

**PLEC DE CONDICIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL  
SERVEI DE SEGURETAT DEL CORREU ELECTRÒNIC PER A  
MICROSOFT 365 EN MODALITAT CLOUD EMAIL SECURITY (CES)**

**EXPEDIENT: 26SER0920**

## ÍNDEX

1	Introducció.....	3
2	Objecte del contracte .....	3
3	Vigència del contracte .....	3
4	Abast del contracte.....	4
5	Condicions específiques del contracte .....	4
6	Característiques Tècniques.....	4
6.1	Arquitectura de la solució.....	6
6.2	Capacitats d'Intel·ligència artificial.....	6
6.3	Informes i gestió de la plataforma. ....	7
7	Suport i garanties.....	7
7.1	Compliment normatiu. ....	8
8	Servei i dates de lliurament .....	8
9	Suport Configuració .....	8
10	Qualitat i Mediambient .....	8

## 1 Introducció

El Consorci Corporació Sanitària Parc Taulí de Sabadell és un consorci públic de la Generalitat de Catalunya, el màxim òrgan de govern del qual és el Consell de Govern, i que gestiona els següents centres: Hospital de Sabadell, UDIAT Centre Diagnòstic, Albada Centre Sociosanitari, Salut Mental Parc Taulí, Atenció Primària Parc Taulí, Atenció a la Dependència Parc Taulí, i també els serveis de Sabadell Gent Gran Centre de Serveis, a través d'una societat anònima. El Consorci és el soci únic d'aquesta darrera entitat i nomena a tots els membres del seu consell d'administració. A més a més, és Unitat Docent de la Facultat de Medicina de la Universitat Autònoma de Barcelona (UAB) i té la consideració d'Hospital Universitari.

El Consorci Corporació Sanitària Parc Taulí es troba vinculat a la Fundació Institut Investigació i Innovació Parc Taulí, el patronat de la qual nomena a la majoria de membres. Les institucions del Consorci reben el suport de la Fundació Parc Taulí en aspectes de recerca, innovació i docència, en la formació científica i mèdica dels professionals i, en general, en el desenvolupament dels coneixements que sustenten el model assistencial.

En aquest document ens referirem al Consorci Corporació Sanitària Parc Taulí com a **CCSPT**.

La missió del CCSPT és donar assistència resolutiva, integral, personalitzada i de qualitat als ciutadans de la seva àrea de referència tot fomentant l'equitat, la continuïtat assistencial, la satisfacció, l'eficiència i la sostenibilitat.

Actualment el CCSPT atén una població de referència de 407.864 habitants, disposant d'una infraestructura de 670 llits d'aguts i 196 llits sociosanitaris. Una mostra de la seva activitat assistencial serien les més de 400 urgències diàries de mitjana, més de 250 intervencions quirúrgiques diàries de mitjana o més de 2.700 consultes externes diàries, també de mitjana. Gestiona diverses empreses amb Convenis Col·lectius diferents (SISCAT, Oficines i Despatxos, Sociosanitari i Dependència) amb una plantilla mensual contractada d'aproximadament uns 4.300 professionals, que també inclou Sabadell Gent Gran (SGG) i la Fundació Institut d'Investigació i Innovació Parc Taulí (FI3PT).

## 2 Objecte del contracte

Contractació d'un **servei de seguretat del correu electrònic per a Microsoft 365** en modalitat **cloud email security** (CES), que inclogui llicències, desplegament, configuració, suport i manteniment

CODI CPV: <https://contractacio.gencat.cat/ca/gestionar-contractacio/eines/cpv/>

72222300-0 Serveis de tecnologies de la informació

## 3 Vigència del contracte

El Contracte tindrà una durada aproximada de 1 any, si pertoca el contracte preveu possibilitat d'ampliació d'un 20%. El contracte preveu possibilitat de prorroga anualment.

## 4 Abast del contracte

L'abast del servei és el següent:

PBL	Entitat	Import sense IVA	Import IVA	Import amb IVA
Exercici 2026	CCSPT	48.600,00 €	10.206,00 €	58.806,00 €
<b>TOTAL</b>		<b>48.600,00 €</b>	<b>10.206,00 €</b>	<b>58.806,00 €</b>

## 5 Condicions específiques del contracte

L'oferta es farà per la totalitat dels elements que componen el LOT. No s'acceptaran en cap cas ofertes parcials que no compreguin tots els elements del LOT.

L'oferta presentada no podrà ser superior a l'import total de la licitació del LOT.

A tots els efectes, s'entendrà que en l'oferta i en els preus proposats per l'adjudicatari s'inclouen totes les despeses que hagi de realitzar per al compliment del contracte (transport, taxes, treballs, garanties, accessoris i mà d'obra).

