poder-se monitoritzar mitjançant web
- La unitat de cinta aprovionada LTO9 s'haurà de connectar mitjançant direct attach FC contra la HBA del servidor dedicat, a 8Gbps. S'haurà d'oferir garanties escrites de compatibilitat per aquesta connexió.
- L'arquitectura de la unitat de cinta en l'autocarregador ha de complir amb l'estàndard INCITS/T10 o més moderns
- La unitat de cinta aprovionada ha d'oferir la possibilitat opcional de suport a WORM i possibilitat opcional de suport a encriptació AES-256
- Tres (3) anys de suport del fabricant 24x7

Consumibles mínims requerits en la proposta inicial.

- Vint (20) cintes RW LTO9
- Dues (2) cintes universals de neteja
- Un (1) pack d'etiquetes addicional, que ha de contenir:
 - Cent (100) etiquetes RW LTO9
 - Deu (10) etiquetes per a cinta de neteja

3.1.3 Característiques del programari de backup

La solució proposada ha de complir les següents característiques:

- La solució ha de permetre fer còpies de seguretat d'entorns virtuals, físics o cloud així com la replicació de màquines virtuals (VMware i Hiper-V) des d'una consola única i sense cap cost addicional.



- La solució haurà de permetre fer replicació contínua (Continuous Data Protection) per a màquines virtuals a plataforma vSphere de manera asíncrones i proporcionant un RPO de l'ordre de segons (inferior a 20 segons).
- Cal una solució global de protecció que permeti copiar servidors, aplicacions i dades en una única passada. Les còpies hauran de realitzar-se a nivell d'imatge de les VMs i sense instal·lar cap element tant en VMs com en els hypervisors. Cal mantenir la consistència tant des del punt de vista del sistema operatiu com des del punt de vista d'aplicacions i dades.
- Cal que la solució s'integri amb sistemes d'emmagatzematge i que permeti fer còpies de seguretat directament utilitzant imatges de VMs basades en snapshots del sistema d'emmagatzematge. Si aquestes VMs contenen bases de dades (SQL o Oracle), els snapshots també hauran de permetre gestionar i protegir els fitxers de logs.
- La solució permetrà fer còpies de servidors NAS (SMB o NFS) així com FileServers basats en Windows o Linux utilitzant el protocol natiu dels mateixos, no NDMP. Hauréu d'implementar polítiques d'incremental forever de manera que no es requereix fer còpies completes de forma periòdica.
- La solució ha d'admetre com a repositori de backup qualsevol tipus d'emmagatzematge basat en disc (DAS/NAS/SAN/Appliance de deduplicació). El repositori (físic o lògic) haurà de poder realitzar scale-out i scale-in en funció de les necessitats del client i fins i tot podrà utilitzar diferents proveïdors/tecnologies d'emmagatzematge.
- La solució s'haurà de poder integrar de manera òptima amb repositoris HPE StoreOnce utilitzant l'API de Catalyst. Així mateix ha de tenir o ha d'estar al roadmap del producte certificat pel fabricant la funcionalitat d'integrar-se amb la immutabilitat de StoreOnce per garantir que les còpies no poden ser esborrades, modificades o encriptades en cap cas.
- Addicionalment a la integració amb la immutabilitat de StoreOnce, la solució haurà de tenir la capacitat de crear repositoris locals immutables que impedeixin la modificació o esborrament de les dades emmagatzemades durant un període definit. Aquests dipòsits s'han de poder crear a partir de servidors de propòsit general.
- Es requereix la capacitat d'integració del sistema de còpia de seguretat amb emmagatzematge basats en objectes, tant locals compatibles amb S3/SWIFT, com serveis d'emmagatzematge de núvol públic com Microsoft Azure Blob o Amazon S3. En el cas de proveïdors de núvol públic amb diferents nivells d'emmagatzematge, el sistema haurà de tenir la capacitat de realitzar Tiering entre aquests (per exemple, arxivat d'Amazon S3 Standard a Amazon S3 Glacier/DA).
- El sistema ha de permetre qualsevol nivell de recuperació. Iniciar una VM, un servidor físic, una base de dades o un share de NAS o FileServer directament des del repositori de backup, recuperació de tota la màquina o d'un disc a l'entorn de producció, recuperació d'un fitxer d'una VM, recuperació baremetal, fitxer o carpetes.
- S'aportaran mecanismes nadius, sense eines de tercers, i senzills que permetin la recuperació granular d'aplicacions/BBDD tradicionals com ara Active Directory/SharePoint/Exchange/SQLServer/Oracle. Per als casos de BBDD permetrà gestionar logs de manera adequada, així com recuperació d'un component de la BBDD copiat anteriorment, o recuperació a un punt en el temps mitjançant l'aplicació dels logs. De la mateixa manera que al backup, no es requerirà la instal·lació d'agents específics per poder fer qualsevol restauració.
- S'haurà de garantir al 100% la consistència dels backups, amb mecanismes automàtics que permetin validar els backups una vegada realitzats, podent arrencar les VMs en un entorn aïllat i realitzar-ne proves automàtiques de consistència i operativa.
- Es permetrà reutilitzar les còpies realitzades per crear un entorn de sandbox, aïllat de l'entorn de producció, i poder-lo utilitzar com a entorn de test/desenvolupament, formació o resolució d'incidències.



