PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SERVEI DE MANTENIMENT DEL CLÚSTER DE VIRTUALITZACIÓ DEL CONSORCI SOCIOSANITARI DE VILAFRANCA DEL PENEDÈS

EXPEDIENT CSSV 36-26

ÍNDEX

1. OBJECTE DEL PLEC 3

2. ANTECEDENTS 4

3. SITUACIÓ ACTUAL 4

4. MANTENIMENT DE LA INFRAESTRUCTURA DE VIRTUALITZACIÓ 5

4.1. MANTENIMENT DE LA INFRAESTRUCTURA DE VIRTUALITZACIÓ 5

4.1.1. MANTENIMENT PROACTIU 5

4.1.2. SERVEI DE SUPORT 24X7 5

4.1.3. RESOLUCIÓ D'INCIDÈNCIES 5

4.2. PLATAFORMA DE VIRTUALITZACIÓ 8

4.3. SISTEMA DE CÒPIES DE SEGURETAT 8

4.4. SISTEMA DE CÒPIES DE SEGURETAT IMMUTABLES 8

4.5. SERVEI DE VIGILÀNCIA DE LA SEGURETAT 8

4.6. SERVEI DE MONITORITZACIÓ 9

5. REQUISITS TÈCNICS OBLIGATÒRIS 9

6. CONFIDENCIALITAT I PUBLICITAT DEL SERVEI 10

7. PROPIETAT INTEL·LECTUAL 10

8. RESPONSABLE DEL CONTRACTE 10

1. OBJECTE DEL PLEC

Aquest plec té per objecte la regulació de la contractació del servei de manteniment de la infraestructura de virtualització del Consorci Sociosanitari de Vilafranca del Penedès (en endavant, CSSV), per garantir el correcte funcionament, reforçar la seguretat de la informació, la protecció davant ciberamenaces i la continuïtat dels serveis TIC corporatius.

La infraestructura de virtualització constitueix la plataforma sobre la qual s'executen els principals sistemes d'informació del CSSV, incloent-hi les aplicacions assistencials, administratives, bases de dades, serveis de fitxers, sistemes d'autenticació, còpies de seguretat i altres serveis essencials per al funcionament de l'organització.

La indisponibilitat d'aquesta infraestructura podria afectar de manera directa la prestació dels serveis assistencials i administratius.

A més, el context actual de ciberseguretat ha experimentat una evolució molt significativa durant els darrers anys, amb un increment dels atacs dirigits contra organitzacions sanitàries i administracions públiques.

Per aquest motiu resulta necessari reforçar la infraestructura existent mitjançant:

- El manteniment dels equips que formen el clúster de virtualització.
- La renovació de les llicències dels diferents fabricants.
- La continuïtat del sistema de còpies de seguretat local.
- La continuïtat del servei de còpies de seguretat al núvol.
- La incorporació d'un sistema de còpies de seguretat immutables que garanteixi la recuperació de la informació davant atacs de ransomware.
- La implantació d'un servei de monitorització de seguretat 24x7 que permeti detectar, analitzar i respondre davant incidents de ciberseguretat.
- La renovació dels sistemes de protecció antivirus dels equips corporatius, quan s'escaigui.
- El suport tècnic especialitzat dels diferents fabricants.

Aquest conjunt de serveis constitueix una necessitat imprescindible per garantir la disponibilitat dels sistemes d'informació i la continuïtat dels serveis del CSSV.

Per tant, estan incloses les tasques de suport tècnic, administració, configuració, supervisió, actualització i manteniment necessàries per garantir-ne el correcte funcionament.

Queden incloses dins del servei les actuacions ordinàries derivades de:

- Resolució d'incidències i problemes tècnics.
- Suport tècnic i assistència als sistemes mantinguts.
- Resolució d'incidències relacionades amb Microsoft Office 365, incloent-hi problemes d'accés, autenticació, llicenciament, configuració, sincronització, correu electrònic i funcionament de les aplicacions del paquet.

