

Expedient: EDP STE CT2023223

Entitat: Salut Terres de l'Ebre

Tipus: Mixt (subministrament i serveis)

Procediment: Obert

Tràmit: Ordinari

Objecte: Contractació de la millora de la infraestructura del CPD de l'Hospital Comarcal de Móra d'Ebre

PLEC DE PRESCRIPCIONS TÈCNIQUES

ÍNDEX

1.	OBJECTE DEL PLEC.....	3
2.	IMPLEMENTACIÓ.....	3
3.	SITUACIÓ ACTUAL	3
3.1.	SERVIDOR.....	4
3.2.	EMMAGATZEMATGE	5
3.3.	XARXA.....	5
3.4.	LLICÈNCIES	5
4.	CLÀUSULES: ESPECIFICACIONS GENERALS	5
	REQUERIMENTS GENERALS	5
	REQUERIMENTS TÈCNICS	6
5.	DETALL D'EQUIPS I SERVEIS A CONTRACTAR	6
5.1.	RENOVACIÓ TECNOLÒGICA	6
5.1.1.	HOSTS.....	6
5.1.2.	EMMAGATZEMATGE SAN CPD PRINCIPAL.....	7
5.1.3.	COMUNICACIONS.....	9
5.1.4.	SOFTWARE INFRAESTRUCTURA.....	9
5.1.5.	SOLUCIÓ DE BACKUP I RÈPLIQUES.....	10
5.2.	CONFIGURACIÓ DE L'ENTORN	13
5.3.	MANTENIMENT PREVENTIU.....	13
5.4.	RESOLUCIÓ D'INCIDÈNCIES	13
5.5.	MEMORIA TÈCNICA	15
	FORMACIÓ.....	16
6.	CONFIDENCIALITAT I PUBLICITAT DEL SERVEI	16
	COMPLIMENT AMB L'ESQUEMA NACIONAL DE SEGURETAT.....	16
7.	PROPIETAT INTEL·LECTUAL	17
8.	TERMINI D'EXECUCIÓ	17

PLEC DE PRESCRIPCIONS TÈCNIQUES PER LA CONTRACTACIÓ DE LA MILLORA DE LA INFRAESTRUCTURA DEL CPD DE L'HOSPITAL COMARCAL DE MÓRA D'EBRE

1. OBJECTE DEL PLEC

L'objectiu del document és detallar els objectius i les especificacions tècniques per a la renovació tecnològica dels Centres de Procés de dades (CPD) de Salut Terres de l'Ebre (STE) ubicats al Hospital Comarcal Móra d'Ebre (HCME), amb la finalitat de continuar assegurant tant el nivell tecnològic necessari com els mínims de qualitat de servei exigits per la Direcció de Sistemes d'Informació i Comunicació (DSIC).

Aquests objectius venen marcats per les necessitats estratègiques de STE, tot i que estan influïts per les decisions respecte als Sistemes d'Informació, l'aplicació i desenvolupament de les noves tecnologies i per les decisions estratègiques marcades per la DSIC.

En general, es tracta de substituir l'actual infraestructura de virtualització per nous servidors de virtualització basats en VMware i la millora de l'actual sistema d'emmagatzematge així com implementar un CPD de Contingència que disposa l'HCME.

Presentem a continuació una breu descripció dels objectius que es marquen en la renovació de la infraestructura:

- Adquisició de nou maquinari per substituir l'actualment existent, en obsolescència, en els nostres CPDs.
- Disposar d'un contracte de manteniment preventiu i garantia dels nous CPD i del seu entorn a nivell hardware i software durant la durada del present contracte a partir de la data de la recepció de la instal·lació efectuada. Incloent una bossa d'hores per servei d'enginyeria i manteniment correctiu.
- Formació per als tècnics locals en l'ús de la nova plataforma, el tractament del primer nivell i incidències més bàsiques i la gestió de possibles incidències més greus al suport.

2. IMPLEMENTACIÓ

Per la correcta implementació es realitzaran totes les tasques necessàries per deixar en producció el nou sistema al CPD del HCME que indicarà la DSIC. Per aquest motiu s'haurà de posar en producció el maquinari i programari que es demana al plec, així com el maquinari i programari existents, que es detallen als subapartats 3.1, 3.2, 3.3 i 3.4.

3. SITUACIÓ ACTUAL

Es disposen de dos CPDs al HCME:

- CPD1: Planta 0 : CPD principal.
- CPD2: Planta 2 : CPD contingència.

Es disposa d'una solució actual de virtualització amb VMware, ubicada al CPD2, desfasada que serà retirada un cop es migrin tots els serveis a la nova plataforma. Aquesta és:

Servidor	Descripció
VMWARE-HCME01	Servidor de la Granja Vmware, Bull Novascale R460F3 65GB RAM
VMWARE-HCME02	Servidor de la Granja Vmware, Bull Novascale R460F3 65GB RAM
2 x Cabina NETAPP	Cada una amb 11 discs de 600GB SAS 10Kr pm RAID 6, i 1 disc spare

La granja de vmware es compon de 2 servidors connectats a les dues cabines Netapp. Estan activades les funcionalitats de HA (permet que les màquines s'arranquin automàticament en un node si l'altre cau), DRS (Distribueix la càrrega i mou màquines en calent segons us dels servidors).

La cabina Netapp publica per CIFS les carpetes compartides, fent de servidor de fitxers. El volum d'aquest és de 1,6TB.

