



**PLEC DE PRESCRIPCIONS TÈCNIQUES QUE HA DE REGIR LA
CONTRACTACIÓ DEL SUBMINISTRAMENT DE
SUBSCRIPCIONS DE SOFTWARE I LLICÈNCIES PER A LA
SECURITZACIÓ DEL TELETREBALL, DELS PROVEÏDORS I DE
LA INFORMACIÓ**

(1-2026/0088-GEC)

ÍNDEX

PRIMERA. OBJECTE DEL CONTRACTE.....	2
SEGONA. PRODUCTES QUE INCLOU L'OFERTA	2

PRIMERA. OBJECTE DEL CONTRACTE

L'objecte del present contracte és el subministrament de subscripcions de software de seguretat per millorar i securitzar l'entorn de teletreball, així com per millorar i securitzar l'accés dels partners de Sistemes als servidors i reforçar la prevenció i protecció de les dades als llocs de treball, amb l'objectiu de:

- Millorar la seguretat de l'entorn de teletreball i garantir un accés segur als recursos i sistemes de l'organització.
- Reforçar la seguretat en l'accés dels partners de Sistemes als servidors, garantint un accés controlat i protegit.
- Millorar les mesures de prevenció i protecció de les dades als llocs de treball, reduint els riscos associats a possibles amenaces de seguretat.

SEGONA. PRODUCTES QUE INCLOU L'OFERTA

Producte	Descripció	Quantitat
Subscripció d'Agents d'Endpoint de Protecció Avançada (EPP/ATP) i Seguretat de Xarxa (VPN/ZTNA)	Subscripcions d'agents per a equips terminals (endpoints) que unifiquen capacitats de protecció de plataforma d'endpoint (EPP) i protecció avançada contra amenaces (ATP), integrant de forma nativa capacitats d'accés segur mitjançant client ZTNA (Zero Trust Network Access) i serveis VPN tradicionals.	250
Subscripció de Gestió d'Accessos Privilegiats (PAM) en Alta Disponibilitat	Subscripcions per a una solució de Gestió d'Accessos Privilegiats (PAM, Privileged Access Management). La solució ha de permetre el control, la monitorització i l'auditoria d'accessos per a usuaris i comptes privilegiats (administradors de xarxa, sistemes, etc.).	10
Subscripció de Prevenció de Pèrdua de Dades d'Empresa (DLP) i Servei d'Implementació de Millors Pràctiques	Subscripcions per a una solució integral de Prevenció de Pèrdua de Dades (DLP – Data Loss Prevention), orientada a la protecció de la informació sensible en ús endpoints	300

1. Les especificacions tècniques de les subscripcions d'Agents d'Endpoint de Protecció Avançada (EPP/ATP) i de Seguretat de Xarxa (VPN/ZTNA) són les següents:

1.1. Agent Unificat de Seguretat i Protecció

- La solució ha de proporcionar un únic agent instal·lable als equips terminals (Windows, macOS, i opcionalment Linux) que integri múltiples capacitats de seguretat, protecció i connectivitat de forma nativa, sense dependència de components de tercers.
- L'agent ha de permetre l'activació modular de funcionalitats (Antimalware/EPP, Sandbox/ATP, VPN, ZTNA, control de postura, filtratge web, etc.) des d'una mateixa plataforma de gestió.

1.2. Protecció de l'Endpoint i Defensa contra Amenaces Avançades (EPP/ATP)

- Protecció de Plataforma (EPP): L'agent ha d'incloure capacitats de seguretat de nova generació (NGAV), incloent protecció automatitzada contra programari maliciós (*malware*), ransomware i exploits de vulnerabilitats.
- Protecció Avançada (ATP): Ha d'integrar capacitats de detecció d'amenaces avançades i de zero-day mitjançant la integració nativa amb serveis de *Sandbox* (al núvol o local) per a l'anàlisi dinàmica de fitxers sospitosos.
- Seguretat Web i Filtratge de Continguts: L'agent ha de realitzar filtratge web i control d'aplicacions directament des del terminal, protegint l'usuari tant si es troba dins com fora de la xarxa corporativa (on-net i off-net).
- Anàlisi de Vulnerabilitats: Ha d'incloure un motor de detecció i escaneig de vulnerabilitats en el programari instal·lat a l'equip terminal per mitigar la superfície d'atac.

1.3. Accés Segur: VPN i ZTNA

- L'agent d'endpoint ha d'incloure de forma nativa les següents funcionalitats d'accés segur:
 - o Client VPN: Suport complet per a connexions IPsec i SSL/TLS, amb xifrat robust i mecanismes d'autenticació forta (incloent SAML/IdP externs i MFA).
 - o Capacitats de ZTNA: Accés basat en la filosofia *Zero Trust*, validant contínuament la identitat de l'usuari i l'estat/postura del dispositiu per a cada aplicació, sense necessitat d'establir un túnel de xarxa complet (full-tunnel).
- El sistema ha de permetre la coexistència i interoperabilitat transparent per a l'usuari entre la VPN tradicional i l'accés ZTNA dins del mateix agent.

