Salut/ Consorci Sanitari de l'Anoia

PLEC DE PRESCRIPCIONS TÉCNIQUES PER A LA CONTRACTACIÓ DEL SUBMINISTRAMENT D'ANTIVIRUS AMB DETECCIÓ I RESPOSTA GESTIONATS AL CONSORCI SANITARI DE L'ANOIA-

EXP. NÚM. 1_CSA_2025

1. INTRODUCCIÓ

El Consorci Sanitari de l'Anoia (en endavant CSA) és l'empresa que gestiona l' Hospital d'Igualada, ubicat a l'Avinguda Catalunya, 11 d'Igualada i on hi realitza la seva activitat des de març de 2007. Tecnològicament està dotat d'una infraestructura complexa i adequada a les característiques d'un hospital que ha de donar servei a les necessitats de la seva població de referència.

El CSA gestiona també, l'Àrea Bàsica de Salut Igualada Nord, ubicada en l'edifici del Carrer Bèlgica, número 5 d'Igualada, situat a 80m de l'edifici de l'Hospital.
El Centre de Salut Mental, Centre de Dia i CASD, gestionats també pel CSA desenvolupen la seva activitat en el mateix edifici del carrer Bèlgica número 5.
Els dos edificis actuals estan connectats mitjançant fibra fosca i amb un backup per radiofreqüència.

1.1 Descripció de la situació actual

El Departament de Sistemes d'Informació del Consorci Sanitari de l'Anoia (en endavant CSA) és el responsable de gestionar les Tecnologies de la Informació i les Comunicacions de l'Organització.

A títol orientatiu, la plataforma tecnològica que gestiona el Departament de Sistemes del CSA és la següent:

Nucli de xarxa
Nucli a 10Gbps basat en 2 equipaments Cisco distribuïts en 12 armaris rack i centralitzat en CPD.

Xarxa WIFI.
75 punts d'accés Aruba

Tallafocs i enrutament
2 Firewalls perimetrals
2 Firewalls interns per segmentació i seguretat del tràfic de xarxa intern.

Centraleta i Telefonia
1 Centraleta Asterisk de telefonia IP
2 Gateways de veu

Sistema de Megafonia IP a les zones d'Urgències, Diagnòstic per la Imatge, i Àrea Ambulatòria.

PC's
Parc de 750 pc's, amb SO Windows.

Impressores
280 impressores làser marca Kyocera en la seva major part, gestionades per xarxa.

Servidors:
9 servidors físics, dels quals 6 són Hosts amb Hypervisor de Vmware .
275 servidors virtuals amb l' entorn VMware gestionats mitjançant Virtual Center.

Sistema d'emmagatzematge en Xarxa (SAN – Storage Area Network).
Cabina principal amb 37,9TB nets de discs SSD Flash i 64,4 TB de disc NLS-SAS
Cabina secundaria , amb 23Tb nets de discs SSD Flash, 8,5 TB Disk SAS i 52,9Tb de disc NLS-SAS
Servidor NAS amb 140 TB de Capacitat

Servei de correu: Exchange M365

A nivell d'antivirus i prevenció a nivell de client el CSA disposa de 1.100 llicències de la Suite Cynet 360 complete, amb els següents productes:

Antivirus NGAV
Sistema EDR
Network Analytics
Threat Intelligence
24x7 Threat Hunting
Control de dispositius

2. OBJECTE DEL CONTRACTE

L'objecte d'aquest plec és la contractació del llicenciament d'un programari de ciberseguretat que doni cobertura a 1.100 equipaments durant un període de 3 anys.

Els requeriments mínims ha de tenir aquest programari són els següents:

2.1 CARACTERÍSTIQUES MÍNIMES TÈCNIQUES

a) La versió subministrada haurà de poder ser instal·lada en els sistemes operatius:

<u>Windows:</u>

Workstation Operating System: Windows XP Service Pack 3 i superior, Windows Vista Service Pack 1 i superior, Windows 7 Service Pack 1 i superior, Windows 8, Windows 8.1, Windows 10, Windows 11.

Server Operating System: Windows Server 2003 Service Pack 2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022.

