Plec de prescripcions tècniques que regeixen el contracte de subministrament en modalitat d'arrendament d'ús de llicències i actualitzacions del programari antivirus. Exp. C-2025-17

Sumari

1. Objecte del contracte

L'objecte del contracte és el subministrament en modalitat d'arrendament d'ús de les llicències i actualitzacions del programa antivirus *Panda Adaptative Defense 360* per 3 anys per a llocs de treball i servidors que controli el comportament dels processos executats en cadascun dels equips del parc informàtic d'Aigües del Prat, SA a més a més de proveir les eines necessàries per a la detecció i desinfecció de programari maliciós. També han d'estar incloses les eines necessàries per a la gestió i administració per part del personal d'Aigües del Prat de la distribució i control del programa en els diferents equips.

Actualment Aigües del prat, SA disposa de 70 llicències de "*Panda Adaptative Defense 360*" en modalitat d'arrendament d'ús que finalitza el 20 de gener de 2026. Serà a partir d'aquesta data que ha de tenir efecte el nou contracte.

2. Abast

La solució ha de donar protecció inicialment als 60 equips que tenen instal·lat actualment la solució Panda Endpoint Protection i 10 llicències addicionals que s'instal·laran en servidors virtuals que actualment no disposen de protecció. La solució ha de permetre integrar en la mateixa plataforma les llicències addicionals que fossin necessàries durant la durada del contracte.

També ha de ser una solució que permeti protegir els mòbils amb sistema android que disposa Aigües del Prat, SA.

La solució ha d'estar instal·lada en la plataforma *cloud* del fabricant que actualment ja està utilitzant Aigües del Prat SA de forma que no sigui necessari l'ús de servidors interns per al seu funcionament i permeti reduir els costos d'explotació i manteniment del sistema.

La plataforma on s'allotgi la solució haurà d'estar ubicada a la Unió Europea.

3. Components del servei i funcionalitats tècniques

- Infraestructura cloud: Ha de permetre que els serveis es gestionin des de la infraestructura que el fabricant posa a disposició a tal efecte. La gestió ha de ser centralitzada des d'una única consola al núvol. Els processos capturats dels clients seran tractats al núvol de forma que l'impacte als sistemes corporatius sigui mínim.

- Agent únic a desplegar als equips (endpoint) que permetrà la protecció d'antivirus tradicional així com la protecció de processos desconeguts. L'agent ha de funcionar en els sistemes Windows actualitzats a les darreres versions i a més amés, en els mateixos sistemes que ja estan funcionant actualment i que van de Windows 7 fins a Windows 11 i de Microsoft Windows Server 2003 fins Microsoft Windows Server 2022. L'impacte sobre els dispositius del parc haurà de ser inferior o igual al 5% de rendiment de la CPU, memòria i disc.

- La desinstal·lació s'ha de protegir per contrasenya i el desplegament s'ha de poder fer per adreça IP, rang d'adreces IP, nom de la màquina i grups de Directori Actiu basat en polítiques de domini.

- Consola web: Ha de proporcionar una interfície per consultar les dades en temps real, gestionar informes i alertes i gestionar les actualitzacions dels equips. La consola web ha de ser única per totes les gestions.

- La protecció haurà de tenir dos components amb funcionalitats diferents però integrats a nivell de configuració i en un sol agent:

    - Protecció EPP (End Point Protection)

    - Protecció EDR (Endpoint Detection and Response)

- La plataforma EPP ha de comptar amb les següents funcionalitats:

    - Antivirus per arxius, correu i web. Ha de permetre la detecció i desinfecció de qualsevol tipus d'amenaça i detectar comportament d'aplicacions malicioses (malware). El correu es detectarà tant en SMTP com en POP3. Bloquejarà accessos a web amb possible contingut maliciós.

    - Protecció d'scripts i macros malicioses en documents office etc.

    - Firewall personal gestionat en local o des de la web que permeti bloquejar connexions entrants o sortints a petició, prevenció d'intrusions i crear regles de firewall.

    - Bloquejar tots els dispositius o dispositius específics (unitats d'emmagatzematge extraïbles, DVD, USB ...) per cada dispositiu ha de permetre configurar accions diferents (lectura, escriptura, bloqueig ...)

