Consell Comarcal
de la Conca de Barberà

SUBMINISTRAMENT DE LA LLICÈNCIA DEL TALLAFOC I LES LLICÈNCIES DELS EDR PER LES MÀQUINES DE LA XARXA DEL CONSELL COMARCAL DE LA CONCA DE BARBERÀ

Plec de prescripcions tècniques

1. Objecte del contracte

És objecte del contracte el cobrir i millorar la seguretat de la xarxa del Consell Comarcal de la Conca de Barberà, consistent en la renovació del sistema actual de seguretat perimetral Watchguard M4800, i contractació d'un servei de protecció completa d'equips (els llocs de treball d'usuaris i servidors) controlant el comportament de cadascun dels processos executats al parc informàtic del Consell Comarcal de la Conca de Barberà. Aquest servei permetrà la classificació de tot el programari que s'executa en el lloc de treball, monotonitzarà el comportament del mateix, assegurarà la identificació del programari confiable i no confiable i bloquejarà l' execució del programari no confiable. S'ha d'incloure també un servei de gestió i manteniment d'equips que permeti el control de l'estat dels equips així com poder aplicar polítiques i instal·lar remotament.

2. Situació actual

Actualment, el Consell Comarcal de la Conca de Barberà, i l'Ajuntament de Montblanc gestionen i comparteixen una xarxa de comunicacions implementada en fibra òptica i radioenllaços, que connecten tots els centres de treball, les quals comparteixen una única sortida a Internet, ubicada al CTIC Montblanc Digital, on es troben els tallafocs, objecte de la present contractació, dos tallafocs Wathcguard M4800, funcionant com un clúster en actiu / passiu.

Aquests tallafocs tenen la missió de gestionar la seguretat perimetral de la xarxa, bloquejant qualsevol accés no autoritzat des de l'exterior i permetent una navegació segura als usuaris, restringint l'accés a determinats ports, protocols, tipologies de pàgines continguts, ...

Els equips que es disposen actualment són els següents:

Model	Descripció	Fi suport actual	Nº de sèrie
M4800	Node actiu clúster FW	12/09/2025	80D8028E25D4C
M4800	Node passiu clúster FW	12/09/2025	80D8029149FBA

Els serveis activats actualment en el clúster corresponen a Total Security Suite, que actualment estan a nom de l'Ajuntament de Montblanc, són els següents:

- Fireware XTM Pro
- Application Control

- Gateway AntiVirus
- IPS
- Bootnet Detection
- Reputation Enabled Defence
- TDR
- SpamBlocker
- WebBlocker
- intelligent AV
- Access Portal
- DNSWatch
- Data Loss Prevention
- Advanced Persistent Thread
- Dimension Command
- Thread Detection & Response
- Host Sensors
- Mobile User VPN

Actualment el Consell Comarcal no disposa de cap servei de protecció de dades ni tampoc cap sistema de gestió i manteniment d'equips.

3. Requisits tècnics

3.1. Subministrament de les llicències de subscripció detallades al punt 2

La renovació de la subscripció de les llicències / serveis relacionats al punt 2 d'aquest plec, consistent en les llicències i serveis Total Security Suite per als dos equips M4800 per un període de 3 anys.

La renovació només es permet sota llicència oficial de Watchguard.

Tal i com s'ha comentat en el punt 2 d'aquest plec, actualment el Consell Comarcal i l'Ajuntament de Montblanc comparteixen la infraestructura comuna dels dos UTM M4800 i conseqüentment les llicències del Total Security Suite, però cal tenir en compte que les llicències actuals estan a nom de l'Ajuntament de Montblanc. Per això, el licitador s'haurà de fer càrrec de l'actualització de les llicències, tenint en compte que aquestes caduquen el 12/09/2025 d'acord amb la durada total del contracte, i actualitzant el client dins la plataforma de Watchguard, sense que això suposi cap despesa pel Consell Comarcal ni per l'Ajuntament de Montblanc.

Qualsevol despesa associada al canvi de nom de les llicències anirà a càrrec del licitador.

