



Plec de prescripcions tècniques per a la contractació del subministrament i manteniment d'eina centralitzada de desplegament de software a tots els centres de la Corporació de Salut del Maresme i la Selva

Expedient CSMS 16/25-D

(IMP-SC-006)



1 Introducció

La Corporació de Salut del Maresme i la Selva (CSMS) és una entitat sanitària de caràcter públic, que vol establir un procediment per incorporar una nova eina centralitzada de desplegament de software als seus actius TI.

En aquest document es determinaran els requeriments tècnics que s'hauran d'acomplir per a poder ser adjudicatari d'aquesta licitació.

2 Abast

L'abast de la licitació és la d'establir els requeriments necessaris per a l'adquisició d'una eina software centralitzada que sigui capaç de fer desplegament de software a endpoints i servidors de la infraestructura de la CSMS.

A part ha d'incorporar un mecanisme de gestió de dispositius mòbils (MDM), i desplegament de sistemes operatius a través de xarxa.

3 Situació actual

Actualment la CSMS no té una eina concreta per a fer el desplegament de software sobre els seus actius.

4 Requeriments de la solució

4.1 Solució desplegament de software

De forma genèrica, l'eina de desplegament de software ha de poder fer:

1. **Gestió d'endpoints i servidors Windows/Linux**
2. **Desplegament de software**
3. **Gestió d'actualitzacions (pegats de software)**
4. **Aplicació de configuracions**
5. **Eines de gestió**
6. **Inventari**
7. **Informes**
8. **Gestió de dispositius mòbils (MDM)**
9. **Desplegament d'imatges ISO sobre dispositius, a través de xarxa**



4.1.1 **Arquitectura**

Solució On-premise, compatible amb SQL Server i possibilitat de configurar alta disponibilitat.

4.1.2 **Interface**

Possibilitat d'accés a la solució via HTTPS amb certificats propis o certificats de la CSMS.

4.1.3 **Llicenciament**

El software s'ha de llicenciar per:

- Nombre de endpoints
- Nombre de servidors
- Nombre de tècnics

4.1.4 **Integracions**

L'eina ha de permetre el següent llistat d'integracions de software:

- Integració amb Directori Actiu i LDAP per la sincronització d'usuaris i autenticació.
- SSO amb autenticació basada en SAML 2.0
- Integració amb eines de tercers:
Jira, ServiceNow, Tenable, REST API

4.1.5 **Capacitats funcionals**

4.1.5.1 Gestió d'endpoints i servidors

La solució ha de poder gestionar endpoints i servidors amb sistema operatiu Windows o Linux, a partir de les versions Windows 7/Windows 2008R2 Server i Linux Ubuntu 18.04

Es permet que per a la gestió dels dispositius s'hagi d'instal·lar un agent a cada dispositiu.

Aquest agent s'ha de poder desplegar, com a mínim, de les següents formes:

- Consola centralitzada de la solució



- Des d'un servidor de distribució
- GPO de Directori Actiu
- Línia de comandes

La comunicació entre els dispositius i el servidor podrà ser directa a través de LAN, o bé es podran desplegar servidors proxy intermitjos (servidors de distribució).

4.1.5.2 Desplegament de software

La solució ha de permetre definir un repositori on ubicar els fitxers instal·lables de software (MSI, EXE, APPX, etc) de forma que el repositori sigui possible configurar-se local al servidor o a una ubicació remota de xarxa.

S'han de poder configurar els paquets d'instal·lació/desinstal·lació de software per fer-se de forma silenciosa. El desplegament pot estar subjecte a condicions prèvies com espai en disc, valors de claus de registre, software específic instal·lat/no instal·lat. També ha de permetre tasques prèvies/posteriors com execució d'scripts, canvis de claus de registre, gestió de processos o serveis, etc. El post instal·lació ha de permetre instal·lar paquets de forma seqüencial.

Els desplegaments s'han de poder configurar en funció d'una sèrie de polítiques on es podrà definir:

- Moment del desplegament, ja sigui immediat o programat. També ha de ser configurable en base al Patch Tuesday de Microsoft.
- Activitats prèvies i/o posteriors, tals com encesa/reinici/apagat dels equips o execució d'scripts.
- Notificació al tècnic que configuri el desplegament.
- Possibilitat d'avortar el desplegament.
- Notificació als administradors d'estat de desplegaments i possibles errors apareguts durant el mateix.

