Àrea de Serveis Generals i Transició Digital
Direcció de Serveis de Tecnologies i Sistemes Corporatius

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA CONTRACTACIÓ DE SERVEIS DE CIBERSEGURETAT DE LA DIPUTACIÓ DE BARCELONA, DIVIDIT EN DOS LOTS.

Exp. 2025/0021286

Índex

1. Antecedents
2. Objecte
3. Abast
4. Descripció del servei
   4.1 Lot 1: Administració i monitorització de seguretat
   4.1.1 Especificacions de l'entorn o de la plataforma tecnològica
   4.1.2 Gestió del monitoratge
   4.1.3 Tasques d'administració i suport
   4.1.4 Gestió de les incidències
   4.1.5 Horari del servei
   4.1.6 Equip de treball
   4.2 Lot 2: Auditories de seguretat.
   4.2.1 Descripció del servei d'auditories
   4.2.2 Horari del servei
5 Seguiment del contracte
6 Posada en marxa
7 Acords de Nivell de Servei (ANS)
8 Penalitats
9 Devolució del servei
10 Transferència tecnològica i/o de coneixement
11 Accés remot per la prestació dels serveis contractats

1. Antecedents

La Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC) de la Diputació de Barcelona té com a missió proporcionar tots els serveis i infraestructures d'informàtica i telecomunicacions de la corporació, tant per a l'àmbit intern, com també en relació amb el suport als ens locals, establint estratègies de futur alineades amb les necessitats funcionals corporatives i optimitzant la relació cost-benefici.

Els serveis de tecnologies i sistemes corporatius s'entenen com la integració dels àmbits clàssics de la informàtica i les telecomunicacions. S'assegura una direcció única per al tractament lògic de la informació i les seves xarxes de transmissió, independentment del seu format físic (veu, dades o imatge).

Entre d'altres té assignades les funcions següents:

- Dur a terme els criteris fixats per la corporació en matèria de tecnologies de la informació (informàtica, telecomunicacions i, en general, aquelles tecnologies relacionades amb el tractament automatitzat de la informació) i proposar els recursos necessaris que cal habilitar per a aquesta finalitat.
- Coordinar les tasques administratives de l'àmbit TIC de totes les unitats de la corporació i, de forma particular, aquelles que tenen interrelació, i proposar les mesures adequades per a una màxima normalització.
- Controlar i fer el seguiment d'aquelles tasques en matèria TIC realitzades per a la corporació mitjançant recursos externs.
- Proposar i gestionar les actuacions a desenvolupar per la corporació en matèria TIC que, dins dels supòsits de la cooperació i assistència, es realitzin per als ens locals de la demarcació de Barcelona.
- Desenvolupar i gestionar els projectes TIC que es produeixin a proposta de les àrees, direccions i serveis.
- Coordinar la formació i reciclatge del personal corporatiu en matèria TIC.
- Informar la despesa econòmica que generin les àrees, direccions i serveis de la corporació i els seus organismes autònoms en matèria TIC.
- Assessorar els organismes autònoms de la corporació en matèria TIC, quan així es requereixi i tutelar, si escau, l'homogeneïtat en el tractament dels sistemes d'informació comuns.
- Prestar suport per a l'adequació corporativa a l'acompliment de la normativa de protecció de dades i de l'Esquema Nacional de Seguretat, en els aspectes jurídics, organitzatius i tecnològics dels tractaments que duu a terme la Diputació de Barcelona, no només com a responsable d'aquest tractament per als ens locals sinó també com a encarregada.

En relació amb aquest expedient en concret la DSTSC promou la contractació dels serveis d'administració i monitorització de seguretat i auditories de seguretat dels

sistemes informàtics de la Diputació de Barcelona, amb l'objectiu de millorar la protecció davant de les ciberamenaces a les quals estan exposats.

En l'actualitat els sistemes informàtics de les organitzacions suposen la base del funcionament i coneixement. Cada vegada resulta més necessari augmentar la seguretat d'aquests sistemes, davant de programaris maliciosos o atacs de robatori de dades, i fer front als incidents de seguretat les 24 hores del dia.

Davant d'un incident de seguretat és important disposar d'un servei que permeti el monitoratge dels esdeveniments de seguretat generats a partir de les transaccions que realitzen els servidors i els equips de comunicacions, ubicats als diferents CPD de la Diputació de Barcelona, i que permeti reaccionar immediatament. Aquest tipus de servei s'ofereix des de centres especialitzats anomenats SOC (Security Operation Center).

Altrament, per tal de complir els requeriments de l'Esquema Nacional de Seguretat cal realitzar periòdicament auditories de seguretat dels sistemes per verificar la seva protecció davant unes amenaces que van canviant contínuament de forma i que cada cop assoleixen major nivell de sofisticació.

Aquestes auditories han de permetre detectar tant les vulnerabilitats a atacs provinents de fora de la xarxa corporativa, com les que es puguin produir des de l'interior i que puguin posar en perill la disponibilitat dels serveis i la seguretat de les dades.

Les especificacions que figuren en el present document s'ajusten al que es preveu a l'article 126, *Regles per a l'establiment de prescripcions tècniques*, de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, per la qual es transposen a l'ordenament jurídic espanyol les Directives del Parlament Europeu del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.

2. Objecte

L'objecte és la contractació de Serveis de Ciberseguretat de la Diputació de Barcelona.

3. Abast

Els serveis estan dividits en dos lots:

- Lot 1: Administració i monitorització de seguretat
- Lot 2: Auditories de Seguretat

Lot 1: Administració i monitorització de seguretat

Servei de prevenció:

- Anàlisis de vulnerabilitats: Identificar i remeiar les vulnerabilitats existents en els sistemes i aplicacions per evitar que siguin explotades per atacants. Gestió del cicle de vida de les vulnerabilitats.
- Inspeccions tècniques de seguretat: Detectar debilitats de la infraestructura de les tecnologies de la informació (TI) i avaluar la eficàcia de les mesures de seguretat existents.
- Vigilància digital: Detectar de forma proactiva amenaces i riscos externs (publicacions a internet o a la *dark web*) abans que es materialitzin en un incident de seguretat com per exemple filtracions de credencials, generació de dominis per campanyes de *phishing* dirigit o publicació d'aplicacions de mòbil malicioses que intentin suplantar les corporatives.