- S'ha de suportar l'accés per aplicació (*application-based access*) amb inspecció, verificació de context i control granular.

1.4. Integració amb Infraestructura NGFW existent

- La solució d'endpoint ha d'integrar-se de forma nativa amb la plataforma de tallafocs NGFW existent de la mateixa arquitectura del fabricant (Fortinet Security Fabric), sense requerir passarel·les addicionals ni connectors externs de tercers.
- L'agent ha de:
 - o Identificar de manera contínua l'usuari i el dispositiu davant el NGFW corporatiu.
 - o Proporcionar telemetria en temps real sobre l'estat de seguretat de l'endpoint (postura, infeccions, vulnerabilitats).
 - o Permetre la generació i assignació dinàmica d'etiquetes de seguretat (*tags*) basades en aquesta telemetria i en l'estat de compliment de l'equip.
- El NGFW ha de poder utilitzar aquestes etiquetes de manera immediata dins de les seves polítiques de seguretat (*policies identity-aware i posture-aware*), tant per al trànsit local com remot.

1.5. Control de Postura i Compliment (Endpoint Compliance)

- L'agent ha de permetre definir polítiques estrictes de postura del dispositiu (com a mínim: estat de l'antivirus, detecció de vulnerabilitats, sistema operatiu, nivell de pegats, xifrat de disc, firewall actiu, presència de programari prohibit, etc.).
- Aquestes polítiques de postura han de poder-se utilitzar com a condició indispensable per a l'accés a recursos interns o externs (polítiques ZTNA/VPN).
- S'ha de permetre la remediació automàtica o assistida de l'estat de l'endpoint en cas d'incompliment d'alguna directiva.

1.6. Consola de Gestió Centralitzada

- La solució ha d'incloure una consola centralitzada de gestió (FortiClient EMS) amb les següents característiques:
 - o Model SaaS: Consola en modalitat de servei al núvol (SaaS) altament disponible i integrada amb la infraestructura de seguretat existent.
 - o Gestió Centralitzada: Administració unificada de tots els agents, configuracions de seguretat, perfils de protecció EPP/ATP, configuracions VPN i regles ZTNA.

1.7. Desplegament i Actualització: Capacitats de desplegament massiu (*mass deployment*) compatible amb eines Active Directory / MDM i actualització remota/esglaonada dels agents.

1.8. Volumetria i Durada

- Total Subscripcions: 250
- Durada: 3 anys.

2. Les especificacions tècniques de la Subscripció de Gestió d'Accessos Privilegiats (PAM) en Alta Disponibilitat són les següents:

2.1. Funcionalitats Core de Privileged Access Management (PAM)
La solució ha d'incloure de forma nativa les següents capacitats:

- Vaulting segur de credencials amb xifrat robust i control d'accés granular.
- Gestió del cicle de vida de credencials privilegiades, incloent rotació automàtica, expiració i descobriment de comptes.
- Accés privilegiat sense exposició de credencials (password-less o proxy d'accés).
- Gravació completa de sessions (RDP, SSH, web) amb possibilitat de reproducció i cerca.
- Auditoria completa i traçabilitat de totes les accions privilegiades.
- Protecció davant comandes malicioses o patrons d'injecció mitjançant inspecció de sessió en temps real.

2.2. Integració amb Sistemes d'Identitat i Infraestructura existent

- Integració nativa amb directoris corporatius (Active Directory, LDAP o equivalents) per a autenticació i autorització.
- Suport per autenticació multifactor (MFA) mitjançant integració amb proveïdors externs o mecanismes propis.
- La solució ha de permetre la definició de rols i polítiques basades en identitat i context.

2.3. Integració amb la Plataforma d'analítica i logging

- La plataforma ha de contemplar, com a mínim:

- o Exportació estructurada de logs i esdeveniments en temps real, mitjançant protocols estàndard
- o Correlació immediata entre esdeveniments d'accés privilegiat i esdeveniments de xarxa, permetent una visió unificada de l'activitat de l'usuari.
- o Inclusió d'informació contextual completa (identitat, origen, destinació, tipus de sessió, accions executades).
- o Integració nativa amb plataformes d'analítica i logging de seguretat existents, permetent correlació avançada sense desenvolupaments addicionals.
- o Capacitat de visualització unificada d'esdeveniments de xarxa i accessos privilegiats.
- o Definició de regles de detecció i alertes basades en comportament d'usuaris privilegiats.

2.4. Arquitectura i Alta Disponibilitat (HA)

- La solució s'ha de desplegar en format virtual appliance compatible amb entorns de virtualització corporatius (mínim VMware vSphere 8.x o equivalent).
- Ha de suportar configuracions d'Alta Disponibilitat en clúster per garantir la continuïtat del servei.
- Es requereix:
 - o Desplegament mínim de dues instàncies amb funcionalitat de failover automàtic.
 - o Mode d'operació Active-Passive amb sincronització d'estat i configuració en temps real.
- La solució ha de garantir:
 - o Persistència de sessions en cas de fallada.
 - o No pèrdua de dades de registre ni d'auditoria.