- Suport i assistència en l'ús i funcionament dels serveis de Microsoft 365, incloent-hi Outlook, Teams, SharePoint, OneDrive i les aplicacions ofimàtiques associades.
- Canvis de configuració i ajustos dels serveis existents.
- Tasques d'administració i manteniment preventiu i correctiu.
- Actualitzacions, revisions i comprovacions del sistema.
- Modificacions i adaptacions sobre la infraestructura i els serveis ja contractats.

2. ANTECEDENTS

L'any 2021 el CSSV va renovar la seva infraestructura de virtualització mitjançant la implantació d'un clúster basat en tecnologia Hewlett Packard Enterprise (HPE), amb l'objectiu de disposar d'una plataforma d'alta disponibilitat sobre la qual allotjar els principals sistemes d'informació corporatius.

La infraestructura està formada per:

- Dos servidors HPE ProLiant DL360 Gen10.
- Una cabina d'emmagatzematge HPE MSA 2062 Gen5.
- Dos commutadors HPE OfficeConnect destinats a la xarxa SAN.
- Un servidor NAS Synology RS818+RP per al repositori local de còpies de seguretat.

La plataforma de virtualització es basa en VMware vSphere, mentre que les còpies de seguretat es gestionen mitjançant Veeam Backup & Replication.

Durant els darrers anys el servei s'ha ampliat amb la incorporació de serveis de còpia de seguretat al núvol, eines de protecció antivirus i sistemes de suport remot, adaptant-se a les noves necessitats de seguretat.

3. SITUACIÓ ACTUAL

Després de cinc anys de funcionament s'ha dut a terme una revisió tècnica de la infraestructura.

L'avaluació realitzada conclou que la infraestructura principal de virtualització continua oferint un nivell de rendiment adequat a les necessitats actuals del CSSV.

Els dos servidors HPE disposen encara d'un ampli marge de creixement en recursos de processament i memòria RAM, mentre que la cabina d'emmagatzematge continua oferint capacitat suficient per suportar les màquines virtuals existents i el creixement previst.

Per aquest motiu no es considera necessari renovar la infraestructura principal de virtualització, limitant-se les necessitats de maquinari al manteniment dels equips existents.

No obstant això, l'evolució de les amenaces de ciberseguretat i les recomanacions actuals en matèria de protecció davant ransomware fan necessari incorporar noves mesures de seguretat que no existien quan es va desplegar la infraestructura l'any 2021.

En concret, es considera necessari disposar d'un sistema específic d'emmagatzematge destinat a allotjar còpies de seguretat immutables, físicament independent de la infraestructura principal, així com implantar un servei permanent de monitorització de seguretat que permeti detectar i respondre davant incidents de ciberseguretat.

4. MANTENIMENT DE LA INFRAESTRUCTURA DE VIRTUALITZACIÓ

4.1. MANTENIMENT DE LA INFRAESTRUCTURA DE VIRTUALITZACIÓ

- Manteniment de dos servidors HPE ProLiant DL360 Gen10.
- Manteniment d'una cabina HPE MSA 2062 Gen5.
- Manteniment de dos commutadors HPE OfficeConnect.

Inclourà suport tècnic, manteniment preventiu i correctiu, substitució de components sense cap cost addicional per al CSSV, actualitzacions de firmware i assistència tècnica especialitzada.

4.1.1. MANTENIMENT PROACTIU

Com a mínim, es requerirà presència al CSSV un cop cada 15 dies 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 dels Sistemes Operatius (VMware ESXi i Microsoft Windows Server).
- Actualitzacions de la consola de Veeam Backup.
- Manteniment de l'inventari d'actius del CPD.
- Manteniment de documentació del sistema.

4.1.2. SERVEI DE SUPORT 24X7

El servei de suport 24x7 garantirà la disponibilitat d'atenció tècnica telefònica o presencial, depenent de la incidència, durant les 24 hores del dia, els 7 dies de la setmana, inclosos caps de setmana i festius, per a la gestió d'incidències crítiques que puguin afectar la disponibilitat, seguretat o correcte funcionament dels sistemes informàtics.