Linux:

Ubuntu 16.04 i superior, RedHat 7 isuperior, Centos 6.9 i superior, Fedora 23 i superior, Debian 9.X i superior, Suse 12 i superior, Oracle Enterprise Linux 7.6 i superior, Amazon Linux, Amazon Linux 2.

Mac OS:

10.13 ó superior.

b) Els productes han de suportar els sistemes operatius anteriors i disposar de les següents capacitats:

Capacitat de protecció:

Proporcionar múltiples tecnologies natives de detecció necessàries per identificar i prevenir les amenaces en tot l'entorn, amb capacitats EPP, EDR, regles de detecció de xarxa, regles d' anàlisi de comportament de l'usuari, intel·ligència de detecció d'amenaces, entorn de prova, tecnologies d' engany i opcionalment gestió de la postura de seguretat al núvol i en aplicacions SaaS.

Capacitat de correlació:

Analitzar totes les dades rellevants procedents de l'agent incloent les dades de registre i opcionalment sensors de tercers permetent la correlació d'aquests per crear incidents processables i la seva gestió centralitzada de registres.

Capacitat d'investigació i resposta:

Investigar les amenaces existents i automàticament orquestrar accions de resolució i reparació en tot l'entorn.

Capacitat MDR 24x7:

Proporcionar monitorització, investigació, anàlisi sota demanda, resposta a incidents i cerca proactiva d'amenaces.

c) Les funcionalitats principals que han de complir aquests productes són, en concret, les següents:

- Vista d'alertes 360º
- Protecció dels punts de connexió

➢ **Antivirus NGAV:**

Analitzar els arxius en repòs i els arxius no executables per protegir-los contra codi maliciós conegut.

- ✓ Protecció contra codi maliciós mitjançant anàlisis estàtic basat en intel·ligència artificial.
- ✓ Protecció contra l'explotació basada en el comportament.
- ✓ Protecció de macros i scripts contra els atacs sense arxius basat en el comportament.
- ✓ Identificar i prevenir l'execució de malware amb signatures conegudes.

➢ **Control de dispositius:**

Detectar i bloquejar els dispositius d'emmagatzematge externs que s'insereixen en el punt de connexió (per exemple, un dispositiu USB o una targeta SD).

➢ **Protecció de recursos crítics:**

Protegir a usuaris, xarxes, endpoints i servidors (físics i virtuals), arxius, processos, components en el núvol i configuracions del client, alimentant les dades a un punt centralitzat.

➢ **Detecció extensa d'amenaces:**

Sistema EDR: Detecció i resposta per a prevenir, detectar i respondre a les amenaces a nivell més avançat tan conegudes como desconegudes en tot l' entorn.

- ✓ SSDEEP Scan
- ✓ Patronss de memòria
- ✓ Tecnologia de detecció avançada (ADT)
- ✓ Controlador en mode kernel

➢ **Regles d'anàlisi del comportament de l' usuari (UBA/UEBA):**

Aprendre el comportament d'usuaris i entitats per a detectar activitats inusuals i alertar sobre aquests comportaments sospitosos.

➢ **Detecció i resposta de xarxa (NDR):**

Analitzar l' activitat per a detectar ataques en la xarxa, incloent

- ✓ Robatori de credencials basat en la xarxa(suplantació de ARP, responidor DNS)
- ✓ Moviment lateral en la xarxa

- ✓ Comunicació sortint maliciosa (C2C, suplantació d' identitat o phishing)
- ✓ Reconeixement basat en la xarxa (atacs d' escaneig)
- ✓ Filtració de dades basada en la xarxa (tunelització a través de varis protocols)

➢ Entorn de proves: Enviar arxius per a la seva inspecció a través de l'entorn de proves Smart Simulation Execution (SSE) Sandbox.

- Operacions de IT, seguretat i higiene:

➢ **Gestió de la vulnerabilitat.**

➢ **Inventari d'actius.**

- Threat Intelligence:

➢ **Protecció de memòria en temps real:**

Detectar i bloquejar les cadenes de memòria que estan associades amb el ransomware.