- L'eina aportarà un sistema de detecció proactiu que escanegi els logs i notifiqui qualsevol potencial incidència tals possibles com a problemes de rendiment, possibles incompatibilitats, etc. així com tota la informació necessària per resoldre aquest problema.
- El programari de backup ha de suportar el hardware snapshot amb la cabina HP 3PAR.
- Capacitat de fer còpies full virtuals sintètiques integrades amb la cabina. D'aquesta manera, a l'hora de realitzar un backup sintètic, no caldrà que el media server torni a llegir el backup full i els seus incrementals per consolidar-lo i tornar-lo a escriure, delegant directament aquesta capacitat al sistema proposat.
- Possibilitat de configurar una tasca tipus "Backup Copy Job" que els dispositius de còpies entendran i realitzaran de forma autònoma (amb compressió, deduplicació, sense haver de llegir novament el backup per replicar-ho per part dels media servers i amb control per part de l'ISV).

A part d'aquestes característiques funcionals, es requereix com a mínim, la mateixa persistència i freqüència que les descrites en l'apartat anterior 2.

Els processos de còpies de seguretat han de poder-se efectuar sense requerir l'aturada dels sistemes operatius en producció. No s'acceptarà aturada o reinici de serveis per instal·lació o actualització d'agents locals del sistema de backup.

Integració amb els sistemes d'informació i infraestructures corporatives a salvaguardar

La solució servida haurà d'oferir la integració amb els diferents hypervisors, sistemes operatius, directori actiu, sistemes de gestió de bases de dades, sistemes de gestió documental i sistemes d'emmagatzematge que utilitza la corporació per tal d'assegurar la continuïtat dels serveis en cas de problemes físics o lògics en la infraestructura resident a l'Ajuntament:

- Hypervisors:
 - VMware ESX 6.5.0 gestionats per un vSphere vCenter Enterprise.
 - Hypervisors VMware ESXi 6.0.0 gestionats per un vSphere vCenter, llicència Essentials.
 - Es requereix també la compatibilitat amb Hypervisors Microsoft Hyper-V 2012 o superiors, i Hypervisors Xen / Citrix. Tot i que aquest tipus de plataformes no estan en explotació actualment, sí es requereix aquesta capacitat, per previsió de futurs projectes.
- Sistemes de gestió documental:
 - Es requereix també la compatibilitat integrada amb el servidor documental Documentum versió 7.2, component del que actualment no tenim agent local contractat/instal·lat.
- Sistemes de Gestió de Bases de Dades (SGBD):
 - Oracle 12.1.0.2.0 Standard Edition, que s'executa sobre un cluster actiu/actiu OracleRAC.
 - Microsoft SQLserver de diferents distribucions 2012 i superior.
 - MySql Server v5 o superior
 - Es valorarà la integració directa del sistema de còpies de seguretat amb aquests SGBD, permetent diferents tipus de granularitat de recuperació a nivell de base de dades, d'esquema, de taula...etc.
- Directori actiu de Microsoft (MSAD)
 - Es demana la integració amb MSAD que permeti la recuperació selectiva de part dels directori actiu. La memòria tècnica ha d'exposar el nivell de granularitat amb la que aquesta integració permet treballar, i les versions de MSAD amb les que té compatibilitat. Aquests MSAD estan a nivell Microsoft Server 2019 actualment.



- Sistemes de correu electrònic:
 - El correu electrònic corporatiu es basa en una plataforma de Zimbra Collaboration Suite (ZCS), actualment en la seva versió 8.8.15, el qual executa les seves pròpies polítiques i tasques de backup, deixant les còpies de seguretat sobre el sistema d'arxius del seu sistema operatiu. Per tant, no és necessari cap agent o element d'integració específic per a Zimbra, tot i que fa imprescindible la salvaguarda del contingut de seu disc local.
- Sistemes operatius de servidors corporatius:
 - Els sistemes operatius corporatiu (de servidors corporatius i plantilles d'escriptoris corporatius) s'executen com a màquines virtuals sobre algun dels hypervisors esmentats. Es permet salvaguardar-los mitjançant tecnologia SnapShot dels propis hypervisors, com s'ha comentat en l'apartat 2. Ara bé, alguns d'aquests servidors tindran que ser compatibles amb els agents locals del sistema de backup que permetin la salvaguarda d'objectes de les diferents tipologies ja indicades en aquesta mateixa llista. Són servidors virtuals amb sistemes operatius de la família de Microsoft Servers, així també com distribucions LINUX, majoritàriament CentOS v6 i CentOS7, entre d'altres distribucions puntuals.