El servei haurà de disposar de personal tècnic qualificat per a rebre, analitzar i gestionar les incidències, iniciant les actuacions necessàries per a minimitzar el seu impacte i restablir el servei amb la major rapidesa possible.

4.1.3. RESOLUCIÓ D'INCIDÈNCIES

L'empresa adjudicatària realitzarà el servei de resolució d'incidències i destinarà tot el temps necessari per a garantir la continuïtat del servei del CSSV. Aquestes incidències són:

- Resolució d'incidències del sistema (VMware ESXi, Veeam Backup, Windows Server, Directori Actiu, DNS, DHCP, ESET REMOTE AGENT, etc).

Es defineix com a horari laboral del servei de 8:00 a 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 que es rep l'avís d'una incidència fins que els tècnics de l'empresa adjudicatària inicien les tasques de resolució de la incidència. L'horari de resolució d'incidències serà l'horari laboral establert en aquest apartat.

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

La prioritat de la incidència serà determinada inicialment pel CSSV en el moment de la comunicació, d'acord amb els criteris establerts en aquest PPT, sens perjudici que l'adjudicatari pugui proposar-ne la reclassificació quan, d'acord amb l'impacte tècnic detectat, correspongui. En cas de discrepància, prevaldrà la classificació determinada pel responsable del contracte del CSSV.

Les incidències es classificaran d'acord amb la seva prioritat en:

<u>Prioritat ALTA</u>

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...). En el supòsit que les incidències impliquin ser elevades a un tercer, l'empresa adjudicatària haurà de buscar una solució momentània mentre no es resolgui la incidència del tercer.

Seran considerades com a incidències de prioritat alta:

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

<u>Prioritat MITJA</u>

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...). En el supòsit que les incidències impliquin ser elevades a un tercer,

l'empresa adjudicatària haurà de buscar una solució momentània mentre no es resolgui la incidència del tercer.

Seran considerades com a incidències de prioritat mitja:

- 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 laborable 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...). En el supòsit que les incidències impliquin ser elevades a un tercer, l'empresa adjudicatària haurà de buscar una solució momentània mentre no es resolgui la incidència del tercer.

Seran considerades com a incidències de prioritat baixa:

- 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

Tipus de prioritat	Temps màxim de resposta	Temps màxim de resolució
Alta	60 minuts laborables	8 hores laborables
Mitja	4 hores laborables	Següent dia laborable
Baixa	Següent dia laborable	5 dies laborables

Per evitar que una incidència mai sigui atesa perquè 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 des de la comunicació de la incidència, pujaran a prioritat mitja, i així consecutivament.

L'empresa adjudicatària disposarà d'un portal de suport (ServiceDesk) i gestió d'incidències on el responsable TIC del CSSV 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'aquestes, 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 CSSV. 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.

Cal destacar, que l'empresa adjudicatària prestarà un servei de manteniment de 24x7 per les incidències crítiques que puguin sorgir fora d'aquest horari laboral, en els termes establerts en l'apartat anterior.

4.2. PLATAFORMA DE VIRTUALITZACIÓ

Mantenir i donar suport a la plataforma VMware vSphere compatible amb la infraestructura existent.

4.3. SISTEMA DE CÒPIES DE SEGURETAT

Estarà inclòs en el contracte, la continuïtat de quatre llicències Veeam Backup & Replication Standard.
El servei IBS Veeam VM Cloud Connect inclourà:

- Monitorització del sistema de còpies.
- Resolució d'incidències, en els termes establerts en l'apartat 4.1.3. d'aquest Plec.
- Llicència Veeam Cloud Connect.
- Servei Insider Protection.

El servei IBS Veeam DataStore tindrà la capacitat necessària per allotjar les còpies de seguretat externes.

4.4. SISTEMA DE CÒPIES DE SEGURETAT IMMUTABLES

Subministrament, instal·lació i configuració d'un sistema específic d'emmagatzematge destinat a allotjar còpies de seguretat immutables.

Aquest equipament haurà de ser compatible amb la plataforma Veeam Backup & Replication existent i permetre la implementació d'un repositori immutable que garanteixi la conservació de les dades davant modificacions o eliminacions no autoritzades durant el període de retenció definit.