➢ **Filtrat d'arxius en temps real:**

Detectar i evitar que las aplicacions no aprovades escriguin en diversos tipus d' arxius

➢ **Filtrat de components crítics:**

Protegir la volta (bóveda) de contrasenyes del sistema operatiu perquè el ransomware no pugui recopilar credencials / propagar-se per tota la xarxa.

- **24x7 Threat Hunting:**

Disponibilitat 24/7, Exclusions, llistes blanques, Anàlisis sota demanda, Instruccions de correcció, Monitoratge d'alertes, Caça d'amenaces i Investigacions d'atacs.

- **Security Operations Center (SOC):**

Centre d'Operacions de Seguridad, per prevenir, monitoritzar i controlar la seguretat en la xarxa de l'organització 24x7. El SOC ha de tenir un servei de control d'alertes, resposta remota a incidents (IR) i informes sobre ataques.

2.2 PREVENCIÓ I DETECCIÓ

La solució ha d'identificar:

- Arxius maliciosos i evitar la seva execució, inclosos virus, troians, ransomware, spyware, cryptominers i qualsevol altre tipus de malware, utilitzant com a mínim les següents tecnologies:

  - ➢ Protecció per signatures/firmes.
  - ➢ Anàlisis estàtics de Machine Learning.
  - ➢ Anàlisis dinàmics amb Sandbox en Temps Real.
  - ➢ Intel·ligència d' amenaces vinculat a VT.
  - ➢ Intel·ligència d'amenaces externa a VT.
  - ➢ Integració AMSI.

- Comportament maliciós d'arxius executats, processos en execució, modificacions de registre, accés a la memòria i finalitzar-los en temps d' execució, o generar una alerta (exploits, fileless, macros, Powershell, WMI, etc.), utilitzant como a mínim les següents tecnologies:

  - ➢ Supervisió de l'accés a la memòria.
  - ➢ Procés d'anàlisi de comportament (heurística).
  - ➢ Alta similitud (fuzzi hashing).
  - ➢ Intel·ligència d'Amenaces.

- Comportament maliciós del compte d'usuari, indicatiu de compromís previ, utilitzant como a mínim les següents tecnologies:

  - ➢ Configurar polítiques d'activitat d'usuari (infracció de política).
  - ➢ Línia base de perfil de compte d'usuari (detecció de anomalies).

- Interacció maliciosa amb arxius de dades, utilitzant la tecnologia de Señuelos, generant fitxers "Decoy".

- Filtració de dades a través de protocols legítims (túnels DNS, túnels ICMP), utilitzant com a mínim les següents tecnologies:
  - ➢ Seguiment de Tráfic de xarxa (File Access Monitoring).
  - ➢ Seguiment d'Accés a Ficheros (File Access Monitoring).

La solució ha de suportar:

- La creació de regles per a excloure rangs de IP/direccions específiques, bloquejant IPs malicioses i dominis.

La solució ha d'identificar, bloquejar i alertar:

- Atacs d'escalat de privilegis, utilitzant com a mínim la tecnologia de Seguiment de processos.
- Atacs de reconeixement (escaneig), utilitzant com a mínim la tecnologia de Seguiment de Tráfic de Xarxa (NTA).
- Intents de robatori de credencials des de la memòria (bolcat de credencials, força bruta) o tràfic de xarxa (suplantació d' identitat ARP, responedor DNS), utilitzant com a mínim les següents tecnologies:
  - ➢ Seguiment de memòria.
  - ➢ Seguiment de Comptes d'usuari.
  - ➢ Seguiment de Tràfic, Comportament i Resposta de Xarxa (NDR).
  - ➢ Tecnologia d'esquers ("Señuelos"), generant usuaris "Decoy".
- Us d'eines d'atac comuns (Metasploit, Empire, Cobalt, etc.), utilitzant com a mínim la tecnologia de Seguiment de processos.
- Moviments laterals (SMB relay, pass the hash, etc.), utilitzant como a mínim les següents tecnologies:
  - ➢ Seguiment de Tràfic de Xarxa (NTA).
  - ➢ Tecnologia d'Esquers (Señuelos), generant usuaris "Decoy".
  - ➢ Tecnologia d'Esquers (Señuelos), generant connexions de xarxa "Decoy".
  - ➢ Tecnologia d'Esquers (Señuelos), generant equips "Decoy".

