# PLEC DE CONDICIONS TÈCNIQUES PER LA CONTRACTACIÓ DE SERVEIS DE SUPORT EN TECNOLOGIES CHECK POINT

## 1 MOTIVACIÓ

Els sistemes tallafocs de xarxa constitueixen la primera i més imprescindible barrera de protecció de les xarxes de dades modernes. Es basen en una combinació de maquinari i programari dedicat a analitzar en profunditat tot el tràfic entrant i sortint de l'organització, així com el tràfic entre els principals segments interns. Els tallafocs són la base del sistema de seguretat municipal i es descriuen al document intern de l'Ajuntament de Girona "PR-01 Arquitectura de la Seguretat", que sustenta la certificació municipal en el marc de l'**Esquema Nacional de Seguretat**, regulat pel Reial decret 311/2022.

Per protegir la xarxa de dades municipal, es disposa de sistemes tallafocs del fabricant Check Point Software Technologies, configurats en alta disponibilitat, adquirits l'any 2014 i ampliats els anys 2019 i 2023. Aquest fabricant ha estat i continua essent reconegut com un dels líders del sector per analistes independents com Gartner, i els seus productes estan homologats dins el Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i la Comunicació (CPSTIC) del Centre Criptològic Nacional, en coherència amb les recomanacions de l'Esquema Nacional de Seguretat.

En aquests sistemes, el maquinari determina la capacitat de processament del trànsit, mentre que el programari evoluciona de manera contínua per fer front a noves amenaces. És aquest programari el que incorpora les funcionalitats avançades de prevenció d'intrusions, filtratge d'aplicacions, control d'amenaces avançades i integració amb altres mecanismes de seguretat.

Al llarg dels darrers anys, el Servei de Sistemes i Tecnologies de la Informació ha realitzat una inversió molt significativa en formació especialitzada del personal tècnic en la plataforma de Check Point Software Technologies, així com en la definició, ajust i optimització de les polítiques de seguretat. Aquesta configuració no és estàndard ni genèrica, sinó altament adaptada a la realitat organitzativa, als fluxos de comunicacions interns i externs i als requisits normatius municipals i cal adaptar-ho de forma continuada a les noves amenaces que apareixen i a les noves funcionalitats que publica el mateix fabricant.

Cal destacar igualment que els tallafocs actuals es troben plenament integrats amb la resta de l'ecosistema de seguretat municipal: sistemes de monitoratge, plataformes de registre i correlació d'esdeveniments, eines de gestió centralitzada, mecanismes d'autenticació i serveis corporatius i, molt especialment, amb la plataforma MDR que actua com a centre d'operacions de ciberseguretat (SOC) municipal. Aquesta integració s'ha consolidat progressivament al llarg dels anys, garantint coherència en les polítiques de seguretat, traçabilitat dels esdeveniments i eficiència en la gestió operativa.

Tot i que els tècnics de sistema municipals disposen de bons coneixements de la plataforma Check Point que permeten la gestió diària dels sistemes, no es disposa de les certificacions per part del fabricant per poder realitzar operacions més complexes, que a més, s'haurien d'actualitzar de forma continuada. Aquestes operacions poden tenir un impacte importantíssim en la seguretat dels sistemes municipals i comprometre o protegir la seguretat de les dades que es custodien i la continuïtat de les operacions de la corporació.

La present licitació te per objecte la contractació de serveis de suport en tecnologies Check Point per recolzar la tasca dels tècnics municipals en aquelles necessitats especialitzades que requereixen un coneixement més profund de la tecnologia, aportant un valor addicional en els aspectes de seguretat del sistema i de continuïtat dels serveis.

## 2 OBJECTE DEL CONTRACTE

L'objecte del contracte son els serveis de suport, per un període de 36 mesos, del clúster de tallafocs municipals:

- Serveis de gestió i optimització avançada
- Serveis d'operativa tècnica avançada i control mensual
- Serveis de suport 24x7

## 3 SERVEIS REQUERITS

Es requereixen serveis professionals per part de l'integrador per realitzar tasques especialitzades que queden fora de l'abast dels tècnics municipals i que requereixen certificacions específiques per part del fabricant Check Point Software Technologies, per un període de 36 mesos.