Servei de protecció:

- Operació de ciberseguretat: Implementar mesures als diferents sistemes que conformen la seguretat operativa de la Diputació de Barcelona. Mantenir actualitzat el programari i firmware dels sistemes i dispositius i corregir les vulnerabilitats i millorar la seguretat.

Servei de detecció:

- Monitorització de ciberseguretat: Monitoritzar la infraestructura de TI i detectar possibles incidents de seguretat.
- Anàlisi de logs: Recopilar i analitzar els logs de seguretat per detectar possibles intrusions o activitats anòmales.
- *Threat Hunting*: Buscar proactivament amenaces per detectar anomalies que podrien indicar un atac en curs o imminent.

Serveis de resposta:

- Equip de resposta a Incidents: Mitjançant un equip especialitzat gestionar els incidents de seguretat i contenir els danys, remeiar l'incident i restaurar els sistemes afectats. Definir i operar el pla de resposta a incidents on s'estableixin les accions a prendre en cas d'un ciberincident. Realitzar anàlisi forense i determinar la causa de l'incident i l'abast dels danys.

Suport en la governança:

- Assessorament en ciberseguretat: Assessorar a l'organització sobre com millorar la postura i complir amb les normes vigents. Assessorar a l'organització per incorporar-se a la Red Nacional de SOC del CCN-CERT.
- Compliment legal i normatiu: Assegurar que l'organització compleix amb les lleis i regulacions relacionades amb la seguretat de la informació.
- Conscienciació en ciberseguretat: Assessorar i promoure accions per la conscienciació en seguretat als treballadors per tal que puguin ser conscients de les amenaces i saber com actuar en cas d'incident.

- Quadres de comandament: Definir i implantar quadres de comandament que proporcionin informació sobre l'estat de la seguretat de la organització, com el número d'incidents de seguretat, vulnerabilitats existents i l'estat de les mesures de seguretat.

Lot 2: Auditories de seguretat.

Les auditories de seguretat anuals són un requeriment pel compliment de l'Esquema Nacional de Seguretat.

- Auditories de seguretat: auditar els sistemes de seguretat perimetral i de les condicions de seguretat dels sistemes d'informació, amb la finalitat de descobrir possibles forats de seguretat i possibles vulnerabilitats i aconseguir explotar-les amb l'objectiu final d'accedir a recursos no accessibles o fer-se amb el control del sistema d'informació (*pentesting*).

  Anualment es faran les següents accions:

  - Xarxa interna. Intrusió des de les diferents xarxes internes (LAN i WIFI)
  - Xarxa externa. Intrusió des de les aplicacions i serveis publicats a les xarxes externes.
  - Simulació de ciberincident. Exercici de *Red/Blue Team* i gestió de cibercrisi.

Suport a la remediació a les vies d'explotació detectades: Suport i assessorament en les accions necessàries per solucionar els problemes detectats. Es lliurarà els resultats en un informe amb el pas a pas amb captures seguit pels auditors per realitzar l'explotació i es facilitarà la càrrega de cada pas com un incident de seguretat independent, amb categoria Auditoria, dins de la eina de gestió d'incidents del Lot 1 per poder gestionar tot el cicle de vida.

4. Descripció del servei

4.1 Lot 1: Administració i monitorització de seguretat

4.1.1 Especificacions de l'entorn o de la plataforma tecnològica

Per complir amb els diferents serveis indicats a l'abast, l'adjudicatari farà servir els diferents sistemes que conformen la seguretat operativa de la Diputació de Barcelona:

- **Servei de protecció de correu (antispam).**
  - Exchange online Protection de Microsoft
- **Tallafocs:**
  - 2 equips Palo Alto 5520
- **Seguretat Endpoint:**
  - Defender for EndPoint Pla 2 de Microsoft

  - Microclaudia del CCN-CERT
- **VPN:**
  - Citrix NetScaler
- **WAF:**
  - Citrix NetScaler
- **Seguretat entorn Microsoft 365:**
  - Protecció de la identitat i accés condicional
  - Protecció contra amenaces
  - Protecció de la informació
  - Compliment normatiu
  - Gestió de vulnerabilitats
- **SIEM:**
  - Microsoft Sentinel
- **Exposició Local i Superfície d'atac:**
  - ELSA del CCN-CERT
- **Gestió d'indicadors de compromís:**
  - MISP
- **Gestió de tiquets interns**:
  - HP Service Desk
- **Registre i Gestió de ciberincidents**:
  - Gestor propi de Sentinel
  - LUCIA-NUBE CCN-CERT

Paral·lelament l'empresa contractista farà servir eines pròpies per cobrir el servei de **Vigilància Digital** proporcionant un portal pels tècnics de la DSTSC.

La tecnologia utilitzada durant l'execució del contracte podrà variar sense que el sistema quedi exclòs de l'abast.

Els serveis és desglossen en tres activitats:

- Gestió del monitoratge.
- Tasques d'administració i suport.
- Gestió de les incidències.

4.1.2 Gestió del monitoratge

L'empresa contractista haurà de monitorar els sistemes de manera ininterrompuda (24x7). Això vol dir:

- Monitorar la disponibilitat, la capacitat, la seguretat i l'ús dels sistemes.
- Obrir una incidència si la disponibilitat o funcionalitat del servei està afectada.
- Obrir tasques d'administració de forma proactiva si la seguretat està en risc o han de permetre millorar la capacitat.

- Detectar les alertes de seguretat amb el menor temps possible per tal de poder actuar de manera immediata.

La DSTSC posarà a l'abast de l'empresa contractista una eina de monitoratge que podrà utilitzar remotament, paral·lelament l'empresa contractista pot fer servir eines de monitoratge pròpies segons necessitats.

4.1.3 Tasques d'administració i suport

Són totes les tasques, proactives o reactives, que cal realitzar dins de cada servei. Com per exemple:

Servei de prevenció:

Anàlisis de vulnerabilitats:

- Notificar i revisar els avisos dels propis fabricants o butlletins de seguretat respecte a vulnerabilitats de programari en ús desplegat a la corporació.
- Tasques de remediació seguint la proposta de correcció dels fabricants d'aquelles vulnerabilitats que afectin als equips administrats.