La solució ha de tenir:

- Un mecanisme intern de protecció contra l'accés i manipulació d'usuaris no autoritzats. Alerta i bloqueig davant qualsevol intent de manipulació o desactivació.
- Un funcionalitat de creació de perfiles de control de dispositius d'emmagatzematge que permetrà detectar i bloquejar els dispositius d'emmagatzematge externs que s'insereixen en el punt de connexió (per exemple, un dispositiu USB o una targeta SD).

La solució ha d'incloure:

- La capacitat de detectar i bloquejar comunicacions a dominis maliciosos, utilitzant com a mínim la tecnologia d' Anàlisi de Dominis.

- La capacitat de crear esquers (señuelos) (Decoys, també coneguts como Honeypots) sense necessitat d' instal·lar cap servidor On-Prem i gestionats por l'agent únic de tota la solució. Els esquers hauran de ser com a mínim de la següent tipologia:

  ➢ Fitxers
  ➢ Hosts
  ➢ Usuaris

2.3 RESPOSTA, INVESTIGACIÓ I REMEDIACIÓ

La solució ha de suportar:

- Aïllament, mitigació de presència i activitat maliciosa, localment en l' endpoint amb les següents capacitats mínimes:

  - ➢ Executar una comanda coordinada (com la interfície CMD).
  - ➢ Obrir un Shell remot.
  - ➢ Executar scripts o un arxiu des d'una ubicació de xarxa o mapejar una unitat.
  - ➢ Tancar un endpoint i/o un servidor.
  - ➢ Aïllament d'un endpoint/servidor de la xarxa.
  - ➢ Eliminació d'un arxiu (inclosos els arxius d' execució actius).
  - ➢ Posar un arxiu en quarantena (inclosos els arxius d' execució actius).
  - ➢ Matar un procés.
  - ➢ Eliminació i/o eliminació d'un servei/tasca programada.
  - ➢ Bloqueig d'un compte d'usuari local o d'un usuari de domini.
  - ➢ Posar a zero de la contrasenya d'usuari.
  - ➢ Desconnexió de targetes de xarxa.
  - ➢ Canvi de direcció IP.
  - ➢ Capacitat d'editar un arxiu HOST.
  - ➢ Funcionament renovat d'un endpoint i/o un servidor.

- Aïllament i mitigació de presència i activitat maliciosa a nivell mundial en tot l' entorn amb les següents capacitats mínims:

  - ➢ Deshabilitar usuari.
  - ➢ Restablir contrasenya.
  - ➢ Bloquejar IP.
  - ➢ Bloquejar domini.
  - ➢ Bloquejar port.

- Respostes automatitzades:

  - ➢ Playbooks de resposta preestablerts que es proporcionen llestos per ser utilitzats.
  - ➢ Playbooks de resposta personalitzats creats per l'administrador.
  - ➢ Rollback.

La solució ha de mostrar:

- La cadena d'esdeveniments, objectes relacionats resultants d'un incident amb una visualització gràfica de l'incident mostrant:

- ➢ Esdeveniments.
- ➢ Dades relacionades sobre la víctima.
- ➢ Dades relacionades sobre el agressor.
- ➢ Dades relacionades sobre la relació dels artefactes .
- ➢ Dades amb tot l'arbre de processos.
- ➢ Cadena d'esdeveniments.

La solució ha d'incloure:

- Motor d'investigació automàtic sobre els esdeveniments de seguretat detectats que:

  - ➢ Permetrà identificar qualsevol persistència,
  - ➢ Mostrarà la causa arrel
  - ➢ Mostrarà els elements compromesos en tota la infraestructura protegida.

- Capacitat de guarir, sempre de forma autònoma, allò identificat, eliminant de forma automatitzada els elements maliciosos identificats durant la fase d'investigació.

La solució ha de recopilar contínuament dades sobre totes les entitats i les seves activitats dins l'entorn permetent:

- Interacció amb arxius:

  - ➢ crear
  - ➢ obrir
  - ➢ renombrar
  - ➢ eliminar
  - ➢ executar

- Execució de processos (inclosa la visualització de l'arbre de processos)

- Inici de sessió d'usuari
- Canvis en el registre
- Programari instal·lat

La solució ha d'admetre:

- La visualització de dades d'entitat i activitat:

  - ➢ Recerca basada en patrons de comportament en tots els camps de cobertura (usuaris, arxius, màquines i tràfic de xarxa).