Els licitadors hauran d'aportar, dins del sobre digital, tant les fitxes tècniques del fabricant, com qualsevol altre documentació tècnica necessària que permeti validar els requeriments que el CCSPT detalla en aquest plec, així com la seva ubicació dins de la documentació aportada. En cas que falti aquesta informació o no es compleixi algun requeriment, el licitador quedarà exclòs.

Es requerirà que el licitador asseguri l'entrega dels elements que componen el LOT en la data acordada en el Kick-off inicial d'implantació del projecte, i no mes enllà de 15 dies un cop signat el contracte. El no compliment d'aquest apartat suposarà l'aplicació de les penalitzacions estàndards del contracte.

Les comandes seran enviades per el CCSPT via email, en format PDF, a la direcció de correu electrònic que així indiqui l'adjudicatari.

## 6 Característiques Tècniques

El CCSPT es troba **en ple procés de migració** del servei de correu corporatiu **on-premises** basat en **GroupWise** —que ja disposa d'un antispam propi— cap a **Microsoft 365 en el núvol**. En aquest escenari de **convivència i transició** (coexistència de plataformes, canvis d'MX i d'enrutament, nous fluxos d'autenticació i federació), l'exposició al **phishing, malware i BEC** augmenta, i les capacitats estàndard d'M365 (**EOP/Defender**) són

**necessàries però no suficients** per fer front a tècniques avançades (URLs que muten després del lliurament, adjunts polimòrfics, enginyeria social sense codi maliciós, atacs dirigits al sector salut).

Per tal de **garantir la continuïtat assistencial**, protegir la **confidencialitat de dades de salut** i reduir la finestra d'exposició durant i després de la migració, es requereix incorporar una **capa especialitzada addicional** de seguretat de correu, en modalitat **servei cloud i neutral de fabricant**, amb, com a mínim:

- **Prevenició post-delivery via API** amb **retirada automàtica** de missatges ja lliurats quan es detectin indicadors de compromís.
- **Anàlisi profunda d'URLs i adjunts** (detonació/sandboxing) i **protecció time-of-click**.
- **Detecció de BEC/frau** basada en context i comportament, més enllà de signatures.
- **Cobertura de correu sortint (Outbound)** per evitar **fuites de dades** i propagació a tercers.
- **Quarantena i governança centralitzades, RBAC**, traçabilitat i **informes** executius/operatius.
- **Integració amb SIEM** corporatiu (p. ex., GLORIA del CCN-CERT) i polítiques de **retenció/immutabilitat** d'evidències d'acord amb **ENS** i guies **CCN-STIC**.
- **Opcions de desplegament flexibles** (API sense canvi d'MX i/o inline) per minimitzar risc operatiu durant la migració i facilitar pilots per fases.

Aquesta contractació permet **homogeneïtzar** la protecció en el nou entorn M365, **reduir el risc** d'incidents que podrien afectar serveis crítics, **agilitzar la resposta** (MTTR) i **demostrar compliment** de l'ENS, les guies CCN-STIC, les directrius de l'Agència de Ciberseguretat de Catalunya i el **RGPD**, mantenint un model de cost **previsible i escalable** propi d'un servei cloud.

La solució haurà de proporcionar cobertura en els àmbits següents:

- Protecció del correu entrant i intern.
- Prevenició d'amenaques conegudes i desconegudes (dia zero).
- Protecció davant d'atacs basats en adjunts, enllaços i text interpretant el llenguatge natural (LLM).
- Detecció i mitigació d'atacs BEC, ATO i de pesca avançat.
- Integració amb plataformes de col·laboració i emmagatzematge al núvol (Microsoft 365, Google Workspace, Exchange, etc.).
- Capacitats de remediació post-lliurament i eliminació de correus maliciosos.
- La plataforma ha de proveir l'opció futura d'ampliar les funcionalitats de protecció del correu a la protecció del navegador i els entorns col·laboratius.

Es pretén securitzar totes les comptes que estiguin actives en l'entorn M365, actualment unes 6.400 comptes entre comptes personals i comptes compartits (Shared mail box), amb una fluctuació per cobertures en èpoques vacacionals aproximada d'un màxim del 15%. S'ha de donar servei a totes i cadascuna dels comptes

independentment del nombre, que s'haurà d'anar regularitzant durant la durada del contracte, tant d'increment com de decrement.

Cal fer-ne un seguiment del servei un cop al mes, amb l'entrega d'informes sobre comptes compartides, fluctuacions mensuals, incidències de securització, etc...