Inspeccions tècniques de seguretat

- Tasques de revisió de les configuracions aplicades en els diferents equips de seguretat seguint les guies CCN-STIC.
- Tasques de revisió de les maquetes dels equips personals i dels servidors
- Tasques d'implementació de millores proposades per l'entorn Microsoft 365 a través dels seus portals de Score.

Vigilància digital

- Creació d'alertes en el portal proporcionat per aquest servei i execució de procediments interns en cas de detecció de credencials en venda, detecció d'apps fraudulentes i dominis de suplantació.
- Tasques per gestionar la retirada (TakeDown) de pàgines de suplantació.
- Revisió de les alertes de l'eina d'exposició i superfície d'atac.

Servei de protecció:

Operació de ciberseguretat

- Creació de regles als tallafocs segons necessitats dels projectes de la direcció.
- Creació d'accessos externs a recursos interns
- Tasques de suport als usuaris que fan us de les VPN de la corporació.
- Instal·lació i gestió de les llicències.

- Canvis de versió dels diferents components tecnològics dels sistemes de seguretat.
- Gestió i control dels usuaris administradors o de sistema, així com la seva seguretat, rols i perfils.
- Aplicació de pegats de seguretat en els sistemes mantinguts.
- Configuració segura dels sistemes i revisions periòdiques.
- Càrrega d'Indicadors de compromís en la instància MISP corporativa.
- Execució de procediments de resposta a incidents de seguretat de primer nivell seguint els playbooks corporatius.

Servei de detecció:

Monitorització de ciberseguretat

- Creació d'alertes de correlació en el SIEM central.
- Creació de regles d'orquestració i respostes automàtiques SOAR

Anàlisi de logs

- Revisió de la ingesta i retenció dels logs dels diferents equips.
- Creació de consultes a les taules dels logs

Threat Hunting

- Execució de consultes proactiva en base a IoC publicats o comportaments sospitosos.

Serveis de resposta

Equip de resposta a Incidents

- Tasques de suport i execució de procediments de resposta a incidents de seguretat.
- Tasques de suport en la gestió de crisi.
- Tasques d'anàlisi forense.
- Anàlisi de programari maliciós.

Suport en la governança

Assessorament en ciberseguretat

- Tasques de coordinació amb la resta de serveis de ciberseguretat gestionats des del SOC perimetral.
- Tasques d'implementació de la guia CCN-STIC-896 de certificació d'un SOC.
- Creació i actualització de procediments de seguretat, salvaguarda i recuperació.
- Tasques relacionades amb la integració de la Red Nacional de Seguridad del CCN

Compliment legal i normatiu

- Tasques de coordinació amb els serveis per al compliment normatiu per l'Esquema Nacional de Seguretat i pel Reglament General de Protecció de Dades gestionats des dels departaments responsables.

Conscienciació en ciberseguretat

- Tasques de coordinació i supervisió dels materials realitzats des dels serveis de formació corporatiu o proposats per la direcció.

Quadres de comandament

- Tasques de creació i actualització dels quadres de comandament propis dels diferents productes de l'abast segons necessitats.

Totes les accions realitzades en cada tasca hauran de quedar documentades en l'eina de gestió de peticions.

Per les tasques no procedimentades l'empresa adjudicatària presentarà un document de canvi que els tècnics de la DSTSC hauran de validar.

Per les tasques que suposin una aturada de servei o puguin posar en risc la disponibilitat dels serveis els tècnics de la DSTSC fixaran un horari d'execució que minimitzi l'impacte en el servei. L'execució de tasques durant caps de setmana o horari nocturn no suposarà cap cost afegit.

S'estableixen quatre categories de tasques amb diferents ANS pels temps de resolució (els temps són sempre dins de l'horari de servei):

- **Crítica.** Son tasques que cal realitzar de forma immediata davant de ciberatacs o situacions que posen en risc la disponibilitat, la seguretat o la integritat dels sistemes.
  - Temps de resolució: 1 hora
- **Urgent.** Tasques que afecten a la configuració dels sistemes per la posada en marxa d'un servei.
  - Temps de resolució: 8 hores
- **Important**. Tasques de millora o ampliació del servei.
  - Temps de resolució: 72 hores (de dilluns a divendres no festius a Barcelona ciutat)
- **Estàndard.** Tasques de manteniment del servei.
  - Temps de resolució: 7 dies laborables (de dilluns a divendres no festius a Barcelona ciutat).

Respecte els incidents de seguretat, s'hauran de registrar seguint l'actual metodologia proposada pel CCN-CERT per la gestió d'incidents de seguretat en l'Esquema Nacional de Seguridad (ENS), detallada en la guia CCN-STIC-817, dins del gestor d'incidents de Microsoft Sentinel i de la instància LUCIA NUBE del CCN CERT o bé aquelles en vigor en el moment dels incidents.

4.1.4 Gestió de les incidències

Es tracta d'aquelles actuacions que tenen com a objectiu resoldre disfuncions en el servei contractat i que tendeixen a minimitzar el nombre d'incidències i la seva resolució en el mínim temps possible, fins i tot si es deriven d'un mal ús de l'usuari o de la configuració o parametrització de la solució.

La resolució d'incidències ha de resoldre en el mínim de temps possible qualsevol mal funcionament dels sistemes inclosos a l'abast del contracte.

Totes les accions realitzades en la resolució de les incidències hauran de quedar documentades en l'eina de gestió.

Si per la resolució de la incidència es necessària l'execució de tasques d'administració, aquesta incidència no es tancarà fins que estiguin totes realitzades.

Davant els incidents de seguretat, l'empresa contractista ha de tenir en compte:

- La classificació dels incidents de seguretat es farà segons indica la guia CCN-STIC 817 o la que sigui vigent en el moment dels incidents, tenint l'empresa contractista la obligació de comunicar a la Diputació de Barcelona de forma immediata tots aquells que puguin ser classificats L3-Nivell Alt o superior per la via que determina el contracte.

La DSTSC treballarà conjuntament amb l'empresa contractista per reduir el temps de resolució, ja sigui proporcionant informació, fent proves o a través de qualsevol altre acció que estigui al seu abast.

Una incidència estarà resolta si està plenament documentada i té el vistiplau funcional i tècnic de la DSTSC. Tota incidència resolta per l'empresa contractista que no rebi el vistiplau de la DSTSC serà retornada a l'empresa contractista acumulant els temps de resolució.