- ➢ Determinació de les regles i/o creació d'alertes i/o determinació del nivell de risc, en base a una resposta al patró de recerca i en temps real.
- ➢ Habilitació de nombre d'usuaris per realitzar activitats en paral·lel, en base als permisos dels usuaris, i sense necessitat de desconnexió d'un altre usuari per l'execució de l'activitat.

- L'anàlisi dinàmic (es a dir, sandbox) inclòs podent enviar manualment arxius pel seu anàlisis.

- Consultes entre organitzacions permetent recerques d'ocurrències d' activitats de procés, arxius, xarxa i/o usuaris en tots els equipaments de l'entorn.

La solució ha de sustentar els mitjans per executar la investigació forense, tals com:

- Procés en execució
- Arxiu en execució.
- Nivell de màquina.
- Activitats de memòria.
- Obtenir bolcat de memòria.

2.4 MONITORITZACIÓ I CONTROL

La solució ha de suportar:

- File Integrity Monitoring (FIM) que asseguri la política en entorns fixes per alertar sobre qualsevol canvi en un arxiu.
-
- El descobriment desatès de diferents tècniques d'atac, buscant arxius, processos, connexions de xarxa i comptes d'usuari susceptibles de risc amb contrasenyes antigues.
-

La solució ha de proporcionar:

- Els mitjans per portar a terme la gestió d'inventari permetent mapejar i correlacionar tots els actius dins de l'entorn, com equipaments finals, servidors, aplicacions instal·lades, comptes d'usuari i informes periòdics generats.

- Recopilació i retenció de registres d'activitat i autenticació permetent la conservació durant el període de temps que exigeixen las diferents normatives.

La solució ha d'incloure :

- 24x7 Cerca Proactiva d' amenaces global (Threat Hunting).`
- 24x7 Cerca Proactiva d'amenaces en Deepweb (Deep Hunting)
- 24x7 Cerca Proactiva d'amenaces en Darkweb (Dark Hunting)

La solució ha de tenir:

- Avaluació de vulnerabilitats integrada en el mateix agent, que descobreixi les actualitzacions de seguretat que falten en els sistemes i aplicacions. Els requeriments mínims son:
  - ➢ Revisió automatitzada de pegats de Windows
  - ➢ Control d'aplicacions instal·lades no desitjades.
  - ➢ Control de versió mínima permesa d'aplicacions de tercers
  - ➢ Validació d'operativitat constant d'agents de tercers.

2.5 INFRAESTRUCTURA

La solució ha de tenir:

- Agent únic per a totes las tecnologies que inclouran:
  - ➢ EPP
  - ➢ EDR
  - ➢ NDR
  - ➢ UBA
  - ➢ Comunicació
  - ➢ Deception
  - ➢ Posture Management (Saas & Cloud)
- Una protecció amb contrasenya per la desinstalació de l'agent únic.
- Una protecció total contra la finalització del servei
- Un mínim impacte de l'agent en el rendiment de l'endpoint i/o servidor amb:
  - ➢ Consum màxim recomanat pel fabricant del 15%
  - ➢ 50 Mb (mitjana) de consum RAM en cada Endpoint o Servidor
- Opcions flexibles d'implementació per la consola de gestió per adaptar-se a varis tipus d'entorns:
  - ➢ On-Prem.
  - ➢ SaaS.
  - ➢ Híbrid.
- Paquets d'instal·lació lleugers de como màxim:
  - ➢ 20 Mb per a sistemes Operatius Windows
  - ➢ 14 Mb per a sistemes Operatius Linux
  - ➢ 14 Mb per a sistemes Operatius Mac OS

La solució ha de suportar:

- Instal·lació ràpida en tots els endpoints i servidors de l'entorn.

- Suport per Sistemes Operatius Legacy Windows XP SP3 i Windows Server 2003 SP2
- Instal·lació sense la necessitat de desinstalació de l'anterior Antivirus.