Hi ha també una carpeta compartida per a fer els backups, de 300GB.

Les màquines virtuals que s'hauran de migrar a la nova plataforma seran les següents (a banda d'alguna que s'hagi pogut crear les darreres setmanes):

VM	CPU	Memory	Provisioned	CPD2	Cluster
9TREELOGIC	4	4.096	54.110	Mora	Cluster_HCME
BDMORA	4	8.192	562.592	Mora	Cluster_HCME
MORADC	2	2.048	78.170	Mora	Cluster_HCME
MIRTHMINT	4	8.192	108.090	Mora	Cluster_HCME
MIRTHCME2	1	2.048	27.090	Mora	Cluster_HCME
CONTINGENCIA	2	4.096	84.210	Mora	Cluster_HCME
TELEICTUS	1	2.048	42.090	Mora	Cluster_HCME
TSMORA12	4	4.096	240.192	Mora	Cluster_HCME
WEBMORA32	2	4.096	64.620	Mora	Cluster_HCME
CONTROL DE PRESENCIA	4	8.192	92.180	Mora	Cluster_HCME
PALEX	8	8.192	188.110	Mora	Cluster_HCME
STE	1	2.048	32.090	Mora	Cluster_HCME
SFTPHCME	1	1.024	33.090	Mora	Cluster_HCME
VDPHCME	4	4.096	972.090	Mora	Cluster_HCME
WEBMINT	4	8.192	216.100	Mora	Cluster_HCME

3.1. SERVIDOR

Es disposa d'un servidor nou que haurà de ser utilitzat i configurat pel proveïdor com a vCenter i gestió de Backups. Es tracta de:

- HPE ProLiant DL160 Gen10
 - Intel Xeon silver 4208
 - 2 x 16 GB RAM
 - 2 x 480 SSD SATA mixed Use

- 2 x 500W RP
- 4 x 1GbEthernet
- 1x 1Gb ILO Port + license
- 5 years Tech Care Essentials (24x7)

3.2. EMMAGATZEMATGE

Es disposa d'una cabina que haurà de ser utilitzada i configurada pel proveïdor com a repositori de Backups. Es tracta de:

- Synology RackStation RS820RP+
- 3 discs durs de 8TB Seagate NAS compatibles (per RAID5).

3.3. XARXA

Es disposa d'aparells de xarxa que hauran de ser utilitzats i configurats pel proveïdor. Es tracta de:

- 2 HPE Aruba IOn 1960 12XT

Es disposa d'un core CISCO en clúster (stackwyse) en HA amb connectivitat a 40G redundada entre els dos equips que estan repartits cadascun en un dels CPDs.

Cadascun d'ells son el model C9500-48Y4C amb les següents característiques (per node):

- 48 ports 1/10/25G
- 4 ports 40/100 QSFP+ Uplink
- Switching capacity: up to 3,2 Tbps
- Forwarding capacity: up to 1 Bpps



3.4. LLICÈNCIES

Es disposa de llicències de VMware útil que haurà de ser utilitzada i configurada pel proveïdor. Es tracta de:

- Llicència VMWare Essentials Kit Plus amb suport vigent fins 2027

4. CLÀUSULES: ESPECIFICACIONS GENERALS

Requeriments generals

Els licitadors presentaran una Proposta Tècnica, que haurà de complir les especificacions descrites en el present plec. Les ofertes hauran d'incloure tota la documentació relativa als equips, sistemes i serveis oferts, per tal que es pugui valorar adequadament cadascuna de les propostes, així com el procés de migració de la situació actual a la nova.

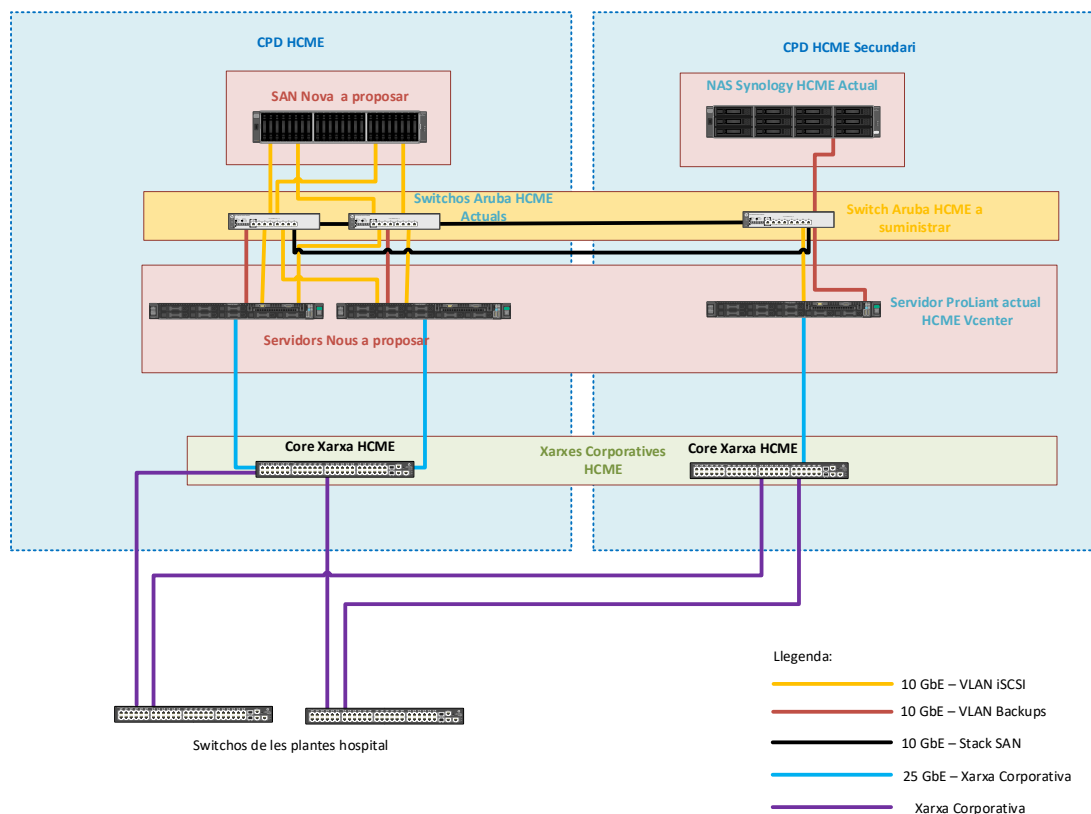
Tots els següents requeriments són mínims, per tal de què els licitadors puguin dissenyar la seva solució tècnica.