S'estableixen quatre categories d'incidències amb diferents ANS pels temps de resposta i de resolució (els temps són sempre dins de l'horari de servei):

- **Crítica.** Incidències que afecten de manera molt global a tota la plataforma.
  - Temps de resposta: Immediata
  - Temps de resolució: 4 hores
- **Urgent.** Incidències que suposen l'aturada parcial de l'entorn o suposen un greu impacte en la plataforma.
  - Temps de resposta: 4 hores

  - Temps de resolució: 24 hores
- **Important**. Incidències que generen un funcionament incorrecte en l'ús de la plataforma.
  - Temps de resolució: 72 hores (de dilluns a divendres no festius a Barcelona ciutat)
- **Estàndard.** Incidències que no repercuteixen sobre l'explotació diària de la plataforma.
  - Temps de resolució: 7 dies laborables (de dilluns a divendres no festius a Barcelona ciutat).

4.1.5 Horari del servei

És l'interval horari on es comptabilitzaran els acords de nivells de servei. Per qualsevol de les activitats definides en el servei (monitorització, tasques i incidències) l'horari serà de 24x7.

4.1.6 Equip de treball

L'empresa haurà de dimensionar l'equip de treball de forma que pugui complir els ANS establerts durant tota la prestació del servei.

En relació els integrants de l'equip de treball que l'empresa contractista ha de disposar a la seva plantilla per a la prestació del contracte, amb independència del seu percentatge de dedicació final, s'hauran de correspondre amb els perfils següents (els que conformen l'equip de treball):

- 1 Delegat de protecció de dades.
- 1 Responsable del contracte.
- 1 Referent tècnic.
- 1 Tècnics.

D'aquest perfils, es preveuen 2 persones dedicades plenament al servei:

  - 1 Referent tècnic
  - 1 Tècnic de suport

Aquestes 2 persones realitzaran un màxim de dues jornades de teletreball setmanal.

Amb el seu horari donaran, com a mínim, el servei de forma presencial entre les 7:30 del matí i les 16:00 de la tarda (de dilluns a divendres no festius).

En canvi, el delegat de protecció de dades i el responsable del contracte tindran una dedicació parcial en tant que les seves tasques no impliquen un seguiment continu.

El terme festiu emprat en aquesta clàusula fa referència als dies que es declaren festius a tot el territori català (segons el calendari oficial publicat en el DOGC), inclosos els festius locals a la ciutat de Barcelona.

- Servei 24x7 per cobrir la resta de la jornada.

El contractista ha de tenir present, en relació amb l'equip de treball, les directrius següents.

L'empresa contractista haurà d'estar en disposició de donar cobertura immediata en cas de malaltia, vacances o qualsevol altra contingència que afecti el seu personal, a fi que en cap supòsit la prestació resti sense cobrir.

Delegat de protecció de dades

Serà el responsable de garantir l'acompliment del Reglament General de Protecció de Dades (RGPD) per part de l'equip de treball de l'empresa contractista. Figura obligatòria al Reglament europeu 2016/679, de 27 d'abril, general de protecció de dades (RGPD), per a les administracions públiques i els seus encarregats del tractament de dades de caràcter personal.

Tindrà com a mínim les funcions següents:

- Assessorar sobre l'aplicació dels principis de privacitat des del disseny i per defecte del projecte.
- Informar i assessorar a l'encarregat del tractament i als empleats que s'ocupin del tractament de les obligacions que els incumbeixen en virtut del RGPD i d'altres disposicions de protecció de dades de la Unió o dels estats membres.
- Supervisar el compliment del que disposa el RGPD, d'altres disposicions de protecció de dades de la Unió o dels estats membres i de les polítiques de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
- Cooperar amb els responsables de protecció de dades de la Diputació de Barcelona en qüestions relatives al tractament objecte del present plec, inclosa l'avaluació d'impacte relativa a la protecció de dades, la consulta prèvia davant l'autoritat, i, si escau, sobre qualsevol altre assumpte.
- Exercir les seves funcions prestant la deguda atenció als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i fins del tractament.

S'ha valorat el percentatge de dedicació del Delegat de protecció de dades en un 1% de la seva jornada laboral segons el conveni col·lectiu aplicable d'acord amb la clàusula 1.3 del PCAP, aplicat sobre el còmput total anual d'hores.

Responsable del contracte

Realitzarà les tasques de coordinació, seguiment i control de la gestió del contracte. Per part de la DSTSC es designarà un coordinador que realitzarà funcions anàlogues.

Serà funció del Responsable del contracte de l'empresa contractista conèixer en profunditat les prestacions cobertes i assegurar que tot el personal de l'empresa contractista que participa en el contracte disposi dels coneixements adients i assumeixi els compromisos adquirits i vetlli pel compliment de tots els requeriments inclosos en el contracte.

A títol d'exemple, el Responsable del contracte realitzarà les funcions següents:

- Definició del pla de treball que servirà com a guia per a l'execució de les prestacions durant la vigència del contracte. Els components del pla hauran d'incloure les mètriques de satisfacció, recursos necessaris i una agenda de les activitats planificades i les reunions de seguiment. Aquest pla de treball es revisarà periòdicament per repassar els objectius, i serà acordat i supervisat per la DSTSC.
- Supervisió de la posada en marxa per complir amb el pla presentat, d'acord amb els requisits que determini el coordinador de la DSTSC.
- Supervisió de la qualitat. Es prepararà un informe de seguiment que resumirà les prestacions proporcionades, permetent l'avaluació i seguiment de l'últim període realitzat sobre el pla de treball.
- Supervisió dels riscos. Mantenint actualitzada la llista de riscos i dels derivats dels possibles canvis no efectuats.
- Supervisió dels incidents, problemes, consultes, peticions, entre d'altres.
- Gestió de l'escalat. Els incidents (o qualsevol altra acció) que necessitin ser escalats a recursos tècnics o a nivells de responsabilitat superiors dins de la pròpia empresa o en el cas de subcontractació a altres empreses, seran gestionats estretament per accelerar la seva resolució.

S'ha valorat el percentatge de dedicació del Responsable del contracte en una estimació del 5% de la seva jornada laboral segons el conveni col·lectiu aplicable d'acord amb la clàusula 1.3 del PCAP, aplicat sobre el còmput total anual d'hores.

