

**PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA
CONTRACTACIÓ DEL SERVEI DE CÒPIES DE SEGURETAT I
EXTERNALITZACIÓ (EXPEDIENT SGC 2025-07)**

ÍNDIX

I.	Objecte del contracte	3
II.	Context actual	3
III.	Requeriments per la proposta	3
IV.	Pla de treball:	8

I. Objecte del contracte

En la política de còpies de seguretat que tenim, fem en diferents finestres còpies de seguretat locals i externalitats en un cpd intern i un extern. L'objecte d'aquest lot es el de licitar aquest servei gestionat de còpies de seguretat local i externalitzades amb les característiques tècniques pertinents com xifrat, contrasenya, i immutabilitat

- Ampliació de l'actual solució de backup.
- Servei gestionat amb monitoratge de les còpies de seguretat locals i externalitzades
- Còpies de seguretat de màquines virtuals vmware, fitxers (no NDMP i agnòstic al origen), bases de dades, office 365 (correu, teams, onedrive, sharepoint,...)
- Repositori de còpies on-prem o externalitzat en un cpd extern o en cloud
- Backup d'O365 com a servei

II. Context actual

El síndic de Greuges de Catalunya disposa de backup en doble ubicació, un primer punt de restauració en local i un segon punt extarnalitzat mitjançant la tecnologia de veeam i actual programari de còpies de seguretat.

Descrivim els elements dels que fem backup externalitzat que en la pitjor situació ens definirien que podem restaurar (cas de caiguda de cpd local completa), no especifiquem finestres ni períodes per temes de seguretat.

- Servidores virtuals
- Bases de dades SQL Server
- Servidor de fitxers
- Servidor de fitxers arxivats
- Office365 (correu, teams, ondrive, sharepoint)

III. Requeriments per la proposta

Per la criticitat del servei i de cara la instal·lació, migració i configuració de la nova solució, cal garantir el nivell de coneixement de la solució anterior. L'empresa haurà de tenir certificat del fabricants de la solució anterior per poder prestar aquestes tasques. En aquest sentit l'adjudicatari haurà d'estar certificat pels fabricants amb nivell alt (netapp, vmware, Microsoft 365, SQL server, veeam backup i fabricants de la nova solució aportada)

Es relacionen a continuació els articles a subministrar amb les característiques tècniques que com a mínim, hauran de complir:

Requeriments mínims d'emmagatzematge i llicenciament

- 25 TB de repositori cloud sense cost per descarrega ni ingesta
- 2 TB de repositori CIFS
- 30 Servidors virtuals
- 10 servidors físics
- 100 contes de O365 en modalitat de pagament per us.

- Llicenciament necessari per a cobrir el backup de les màquines físiques, virtuals i CIFS

Requeriments tècnics mínims de la solució de backup on-prem

- El programari pot ser en mode subscripció o lloguer
- Servidor de backup local amb el seu llicenciament per a cobrir el backup de les màquines físiques, virtuals i NAS (NetApp A150)
- Externalització de còpies de seguretat Ha de ser mitjançant el mateix programari ofertat, el licitador oferirà la mateixa plataforma en el seu propi cloud y poder oferir un DR si fos necessari.
- Externalització del NAS mitjançant la mateixa tecnologia origen, el licitador ha de disposar del mateix maquinari o software (NetApp ONTAP) per a replicació via bloc.
- Capacitat de realitzar Tiering en serveis d'emmagatzematge al núvol públic amb protocol S3, immutable i sense cost de transferència de fitxer en carrega i descarrega. Preu tancat per GB
- El backup de CIFS pot ser replicat entre NetApp ONTAP el destí o mitjançant un programari de backup, aquest ha de poder restaurar qualsevol fitxer a qualsevol destí, queden exclosos els sistemes NDMP

Requeriments tècnics mínims del backup O365

- Solució gestionada com a servei que permeti en un futur disposar del repositori de còpies en local y poder restaurar en local amb el mateix producte.
- Permetre restauració local en cas de baixa del servei
- Repositori de backup en un service provider local o S3
- Backup directe e immutable i sense cost per enviament i descarrega preu tancat per GB
- Disposar del portal d'autorestauro del empleat
- En cas de baixa de la solució es te que garantir la disponibilitat del repositori de backup per poder restaurar.
- Retenció durant 5 anys