Els preus proposats per a la provisió i posterior gestió dels sistemes i serveis sol·licitats han d'incloure tots els possibles elements de cost. El HCME no assumirà cap cost extra associat a la implantació dels serveis contractats.

El HCME no té previst cap tipus de dedicació del seu personal en tasques associades a la posada en marxa, exceptuant les tasques de coordinació de l'execució del projecte.

Requeriments Tècnics

El HCME requereix d'una solució integral de de servidors, emmagatzematge i xarxa SAN que assoleixi l'objectiu descrit en el present PPT i compleixi tots els requeriments tècnics descrits en aquest apartat. L'esquema simplificat de la solució a implementar és el següent:



L'objectiu es que en el Segon CPD en un curt termini es pugui incorporar un tercer Servidor de característiques similars als 2 principals per formar un clúster HA de VMWare de 3 nodes ESXi i/o una cabina de discs SAN al segon CPD per poder disposar d'un Disaster Recovery entre CPDs.

5. DETALL D'EQUIPS I SERVEIS A CONTRACTAR

5.1. RENOVACIÓ TECNOLÒGICA

5.1.1. HOSTS

Els hosts del CPD Principal del HCME seran com a mínim 2, i cada host disposarà de les següents característiques tècniques o superiors:

- Processador : 1x Intel Xeon 4314 (16 nuclis de 2,4 GHz).
- Memòria RAM : 256 Gb DDR4 en mòduls de 64 Gb.

- 2 x 500 Gb Boot disk
- 2 x 10 Gb Base T o SFP+ (Xarxa iscsi SAN)
- 2 x 10/25 Gb SFP28 (Xarxa LAN corporativa).
- Gestió remota independent amb connexió dedicada Ethernet amb la corresponent llicència. Gestió sense agent ni instal·lació d'aplicacions, només via navegador. Mapeig de ISO o DVD remota.
- 2 x fonts d'alimentació redundants instal·lables/substituïbles en calent d'un mínim de 800W.
- Kit d'instal·lació per rack.
- 5 anys de garantia i suport de tot l'equipament in-situ per part del fabricant segons criteris detallats en el 5.4 d'aquest PPT.

El tercer Host que ja disposa el HCME caldrà ser configurat per allotjar vCenter i Servidor de Backups, configurant-lo per a que realitzi els backups contra el NAS Synology que disposa el HCME. Tant Servidor com NAS, com el Switch ARUBA

Tots Els servidors haurà de proporcionar una arrel de confiança de silici a nivell de hardware (Silicon root of Trust), creant una empremta digital amb el propi silici que permeti garantir que el servidor no arrancarà amb un firmware que no coincideixi amb l'empremta.

Haurà de mantenir un repositori de versions de firmware i divers que permeti restablir nivells de firmware segurs o aplicar pegats en cas de risc potencial. També haurà d'existir la possibilitat de restaurar directament al nivell de firmware carregat i testat de fabrica.

El sistema, durant la seva operació, haurà de realitzar una validació periòdica dels nivells de firmware cercant possible codi compromès. En cas de que es produeixi una infracció, es produirà una restauració automàtica a un estat de confiança conegut.

El servidor haurà d'incorporar la suite criptogràfica CNSA per mantenir la protecció de la informació mes confidencial que allotgi.

El servidor haurà d'implementar un sistema d'intel·ligència artificial al núvol per a aprenentatge automàtic amb anàlisi predictiu i supervisió de l'estat dels sistemes per optimitzar el seu rendiment, prevenir i evitar problemes. Aquesta solució haurà de com a mínim disposar de les següents funcionalitats:

- Recol·lecció automàtica de telemetria i informació de sensors de cada servidor
- Anàlisi predictiu de cada component
- Anàlisi de l'estat de seguretat de cada servidor
- Inventari de tots els equips, amb capacitats de visualització de la seva salut i garantia.
- Notificacions de nous firmwares i divers disponibles, així com notificacions de l'estat de compliment dels equips amb els nivells establerts.
- Creació de casos de suport manual i automàtica.

5.1.2. Emmagatzematge SAN CPD Principal

La cabina SAN del CPD Principal cabina disposarà de les següents característiques tècniques o superiors:

- 2 U d'alçada enracables en armaris de 19" standards
- 24 bahies SFF (2,5") disponibles

- 2 discos de 1,96 TB SSD SATA SFF (2,5") Hot Plug a mode de Flash Cache ampliables sense canviar els existents
- 6 discos de 1,8 TB SAS a 10k rpm SFF (2,5") Hot Plug
- 2 controladores ISCSI.
- 5 Anys de Suport i manteniment correctiu del Fabricant característiques detallades en el 5.4 d'aquest PPT.