Referent tècnic

Serà l'interlocutor únic amb els tècnics de la DSTSC i qui coordinarà els tècnics de l'empresa contractista que puguin intervenir en qualsevol activitat sol·licitada. Assumirà les funcions següents:

- Coordinar les relacions entre l'equip tècnic i els tècnics de la DSTSC.
- Comunicar periòdicament l'estat del contracte.
- Transmetre a l'equip tècnic les directrius per al correcte desenvolupament del contracte.
- Supervisar l'aplicació dels procediments que sol·liciti la DSTSC.
- Assistir a les reunions periòdiques de seguiment del contracte.
- Gestionar les tasques o procediments, aplicant mesures correctives en cas de desviació.
- Garantir la qualitat dels procediments i tasques.
- La gestió de les intervencions planificades.
- Elaborar els informes tècnics de seguiment i sota demanda.
- Analitzar la prestació per tal de proposar millores.

Aquesta persona haurà de tenir una dedicació efectiva ordinària del 100% de la seva jornada laboral segons el conveni col·lectiu aplicable d'acord amb la clàusula 1.3 del PCAP, aplicat sobre el còmput total anual d'hores. Tot i això ha de tenir present que en qualsevol moment ha de poder respondre a consultes sobre l'estat d'incidències o peticions i podrà requerir-se la seva presencia, sense que això suposi cap cost econòmic addicional a la Diputació de Barcelona. És imprescindible que aquesta persona disposi d'un telèfon mòbil destinat a la seva localització.

El Referent tècnic haurà de realitzar la prestació del servei presencialment a les instal·lacions de la Diputació de Barcelona (en endavant, DIBA), com a mínim tres dies a la setmana, entre les 7:30 hores i les 16:00 hores (de dilluns a divendres no festius a Barcelona ciutat).

Tècnic de suport

L'empresa contractista haurà de disposar per a la prestació adient del contracte de com a mínim un tècnic amb un nivell de dedicació del 100% de la seva jornada laboral segons el conveni col·lectiu aplicable d'acord amb la clàusula 1.3 del PCAP, aplicat sobre el còmput total anual d'hores.

El tècnic de suport adscrit al contracte haurà de ser capaç d'executar, amb el nivell de qualitat suficient, les tasques derivades del servei i assumir puntes de treball per cobrir convenientment totes les necessitats que es plantegin en cada moment, de forma que la prestació no es vegi afectada per augments esporàdics del nombre d'incidències o peticions concretes.

El tècnic de suport assumirà la resta de les tasques identificades en el present plec de prescripcions tècniques. A títol d'exemple:

- Resolució d'incidències, problemes, consultes, adaptacions.

- Operacions ordinàries de manteniment i administració.
- Documentació dels sistemes, configuracions, desplegaments, adaptacions.
- Actualitzacions de versions (pedaços, menors, majors), així com qualsevol altra tasca derivada del desplegament en els diferents entorns identificats a nivell de contracte.

El tècnic de suport amb dedicació del 100% de la jornada haurà de realitzar la prestació del servei presencialment a les instal·lacions de la DIBA, com a mínim tres dies a la setmana, entre les 7:30 hores i les 16:00 hores (de dilluns a divendres no festius a Barcelona ciutat).

Regles especials respecte del personal laboral de l'empresa contractista

Amb caràcter general i en relació a l'equip de treball determinat, en el seu conjunt, la contractista ha de tenir present:

- Correspon exclusivament a la contractista la selecció del personal que, reunint els requisits exigits en els plecs, formarà part de l'equip de treball adscrit a l'execució del contracte, sense perjudici de la verificació per part de la DSTSC del compliment d'aquells requisits.
- La contractista vetllarà per l'estabilitat de l'equip de treball, i perquè els canvis en la seva composició siguin puntuals i obeeixin a raons justificades, en ordre a no alterar el bon funcionament del contracte, informant en tot moment a la DSTSC.
- La contractista assumeix l'obligació d'exercir de forma real, efectiva i continua, sobre el personal integrant de l'equip de treball encarregat de l'execució del contracte, el poder de direcció inherent a tot empresari. En particular, assumirà la negociació i el pagament dels salaris, la concessió de permisos, quan procedeixi, les obligacions legals en matèria de prevenció de riscos laborals, l'exercici de la potestat disciplinària, així com els drets i obligacions derivats de la relació contractual entre empleat/ocupador.
- La contractista haurà de vetllar especialment perquè els treballadors adscrits a l'execució del contracte desenvolupin la seva activitat sense extralimitar-se en les funcions desenvolupades respecte de l'activitat delimitada en els plecs objecte del contracte.
- En cas que els tècnics no satisfacin els mínims d'eficiència, de metodologia, aptitud i eficàcia desitjats, la DSTSC podrà demanar la seva substitució a la contractista, que l'haurà de fer efectiva en un temps màxim de dues setmanes.
- Qualsevol modificació dels tècnics haurà de ser comunicada a la DSTSC amb una antelació mínima d'1 setmana i haurà de presentar un pla de traspàs de coneixement al nou membre de l'equip que s'haurà de concretar en un màxim de 2 setmanes, que s'entendrà el temps màxim a partir del qual el nou recurs s'incorpori a l'equip de treball.
- La contractista haurà d'informar a la DSTSC de qualsevol contingència que afecti el seu personal i haurà de disposar de personal per donar-ne cobertura immediata si es considera necessari.

- Qualsevol absència planificada del personal de la contractista haurà de ser aprovada per la DSTSC.

4.2 Lot 2: Auditories de seguretat.

El servei ha de permetre descobrir les vulnerabilitats presents en la infraestructura tecnològica de la Diputació de Barcelona, comprovar els efectes que l'explotació d'aquestes vulnerabilitats poden produir en les diferents dimensions de la seguretat de la informació - disponibilitat, integritat i confidencialitat-, documentar tant els riscos de la situació actual com les solucions a curt, mitjà i llarg termini. El servei també inclou el suport en la implementació de les solucions.

L'auditoria de seguretat externa es realitzarà des de dependències de l'empresa contractista, mentre que l'auditoria de seguretat interna i la simulació de ciberincident es realitzaran des de dependències de la DIBA i de manera coordinada amb els seus tècnics.

4.2.1 Descripció del servei d'auditories

Auditoria de seguretat externa

El servei d'auditoria de seguretat externa anual tindrà el següent abast:

- Test d'intrusió de serveis externs a tot el rang d'adreces públiques de la DIBA.
- Test d'intrusió a pàgines web de la DIBA de 20 dominis diferents.