- Serveis de gestió i optimització avançada:
    - Monitorització dels tallafocs per detectar variacions inusuals en el consum de recursos, en especial de la CPU i de les interfícies de xarxa
    - Optimització del maquinari dels tallafocs per evitar colls d'ampolla
    - Revisió dels sistemes per garantir el compliment normatiu, en especial l'**Esquema Nacional de Seguretat (RD311/2022)** i la **Directiva (UE) 2022/2555** del Parlament Europeu i del Consell Europeu, de 14 de desembre de 2022 NIS2 (*Network and Information Security 2*)
    - Serveis de resposta experta per part d'enginyers amb alta qualificació L3 enfront d'incidents
- Serveis d'operativa tècnica avançada i control
    - Serveis mensuals d'enginyeria sobre el clúster de tallafocs
        - Optimització del sistema operatiu GaiaOS per permetre les màximes prestacions dels mòduls SecureXL i CoreXL
        - Optimització dels mòduls Sandblast i de filtrat de capa 7
        - Auditoria del sistema d'alta disponibilitat del clúster per garantir un temps d'indisponibilitat zero
    - Serveis mensuals de manteniment continu
        - Informes mensuals de seguretat i de logs, amb analítica detallada mitjançant SmartEvent per identificar patrons d'atac i intents de fuita de dades

        - Ajustament mensual de les regles del mòdul de IPS (*Intrusion Prevention System*) per identificar patrons d'atacs reals sense afectació al rendiment del sistema
        - Suport especialitzat L3 per gestió de canvis complexos i resolució d'incidències de xarxa d'alt nivell
    - Actuacions evolutives amb freqüències a determinar en funció de les necessitats reals (trimestrals o anuals)
        - Auditories de *hit count* per neteja de regles obsoletes
        - Actualització de *Jumbo hotfixes* i tancament de vulnerabilitats del sistema operatiu
        - Integració amb *Identity Awareness* per control de trànsit en base a usuaris reals
        - Actuacions de *disaster recovery* i verificació de còpies de seguretat per garantir temps de recuperació d'acord amb el BIA municipal
    - Actuacions evolutives sobre el mòdul de SmartEvent, al llarg de tot el període de contracte, amb la finalitat de reduir els falsos positius, millorar la priorització dels esdeveniments crítics i permetre actuacions automàtiques més segures
        - Revisió de SmartEvent, Correlation Unit, Log Server i les fonts de logs
        - Ajust dels llindars , severitats, finestres temporals i excepcions de la Event Policy
        - Identificació i reducció d'esdeveniments repetitius o poc rellevants
        - Priorització d'alertes IPS, anti-bot, VPN, d'administració, d'escanejos i accessos anòmals
        - Definició de casos d'ús i de la matriu d'accions associades
        - Automatització de l'enviament de correus, *traps* SNMP, scripts, *webhooks* i de bloquejos temporals
        - Informes mensuals en relació a l'evolució de les accions executades, reducció del soroll i recomanacions pel següent periode
- Serveis de suport 24x7
    - Serveis d'atenció ininterrompuda per resolució d'incidències de programari i de configuració
    - Substitució avançada de maquinari

## 4 EXECUCIÓ DE LA PRESTACIÓ

### 5.1 Interlocució

L'empresa adjudicatària nomenarà un *Service Manager* per a la interlocució amb l'ajuntament de Girona, per a qualsevol aspecte (administratiu, tècnic, de serveis, etc.) relacionat amb el contracte.