Sistema d'emmagatzematge extern de canal de fibra amb doble ISCSI actiu – controladors RAID actius amb un mínim de 12 GB de memòria cau per controlador.

L'emmagatzematge ofert tindrà suport opcional per a la memòria cau basada en SSD / Flash. L'emmagatzematge ofert admetrà almenys 8 TB de memòria cau Flash. El proveïdor oferirà com a mínim un nombre dual de disc SSD de 1.92 TB per a la memòria cau flash.

La memòria cau Flash oferta s'ajustarà per a operacions de lectura aleatòria i romandrà activada fins i tot a menys del 70% de la càrrega mitjana de treball de lectura aleatòria.

El sistema d'emmagatzematge ofert es subministrarà amb un mínim de 2x 10Gb ISCSI Ports per controlador

Es farà una còpia de seguretat de la memòria cau (ja sigui mitjançant bateria, condensadors o qualsevol altra tecnologia equivalent) per temps indefinit o almenys de 5 a 7 anys de temps.

Hauria de suportar l'expansió d'endolls calents i la substitució de discs durs, controladors redundants, ventiladors i fonts d'alimentació.

L'emmagatzematge ofert serà compatible amb Raid 1, Raid 10, Raid 5 i Raid 6. L'avitallament prim serà compatible amb tots els conjunts de raid, així com amb la memòria cau Flash.

El subsistema d'emmagatzematge ofert ha de suportar un mínim de 512 unitats lògiques amb suport de mida LUN superior a 100 TB a nivell de controlador d'emmagatzematge.

El sistema d'emmagatzematge admetrà unitats SAS empresarials, SSD i unitats SAS de línia propera / unitats de 7.2 k rpm.

La matriu d'emmagatzematge admetrà almenys 240 unitats SAS SFF empresarials.

L'emmagatzematge ofert s'oferirà i es configurarà amb capacitat de virtualització de manera que un volum donat es pugui ratllar a través de tots els eixos d'un tipus d'unitat donat dins d'una agrupació de discs donada. El grup de discos donarà suport a tots els conjunts de raids llistats de Raid 1, Raid 10, Raid 5 i Raid 6.

El processament de raids es descarregarà a un ASIC dedicat en lloc de CPU. En cas que el proveïdor no ho admeti, el proveïdor s'ha d'assegurar que la memòria cau addicional de 12 GB per controlador estigui configurada per compensar la càrrega de treball de processament de raids.

L'emmagatzematge ofert també es llicenciarà per a la classificació de dades Sub-Lun en temps real a través de diferents tipus d'unitats dins d'un grup determinat com SSD, SAS, NL-SAS, etc. S'oferirà llicència per a la mateixa per a la capacitat màxima suportada de la matriu.

L'emmagatzematge ofert ha de tenir un programari de gestió de rendiment integrat i el tauler de configuració mostrarà el rendiment general de IOPS i MB/seg.

El subsistema d'emmagatzematge ofert tindrà suport Snapshot i Clon basat en controladors. Al subsistema d'emmagatzematge se li subministraran llicències per a 512 instantànies.

El sistema d'emmagatzematge ofert ha de suportar un mínim de 512 números d'instantànies i 128 números de còpies de volum / clonació.

La matriu d'emmagatzematge hauria de tenir la capacitat de configurar discs d'intercanvi en calent i discs de recanvi distribuïts globals, així com disc de recanvi dedicat als conjunts raid.

El subsistema d'emmagatzematge ofert admetrà funcions de recuperació de desastres, com ara la replicació a la ubicació de DR. Es proporcionaran llicències per a la capacitat màxima suportada de la matriu.

El subsistema d'emmagatzematge ofert admetrà la replicació a diverses matrius d'emmagatzematge de la mateixa família en mode fan-out. S'admetrà com a mínim el mode 1:4.

La matriu d'emmagatzematge oferta tindrà un connector per a VMware VCenter, el centre del sistema de Microsoft, així com les API vStorage (VAAI) per a la integració de matrius.

Hauria de ser compatible amb Windows servidor 2016 / 2019 / 2022, Linux, VMware, etc.

L'emmagatzematge ofert haurà d'haver indicat un punt de referència per al rendiment de més de 250,000 en el Raid 5 utilitzant unitats adequades a la mida del bloc de 8K. El venedor haurà d'acreditar-ho documentalment.

Per a evitar problemes d'incompatibilitats, agilitzar el suport de tercers i garantir la compatibilitat entre components, s'exigeix que Servidors i Cabina siguin del mateix fabricant. Tots els components han de ser compatibles i certificats per a ser utilitzats amb l'hipervisor VMWare ESXi en la seva versió 7.0 o superior (en l'update mes nou disponible) i Veeam Backup and Replication v12 (en la revisió mes nova disponible) ja que es el software que disposa en propietat actualment el HCME i es el que es seguirà mantenint en la nova infraestructura.

5.1.3. COMUNICACIONS

- 1x Switch 12 x 10GBaseT + 4 x SFP+ per la xarxa SAN CPD secundari
- 5 anys de garantia, manteniment preventiu i suport de tot l'equipament in-situ per part del fabricant amb cobertura 24x7 i temps de resposta màxim de 4h durant la durada del contracte.
 - Tot el Cablejat i/o transceivers per intercomunicar la infraestructura proposada (cables RJ45, cables SFP+ o SFP28, cables electricitat, etc).