Aquesta auditoria es realitzarà en el format de "caixa negre", és a dir, sense informació prèvia ni credencials d'usuari, i intentarà recopilar informació, comprovar els diferents sistemes d'autenticació implementats, comprovar l'ús que es fa de la gestió de les sessions i com les aplicacions gestionen la validació de les dades (injeccions de codi).

El resultat de l'auditoria externa documentarà les vulnerabilitats detectades seguint l'estàndard CVE.

La criticitat de les vulnerabilitats seguirà l'estàndard CVSS.

L'informe de l'auditoria també es lliurarà en format electrònic per permetre l'anàlisi estadístic.

Es lliurarà els resultats en un informe amb el pas a pas amb captures seguit pels auditors per realitzar l'explotació i es facilitarà la càrrega de cada pas com un incident de seguretat independent, amb categoria Fals Positiu Auditoria, dins de la eina de gestió d'incidents de Microsoft Sentinel i LUCIA NUBE per poder gestionar tot el cicle de vida.

Auditoria de seguretat interna

El servei d'auditoria de seguretat interna anual tindrà el següent abast:

- Test d'intrusió de serveis interns:
    - 8 xarxes de servidors de màscara 24.
    - Infraestructura SAP (20 servidors).
    - Infraestructura ORACLE (10 servidors).
    - Repositori de codi
- Test d'intrusió a les xarxes WIFI:
    - 4 SSID.

Aquesta auditoria es realitzarà tant en el format de "caixa negre", és a dir, sense informació prèvia ni credencials d'usuari, com en el format "caixa blanca", en el que es proporcionaran unes credencials vàlides, i intentarà recopilar informació, comprovar els diferents sistemes d'autenticació implementats, comprovar l'ús que es fa de la gestió de les sessions i com les aplicacions gestionen la validació de les dades (injeccions de codi).

Les auditories són anuals i es realitzaran coordinadament amb la Diputació de Barcelona i es pactarà el calendari anual amb reunions de seguiment mensual. No s'especifica dates ni període exacte de l'any perquè es planifiquen segons necessitats de la Diputació de Barcelona.

El resultat de l'auditoria interna documentarà les vulnerabilitats detectades seguint l'estàndard CVE.

La criticitat de les vulnerabilitats seguirà l'estàndard CVSS.

L'informe de l'auditoria també es lliurarà en format electrònic per permetre l'anàlisi estadístic.

Es lliurarà els resultats en un informe amb el pas a pas amb captures seguit pels auditors per realitzar l'explotació i es facilitarà la càrrega de cada pas com un incident de seguretat independent, amb categoria Fals Positiu Auditoria, dins de la eina de gestió d'incidents de Microsoft Sentinel i LUCIA NUBE per poder gestionar tot el cicle de vida.

Simulació de ciberincident

L'empresa proposarà un exercici de *Red/Blue Team* i una simulació de gestió de cibercrisi.

L'exercici Red/Blue Team haurà de permetre calcular els temps mig de compromís del sistema, temps mig d'escalat de privilegis, temps estimat de detecció i el temps estimat de recuperació.

Aquestes es realitzaran coordinadament amb la Diputació de Barcelona i es pactarà el calendari. No s'especifica dates ni període exacte de l'any perquè es planifiquen segons necessitats de la Diputació de Barcelona.

Es lliurarà els resultats en un informe amb el pas a pas amb captures seguit pels diferents equips i, com l'auditoria interna, es facilitarà la càrrega de cada pas com un incident de seguretat independent, amb categoria Fals Positiu Auditoria, dins de la eina de gestió d'incidents de Microsoft Sentinel i LUCIA NUBE per poder gestionar tot el cicle de vida.

La simulació de gestió d'una cibercrisi es basarà en la guia BP/29 Buenas Prácticas en la Gestión de Crisis para ciberincidentes en Entidades Locales del CCN-CERT (o la que sigui vigent i d'aplicació en el moment de la simulació) i haurà de permetre el desenvolupament en competències crítiques com la contenció d'atacs, comunicació en moment de crisis i la presa de decisions. Es realitzarà una revisió dels procediments actuals per validar el seu correcte funcionament i s'actualitzarà en funció dels resultats de la simulació.

Es lliurarà un informe de la simulació realitzada amb propostes de millora.

Suport a la solució de les vulnerabilitats detectades

L'empresa contractista haurà d'oferir suport i assessorament en les accions necessàries per solucionar els problemes i vulnerabilitats detectades durant les auditories gestionant el cicle de vida total dels incidents carregats prèviament, categoria Fals Positiu Auditoria, dins de la eina de gestió d'incidents, validant i certificant la correcta solució aplicada, tancant l'incident com Solucionat o com Risc assumit en aquelles on no es pugui aplicar la solució proposada.

Aquest suport i assessorament es realitzarà en les dependències de la DIBA en el format de 10 hores mensuals presencials, obligatòriament i sense cost addicional per a la Diputació de Barcelona.

4.2.2 Horari del servei

L'horari de prestació del servei és el següent: de 7:30 h a 16:00 h de dilluns a divendres no festius.

El terme festiu emprat en aquesta clàusula fa referència als dies que es declaren festius a tot el territori català (segons el calendari oficial publicat en el DOGC), inclosos els festius locals a la ciutat de Barcelona.

5 Seguiment del contracte

En relació amb els dos lots en els quals està dividit l'objecte del contracte, el contractista haurà de seguir les indicacions següents.

Mensualment, hi haurà una reunió de seguiment per tal de treballar per la millora constant del servei. Aquesta reunió es farà entre els dies 10 i 15 de cada mes i hi assistirà per part de l'empresa contractista el responsable del contracte i el referent tècnic, sens perjudici d'altres perfils en el cas de ser necessari. En aquesta reunió es revisaran els informes mensuals, es generaran propostes de millora i, en general, es farà un seguiment de tot el que tingui a veure amb la prestació del servei.

En relació amb les reunions a realitzar durant el termini de vigència del contracte, sigui quina sigui la seva periodicitat i motiu de la seva convocatòria, es podran realitzar tant en modalitat presencial com telemàtica, sempre a criteri dels tècnics de la DSTSC. El contractista disposarà dels mitjans necessaris per tal d'adequar-se a qualsevol dels dos formats, sense que això generi cap cost addicional per a la Diputació de Barcelona.