Criteris de filtratge addicionals en els desplegaments: Directori Actiu (Lloc, Unitat Organitzativa, Grup), nom de màquina, usuari, adreça IP/rang, tipus de processador, tipus de sistema operatiu, tipus de màquina.

El seguiment del desplegament s'ha de poder dur a terme en un quadre de comandament on s'informi de l'estat d'execució i el resultat per equip individual, amb possibilitat d'obtenir la raó d'una possible errada en el desplegament. També a través d'informes exportables a altres formats i que es puguin enviar a través de correu electrònic.

Ha d'existir la possibilitat d'oferir a l'usuari d'un portal autoservei on publicar un conjunt d'aplicacions de manera que l'usuari pugui instal·lar-lo, encara sense ser administrador.

Ha d'existir la possibilitat de configurar plantilles d'actualització de determinades aplicacions instal·lades des de la solució.



4.1.5.3 Gestió d'actualitzacions (pegats de software)

La solució ha de permetre desplegar actualitzacions a equips Windows/Linux, tant de sistema operatiu, aplicacions Microsoft, aplicacions de tercers , així com drivers.

Característiques:

- Descàrrega periòdica al servidor central de la llista d'actualitzacions recopilada pel fabricant per comparar amb les actualitzacions instal·lades als equips. Els servidors de distribució poden descarregar la llista des del servidor central o bé des de Microsoft CDN.
- Informes de pegats absents, instal·lats i aplicables.
- Informes d'estat de vulnerabilitat dels sistemes configurable en base a la criticitat de les actualitzacions que falten.
- Desplegament manual o automàtic de les actualitzacions que falta en els equips. La programació de tasques d'actualització pot incloure funcions prèvies d'encesa d'equips (Wake OnLAN).
- Possibilitat de definir una fase de testeig previ i aprovació abans de poder desplegar massivament actualitzacions aprovades.
- Tasques automatitzades de desplegaments on es poden definir les aplicacions i tipus d'actualitzacions a incloure. Desplegaments subjectes a **Polítiques** on definir:
 - o Moment del desplegament, immediat o programat segons setmana/dia/hora o en base al Patch Tuesday de Microsoft.
 - o Activitats prèvies al desplegament com a encesa/reinici d'equips o execució de scripts (repositori de scripts configurable).
 - o Activitats posteriors al desplegament com a reinici/apagat i execució de scripts.
 - o Notificació a l'usuari del desplegament i dotar-lo de la possibilitat d'avortar el desplegament.
 - o Notificació a administradors sobre estat del desplegament i possibles fallades en la descàrrega/desplegament del parxís.
- Criteris de filtratge addicionals en els desplegaments: Directori Actiu (Lloc, Unitat Organitzativa, Grup), nom de màquina, usuari, adreça IP/rang, tipus de processador, tipus de sistema operatiu, tipus de màquina.
- Possibilitat de publicar un portal autoservei per a la instal·lació per part d'usuari.
- Possibilitat de declinar actualitzacions per a la seva descàrrega i desplegament.
- Possibilitat de deshabilitar les actualitzacions automàtiques de les aplicacions portades per a actualitzacions.
- Definició de repositori de pegats, així com la neteja de pegats antics o declinats.
- El seguiment del desplegament d'actualitzacions s'ha de poder dur a terme en un quadre de comandament on s'informi de l'estat d'execució i el resultat per equip individual, amb possibilitat d'obtenir la raó d'un possible error en el desplegament. També a través d'informes exportables a altres formats i que es poden enviar a través de correu electrònic.



4.1.5.4 *Aplicació de configuracions*

La solució ha de proporcionar un mètode per a passar configuracions als equips, usant plantilles on es configuraran els paràmetres concrets que es vulguin configurar.

Aquestes plantilles han de permetre fer configurar:

A nivell d'equip: Firewall, certificats, variables d'entorn, instal·lació d'impressores, administració de l'energia, modificació de registre, accessos directes escriptori, configuracions de pantalla, notificacions d'inici de sessió, modificació d'usuaris locals, etc.

A nivell d'usuari: Alertes, gestió de permisos, polítiques de seguretat, configuració de navegadors, scripts, modificació de registre, accessos directes, mapeig d'unitats, configuració de Microsoft Office/Outlook, etc.