5.1.4. SOFTWARE INFRAESTRUCTURA

S'aprofitaran les llicències disponibles:

- VMware Essentials Kit Plus:
 - 1 VCenter Server 7 Standard
 - 3 Vsphere 7 Standard (2 sockets)

5.1.5. SOLUCIÓ DE BACKUP I RÈPLIQUES

Disposar d'un bon sistema de Còpies de Seguretat és vital per a garantir la continuïtat dels serveis del HCME, és per això que es requerirà d'una solució completa amb requisits exigents.

La solució de Còpies de seguretat estarà completament llicenciada per a tota la durada del contracte, no requerint de llicenciament addicional per molt que creixi la càrrega de treball (Servidors i emmagatzematge) dels Sistemes del HCME.

La solució ha de ser capaç de proporcionar una protecció completa de la infraestructura (virtual, física, cloud), inclosa una recuperació davant desastres i capacitats de protecció contínua d'entorns virtuals crítics.

La solució de còpia de seguretat ha de funcionar amb la infraestructura virtual de VMware basada en la versió 6.X, 7.0 i 8.0 així com VMWare Cloud Foundation (VCF), Google Cloud VMWare Engine, Microsoft Azure VMWare Solution, VMware Cloud en AWS, Oracle Cloud VMWare Solution, VMware Cloud on Dell; Microsoft Hyper-V Hyper-V 2012, Hyper-V 2012 R2, Hyper-V 2016, Hyper-V 2019 i Hyper-V 2022; Nutanix Acropolis 5.5x fins a 5.19x (incloent CE) i Red Hat Enterprise Virtualization.

La solució ha d'aportar desplegament centralitzat d'agents per als següents sistemes físics Windows, Linux, així com gestió centralitzada per als sistemes anteriors i sistemes UNIX (Almenys Solaris i AIX) i Mac OS.

La solució ha d'admetre hosts administrats per VMware vCenter Server i hosts independents.

La solució ha d'incorporar la còpia de seguretat a nivell d'imatge de màquines virtuals, la replicació basada en host de màquines virtuals i la protecció contínua de màquines virtuals VMWare (amb un RPO menor de 15 segons) des de la consola única sense cost addicional.

Les còpies s'hauran de realitzar en un format comú que permeti la portabilitat, de les càrregues entre diferents plataformes (almenys entre Azure, AWS, VMware, Hiper-V, Nutanix AHV) a través d'una plataforma de gestió unificada de forma automàtica.

La solució ha de ser sense agent i ser capaç de realitzar còpies de seguretat de servidors virtuals, inclosos sistemes operatius i aplicacions, per a entorns virtuals que executin VMware, Hyper-V, AHV i/o RHEV.

La solució ha d'aportar funcionalitats de protecció de màquines físiques o virtuals en un procés de còpia únic facilitant la recuperació a qualsevol nivell. Recuperació tradicional d'un servidor complet, recuperació d'un fitxer d'una VM, fitxer o carpetes o aplicacions.

La solució ha de proporcionar agents per a servidors físics. (Almenys Windows, Linux, Oracle Solaris i MacOS)

La solució ha d'admetre qualsevol tipus d'emmagatzematge basat en disc (DAS/NAS/SAN).

La solució ha de proporcionar un format d'arxiu de còpia de seguretat autosuficient per

evitar el risc de pèrdua de catàleg.

La solució ha de ser escalable i proporcionar una manera fàcil i rendible d' adherir-se al creixement de la infraestructura sense afectar les finestres de backup.

La solució ha d' admetre diverses consoles de còpia de seguretat i proporcionar un punt central per a gestió de múltiples entorns.

La solució ha de permetre l' administració de còpies natives d' entorns Azure VM, Amazon EC2 i Google CE des d' una consola única.

La solució ha de tenir capacitat d'integració amb Oracle RMAN , que permetin gestionar els processos de backup i restauració de B.D. Oracle a través d'aquest interfície.

La solució ha de tenir capacitat d'integració amb SQL Server Management Studio, de manera que permetin als administradors de bases de dades gestionar els processos de backup i restauració (incloent-hi transaction logs) de B.D. Microsoft SQL Server a través d'aquest interfície.

La solució ha de comptar amb interfícies de backup de SAP certificats per al suport de SAP-HANA i SAP sobre Oracle.

La solució ha de proporcionar integració avançada amb dispositius d'emmagatzematge primari per realitzar backups i replicacions directament des de les instantànies d'emmagatzematge (Storage Snapshot) per tal d'augmentar els RPO i, alhora, reduir l'impacte en la producció. (s'aplica a múltiples proveïdors d'emmagatzematge)

La solució haurà de disposar de capacitats de replicació de VMs destinada a escenaris de disaster recovery i recuperació instantània a les instal·lacions locals i restauració directa al núvol.

La solució haurà d' oferir una funció d' acceleració WAN integrada per permetre una replicació més ràpida de la còpia de còpies de seguretat de màquines virtuals.

La solució ha de complir amb un temps objectiu de restauració d' una VM, un disc d' una VM o una màquina física inferior als 10 minuts, amb independència del volum de dades associades al servei involucrat.