A continuació es detalla la informació que haurà de constar en aquest informe de servei, com a mínim, per a cada un dels lots en els quals s'ha dividit l'objecte del contracte.

LOT 1: Administració i monitorització de seguretat

Es presentarà un informe mensual amb 5 apartats, un per cadascun dels serveis principals. L'informe mensual del servei haurà de contenir, com a mínim, la següent informació:

- Tasques executades. Indicant nivell, temps d'execució i compliment d'ANS.
- Alertes del període: tipologia i nivell.
- Incidents de seguretat en el període.
- Propostes de tasques a realitzar per millorar cada servei.
- Situació econòmica del contracte indicant les factures presentades.

LOT 2: Auditories de seguretat

L'informe mensual del servei ha de contenir, com a mínim, la següent informació:

- Estat de l'execució de les auditories anuals.
- Tasques i hores realitzades en el suport a la solució de les vulnerabilitats.
- Propostes de millora del servei.
- Situació econòmica del contracte indicant les factures presentades.

6 Posada en marxa

En relació amb els dos lots en els quals està dividit l'objecte del contracte, el contractista ha de tenir en compte el següent.

La fase de posada en marxa del servei és el període de temps que transcorre entre la formalització del contacte i la posada en marxa de tots els serveis contractats.

Serà responsabilitat de la contractista l'execució de les diferents fases que conformen la posada en marxa del servei.

La DSTSC assignarà un interlocutor que treballarà conjuntament amb l'empresa contractista en la fase de posada en marxa.

El cost que impliqui o que derivi de qualsevol de les actuacions derivades de la posada en marxa s'ha d'entendre inclòs en el pressupost total del contracte.

Pel que fa a les especificitats requerides per a cadascun dels dos Lots en els quals es divideix l'objecte del contracte, el contractista ha de seguir les prescripcions següents:

LOT 1: Administració i monitorització de seguretat

El pla de posada en marxa ha de permetre a l'empresa contractista complir els ANS establerts a partir del quinzè dia laborable de la data d'inici de la prestació efectiva del servei. A partir d'aquest dia s'aplicaran les penalitats corresponents.

A l'inici de l'execució del contracte, l'empresa contractista haurà de presentar el pla de posada en marxa que inclogui els mecanismes necessaris per oferir el servei amb els nivells de qualitat requerit.

Durant aquesta fase es realitzaran les següents tasques:

- Captura de coneixement per part dels tècnics de l'empresa contractista.
- Validació d'accés a tots els sistemes
- Definició protocols d'actuació davant alertes.

LOT 2: Auditories de seguretat

El pla de posada en marxa ha de permetre a l'empresa contractista complir els ANS establerts a partir del vintè dia laborable de la data d'inici de la prestació efectiva del servei.

Durant aquesta fase es realitzaran les següents tasques:

- Captura de coneixement per part dels tècnics de l'empresa contractista.
- Planificació temporal de totes les activitats.

7 Acords de Nivell de Servei (ANS)

En relació als dos lots en els quals està dividit l'objecte del contracte, el contractista ha de tenir en compte el següent.

Els ANS permeten obtenir indicadors per avaluar el grau de compliment del servei.

El càlcul de l'ANS s'haurà de fer per part de l'empresa contractista, amb una periodicitat mensual i considerant l'horari de la prestació dels serveis i el mes natural.

No computaran els períodes de temps en què el contractista està pendent de resposta, reunions, dades o concreció de requeriments per part dels tècnics o usuaris de la Diputació de Barcelona o de tercers proveïdors sempre i quan aquests no tinguin una relació contractual directa amb l'empresa contractista principal, donat que en aquell cas el temps computarà com a temps propi de la contractista a tots els efectes previstos en aquest Plec.

Les peticions només es consideraran finalitzades si es troben completament documentades i tenen el vistiplau funcional i tècnic de la DSTSC, en cas contrari seran retornades a l'empresa contractista acumulant els temps de resolució, a tots els efectes i responsabilitats establertes en l'ANS.

Els temps de resposta i de resolució d'incidències no es podran veure afectats per augments esporàdics del nombre d'incidències, ni per la coincidència amb altres tasques previstes en el present plec.

El temps de resposta és el transcorregut entre la comunicació de la incidència al contractista, pel canal previst, fins que l'empresa contractista assumeix la resolució de la incidència assignant-hi els recursos necessaris per poder complir el temps de resolució.

Pel que fa a les especificitats requerides per a cadascun dels dos lots en els quals es divideix l'objecte del contracte, el contractista ha de seguir les prescripcions següents:

LOT 1: Administració i monitorització de seguretat

Execució de tasques

Temps de resolució: És el temps transcorregut entre la comunicació de la tasca al contractista o la detecció de l'alerta que l'ha generat fins que la tasca queda executada i documentada per l'empresa contractista.

Nivell de qualitat: Els temps màxims per a la finalització de la tasca són:

- Crítica. 2 hores
- Urgent. 8 hores
- Important. 72 hores

Resolució d'incidències

Temps de resolució: És el temps transcorregut entre la comunicació de la incidència al contractista o la detecció de l'alerta que l'ha generat fins que la incidència queda resolta.

Nivell de qualitat: Els temps màxims per a la finalització de les tasques relacionades amb la incidència són:

- Crítica. 4 hores
- Urgent. 4 hores
- Important. 72 hores

Registre i notificació de les alertes de seguretat

Temps de registre i notificació: És el temps transcorregut entre la detecció de l'alerta i el registre i la notificació a la DSTSC

Nivell de qualitat: El temps màxim pel registre i la notificació és de 15 minuts

Execució d'accions d'anàlisi forense

Temps d'execució: És el temps transcorregut entre la detecció de l'alerta i l'execució d'accions d'anàlisi forense.

Nivell de qualitat: El temps màxim per a la finalització de les accions és:

- Alerta nivell alt: 2 hores
- Alerta nivell mitjà: 8 hores

LOT 2: Auditories de seguretat

Aturada de serveis per males pràctiques en les auditories

Nivell de qualitat: En cap cas, l'execució de les auditories pot provocar l'aturada d'un servei en producció.

Auditoria no executada durant l'any

Nivell de qualitat: Totes les auditories es realitzaran un cop cada any.