## **6.1 Arquitectura de la solució.**

La solució haurà d'estar basada en una arquitectura nativa al núvol (ICES), modular i escalable, que permeti la inspecció dinàmica i estàtica del trànsit de correu electrònic. Haurà d'incloure múltiples capes d'anàlisi, entre les quals:

- Capa antispam i intel·ligència d'amenaçes global.
- Capa antievasió per a detecció de contingut ocult o comprimit.
- Capa antiphishing amb motors de reconeixement visual i semàntic.
- Capa anti-BEC amb detecció de suplantació de domini, nom i comportament anòmal.
- Capa d'anàlisi dinàmica (sandbox) amb execució controlada d'arxius i detecció d'exploits de dia zero.
- Mecanisme de decisions i regles que permeti crear polítiques avançades personalitzables.

## **6.2 Capacitats d'Intel·ligència artificial.**

La solució haurà d'incorporar motors de detecció basats en IA/ML capaços d'analitzar patrons visuals, semàntics i de comportament per identificar amenaces desconegudes. Entre les capacitats esperades s'inclouen:

- Detecció visual de llocs de phishing i formularis falsos.
- Detecció semàntica basada en models de llenguatge (LLM).
- Detecció de suplantació de marca mitjançant visió artificial.
- Detecció d'ofuscació, dominis semblants i segrest de fils.
- Detecció d'anomalies d'inici de sessió i de comportament d'usuari.

## 6.3 Informes i gestió de la plataforma.

La plataforma haurà de proporcionar un panell de gestió centralitzat, amb funcionalitats de cerca, filtratge, exportació i informes personalitzables. S'hi han d'incloure:

- Informes periòdics d'activitat i tendències.
- Resums d'incidents gestionats.
- Estadístiques de detecció, falsos positius i remediacions.

## 7 Suport i garanties

Totes les garanties de les que són objecte el material d'aquest plec, que començarà el mateix dia de recepció de l'objecte del contracte, i hauran de ser registrades per l'adjudicatari.

L'adjudicatari ha de disposar i proporcionar, com a mínim, un servei d'atenció telefònica i una persona de contacte per tal de poder gestionar les incidències relacionades.

Ha d'existir i el CCSPT ha de ser coneixedor d'una matriu d'escalat d'incidències.

Servei de Resposta a Incidents (IR) inclòs 24x7. En cas que no s'especifiqui un SLA més restrictiu, el temps de resposta, definit com el període màxim de temps entre la notificació de l'avaria i la resposta d'un tècnic especialitzat, serà de 4h laborables. El temps de resolució, definit com el període màxim de temps entre la notificació de l'avaria i la posta en correcte funcionament de l'equip, ja sigui per resolució de l'avaria o per substitució del material, no ha de ser superior a 8h laborables.

En cas necessari, ja sigui per la naturalesa de l'avaria, o quan la resolució no es pugui realitzar en el termini establert, l'adjudicatari proporcionarà l'alternativa funcional amb característiques iguals o superiors.

L'oferta haurà d'incloure un servei gestionat de Resposta a Incidents (IR) operatiu 24x7, que actuï com a extensió del SOC del client. Aquest servei haurà de:

- Supervisar alertes i incidents detectats per la plataforma.
- Validar falsos positius i falsos negatius.
- Emetre informes i recomanacions periòdiques.
- Permetre l'eliminació de correus maliciosos de les bústies d'usuaris.
- Atendre sol·licituds de recerca i anàlisi forense.

## 7.1 Compliment normatiu.

La solució haurà de complir estàndards internacionals de seguretat i protecció de dades, incloent com a mínim:

- Certificació ISO/IEC 27001 o equivalent.
- Compliment SOC-2 Tipus II o equivalent.
- Compatibilitat amb normativa RGPD i legislació europea en matèria de privadesa.

## 8 Servei i dates de lliurament

L'adjudicatari haurà d'entregar l'objecte del contracte de cada LOT com a màxim, 15 dies després de la signatura del contracte o quan s'acordi en el kick-off inicial d'implantació de projecte.

## 9 Suport Configuració

Per tots els elements objecte d'aquest plec, és imprescindible i obligatori que el material, i software associat, ofert pel licitador, sigui completament compatible amb totes les aplicacions i la infraestructura utilitzats en el CCSPT.

A més, l'adjudicatari haurà de donar suport en la configuració, segons requisits del CCSPT si és necessari, per tal de que el comportament dels dispositius s'ajusti a les aplicacions i la infraestructura en els que s'empraran els diferents aparells, si s'escau.

## 10 Qualitat i Mediambient

El material de la present licitació ha de ser conforme, en el moment del lliurament, amb la normativa vigent de la Unió Europea i de l'Estat pel que fa a aspectes de qualitat, ergonomia, medi ambient, estalvi energètic, compatibilitat electromagnètica, reducció de la petjada CO<sub>2</sub> emesa i seguretat, així com a normatives de disseny, fabricació, embalatge i etiquetatge.