La solució ha de ser capaç de realitzar automàticament còpies de seguretat de totes les configuracions i proporcionar capacitats de restauració senzilles per a la infraestructura de còpia de seguretat en cas d' error.

La solució ha de ser capaç de proporcionar mecanismes de seguiment de blocs de canvis almenys en Hyper-V, VMWare i Red Hat Virtualization el que permet còpies de seguretat incrementals més ràpides.

La solució ha d'assegurar la immutabilitat (WORM) de les còpies de seguretat emmagatzemades en qualsevol repositori de disc, gestionat per un servidor de propòsit general amb sistema operatiu Linux (x64), impedit l'esborrat o modificació (accidental o malintencionat) de les mateixes abans del seu període d'expiració.

La solució ha d' admetre el processament paral·lel de la còpia de seguretat de màquines

virtuals per reduir la finestra de còpia de seguretat.

La solució ha de permetre l'execució de scripts de còpia de seguretat previs i posteriors.

La solució haurà de ser capaç de restaurar instantàniament qualsevol màquina que executi qualsevol sistema operatiu de qualsevol mida directament des de la còpia de seguretat des de qualsevol punt de restauració disponible en la còpia de seguretat basada en disc.

La solució ha d'admetre la reversió ràpida de màquines virtuals mitjançant CBT.

La solució haurà d'admetre la configuració de la màquina virtual com a part del procés de restauració així com la restauració del disc dur virtual.

La solució haurà de proporcionar una manera fàcil de restaurar l'arxiu de SO convidat, inclosos, entre d'altres, Windows, Linux, Unix i BSD.

La solució ha de proporcionar capacitats de restauració granular directament des de la còpia de seguretat per a totes les aplicacions virtualitzades sense necessitat de realitzar còpies de seguretat addicionals basades en agents. Aquesta funcionalitat ha d'incloure almenys Active Directory, MS SQL, Oracle, PostgreSQL, MS Exchange i MS SharePoint.

La solució ha de proporcionar mecanismes de publicació de bases de dades SQL Server (procedents de servidors físics o virtuals, incloent-hi clusters), en mode lectura/escriptura des de qualsevol repositori de backup a disc al seu servidor d'origen o qualsevol altre, que permetin un accés i posada en marxa en menys de 15 minuts, a qualsevol punt en el temps.

La solució ha de proporcionar mecanismes de publicació de bases de dades Oracle (procedents de servidors virtuals), en mode lectura/escriptura des de qualsevol repositori de backup a disc al seu servidor d'origen o qualsevol altre, que permetin un accés i posada en marxa d'aquestes en menys de 15 minuts, a qualsevol punt en el temps.

La solució ha de proporcionar mecanismes de publicació de repositoris NAS (via SMB(NFS) en des de qualsevol repositori de backup a disc, de manera que davant d'un incident proporcioni accés de lectura i escriptura (SMB) i almenys lectura en NFS a tots els arxius en menys de 15 minuts.

La solució ha de proporcionar mecanismes de prova i verificacions automatitzades de cada còpia de seguretat o rèplica per garantir la capacitat de recuperació en cas d'error de producció. La verificació ha d'incloure arxius de màquina virtual, sistema operatiu i aplicacions, incloses proves personalitzades mitjançant scripts.

La solució ha de ser capaç de crear entorns de prova executant una o més màquines virtuals directament des de còpies de seguretat o rèpliques dins d'un entorn aïllat per a l'ús de proves, desenvolupament o formació sense necessitat d'invertir en computació o emmagatzematge addicionals.

La solució ha de poder comprovar que una còpia de seguretat de màquina virtual està lliure de virus abans de restaurar-la en l'entorn de producció.

La solució ha de ser capaç d'organitzar i executar scripts de neteja de compliment del RGPD en una màquina virtual abans de restaurar-la en un entorn de producció.

La solució ha d'estar certificada per alguna entitat externa per al compliment de la normativa SEC (Rule 17a-4(f)), FINRA (Rule 4511(c)) i CTFC (Rule 1.31 (c)-(d)) en relació amb la gravació i emmagatzematge no re-escribible i no esborrable de registres electrònics. En qualsevol repositori de disc, gestionat per un servidor de propòsit general amb sistema operatiu Linux (x64).

5.2. CONFIGURACIÓ DE L'ENTORN

L'empresa es compromet a realitzar les següents tasques:

- Instal·lació i configuració del nou hardware als dos CPDs del HCME, seguint les indicacions dels tècnics de la DISC.
- Instal·lació i configuració del hardware existent, detallat als subapartats 3.1, 3.2, 3.3 i 3.4, als dos CPDs del HCME, seguint les indicacions dels tècnics de la DISC.
- Acoblament dels diferents dispositius, i actualització del firmware dels mateixos a la data d'instal·lació.
- Muntatge dels equips al rack i cablejat de totes les connexions, configuració i posada en servei dels equips. Tant els nous com els existents.
- Proves del sistema.
- Configuració de la plataforma de virtualització VMware (incloent HA) vCenter, vSphere i actualització de tots els elements a la última versió possible.
- Realització de proves de Funcionament prèvies al "pas a producció".
- Migració de les màquines virtuals existents al nou entorn.
- Configuració de Còpies de Seguretat i proves de restauració

5.3. MANTENIMENT PREVENTIU

Aquest abastarà tot el termini de garantia (5 anys) de l'apartat número 5.1.1 del present plec de prescripcions tècniques. Com a mínim, es requerirà presència al HCME un cop cada **12 mesos** d'un dels tècnics qualificats i certificats per a la realització de les tasques de manteniment de la infraestructura de sistemes, que inclouran com a mínim:

- Actualitzacions de firmware dels Servidors, cabina i xarxa.
- Actualitzacions del VMWare (Esxi i vCenter)
- Actualitzacions de la consola de Backup.
- Manteniment de l'inventari d'actius del CPD.
- Manteniment de documentació del sistema.