8 Penalitats

En relació amb els dos lots en els quals està dividit l'objecte del contracte, el contractista ha de tenir en compte el següent.

En el cas d'incompliment dels ANS per part de l'empresa contractista, i en el supòsit que la Diputació de Barcelona opti per la no-resolució del contracte, es preveuen les penalitats que s'indiquen al costat de cada ANS.

La comptabilització de les penalitats es realitzarà mensualment, amb efectes a la facturació del mes calculat i sobre la part fitxa d'aquell període.

La quantitat màxima de penalitat es fixa en un 50% de l'import mensual (IVA exclòs). La quantia no podrà ser superior al 10% del pressupost del contracte, IVA exclòs, ni el total de les mateixes podrà superar el 50% del preu del contracte.

Cas d'incompliment dels acords de nivell de servei les factures hauran de contemplar les penalitats segons el que es preveu en aquesta clàusula. En concret, per a les penalitats derivades de l'incompliment sobre els ANS establerts s'aplicarà el següent procediment:

- Durant la reunió de seguiment mensual entre el contractista i els tècnics de la DSTSC per avaluar la correcta execució de la prestació s'analitzarà, entre altres factors, l'acompliment dels ANS.
- Cas que les parts detectin, acceptin i validin els incompliments, el contractista els recollirà en un apartat específic de l'informe mensual que ha de lliurar a la DSTSC.
- La Diputació de Barcelona, una vegada adoptat l'acord administratiu intern corresponent, notificarà al contractista la quantitat exacta que aquest haurà de descomptar en la factura corresponent al primer període de facturació obert.

Pel que fa a les especificitats requerides per a cadascun dels dos lots en els quals es divideix l'objecte del contracte, el contractista ha de seguir les prescripcions següents.

LOT 1: Administració i monitorització de seguretat

Execució de tasques

Les penalitats associades a l'incompliment del temps de resolució en l'execució de tasques seran:

Per hora o fracció de temps de resolució que superen el nivell de qualitat	**Penalitat**
Per tasques crítiques	300 €
Per tasques urgents	200 €

Registre i notificació de les alertes de seguretat

Les penalitats associades a l'incompliment del temps de registre i notificació seran de:

Per cada 15' complert de retard	Penalitat
Per alertes de nivell alt	200 €
Per alertes de nivell mitjà	50 €
Per alertes de nivell baix	10 €

Execució d'accions d'anàlisi forense

Les penalitats associades a l'incompliment del temps d'execució de les accions d'anàlisi forense seran de:

Per hora de retard en la finalització de les accions	Penalitat
Per alertes de nivell alt	200 €
Per alertes de nivell mitjà	20 €

LOT 2: Auditories de seguretat

Execució d'Auditories

Les penalitats associades a l'incompliment per auditoria no realitzada:

Per cada mes que superi el nivell de qualitat	Penalitat
Per cada auditoria	2.000 €

Aturada de serveis per males pràctiques en les auditories

Les penalitats associades a l'aturada de serveis en producció per males pràctiques en la realització de les auditories seran:

Per cada servei aturat	Penalitat
Si afecta a més de 1.000 usuaris	3.000 €
Si afecta entre 100 i 1.000 usuaris.	2.000 €
Si afecta a menys de 100 usuaris	1.000 €

9 Devolució del servei

En relació amb els dos lots en els quals està dividit l'objecte del contracte, el contractista ha de tenir en compte el següent.

Sis mesos abans de la finalització del contracte, l'empresa contractista haurà de presentar el pla de devolució del servei que inclogui els mecanismes necessaris per tal de traspassar tota la informació relacionada amb el servei prestat a Diputació de Barcelona. Aquest pla inclourà un mínim de 80 hores de dedicació de recursos de l'empresa contractista, sense cost addicional per a la Diputació de Barcelona, per dur a terme les tasques identificades.

Un mes abans de la finalització del contracte, la contractista presentarà una actualització el pla de devolució del servei.

La finalització del contracte exigirà també l'eliminació segura de les dades personals i de tota la informació que s'hagi utilitzat per a l'execució del contracte. S'aportarà certificació de la seva destrucció.

Les tasques d'administració per les quals el seu temps de resolució finalitzi dins del termini de durada del contracte hauran de quedar tancades. Si no és així s'aplicaran les penalitats corresponents.

10 Transferència tecnològica i/o de coneixement

En relació amb els dos lots en els quals està dividit l'objecte del contracte, el contractista ha de tenir en compte el següent.

El contractista està obligat a facilitar a les persones designades per la DSTSC tota aquella informació necessària per disposar d'un ple coneixement tècnic dels treballs realitzats.

Tanmateix, el personal designat per la DSTSC als serveis adjudicats podrà realitzar totes aquelles consultes que consideri oportunes pel correcte seguiment i control dels treballs realitzats, com també, rebent, si escau, el traspàs de la informació que sigui necessària per conèixer i comprendre el funcionament dels serveis desenvolupats.

11 Accés remot per la prestació dels serveis contractats

La DSTSC disposa d'un servei VPN que haurà de ser utilitzat per accedir remotament al sistema d'informació objecte del contracte en cas de connexió des de fora de les seves instal·lacions.

Requereix disposar de certificat digital reconegut, per identificar-se personalment, i la tramitació de la sol·licitud d'accés signada electrònicament per a cada un dels membres de l'equip assignat per la contractista**.** A part del control de l'accés i de l'autenticació de l'usuari caldrà que es puguin registrar accions efectuades sobre el sistema administrat.

La connexió necessària per a aquest accés remot haurà d'estar operativa en el moment d'inici del contracte.

Les despeses que es derivin de l'ús d'aquest enllaç les haurà d'assumir la contractista.

Metadades del document

Núm. expedient	2025/0021286
Tipus documental	Plec de clàusules o condicions
Títol	Plec de prescripcions tècniques particulars relatiu als serveis de ciberseguretat de la Diputació de Barcelona, dividit en dos lots
Codi classificació	D0506SE01 - Serveis obert

Signatures

Signatari		Acte	Data acte
Francisco Javier Gimenez Bruque (SIG)	Responsable directiu Servei Promotor	Signa	16/07/2025 19:25

Validació Electrònica del document

Codi (CSV)	Adreça de validació	QR
4df347647dc29081f309	https://seuelectronica.diba.cat	