2.5. Llicenciament i Capacitat

- La solució ha de llicenciar-se per nombre d'usuaris concurrents.
- Es requereix una capacitat mínima de 10 usuaris concurrents.
- La llicència ha d'incloure totes les funcionalitats descrites sense mòduls addicionals obligatoris.

2.6. Seguretat i Protecció Avançada

- La plataforma ha de disposar de mecanismes de protecció davant amenaces, incloent:
 - o Inspecció de trànsit de sessions privilegiades (AV i DLP)

2.7. Registre, Auditoria i Compliment

- Tots els accessos i accions han de quedar registrats amb:
 - o Identitat d'usuari, sistema accedit, hora i accions realitzades.
- Exportació de logs a sistemes externs en temps real.

2.8. Suport i Manteniment

- Inclou suport tècnic avançat amb SLA 24x7.
- Accés a actualitzacions, pegats de seguretat i noves versions durant la vigència del contracte.

2.9. Volumetria i Durada:

- Usuaris Privilegiats: La solució ha de cobrir l'accés per a un rang de 10 usuaris concurrents.
- Durada: 3 anys

3. Les especificacions tècniques de les Subscripcions de Prevenció de Pèrdua de Dades d'Empresa (DLP) i del Servei d'Implementació de Millors Pràctiques són les següents:

3.1. Cobertura DLP Multivector

La solució ha de proporcionar protecció davant l'exfiltració de dades mitjançant un enfocament multivector basat en agent, sent capaç de:

- Detectar, monitoritzar i bloquejar la sortida de dades a través de canals com:
 - o Dispositius extraïbles (USB i similars)
 - o Navegació web i aplicacions web
 - o Aplicacions locals i de tercers
 - o Serveis cloud i aplicacions SaaS accessibles des de l'endpoint

- o Impressió i portapapers (clipboard)

Es valorarà especialment:

- Capacitat de visibilitat i control independent del canal o protocol utilitzat.
- Capacitat d'aplicar controls fins i tot en escenaris fora de la xarxa corporativa.

3.2. Classificació i Detecció de Dades Sensibles

- La solució ha d'incloure capacitats avançades de classificació de dades, com:
 - o Diccionaris, expressions regulars i patrons predefinits.
 - o Fingerprinting de documents.
 - o Capacitats de classificació automàtica basades en contingut i context.
 - o Capacitats de classificació basades en context (usuari, aplicació, acció...).
 - o Capacitat d'identificar dades sensibles encara que siguin modificades parcialment

3.3. Gestió de Risc d'Usuaris Interns (Insider Risk Management)

- La solució ha d'incloure capacitats específiques per a la detecció i gestió de riscos interns, incloent:
 - o Anàlisi de comportament d'usuaris.
 - o Detecció d'activitats anòmales o sospitoses relacionades amb dades sensibles.
 - o Assignació dinàmica de nivells de risc per usuari.
- Es valorarà especialment:
 - o Capacitat de correlacionar esdeveniments en una línia temporal d'activitat (timeline) per usuari.
 - o Capacitat d'automatitzar accions en funció del nivell de risc.
 - o Integració del risc d'usuari en polítiques de seguretat.

3.4. Consola de Gestió Centralitzada

- La solució ha d'incloure una plataforma de gestió centralitzada que permeti:
 - o Definició i administració de polítiques DLP unificades.
 - o Visibilitat en temps real dels esdeveniments i incidents.
 - o Capacitats d'investigació i anàlisi forense.



- Es valorarà especialment:
 - o Model SaaS.
 - o Integració amb plataformes d'analítica i logging existent.

Capacitat d'exportar o compartir informació amb altres components de seguretat per a una resposta coordinada.

3.5. Volumetria i Durada:

- Total Subscripcions: 300 unitats d'endpoints (agents).
- Durada de Subscripció d'Agents: 1 any

Carles Casas Vidal
Cap de Servei de Serveis Informàtics

DILIGÈNCIA: Per fer constar que el present plec de clàusules administratives particulars que ha de regir la contractació del subministrament de subscripcions de software i llicències per a la securització del teletreball, dels proveïdors i de la informació per a BASE-Gestió d'Ingressos, es va aprovar per decret de la Presidència en data 21 d'octubre de 2026.

El secretari

<signatari1>

Contra aquests plecs es podrà interposar recurs de reposició potestatiu davant del president de BASE-Gestió d'Ingressos en el termini d'un mes o bé directament impugnar-los davant del Tribunal d'Instància de Tarragona, Secció contenciosa administrativa en el termini de dos mesos. En ambdós supòsits el termini d'impugnació es comença a computar des de l'endemà de la publicació dels plecs en el perfil de contractant.