En cas de detecció d'alguna vulnerabilitat crítica que afectes a algun d'aquests components, es planificarà una intervenció urgent per actualitzar i aplicar els "parxes" de seguretat corresponents.

5.4. RESOLUCIÓ D'INCIDÈNCIES

L'empresa adjudicatària realitzarà el servei de resolució d'incidències i destinar totes el temps necessari i sense límit per a garantir la continuïtat del servei del HCME. Aquestes incidències són:

- Resolució d'incidències del sistema (VMware ESXi, Backup, Windows Server,

Directori Actiu, DNS, DHCP, Xarxa SAN, Cabina Discs, etc).

Es defineix com a horari laboral del servei de **8:00 fins a els 18:00** de dilluns a divendres.

Per a la resolució d'incidències es requeriran els següents nivells de serveis:

Es defineix com a "temps de resposta" com el temps transcorregut des de que es rep l'avís d'una incidència fins a que els tècnics de l'Adjudicatari inicien les tasques de resolució de la incidència. El horari de resolució d'incidències serà, en general, l'horari laboral.

Es defineix com a "temps de resolució" el temps transcorregut des de que es notifica la incidència fins que el tècnic aporta la solució al usuari i resol el problema en sí.

Les incidències es classificaran segons l'acord a la seva prioritat en:

Prioritat ALTA

Els casos de prioritat Alta hauran de respondre's en un temps màxim de 60 minuts laborals i resoldre's en un temps màxim de 8 hores laborables sempre que no siguin incidències de tercer nivell i impliqui ser elevada a tercers (garanties de fabricants, proveïdors...).

- Una incidència que afecta als llocs de treball que afectin directament als Serveis Crítics.
- Una incidència que afecta als Servidors de producció o comunicacions a aquests.
- Un incidència que impacti significativament en el negoci.
- Una incidència que no permeti treballar als usuaris.

Prioritat MITJA

Els casos de prioritat Mitja hauran de respondre's en un temps màxim de 4 hores laborables i resoldre's en un temps màxim del següent dia laborable sempre que no siguin incidències de tercer nivell i impliqui ser elevada a tercers (garanties de fabricants, proveïdors...).

- Una incidència que impacti mínimament en el negoci
- Una incidència que causi mal funcionament dels usuaris
- Una incidència que provoqui que les tasques dels usuaris es ralentitzin significativament.

Prioritat BAIXA

Els casos de prioritat Baixa hauran de respondre's en un temps màxim del següent dia laborables i resoldre's en un temps màxim de 5 dies laborables sempre que no siguin incidències de tercer nivell i impliqui ser elevada a tercers (garanties de fabricants, proveïdors...).

- Una sol·licitud de subministrament
- Una incidència que no impacti en el negoci
- Una incidència que no impacti significativament en l'usuari
- Un requeriment d'actualització de Software o maquinari
- Un requeriment d'informació o formació a l'usuari.
- La resta d'incidències
-

Per evitar l'efecte d'inanició d'incidències (que una incidència mai sigui atesa per que sempre hi hagin incidències de major prioritat), quan una incidència no hagi sigut atesa en tres vegades el temps establert en el SLA, la seva prioritat pujarà automàticament al

següent nivell d'urgència. Les incidències de prioritat baixa que no hagin estat ateses en 10 dies, pujaran a prioritat normal, i així consecutivament.

L'empresa adjudicatària disposarà d'un portal de suport (ServiceDesk) i gestió d'incidències on el responsable TIC del HCME podrà reportar i gestionar les diferents incidències del sistema detectades. En tot moment el responsable TIC podrà accedir a l'eina per visualitzar les incidències obertes amb l'adjudicatari i veure l'estat d'aquesta, i sobretot, que l'eina disposi dels indicadors suficients per a la correcta avaluació dels SLAs establerts en aquest punt. Les incidències podran ser reportades mitjançant correu electrònic, portal de suport o telefònicament, i sempre quedaran reflectides al portal de suport. L'eina guardarà un històric de tots els tickets oberts pel HCME. Aquest portal de suport també haurà de tenir informació sobre l'actual contracte i altres possibles contractes que es tinguin vigents entre les dues entitats.

5.5. MEMORIA TÈCNICA

Les empreses licitadores presentaran una memòria tècnica amb Pla d'Implementació que contindrà un estudi de la configuració i posada en marxa, planificació de les fases i terminis, detall de l'organització de les actuacions a realitzar i del seu seguiment, per dur a terme l'execució del projecte.