El seguiment de totes les tasques de desplegament s'han de poder des d'un quadre de comandament central, on s'indiqui l'estat de l'execució i el resultat.

4.1.5.5 *Eines de gestió*

La solució ha d'incloure les següents funcionalitats:

- Control remot, sense importar ubicació de l'equip i sense dependències de VPNs. Possibilitat de sol·licitar confirmació a l'usuari. Possibilitat de definir la visualització compartida o no de la connexió amb l'usuari. Gravació en vídeo de la sessió remota. Durant la sessió remota, possibilitat de transferència de fitxers, comunicació amb l'usuari via xat o trucada de veu/vídeo.
- Gestor del Sistema, amb possibilitat de gestionar processos, serveis, visor d'esdeveniments, consola de comandaments, programador de tasques etc.
- Wake On LAN, per a encesa d'equips sota demanda o de forma programada.
- Apagat remot sota demanda o de forma programada.
- Xat.
- Trucada de veu o vídeo.
- Anuncis.
- Eines del Sistema, com a desfragmentador de disc o gestió de la paperera de reciclatge.

4.1.5.6 *Inventari*

La solució ha d'incloure les següents funcionalitats:

- Anàlisi d'inventari per equips, components maquinari i programari.
- Detall de configuració d'equips amb informació sobre el sistema a nivell de:
 - o Serveis, usuaris, grups, drivers o carpetes compartides.



- Components maquinari com BIOS, discos dur, processador, memòria, ports, dispositius, controladores, etc.
 - Programari instal·lat, incloent versió i fabricant.
 - Certificats instal·lats per tipologia.
 - Nombre de fitxers i espai per tipologia: multimèdia, Office, imatges, etc.
 - Seguretat: Estat de *Bitlocker* per unitat lògica, antivirus, firewall de Windows.
 - Auditoria d'ús de ports USB.
 - Historial de canvis de configuració.
- Gestió del programari, a nivell de programari prohibit (detecció i desinstal·lació), programari per categoria, bloqueig d'executables, llicenciament adquirit i balanç de llicències, mesurament real d'ús del programari.
 - Alertes per canvi de configuració maquinari i programari, també per espai en disc o per expiració de certificats o llicències.

4.1.5.7 Informes

La solució haurà de proporcionar un conjunt d'informes sobre les activitats de gestió dutes a terme en l'eina i sobre l'inventari, podent crear informes amb filtres a mida.

Informes sobre Directori Actiu a nivell d'usuaris (comptes, login, etc.), equips, grups, unitats organitzatives o polítiques.

Exportació d'informes a Excel, CSV i PDF i programació d'informes per a enviament per email.

4.1.5.8 Gestió de dispositius mòbils MDM

La solució haurà de permetre la gestió de dispositius mòbils (Mobile Device Manager), permetent gestionar dispositius iOS, iPadOS, Android, Windows, MacOS, ChromeOS o tvOS, tant corporatius com propietat dels treballadors que es consideri necessaris (BYOD).

Funcions principals:

- Múltiples mètodes de registre segons la tipologia del dispositiu.
- Associació de dispositius a usuaris.
- Establiment de grups de dispositius personalitzats.
- Integració amb contenidors segurs Samsung Knox i Android Enterprise.
- Desplegament de perfils que defineixen el que pot utilitzar l'usuari al terminal (passcode, menús, instal·lació d'apps, localització, roaming, etc.) i accés a recursos corporatius (email, wifi, VPN, etc.). Compatible amb Android i iOS.
- Desplegament d'apps de les botigues en mode silenciós.
- Control d'actualitzacions d'apps.
- Control d'actualitzacions de SO.



- Desplegament de certificats.
- Control remot a Android i visor remot en iOS.
- Desplegament de documents visibles a través d'una app mòbil.
- Inventari detallat de dispositiu a nivell maquinari i xarxa (número de sèrie, IMEI, nivell de bateria, etc.), apps instal·lades, certificats i perfils aplicats.
- Llista negra d'apps amb notificació i desinstal·lació.
- Accions de seguretat: bloqueig del terminal, esborrat complet o corporatiu, alarma remota, mode perdut, reset de passcode, etc.
- Geolocalització actual i històrica.
- Accés condicional a Exchange i Office365.
- Geofencing, notificació o esborrat del terminal en sortir/entrar en una àrea geogràfica determinada.
- Seguiment de l'inventari dels dispositius mòbils es pot a través d'un quadre de comandament i d'informes exportables a altres formats i que es poden enviar a través de correus electrònics.
- Auditoria completa de canvis en els terminals.