    - Bloquejar pàgines web no desitjades basant-se en categories o llistes.

- La plataforma EDR ha de comptar amb les següents funcionalitats:

    - Protegir contra malware avançat, PUP (programes no desitjats), amenaces zeroday tipus randsome i troians de nova generació indetectables pels antivirus.

    - Evitar el màxim d'infeccions de forma proactiva, no reactiva.

  - Evitar solucions que requereixin constants actualitzacions com signatures locals, motors heurístics que carreguin molt la CPU o sistemes de sandboxing que consumeixin molts recursos.
  - El sistema ha de capaç de catalogar el 100%dels processos executats en malware o goodware.
  - Bloquejar els processos desconeguts que s'intentin executar i puguin danyar la màquina o suposar un robatori d'informació.
  - Incloure un sistema Anti-Exploit que permeti la detecció i bloqueig de l'ús d'exploits coneguts o desconeguts.
  - Permetre configurar diferents nivells (més o menys restrictius) de bloqueig així com diferents nivells per permetre a l'usuari desbloquejar processos en funció dels diferents usuaris.

- Plataforma de gestió d'informació auditada que generi informació relacionada amb cada equip respecte:
  - Amenaces detectades i les accions efectuades.
  - Estat de les proteccions de cada equip.
  - Esdeveniments produïts en els processos.
  - Alertes detectades.
  - Timeline d'execució i anàlisi forense.
  - Arxius descarregats de tipus exe o zip.
  - Accessos a fitxers de dades.
  - Usuaris que accedeixin a certs arxius.
  - Informació relacionada amb els accessos al registre de windows.
  - Accions relacionades amb instal·lació, esborrat o modificació de drivers.
  - Aplicacions d'usuari amb gran consum d'ample de banda.
  - Processos executats en les màquines.
  - Aplicacions executades i instal·lades.
  - Consums d'ample de banda per usuari.
  - Màquines on han accedit els usuaris.
- La plataforma de gestió d'informació ha de ser amigable i fàcil de seguir sense tenir grans coneixements d'amenaces avançades.
- Servei d'alerta d'amenaces (Threat Hunting): Ha de poder realitzar l'alerta i incloure al sistema les mesures correctores.

- Neteja de sistemes: Neteja dels rastres d'amenaces o programes no desitjats que l'antivirus no hagi pogut eliminar. Ha de ser configurable de forma transparent a l'usuari final i s'ha de poder llençar en remot en qualsevol moment.
- El sistema ha de generar informació de cada equip de forma que pugui ser exportada posteriorment.
- La solució ha d'estar inclosa obligatòriament al "Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació" (CPSTIC) publicat pel Centre Criptogràfic Nacional (CCN) dins de la família d'antivirus/EPP com a QUALIFICAT.
- La solució ha de complir amb els requeriments fixat per l'esquema nacional de seguretat (ENS).

4. Termini i condicions de lliurament

L'empresa adjudicatària queda obligada a efectuar el subministrament com molt tard el dilluns 20 de gener de 2026, ja que el 21 del mateix mes finalitza la vigència de les llicències actuals.

L'empresa adjudicatària haurà de lliurar un document on consti el nombre de llicències adquirides, el producte i el codi de client assignat pel fabricant i els 3 anys de lloguer de les llicències. Les llicències hauran de ser a nom d'Aigües del Prat, SA

5. Suport i manteniment

S'establirà un manteniment i assistència tècnica que permeti assegurar el correcte funcionament dels llocs de treball i servidors mitjançat:

Servei de suport ofert pel fabricant en català o castellà amb telèfon d'accés.

Accés a les millores i actualitzacions del producte durant els tres anys d'activació del servei.

Web de suport i accés a fòrums i blogs d'informació sobre novetat i amenaces.

Suport tècnic 24x7x365 via correu electrònic ofert per tècnics certificats en la solució implementada.

Accés il·limitat al helpdesk.

Accés a anàlisi online de virus ocults.

Elisabet Vidal Bragulat
Directora de l'Àrea de Digitalització i Energia
El Prat de Llobregat, a novembre de 2025