### 5.2 Temps de resposta

L'empresa adjudicatària haurà de donar resposta a les sol·licituds no programades previstes a l'apartat 3 segons la següent taula:

| Tipus de petició | Temps de resposta | Temps d'intervenció |
|---|---|---|
| Incidències molt greus (afectació molt greu a la seguretat o degradació de | 15 minuts | 30 minuts |

| | | |
|---|---|---|
| l'operativa que afecta als usuaris) | | |
| Incidències greus (possible afectació a la seguretat o potencial degradació de l'operativa) | 15 minuts | 1 hora |
| Incidències lleus o sense afectació al servei | 1 hora | 1 dia |
| Peticions de servei | 1 dia | 2 dies |

### 5.3 Certificacions

Per a la correcta execució, continuïtat del servei i mitigació de riscos en l'administració de la infraestructura de seguretat perimetral de l'òrgan contractant, es requereix que l'empresa adjudicatària disposi de personal tècnic que acrediti de forma oficial les següents certificacions de la línia professional de Check Point Software. Cadascuna d'elles respon a una necessitat operativa i de gestió crítica per al servei:

1. Check Point Certified Security Administrator (CCSA)

- **Justificació de la necessitat:** És la certificació base imprescindible per garantir que els tècnics disposen del coneixement operatiu per a la gestió diària dels tallafocs.
- **Funció en el contracte:** Aquesta certificació assegura que el personal de primer i segon nivell domina les tasques de provisió i manteniment rutinari, tals com la creació i modificació de polítiques d'accés (regles de firewall), la gestió d'usuaris, la configuració de xarxes privades virtuals (VPN) tant de seu a seu com de lloc a lloc per a teletreballadors, i el monitoratge bàsic de logs de trànsit. Sense aquesta certificació, no es pot garantir un control bàsic lliure d'errors humans que puguin exposar l'organització.

2. Check Point Certified Security Master (CCSM)

- **Justificació de la necessitat:** Representa el màxim nivell d'expertesa global en l'arquitectura de Check Point Infinity. Valida una capacitat d'enginyeria superior per sobre de la mera administració.
- **Funció en el contracte:** L'adjudicatari ha d'enfrontar tasques de disseny, canvis estructurals en la xarxa, auditories de seguretat profundes i implementació de mecanismes de prevenció d'amenaces d'última generació (com sandboxing o inspecció de trànsit xifrat SSL/TLS complex). Els perfils CCSM actuaran com a enginyers principals o consultors de màxim nivell per coordinar l'evolució tecnològica de la infraestructura i assegurar que les polítiques s'alineen amb les millors pràctiques globals de seguretat del fabricant.

3. Check Point Certified Maestro Expert (CCME)

- **Justificació de la necessitat:** Check Point Maestro és la tecnologia d'orquestració a hiperescala que permet agrupar múltiples tallafocs físics per treballar com un sol sistema de manera elàstica (tecnologia de *clustering* avançat / *Hyperscale Orchestrator*).
- **Funció en el contracte:** Donat que la infraestructura objecte d'aquest contracte disposa d'entorns d'alta disponibilitat de missió crítica, és fonamental disposar d'experts CCME. Aquests tècnics estan capacitats específicament per gestionar el repartiment de càrrega distribuïda, l'escalabilitat del rendiment sense talls de servei i l'orquestració dels fluxos de dades complexos entre els diferents *gateways*. El desconeixement d'aquesta arquitectura pot provocar greus caigudes de rendiment global de la xarxa corporativa.

## 4. Check Point Certified Troubleshooting Expert (CCTE)

- **Justificació de la necessitat:** En un servei de gestió de seguretat, el temps de resolució d'incidents (MTTR) és un element crític. La certificació CCTE valida exclusivament habilitats avançades de diagnòstic, anàlisi forense de xarxa i resolució de problemes d'alta complexitat sobre el sistema operatiu Gaia de Check Point.
- **Funció en el contracte:** Quan es produeix una degradació de servei, un comportament anòmal del trànsit o un incident de seguretat que el programari de monitoratge estàndard no pot identificar, els perfils CCTE utilitzen eines de línia de comandes de baix nivell i depuració interna de paquets (*kernel debugging*). La inclusió d'aquests especialistes garanteix que les incidències crítiques es resoldran de forma quirúrgica i ràpida, minimitzant els temps d'inactivitat (downtime) de l'organització.