4.5. SERVEI DE VIGILÀNCIA DE LA SEGURETAT

Renovació de les llicències ESET Protect Advanced.

El servei de vigilància de la seguretat informàtica tindrà com a finalitat la supervisió contínua dels sistemes i serveis TIC, amb l'objectiu de detectar possibles amenaces, accessos no autoritzats, manipulacions, comportaments anòmals o incidents de seguretat.

En cas de detectar-se una incidència de caràcter crític, l'adjudicatari haurà d'analitzar-la i comunicar-la a l'entitat en un termini màxim de 30 minuts des de la seva detecció, indicant la seva naturalesa, nivell de criticitat i, quan sigui possible, les mesures inicials adoptades o recomanades.

Es considerarà que una incidència és de caràcter crític quan estigui en risc la seguretat de la informació del centre.

El servei de vigilància de la seguretat és de 24 hores al dia, 7 dies a la setmana (24x7), amb capacitat de:

- Monitorització contínua dels sistemes.
- Detecció d'activitat maliciosa.
- Identificació d'atacs de ransomware.
- Detecció de compromisos de credencials.
- Correlació d'esdeveniments de seguretat.
- Generació d'alertes.
- Assistència especialitzada en la resposta davant incidents.

4.6. SERVEI DE MONITORITZACIÓ

L'empresa adjudicatària prestarà el servei de monitorització de tota la infraestructura fent èmfasi en:

- Elements Hardware dels servidors, (CPU, Discos, RAM, Temperatura, ports, fonts alimentació, etc).
- Sistemes Operatius (Consums de recursos, estat de la VM).
- Xarxa (switchos, Tallafocs, VPNs, etc).
- Metodologia de detecció, report de les incidències i resolucions d'aquestes.

Haurà de ser una eina instal·lada sobre el clúster de virtualització i no suposarà cap cost addicional pel CSSV. L'eina serà gestionada 100% per l'empresa adjudicatària i la persona responsable del Departament de Sistemes del CSSV podrà tenir accés remot per analitzar i veure l'estat de la infraestructura en tot moment.

5. REQUISITS TÈCNICS OBLIGATÒRIS

Per tal de garantir la prestació d'un servei fiable, segur i adequat a les necessitats del CSSV, reduint els riscos d'indisponibilitat, pèrdua de dades i incidències de seguretat que puguin afectar el funcionament dels sistemes d'informació, serà obligatori que l'empresa adjudicatària tingui les acreditacions vigents següents:

- Veeam Cloud Service Provider

  Es demana en tant que el contracte inclou serveis de còpia de seguretat gestionada, allotjament, protecció de dades o recuperació davant de desastres basats en tecnologia Veeam. El programa està orientat als proveïdors de serveis que ofereixen solucions de còpia de seguretat i recuperació.

- Veeam Backup Silver Partner

Acredita una vinculació comercial i tècnica amb Veeam i l'accés als recursos del seu programa de partners. El manteniment inclou l'administració, la configuració, la supervisió o la resolució d'incidències de la plataforma Veeam.

- Silver Partner Sophos

Els servidors i la infraestructura associada estan protegits mitjançant solucions Sophos incloses en el contracte.

- Partner Gold ESET

El servei inclou l'administració, el manteniment o la resolució d'incidències de les solucions de protecció d'ESET desplegades al CSSV.

La possessió de les esmentades acreditacions són rellevants perquè demostren la vinculació tècnica dels proveïdors amb els fabricants i l'accés als seus recursos de suport, tècnics i comercials, específics per al manteniment, la protecció, la còpia de seguretat i la recuperació dels sistemes.

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 CSSV serà aprovat prèviament pel propi CSSV.

7. PROPIETAT INTEL·LECTUAL

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

8. RESPONSABLE DEL CONTRACTE

L'empresa adjudicatària designarà un responsable que serà la persona de contacte amb el CSSV a qui haurà de facilitar les seves dades.

L'empresa adjudicatària s'haurà d'adreçar al Departament de Sistemes del CSSV com enllaç amb el CSSV.