La solució ha de proporcionar:

- Comunicació xifrada entre el servidor d'administració i els agents en els endpoints i servidores.
- Protecció completa per a endpoints i servidors que estan fora de línia de la xarxa de l'organització fins i tot sense connexió a la consola d' administració.

La solució ha de permetre:

- La definició i creació de rols d'administració amb permisos personalitzats en funció dels tipus d'accions disponibles que es puguin assignar a usuaris i grups.

La solució ha de coexistir:

- Amb tot el software comercial instal·lat en els endpoints i servidors.
- Amb tots els Antivirus del mercat que puguin estar instal·lats en els endpoints i servidores.
- Entre Endpoints, arxiu, processos, activitat de l'usuari i tràfic de xarxa de forma totalment autosuficient, eliminant la necessitat de configuració manual de regles o polítiques o la dependència de dispositius addicionals.

2.6 OPERATIVA

La solució ha de tenir la capacitat de:

- Especificar una llista de regles d' exclusió d'alertes per als objectes seleccionats.
- Exportar la configuració actual del programa.
- Habilitar i deshabilitar certs tipus de notificacions.
- Qualificar la gravetat de les alertes de seguretat.
- Bloquejar l' accés a la configuració del programa per als usuaris finals.
- Especificar un programa per a descarregar actualitzacions, inclosa la capacitat de desactivar l' actualització automàtica.
- Mantenir-se totalment oculta en els equips instal·lats
- Mostrar les alertes exclusivament en la consola de gestió centralitzada.

La solució ha de suportar:

- Implementació en múltiples sites que reporten a una sola consola d' administració.
- Integració amb una infraestructura de correu electrònic per a notificar al personal de seguretat en cas d'alertes.
- Integració amb productes SIEM comuns (a través de syslogs sortints, API i a través de json enviats a AWS S3 Buckets, tan per alertes com per registres d'auditoria).
- Informes estandaritzats i personalitzables. Els informes han de ser exportables en diferents formats, programats i enviats per correu electrònic.

La solució ha de proporcionar:

- Una recopilació i processament centralitzada d' alertes en temps real.
- Una distribució centralitzada d' actualitzacions sense necessitat d'intervenció de l'usuari i de reiniciar l' endpoint i servidor.

La solució ha de permetre:

- L'extensió del període de retenció de dades predeterminat per a equilibrar les polítiques corporatives i de privacitat.

La solució ha d'incloure:

L'opció d' ingerir syslogs de tercers provinents de qualsevol font i centralitzar-los tots en un sol panell (aquests registres han de mostrar-se com a dades sense processar o en taulers gràfics a través de diferents tipus de gràfics).

2.7 MÓDULS OPCIONALS

La solució haurà de disposar de manera opcional, amb llicències addicionals si procedeix, de mòduls complementaris integrats de forma nativa en la plataforma i oferts pel propi fabricant, com a mínim amb les següents funcions addicionals:

- Identificar, prioritzar i corregir automàticament qualsevol risc de seguretat en aplicacions SaaS o infraestructura Cloud amb monitorització directa des de la plataforma oferta.
- Supervisi i analitzi les activitats crítiques realitzades en l' entorn corporatiu aprofitant tots els registres existents concentrant-los en una plataforma d' administració de registres centralitzada.
- Monitoratge de la web obscura en particular en l'àrea de robatori de credencials.
- Possibilitat de protegir dispositius mòbils basats en Android, iOS i ChromeOS.
- Possibilitat de sincronització amb solucions avançades de protecció pel correu electrònic.
- Possibilitat d'ingerir dades de marques de tercers.

3. PROVA DE CONCEPTE

Si el CSA ho considera, es demanarà a les possibles empreses adjudicatàries, sense cost addicional, la realització d'una prova de concepte de 14 dies, per tal de validar que la solució tecnològica proposada s'ajusta a les funcionalitats que s'han recollit en aquest plec.

L'empresa licitadora s'encarregarà de preparar un entorn Saas i facilitar l'accés als tècnics del CSA, de manera que, des d'un lloc de treball corporatiu que tingui instal·lada la maqueta estàndard corporativa, es pugui realitzar la comprovació.