Requeriments Servei Gestionat plataforma de backup

- Consola de monitorització dedicada i exclusiva per al síndic
- Gestió de canvis i configuracions dels treballs de backup
- Restauracions sota demanda
- Proves Periòdiques de Recuperació:
Realització de proves periòdiques de recuperació per assegurar-se que les dades puguin ser restaurades amb èxit i ajustar les polítiques de backup si cal.
- Revisió de SLA:
Revisió periòdica del compliment dels SLA i ajustament si cal a les necessitats del client.
- Informe i Retroalimentació:
Generació d'informes periòdics per al client amb informació sobre el rendiment, l'estat del sistema i altres mètriques rellevants. Recopilació de retroalimentació del client per millorar els serveis.
- Generar un document amb un registre de recuperacions i recuperacions periòdiques:

Aquest informe a de recollir qui demana la recuperació, qui fa la recuperació, data de petició, data d'inici de restauració, data i hora d'inici i finalització de la restauració.

- Generar un document amb un informe de les còpies de seguretat local i externalitzades mensual:

Aquest informe ha de servir per avaluar la velocitat de còpia de seguretat i el volum de la informació que es fa còpia. Podent així detectar de forma proactiva incidències en el servei i necessitat d'ampliacions de la infraestructura actual.

Requeriments mínims de Servei Gestionat de la plataforma backup O365

- Gestió del backup
- Revisió i resolució d'errors e incidents
- Gestió de tickets amb al fabricant
- Restauracions sota demanda per part del Síndic de Greuges
- Assegura el correcte funcionament de la plataforma
- Disposar d'un portal amb les llicències i espai contractat

Requeriments tècnics mínims del programari de backup:

- La solució ha de permetre fer còpies de seguretat d'entorns virtuals, físics o cloud així com la replicació de màquines virtuals (VMware i Hyper-V) des d'una consola única i sense cost addicional.
- La solució haurà de permetre realitzar replicació contínua (Continuous Data Protection) per a màquines virtuals a plataforma vSphere. La replicació es basarà en l'API nativa de VMware permetent realitzar rèpliques asíncrones entre dos clústers de VMware.
- Cal una solució que sigui capaç de gestionar les còpies de seguretat d'entorns basats en hypervisors VMware, Hyper-V, Nutanix AHV i Red Hat Virtualization de forma conjunta.
- La solució proposada permetrà instal·lació tant en entorn físic com a virtual.
- Tots els components que formen part de la solució s'hauran de poder instal·lar en entorn físic o virtual.
- Es donarà suport a qualsevol sistema operatiu i sistema de fitxers que estigui suportat pels hypervisors comentats anteriorment.
- Solució global de protecció d'entorns en producció que permeti copiar servidors, aplicacions i dades en un procés únic (sense múltiples còpies). Per això la solució proposada haurà de poder fer backups basats en imatge de les VMs, i evitarà 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.
- En cas necessari es podran excloure fitxers, carpetes o volums de les VMs que s'estiguin protegint.
- Per als treballs de còpia i/o replicació s'hauran de poder construir llistes dinàmiques de VMs
- La ha de ser compatible amb aliances de backup inmutables.
- L'eina disposarà de tecnologia de mecanismes de balanceig de càrrega per repartir els treballs de forma adequada.
- L'eina disposarà de mecanismes d'alta disponibilitat que permetin continuar amb els treballs en cas d'indisponibilitat d'algun dels seus components.