4.1.5.9 Desplegament d'imatges tipus ISO

La solució haurà de permetre la creació d'imatges tipus ISO (de sistema operatiu) i desplegament de les mateixes a través d'un sistema centralitzat i automatitzat, com a mínim amb aquests sistemes:

- A través de la xarxa lan
- A través de protocol pxe
- A d'usb standalone

A més haurà de permetre la opció de capturar imatges del sistema operatiu de màquines ja desplegades i sense aturar-les.

4.1.5.10 Gestió centralitzada

Obligatorietat de que la solució es compngui d'un sol producte gestionat centralitzadament, quedant descartades solucions de varis productes i/o fabricants diferents.

També obligatorietat de que només existeixi un sol agent que s'hagi de desplegar als dispositius corporatius.

5 Ciberseguretat

La solució ha d'estar certificada, com a mínim, amb l'Esquema Nacional de Seguretat (ENS) nivell mig.

Totes les solucions que no estiguin certificades quedaran automàticament excloses.



6 Pla d'implantació

Cal que el licitador presenti un pla d'implantació de la solució, amb informació suficient per a determinar temps d'implantació, necessitats, documentació i relació de tasques per part de les parts.

7 Tasques de desplegament

L'adjudicatari haurà de ser l'encarregat de fer el desplegament de les dues solucions dins la infraestructura de virtualització de la CSMS (VMware Vsphere).

Aquest desplegament es farà de forma coordinada amb la CSMS, i constarà:

- Es desplegarà la o les màquines virtuals necessàries per a posar en funcionament la nova eina.
- Descobriment inicial de dispositius (* la instal·lació de l'agent serà a càrrec de la CSMS).

8 Formació

És necessari que el licitador plantegi un mínim de 3 jornades de formació al personal de la CSMS per a la solució descrita en aquesta licitació.

El cost d'aquesta formació ha d'estar inclosa dins de l'oferta econòmica, no podent generar càrrecs extra a la CSMS.

9 Seguiment del projecte

El licitador hauria de plantejar un sistema de seguiment del projecte, ja sigui amb reunions periòdiques o bé un sistema d'enquestes de satisfacció, per detectar possibles necessitats i explicar possibles millores, com a mínim un cop a l'any.

10 Manteniment i suport

L'adjudicatari haurà d'incloure a la oferta econòmica un suport sobre la solució descrita, en format 8x5.

El suport haurà de basar-se en una borsa mínima d'hores de 30 hores anuals per a les tasques de manteniment i suport.



El suport es farà via correu electrònic/telèfon que l'adjudicatari haurà de facilitar.

El suport haurà de servir per a resoldre dubtes, incidències sobre el servei i tasques d'actualització i/o millores de l'eina.

11 Durada de la licitació

La licitació es planteja amb una durada inicial de 3 anys i dues possibles pròrrogues d'un any cadascuna.

12 Certificacions

El licitador haurà d'estar en disposició d'una certificació tipus Gold o Expert (o similar) com a partner de la solució amb la que es presenti.

A part el licitador haurà de tenir un mínim de 2 tècnics certificats amb un nivell Gold o Expert (o similar) de la solució guanyadora.

Aquests requisits s'hauran de complir durant tota la vigència del contracte.

13 Llicenciament

El llicenciament que es demana és:

- Llicenciament per a 20 tècnics concurrents.

- Llicenciament per a 1300 dispositius gestionats endpoint.

- Llicenciament per a 200 dispositius gestionats servidor.

- Llicenciament per a poder fer deploy d'imatges tipus ISO.

- Tots els 1500 dispositius han de poder activar la opció d'MDM.

- Llicenciament de 1 servidor edge (DMZ) per a control de dispositius fora de la lan.

14 Consideracions

La documentació de la proposta tècnica que porti el licitador haurà de tenir una grandària màxima de 30 pàgines, amb un format de font Calibri 11 o bé Arial 11.

Tota informació addicional que pugui haver-hi no es tindrà en consideració alhora d'avaluar la proposta.

Gerard Rossell
Departament TI
Corporació de Salut del Maresme i la Selva