Per a la realització de la prova de concepte, els tècnics del CSA proporcionaran a l'empresa licitadora equips amb sistemes operatius diversos fins a un total de 20, que podran incloure:

a) Windows XP, SP3
b) Windows 7
c) Windows 10,11
d) Windows Server 2003 SP2
e) Windows Server 2008
f) Windows Server 2016, 2022
g) Linux
h) MacOS

Es considerarà que la solució tecnològica proposada té l'acceptació del CSA si es constata que els resultats de la prova de concepte han permès garantir, de forma objectiva, que la solució proposada ha complert les especificacions tècniques i els criteris de validació inclosos en la prova de concepte i detallats en paràgrafs anteriors.

4. INSTAL.LACIÓ I FORMACIÓ

La instal·lació de la solució anirà a càrrec de l'adjudicatari i comptarà amb el recolzament del departament de Sistemes pel desplegament dels agents. La generació de paquets, polítiques i altres funcionalitats seran consensuades per ambdues parts en reunions periòdiques de 1 hora fins el total desplegament de solució.

La formació de la solució anirà a càrrec de l'adjudicatari a mesura que la instal·lació vagi avançant.

5. MANTENIMENT I SUPORT TÉCNIC DEL PROGRAMARI

a) Manteniment del Software

El manteniment del software haurà de contemplar, al menys, els següents aspectes:

- Informació sobre noves versions
- Actualització de les versions de software, a la fi de disposar de totes les correccions, revisions i millores del seu software, entenent que en cas d' aparèixer noves versions hauran de ser facilitades dins del període en què el contracte tingui el seu efecte i amb la corresponent documentació adaptada als programes suportats
- Serveis de notificació anticipada
- Informació i accés preferent a les presentacions de nous productes, noves versions o conferències d'usuaris organitzats per l'empresa adjudicatària

b) Suport tècnic del Software

L' adjudicatari proporcionarà un suport tècnic que asseguri la resolució de tot tipus d'incidències, tant d'instal·lació del software com d'execució, que poguessin sorgir durant el contracte a partir de la data d'inici del mateix.

Les característiques del suport tècnic seran, com a mínim, les següents:

- Atenció no presencial en suport telefònic, web, correu electrònic davant de problemes o consultes.
- En caso d'incidents crítics, possibilitat de realitzar un diagnòstic remot.
- Suport a un número il·limitat de casos via web, fax, telèfon o correu electrònic.

6. PRESTACIONES OBJECTE DE LA CONTRACTACIÓ

L'adjudicatari haurà de realitzar el subministrament de les llicències en la modalitat de subscripció de tot el programari detallat en aquest plec, així com el manteniment, suport, instal·lació i formació associat a aquest, durant la totalitat del termini del contracte, de manera que es garanteixi la configuració òptima i plena operativitat, cosa que permetrà en tot moment tenir les aplicacions actualitzades a la darrera versió i explotar al màxim les seves funcionalitats.

L'adjudicatari haurà de presentar acreditació de ser distribuïdor oficial del fabricant per al manteniment de les llicències d'aquest producte, havent d'aportar amb aquesta finalitat el certificat oficial comercial del fabricant per al subministrament de llicències així com el certificat oficial tècnic del fabricant, tots dos en vigor, per a la distribució, instal·lació i manteniment del producte licitat.

Amb això s'assegura que es compta amb el suport i el suport del fabricant en cas d'incidències amb la llicència, i es garanteix que la llicència està en condicions òptimes per ser usada pel personal de l'organització.

7. ESPECIFICACIONS TÈCNIQUES COMPLEMENTÀRIES

Durant l'execució dels contractes l'adjudicatari haurà d'atendre les condicions d'execució específiques. A continuació es detallen algunes d'aquestes condicions.

- S'exigirà a l'adjudicatari dels subministraments el lliurament de la documentació i els informes relatius als subministraments realitzats al detall que sigui necessari o qualsevol altra documentació tècnica en el format que es determini
- Es requerirà aportar un Pla de transició i de devolució del subministrament.

A. Documentació obligatòria a incloure en els sobres

Els licitador hauran de presentar les seves ofertes d'acord amb l'estructura i contingut que s'estableix en l'ap. Q del Quadre de característiques.