- L'eina disposarà de mecanismes d'autoprotecció per, en cas de desastre total, poder recuperar el servei de restauració de manera immediata, simplement accedint a les còpies realitzades amb anterioritat i encara que hi hagi indisponibilitat del catàleg.
- Possibilitat de transferir les dades mitjançant SAN, NFS o LAN. Es valorarà qualsevol mecanisme que permeti dotar intel·ligència el sistema de cara a determinar el millor mètode a utilitzar en cada moment.
- Es controlarà l'ús d'amplada de banda, fins i tot es pot limitar durant determinats períodes de temps.
- Haurà de poder treballar amb qualsevol tipus d'emmagatzematge de qualsevol tecnologia i qualsevol fabricant, garantint així la viabilitat de cara a futur.
- Suport integrat de còpies de backup a altres dispositius com Cinta/VTL de forma nativa.
- Capacitat de crear repositoris locals immutables que impedeixin la modificació o esborrament de les dades emmagatzemades durant el període definit. Aquests dipòsits es poden crear a partir de servidors de propòsit general. Aportaran mecanismes que permetin agrupar l'emmagatzematge de diferents tecnologies, fabricants i accés en un model d'emmagatzematge virtualitzat. La capacitat agregada resultant ha de permetre definir polítiques que dirigeixin les còpies de seguretat a l'emmagatzematge més idoni.
- Permet disposar de múltiples còpies en diferents ubicacions de forma controlada, de manera que estiguin 100% accessibles en tot moment de forma immediata.
- Haurà d'incloure una eina que disposi de connexió per treballar en entorns cloud, de manera integrada i senzilla, per poder-la utilitzar en un futur.
- Tot i haver protegit cada VM en un procés de còpia únic es facilitarà la tecnologia necessària per a recuperació de qualsevol nivell. Recuperació tradicional d'un servidor complet, recuperació d'un fitxer d'una VM, fitxer o carpetes.
- Es permetrà recuperar de forma immediata un servei allotjat en una VM de manera que el temps de recuperació sigui inferior als 10 minuts, amb independència del volum de dades associades al servei involucrat.
- S'aportaran mecanismes senzills per a recuperació granular d'aplicacions/BBDD tradicionals com ActiveDirectory/SharePoint/Exchange/SQLServer/Oracle/PostgreSQL. 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. Per al backup d'aquests elements d'aplicació, no es requerirà en cap cas la instal·lació d'agents específics per poder fer la còpia de seguretat.
- La recuperació es farà de manera directa a l'origen de dades, sense necessitat d'utilitzar staging intermedis.
- En cas d'inconsistència d'una VM es podrà optar per un mecanisme de restore diferencial que permeti recuperar únicament les dades canviades a la VM, si cal restaurar la totalitat de la VM.
- S'haurà de garantir al 100% la consistència dels backups, amb mecanismes automàtics de prova dels backups una vegada realitzats, podent executar les màquines virtuals i realitzar proves automàtiques de consistència i operativa de les màquines virtuals recolzades.

- Es permetrà utilitzar les còpies realitzades per disposar de centres de demo, formació i resolució de problemes.
- Integrarà la tecnologia necessària per articular un centre de Disaster Recover que permeti aixecar qualsevol VM de manera immediata. L'operativa de failover i failback haurà d'estar integrada.
- L'eina permetrà també la possibilitat de definir plans de failover.
- Oferirà restauració dels seus backups al núvol Microsoft Azure, Amazon EC2 o Google Cloud Platform o en Service providers locals.
- Oferirà capacitat de restaurar sobre plataforma VMWare, Hyper-V o Nutanix AHV qualsevol backup realitzat independentment de l'origen (VMware, Hyper-V, Nutanix AHV, Servidors físics Windows o Linux, Cloud VMs AWS, Azure o GCP)
- L'eina 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. Permetrà implementar una política d'incremental forever de manera que les còpies siguin sempre incrementals un cop realitzat el primer backup complet.
- L'eina proporcionarà mecanismes per optimitzar la còpia a l'estil del CBT de VMware.
- Oferirà diferents nivells de restauració de lentorn de fitxers, com a mínim permetrà realitzar una restauració completa d'un share, restauració a un punt en el temps i restauració granular de fitxers o carpetes. La restauració es podrà realitzar sobre qualsevol plataforma (NAS o fileserver, de mateix o diferent fabricant) independentment de l'origen de les dades.
- L'eina ha de proveir d'APIs (RESTful, Powershell) per a l'automatització de processos i la integració d'altres fluxos de treball o portals.
- L'eina tindrà suport per accedir-hi MFA.
- L'eina garantirà que les comunicacions i les dades enviades entre les peces d'infraestructura estan encriptades.
- Integració amb sistemes d'emmagatzematge que permetin aprofitar funcionalitats com ara la deduplicació.
- Mecanismes d'aprofitament d'amplada de banda i reducció de dades per a còpies a/des d'ubicacions remotes (acceleradors).
- Control d'impacte de les còpies sobre els entorns de producció. En cas de produir-se latències excessives s'activaran els mecanismes necessaris per controlar aquest impacte, o fins i tot aturar els serveis de còpia, donant prioritat a l'entorn productiu