En aquest document caldrà detallar:

- a) Descripció detallada del maquinari proposat.
- b) Descripció detallada de la solució proposada (a nivell d'arquitectura amb diagrames, dibuixos, esquemes, etc.).
- c) Descripció detallada de les funcionalitats de la solució proposada.
- d) Pla d'implementació:
 - a. Fases del projecte (indicar la duració estimada de cadascuna d'aquestes fases).
 - b. Tasques a realitzar en cadascuna de les fases.
 - c. Personal tècnic assignat per part del licitador, degudament certificat.
 - d. Personal tècnic del HCME que es requereix en cadascuna de les fases.
- e) Garanties i suport del fabricant.
- f) Pla de Formació
 - a. Descripció detallada del contingut
 - b. Hores
 - c. Entregables
- g) Serveis de manteniment : Updates/upgrades del software i firmware de tots els equips entregats com a mínim 1 cop l'any.
- h) Entrega de tota la documentació del projecte (proves de resiliència, esquemes de connexions, procediment de DR, etc) a la DSIC del HCME.
- i) L'empresa adjudicatària oferirà un servei de suport de segon nivell de sistemes de la DSIC del HCME accessible les 24 hores del dia de qualsevol dia de la setmana (24x7) i durant la vigència del contracte associat al present concurs.

Es comprovarà el contingut d'aquest document d'acord amb les prescripcions tècniques requerides, tenint en compte, a més, el menor impacte i interrupcions del treball diari dels empleats del HCME.

Tots els treballs d'instal·lació i muntatge dels equips especificats en el present projecte aniran inclosos en el preu de l'oferta presentada i seran executats per l'empresa adjudicatària. Els treballs inclouran la configuració de tota la instal·lació segons l'esquema funcional detallat.

Tots els treballs necessaris de migració de les dades actuals a la nova configuració especificada en el present projecte estaran inclosos en el preu de l'oferta i seran executats per l'empresa adjudicatària en coordinació amb la DSIC de la GTTE.

Formació

Hi haurà una formació bàsica i obligatòria per a l'administració del sistema que haurà de ser presencial. Els professors que impartiran aquests cursos seran designats per l'empresa adjudicatària.

L'empresa adjudicatària també durà a terme la formació necessària sobre les actualitzacions que s'esdevinguin a nivell de software a la instal·lació durant el període de vigència del contracte.

- Pla de formació en sistemes implementats en la nova infraestructura per a tot l'equip de sistemes de la DSIC del HCME.
- Pla de formació multidisciplinària de 2 jornades anuals per a tot l'equip de sistemes de la DSIC del HCME.

6. CONFIDENCIALITAT I PUBLICITAT DEL SERVEI

L'adjudicatari està obligat a guardar secret respecte les dades o informació prèvia que no essent públics o notoris estiguin relacionats amb l'objecte del contracte. L'adjudicatari subscriurà un contracte d'encarregat de tractament de dades personals per poder garantir aquesta confidencialitat.

Qualsevol comunicat de premsa o inserció als mitjans de comunicació que l'adjudicatari realitzi referent al servei que presta al HCME serà aprovat prèviament pel propi HCME.

COMPLIMENT AMB L'ESQUEMA NACIONAL DE SEGURETAT

L'article 2 del vigent Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, disposa que els plecs de prescripcions administratives o tècniques dels contractes que celebrin les entitats del sector públic incloses en l'àmbit d'aplicació del reial decret de l'ENS contemplaran tots aquells requisits necessaris per assegurar la conformitat amb el mateix dels sistemes d'informació en els quals se sustentin els serveis prestats pels contractistes, tals com la presentació de les corresponents Declaracions o Certificacions de Conformitat amb l' ENS. Aquesta cautela s' estendrà també a la cadena de subministrament d' aquests contractistes, en la mesura que sigui necessari i d' acord amb els resultats de la corresponent anàlisi de riscos".

En conseqüència, l'HCME, considera necessari que els proveïdors que vagin a concórrer a la licitació hauran d' estar en condicions d' exhibir la corresponent Certificació de Conformitat amb l' Esquema Nacional de Seguretat.

Així doncs, en base a l'anterior, i a l'anàlisi dels riscos als quals estan exposats els subministraments i serveis objecte de la licitació, L'HCME estableix com a necessari que l'Empresa Adjudicatària haurà d'estar en condicions d'exhibir la corresponent Declaració o Certificació de Conformitat amb l'Esquema Nacional de Seguretat, per a la categoria de seguretat MITJA, o superior, dels sistemes que intervinguin en la prestació dels serveis indicats, així com mantenir la conformitat en vigor durant la vigència del contracte. Aquest certificat de conformitat amb l'ENS s'entén que ha d'abastar en el seu abast, com a mínim, l'àmbit objecte de la contractació.

En el supòsit que l'adjudicatari no pogués mantenir la conformitat amb l'ENS durant la vigència del contracte -per pèrdua, retirada o suspensió de la Certificació de Conformitat o impossibilitat de mantenir la Declaració de Conformitat-, haurà de comunicar aquesta circumstància, de forma immediata i sense dilació indeguda, a l'HCME, qui considerarà l'impacte d'aquesta circumstància en la prestació objecte del contracte.

7. PROPIETAT INTEL·LECTUAL

Tota la documentació que es generi al llarg del servei és propietat exclusiva del HCME. L'empresa adjudicatària no podrà fer-la servir per altres finalitats sense consentiment exprés del HCME.

8. TERMINI D'EXECUCIÓ

El termini màxim de lliurament i implantació de la solució serà de 2 mesos a partir de l'adjudicació del contracte. El HCME i l'empresa adjudicatària pactaran la planificació definitiva.

Tot el material es lliurarà a les dependències del HCME. Els ports aniran a càrrec de l'empresa adjudicatària.

La finalització de la instal·lació serà efectiva en el moment en que el HCME en certifiqui l'acceptació.

Robert Verge Monclús,
Cap d'Unitat de Sistemes de la Direcció de
Sistemes d'Informació i Comunicació
de l'ICS