3.2. Subministrament de les llicències per a un servei gestionat de protecció de dades basat en el monitoratge de les aplicacions i un sistema de gestió i manteniment d'equips.

a) Període de cobertura

El període de cobertura serà de 3 anys amb possibilitat de pròrroga d'un any.

b) Actius a protegir

La solució haurà de ser capaç de protegir almenys 300 equips, podent créixer durant la vigència del contracte

c) Ubicació de la plataforma

Per tal de reduir els costos de manteniment i explotació de la solució, no haurà de ser necessari l'ús d'una plataforma interna, cal una solució basada en cloud. És requisit mínim que la plataforma on s'allotgi la infraestructura es trobi fora de les nostres instal·lacions i operada pel fabricant de la solució en un model cloud, en el qual no hi hagi un inconvenient en el creixement i escalabilitat de la plataforma. Assegurant que independentment del nombre de nodes de la instal·lació la plataforma funcioni en el mateix nivell d'eficiència. La ubicació de la plataforma ha d'estar allotjada a la Unió Europea. Existeixen nodes que estan distribuïts per diferents seus i fins i tot en mobilitat per la qual cosa aquests aprofitaran la disponibilitat de la infraestructura cloud perquè estiguin integrats de forma completa en la configuració i actualització de la solució.
La plataforma de gestió ha de cobrir els principals nivells de certificació com són: ISO 27001 i es valorés positivament qualsevol altra certificació que disposi la infraestructura.

d) Agent a desplegar en els equips

L'agent desplegat permetrà la comunicació i gestió de tant la protecció d'antivirus tradicional així com de la protecció de processos desconeguts i la gestió i connexió remota als equips. Recollirà la informació corresponent als esdeveniments i els components que els produeixen, sense recopilar informació, ni documents d'usuari. L'impacte sobre els dispositius del parc haurà de ser menor al 5 % de rendiment de la CPU, memòria i disc. L'agent ha de ser capaç de protegir equips de sobretaula i portàtils amb els sistemes operatius següents:

- Sistemes operatius

- Estacions de treball
  - Windows XP SP3 (32 bits)
  - Windows Vista (32 i 64 bits)
  - Windows 7 (32 i 64 bits)
  - Windows 8 (32 i 64 bits)
  - Windows 8.1 (32 i 64 bits)
  - Windows 10 (32 i 64 bits)
  - Windows 11 (64 bits)
- Equips amb microprocessador ARM
  - Windows 10 Pro i Home
  - Windows 11 Pro i Home
- Servidors
  - Windows 2003 (32, 64-bit i R2) SP2 i superiors
  - Windows 2008 (32 i 64-bit) i 2008 R2
  - Windows Small Business Server 2011, 2012
  - Windows Server 2012, 2012 R2
  - Windows Server 2016 i 2019
  - Windows Server Core 2008, 2008 R2, 2012 R2, 2016 i 2019
  - Windows Server 2022 (64-bit)

La desinstal·lació de la protecció s'haurà de protegir mitjançant contrasenya. La solució s'ha de poder desplegar de manera silenciosa mitjançant els mecanismes següents: per adreça IP, rang d' adreces IP, nom de màquina i grups de Directori Actiu de Microsoft basat en polítiques de domini.

e) Consola web

L'adjudicatari proporcionarà un interfície en el qual es puguin consultar dades en temps real, descarregar informes/alertes, accedir a la configuració i polítiques i disposar de les actualitzacions dels agents. Els administradors del servei podran gestionar des d'una única consola i de manera centralitzada, mitjançant qualsevol navegador web la seguretat i productivitat de totes les estacions de treball i servidors Windows fins i tot ordinadors portàtils i oficines remotes.

f) Protecció

La protecció demanada es dividirà en tres parts:

- Endpoint Protection Platform (EPP)

- Endpoint detection and response (EDR)
- Remote Monitoring & Management (RMM)

Les dues primeres parts han d'estar combinades i fusionades a nivell de configuració, tan sols estaran dividides a nivell de funcionalitats, i ha d'estar compost per un sol agent i una sola solució. No es permetrà l'ús de diferents components per tal d'aconseguir una protecció contra amenaces desconegudes en què col·labori l'antivirus tradicional amb la protecció avançada.

g) Endpoint Protection Platform

Es requereix una solució d'EPP (Endpoint Protection Platform) amb les següents funcionalitats:

- Antivirus per a arxius, correu i web, permetent la detecció i desinfecció de qualsevol tipus d'amenaça. Detectant malware per comportament i el correu amb detecció de pop3. Pel que fa a la protecció web es detectaran els intents d'accés a pàgines web que continguin elements maliciosos, bloquejant-los.
- Firewall personal gestionat en local o de forma centralitzada des de la consola web. Ha de permetre:
  - Bloquejar les connexions entrants i/o sortints de les aplicacions que es desitgi.
  - Prevenció d'intrusions.
  - Crear regles de firewall per permetre/denegar el trànsit en sentit entrant/sortint de les màquines que es vulgui per als protocols/ports que es desitgi.
- Bloqueig de tots els dispositius o dispositius específics (unitats d'emmagatzematge extraïble, dispositius de captura d'imatges, unitats de CD/DVD, mòdems USB, Bluetooth, etc.), impedint l'entrada de malware i fuites d'informació. Permetent la definició de diferents accions per a cada tipus de dispositiu (bloqueig, accés, lectura/escriptura).
- Bloqueig d'accés a pàgines web no desitjades. Haurà de ser possible configurar aquesta protecció basada en categories tot i que s'hi podran també afegir llistes blanques i negres de llocs i dominis permesos.

h) Endpoint detection and response

Es requereix una solució de tipus EDR (endpoint detection and response) per protegir de les següents amenaces:

- Malware avançat
- PUP (potential unwanted programs)
- Amenaces zeroday tipus ransomware
- Decoy files
- Shadow Copies
- Troians de nova generació indetectables pels antivirus.

Aquesta solució haurà d'evitar al màxim les infeccions de forma proactiva, mai reactiva. La solució ha d'aportar contramesures diferents a les següents:

- Firmes locals, que requereixen de constants actualitzacions
- Motors heurístics, que necessiten d'un ús de CPU i poden produir falsos positius.
- Sistemes de llistes blanques, ja que no disposem de personal suficient per a l' administració d'aquest tipus de sistemes.
- Sistemes de sandboxing que consumeix recursos i el malware pot eludir-los.

El sistema de protecció ha de ser capaç de classificar el 100% dels processos executats en les màquines, generant una classificació de malware o goodware.

És un requisit que es produeixi el bloqueig dels processos desconeguts que s'intenti executar per evitar la possibilitat danyar les dades accessibles per la maquina (com pot ser el xifrat no desitjat) o el robatori o accés de dades.

Ha d'incloure un sistema Anti-Exploit que permet la detecció i bloqueig de l'ús d'exploits coneguts o desconeguts.

S'ha de poder establir diferents nivells de bloqueig (més o menys restrictius) així com diferents nivells en la capacitat dels usuaris de poder desbloquejar individualment els processos bloquejats pel sistema.

La solució ha d'incloure la possibilitat de bloquejar aplicacions per nom i per hash que l'administrador desitgi.

i) Servei d'alerta d'amenaces (Threat Hunting)

Es requereix un servei que alerti i prengui les mesures correctives adequades quan sigui detectat una activitat anòmala en els equips basada en el comportament normal auditat anteriorment en el parc d'equips.

Aquest servei haurà d'estar ofert pel fabricant de la solució EDR per tècnics especialitzats usant les dades que hagi recollit a l'auditoria forense.

Han de poder realitzar l'alerta i la inclusió en la intel·ligència del sistema EDR de les mesures correctives.

j) Remote Monitoring & Management

Es requereix una solució de tipus RMM (remote monitoring and management) per aconseguir els següents objectius:

- Obtenir informació centralitzada de maquinari i programari.
- Control de llicències utilitzat.
- Capacitat de fer filtres per la informació obtinguda en l'inventari.
- Registre de canvis produïts en l'equip a nivell de maquinari o programari.
- Monitoratge de processos, serveis, memòria, CPU, registre, grandària d'arxius o carpetes.
- Possibilitat de crear nous monitors personalitzats.
- Monitoratge de dispositius de xarxa.
- Capacitat de realitzar tasques de forma automàtica quan es produeixi un fet determinat en un monitor.
- Gestió de pegats de Microsoft, independentment d'on es trobi l'equip.
- Instal·lació, desinstal·lació i parxís de programari de tercers.
- Execució remota de scripts per automatitzar tasques.
- Control remot a equips connectats a Internet independentment d'on es trobin.
- Sistema de comunicació amb l' usuari mitjançant Xat.
- Control de smartphones i tauletes, amb funcionalitat mínima d'esborrat del dispositiu, bloqueig i localització.