Monitorització

- Cal que la solució inclogui funcionalitats de monitorització i control de la plataforma de virtualització de manera reactiva i proactiva, aportant la informació necessària per a la presa de decisions en el moment adequat garantint així el nivell de servei desitjat.
- La solució permetrà controlar l'estat de qualsevol component de la plataforma de virtualització mitjançant un sistema basat en alertes.
- L'eina aportarà tota la informació relativa a qualsevol incidència que es produeixi com ara origen de problema, elements afectats, i tota la informació necessària per resoldre aquest problema.
- Es requereix un sistema d'informes avançats que faciliti funcions d'inventari, capacity planning, optimització de recursos i anàlisi de la plataforma, aportant

qualsevol recomanació que es consideri d'interès per al funcionament correcte de tot l'entorn.

- L'abast de l'eina estendrà igualment totes les necessitats descrites als punts anteriors a la plataforma de protecció de dades (backup).

Agents:

La solució de còpia de seguretat ha de permetre la protecció de servidors i estacions de treball físics mitjançant l'ús d'agents a nivell de sistema operatiu (Windows, Linux, MAC i UNIX). L'ús d'agents a nivell de sistema operatiu no només ha de permetre la protecció d'equips físics sinó qualsevol servidor ubicat al núvol públic o altres hipervisors no suportats.

Serveis

L'empresa adjudicatària es comprometrà a entregar el programari en un termini màxim de 30 dies naturals des de la data de formalització del contracte i a realitzar la instal·lació, configuració i optimització en un termini màxim de 60 dies naturals a partir de l'entrega del programari.

També es requereix la migració i adaptació de les polítiques existents de còpies de seguretat al nou entorn resultant.

També es requereix que tot el històric dels dos últims anys sigui migrat al nou entorn de backup extern.

IV. Pla de treball

Implementació:

El servei d'instal·lació ha d'incloure la configuració del programari i les corresponents llicències, la configuració dels diferents fluxos de còpies de seguretat i el posterior control de qualitat, optimització i correcció d'errors. L'empresa adjudicatària haurà de realitzar la migració de les polítiques existents en l'entorn actual de còpies de seguretat i/o adaptació de les mateixes a l'entorn resultant.

L'empresa adjudicatària aportarà un calendari on detalli les jornades dedicades a la instal·lació, configuració, migració, proves, optimització i correcció d'errors.

L'empresa adjudicatària lliurarà els manuals i documents necessaris on es descrigui la instal·lació, configuració i l'operació.

Es valorarà afegits de valor com ara bossa d'hores anuals i la possibilitat de gaudir de tècnic especialista durant el temps necessari per la posta en marxa i optimització de la solució presentada.

1. Configuració de la Infraestructura de Backup:
Implementació dels components necessaris per a la infraestructura de backup, incloent-hi software, hardware i connexions de xarxa.
2. Configuració de Polítiques de Backup:
Definició i configuració de les polítiques de backup, que inclouen detalls com la freqüència de les còpies, la retenció de dades, i altres paràmetres específics.

3. Xifratge i Seguretat:
Implementació de mesures de seguretat com ara el xifratge de dades per garantir la confidencialitat durant el transport i l'emmagatzematge.
4. Proves de Recuperació Inicials:
Realització de proves inicials de recuperació per garantir que el sistema de backup estigui funcionant correctament i que les dades es puguin restaurar amb èxit.

Jordi Clemente Pascual

Coordinador TIC

Barcelona, en la data de la signatura electrònica