Consola d'administració i operativa

El sistema ha d'oferir una consola d'administració que permeti al personal tècnic de l'Ajuntament de Granollers la gestió, definició, planificació, execució - manual i automàtica – i recuperació de les còpies de seguretat, ja sigui de dades, carpetes o arxius de treball com de la totalitat dels sistemes operatius servidors corporatius virtuals, bases de dades i tot els objectes requerits.

La consola d'administració ha de permetre redefinir la selecció inicial d'objectes salvaguardats per cada perfil de còpies definit, la freqüència i persistència de les còpies.

La consola d'administració ha de permetre definir la ubicació destí, original o alternativa dels objectes/dades a recuperar, sense afectar als sistemes en producció.

El sistema ha de permetre la recuperació de les dades en un entorn aïllat diferent a l'entorn d'explotació, on es pugui validar la integritat i totalitat dels objectes/dades recuperats, ja sigui per un incident concret, o bé simplement a fi i efecte de validar la correctesa de les còpies emmagatzemades. Per «validar» s'entén el següent:

- Garantir que a partir de les còpies es poden recuperar els sistemes originals amb correcte funcionament i amb dades «exactes» que es pretén recuperar.
- Garantir que les pròpies proves de recuperació i validació de les còpies no afectaran als sistemes en producció.

La consola d'administració ha de permetre la monitorització de l'estat de l'execució dels treballs de backup, així com la revisió dels resultats i errors obtinguts en els treballs ja finalitzats o cancel·lats. Preferiblement, la consola ha de permetre també llançar algun tipus de notificacions (com per exemple mitjançant missatges de correu electrònic) per notificar canvis d'estat, alertes o errors en aquests treballs de backup.

Paràmetres de rendiment mínims

Definim RPO (Recovery Point Objective) com el temps màxim acceptable entre un incident amb pèrdua de dades i la darrera versió disponible de les dades que es requereixi recuperar per solucionar l'incident. També s'entén com el màxim temps raonable del que es poden perdre les dades introduïdes o com la periodicitat mínima en la que cal tenir backup de les dades (independentment del tipus de còpia). En aquest sentit, i com ja s'ha esmentat anteriorment, es vol mantenir, com a mínim, els mateixos valors ja esmentats en l'apartat 2.



Definim RTO (Recovery Time Objective) com el temps màxim acceptable que es pot trigar en tenir les dades d'una còpia recuperades després d'un incident. Les solucions presentades no podran superar els temps RTO màxim que s'il·lustren en el següent exemple:

- Recuperació d'una màquina virtual (sobre la plataforma vSphere) de 50 GB de grandària del seu vdisk amb Thick provisioning, recuperant-la a partir de còpia de seguretat i en hora punta (9h-14h dia laborable). En cap cas, aquest RTO pot ser superior a 50 minuts.

3.1.4 Projecte de Migració de infraestructura de backup

El projecte de reconfiguració, optimització implementació i millora de la situació actual, que permeti el compliment del ENS i protegeixi els sistemes informàtics de l'ajuntament de Granollers davant de atacs, desastres o altres elements que provoquessin la caiguda irrecuperable del sistema actiu.

La proposta de projecte ha d'incloure les següents fases:

- Fase d'estudi de la situació actual. Anàlisi de components i presa de requisits per la nova infraestructura
- Proposta de configuració i optimització, ha d'incloure tots els requisits de configuració i equipaments inclosos en aquest ple tècnic més les millores proposades.
- Pla de Migració i convivència dels sistemes de còpies antic i nou per tal de no perdre cap rotació de backup
- Fase d'implementació
- Pla de formació i de traspàs de la nova plataforma de còpies de seguretat

El projecte ha de tenir una durada màxima de dos mesos per tenir el sistema funcional i actiu i d'un màxim de 3 mesos en sistema de convivència. El projecte es considerarà tancat quan el sistema estigui funcionant amb el nou entorn de backup de forma que ja tinguem totes les rotacions funcionals al nou sistema amb les periodicitats exposades en aquest plec.

3.1.5 Bossa d'hores

Els licitadors hauran d'oferir una bossa de 100 hores de suport per futures reconfiguracions, dubtes o solucionar problemes tant de l'entorn de còpies com de tota la infraestructura de servidors i cabines actuals de l'Ajuntament de Granollers vigent durant la durada del contracte. Addicionalment, es valorarà l'augment d'hores de la bossa d'hores, fins a un màxim de 50 hores addicionals.