Totes aquestes funcionalitats estaran integrades com a part d'un sol agent i permetrà tant la gestió com el control remot.

k) Mòduls addicionals

Es requereix que la solució escollida disposi de mòduls addicionals per ampliar la funcionalitat. Aquests mòduls han de complir almenys complir amb les funcionalitats següents:

- Gestió d'actualitzacions de sistema operatiu i tercers
- Gestió del nivell de xifrat dels dispositius
- Gestió de control de dades.

- Orquestrador Big Data de logs per realitzar una gestió avançada d'informació.
- Alimentador de SIEM externs.

l) Extended Detection and Response (XDR)

El programari subministrat haurà d'integrar-se de forma nativa amb els firewalls del Consell Comarcal de la Conca de Barberà per oferir una solució de XDR integrada i sense cost addicional.

m) Sistema d'informació

El sistema ha de generar informació forense relacionada amb cada equip de tal manera que pugui ser explotada posteriorment. El sistema ha d'incloure informes per amenaça detectada en els que se correlacionin les accions que ha fet el procés o en el context que ha estat, per exemple si ha estat descarregat d'Internet o ha estat extret d'un fitxer comprimit. Es valorarà molt un entorn fàcil de seguir, sense exigir grans coneixements d'amenaces avançades. També ha d'incloure informes d'estat de les proteccions, de les deteccions de malware i algun informe executiu amb el resum de la informació global.

Els informes s'han de poder obtenir de forma immediata, amb les dades en temps real i també de forma periòdica per correu electrònic i en diferents formats pel seu posterior tractament.

3.3. Serveis d'assistència tècnica

S'inclou una bossa de 20 hores anuals de suport per eines Watchguard durant la vigència del contracte. Aquesta bossa d'hores consisteix en l'assistència tècnica especialitzada per a realitzar tasques complexes que requereixin de serveis especialitzats.

Aquestes hores s'aniran consumint segons les necessitats, de manera que les hores que no es disposin durant un any, s'acumularan a l'any següent.

Donada la complexitat del sistema es requereix que el licitador sigui partner o col·laborador autoritzat de Watchguard, fabricant dels equips. Caldrà presentar acreditació mitjançant l'aportació del corresponent certificat dels següents aspectes:

a) Ser partner amb nivell SILVER

b) Disposar amb, almenys un tècnic (consultor especialista), amb experiència demostrable d'almenys tres projectes realitzats en els últims 3 anys de suport en entorns similars als exposats, i disposar de les següents

certificacions: *WatchGuard Network Security, WatchGuard Firewall Policies y WatchGuard Fireware Essentials*.

El servei d'assistència podrà ser escalat directament al fabricant en cas que les incidències així ho requereixin.

4. Esquema Nacional de Seguretat

La solució obligatòriament ha d'estar inclosa en el "Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació."(CPSTIC) Publicat pel CCN (Centre Criptogràfic Nacional), dins de la família de protecció del Lloc de Treball com a QUALIFICAT.

Tecnologia Cloud Pública, és obligatòria que tingui la certificació de conformitat davant l'ENS, de categoria alta.

5. Durada del contracte

La durada del contracte serà de 3 anys amb possibilitat de pròrroga d'un any

6. Documentació que cal presentar

- Oferta econòmica
- Document justificatiu del tipus de certificació de partner de Watchguard

7. Confidencialitat

L'adjudicatari es compromet a mantenir la confidencialitat de totes les dades relatives al servei, en especial les contrasenyes, les configuracions, el tipus de programari i les seves versions i l'arquitectura del sistema

8. Obligacions de l'adjudicatari

Seran obligacions de l'adjudicatari, prestar el servei de la manera i forma indicada en el Plec de clàusules administratives i en el Plec de prescripcions tècniques.