Concretament es podrà demanar suport presencial o remot sobre els següents elements:

- Entorn de còpies de seguretat
- Entorn de programari de virtualització Vmware ESX
- Entorn de hardware de cabines HP 3PAR i servidors HP Proliant
- Entorn de hardware de telecomunicacions HP Aruba

El suport pot ser de resolució de dubtes, aplicar actualitzacions, reconfiguracions. Es consideraran com a hores de consultoria i per tant no requereixen un SLA prioritari però sí que ha de garantir com a mínim un SLA de 8x5 NBD. (Atenció de 8 en dies laborables, resposta al següent dia laborable) i horari d'actuació a convenir segons disponibilitat.

El consum de la bossa d'hores serà independent de la facturació mensual fixa que es faci de la partida de serveis. Es farà un seguiment del consum de la bossa a efectes de portar-ne un control, però en cap cas les hores tindran una data de caducitat i, per tant, el volum total de la bossa podrà emprar-se per l'Ajuntament sense cap condicionant temporal.



4 Accions per a una contractació pública responsable

El servei objecte del contracte es desenvoluparà respectant les normes sociolaborals vigents a Espanya i en la Unió Europea, i de l'Organització Internacional del Treball.

- En la determinació del pressupost del contracte s'haurà de tindre en compte el salari base i totes aquelles retribucions establertes en el conveni, pactes o contractes laborals que resultin de l'aplicació al contracte.
- En el desenvolupament del servei objecte del contracte s'hauran d'adoptar, en tot cas, les mesures previstes en matèria de seguretat i salut en el treball, i les mesures necessàries per evitar que de l'execució del contracte es puguin derivar danys al personal municipal o a la ciutadania en general.
- L'empresa adjudicatària en el moment de formalitzar el contracte, acreditarà mitjançant declaració responsable l'afiliació i l'alta en la Seguretat Social de les persones treballadores destinades a l'execució del contracte. Aquesta obligació s'estendrà a tot el personal subcontractat per l'empresa adjudicatària principal.
- En tot cas s'haurà de respectar el principi de no discriminació per raó de gènere i s'haurà d'evitar l'ús del llenguatge i imatges sexistes, que es fa extensiu a la documentació que present el/s licitador/s.
- A l'inici de l'execució del contracte l'empresa adjudicatària haurà de presentar un Pla d'igualtat entre homes i dones durant l'execució del contracte, en els termes que estableix la Llei orgànica 3/2017 sobre la igualtat efectiva entre homes i dones.
- L'empresa adjudicatària haurà de complir en tot moment tots els requisits de gestió ambiental que disposa l'Ajuntament de Granollers, amb el propòsit d'utilitzar productes de baix consum de recursos i materials, reduir les emissions contaminants, i minimitzar la generació de residus i incentivar la seva valorització energètica, així com l'economia circular.

Finalment, aquest Plec de prescripcions tècniques particular s'ha confeccionat tenint en compte allò previst a la Convenció de Nacions Unides sobre els drets de les persones amb diversitat funcional, així com els criteris d'accessibilitat universal i de disseny universal o disseny per a totes les persones, tal com són definits en la legislació vigent.



5 Pla de qualitat

La taula a continuació detalla els acords de nivell de servei mínims requerits:

Paràmetre	SLA requerit	Penalització requerida
Gestió de peticions i canvis		
Temps màxim per aplicar peticions i canvis	8x5 NBD	1% de l'import de la mensualitat per cada dia de desviació.
Gestió d'incidències i instal·lacions		
Temps de resposta	30 minuts	No aplica
Temps de resolució d'avaries	8x5 NBD	1% de l'import de la mensualitat per cada hora de desviació.

- Temps de resposta: temps transcorregut en hores entre el moment en que es notifica una incidència i el moment en que el tècnic de l'adjudicatari realitza la primera actuació.
- Temps de resolució: temps transcorregut en hores entre la notificació de la incidència i la resolució efectiva de la mateixa.



6 Termini de provisió

El termini de provisió dels subministraments i serveis contemplats en el present procediment ha de ser com a màxim de 30 dies naturals a comptar a partir de la data de signatura del contracte.



7 Model de proposta

Els licitadors entregaran les seves propostes segons el contingut que es detalla al Plec de Clàusules Administratives Particulars.

Els licitadors han de tenir en compte, que al sobre que conté la informació dels criteris avaluables mitjançant Judici de valor no es pot incorporar cap informació que permeti conèixer les característiques avaluades mitjançant criteris automàtics, per evitar exclusions.



Ajuntament de Granollers