Expedient: **260269**
Objecte: **Servei de capa de seguretat perimetral per a betevé**
Entitat contractant: **Informació i Comunicació de Barcelona, S.A., Spm (ICB)**

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SERVEI DE CAPA DE SEGURETAT PERIMETRAL PER A betevé

1. OBJECTE I ABAST DEL CONTRACTE

L'objecte d'aquest plec és regular la contractació del servei de manteniment, suport, operació tècnica i millora contínua de la capa de seguretat perimetral de Betevé, incloent-hi els equips de tallafocs principals, els equips remots de seguretat i interconnexió tant cablejats com sense fils (switches securitzats FortiSwitch i antenes wifi Fortinet), la plataforma d'anàlisi i correlació d'esdeveniments, les llicències de seguretat, els serveis de suport del fabricant, la gestió d'incidències, l'execució de tasques preventives i correctives, i l'acompanyament tècnic especialitzat durant tota la vigència contractual.

L'adjudicatari haurà d'assumir un servei extrem a extrem sobre la infraestructura de seguretat perimetral inclosa en l'abast, sense limitar-se a la mera tramitació de garanties o a la intervenció reactiva.

L'oferta haurà d'incloure una acceptació expressa i incondicionada de tots els requisits d'aquest plec, incloent-hi aquells formulats com a obligacions de resultat, obligacions de mitjà, lliurables periòdics i compromisos de nivell de servei.

L'adjudicatari haurà de mantenir totes les funcionalitats existents i les millores implantades durant el contracte, garantint continuïtat operativa, traçabilitat dels canvis i mínima afectació al servei.

2. SITUACIÓ ACTUAL I ACTIUS INCLOSOS

La capa de seguretat perimetral objecte d'aquesta licitació està formada per una arquitectura de tallafocs en alta disponibilitat ubicada als CPD principals, per equips remots de seguretat per a seus, per serveis de seguretat del fabricant i per una eina d'anàlisi i seguiment d'esdeveniments. La infraestructura actua com a punt de control del trànsit nord-sud i est-oest, realitza funcions de nivell 3, segmentació per zones, autenticació integrada amb directori corporatiu, sortida balancejada a Internet i terminació de VPN SSL i IPsec.

Element mínim inclòs	Quantitat mínima	Abast funcional
Tallafocs principals Fortigate FG-600E	actualment 2	Clúster actiu-actiu, VDOM, encaminament, polítiques interzones, VPN, perfils de seguretat i sortida a Internet.
FortiSwitches	actualment 18	Connectivitat VPN amb seus o serveis que requereixin accés a recursos interns avançats.
FortiAPs	actualment 17	Proporcionar acces Wi-Fi per producció i convidats
Plataforma Fortianalyzer	actualment 1	Gestió, registre, anàlisi, reporting, correlació i suport a l'explotació d'esdeveniments de seguretat.

L'oferta haurà d'identificar de manera nominal tots els actius inclosos, número de sèrie quan sigui possible, modalitat de suport, data d'expiració de llicències, versió de firmware, rol operatiu i criticitat.

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486. Llibre 4.788. Foli 17. Full 62.254. Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

Es consideraran inclosos tots els elements actualment operatius i els que s'incorporin durant la vigència del contracte per renovació, ampliació, substitució, RMA, creixement de seus o reconfiguració de l'arquitectura.

La solució haurà de preservar tota la configuració actual, és a dir, l'arquitectura multi-VDOM, la integració amb directori actiu, els perfils de navegació, el balanceig de sortides a Internet, les VPN SSL/IPsec i la interacció amb Fortianalyzer o eina equivalent.

3. OBJECTIUS TÈCNICS I PRINCIPIS DE SERVEI

- Assegurar la disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat de la capa de seguretat perimetral.
- Reduir la superfície d'atac mitjançant la neteja de regles, l'eliminació d'objectes obsolets, la revisió de certificats i l'enduriment de configuracions.
- Garantir suport expert del fabricant i del partner, amb escalat operatiu i seguiment fins a la resolució.
- Implantar un model de millora contínua basat en auditoria inicial, pla d'acció, indicadors, quadres de comandament i reunions periòdiques.
- Estandarditzar nomenclatura, documentació, gestió de canvis i evidències tècniques.
- Mantenir el servei amb mínima interrupció i amb plans de reversió documentats per a actuacions de risc.

L'adjudicatari haurà d'operar sota un principi de prevenció, no només de reacció, aportant recomanacions periòdiques de seguretat i optimització.
Tota intervenció que afecti producció haurà d'estar precedida d'una anàlisi d'impacte, finestra de canvi aprovada, còpia de configuració, pla de validació i pla de reversió.

4. REQUISITS D'AUDITORIA INICIAL I PLA DE MILLORA

Durant la fase inicial del servei es durà a terme una auditoria tècnica exhaustiva dels equips, regles, objectes, serveis, llicències, rutes, VPN, perfils i mecanismes de monitorització. L'auditoria no serà un document declaratiu, sinó una revisió tècnica amb evidències i accions prioritzades.

Bloc d'auditoria	Revisió mínima exigida	Evidència exigible
Inventari i llicències	Actius, números de sèrie, firmware, modalitat de suport, expiració, serveis actius i dependències.	Inventari signat, exportació de llicències i matriu de criticitat.
Polítiques de seguretat	Regles duplicades, genèriques, sense ús, excessivament permissives, obsoletes, sense registre o sense propietari.	Informe de regles amb recomanació: mantenir, ajustar, consolidar o retirar.
Objectes i nomenclatura	Objectes no utilitzats, grups incoherents, nomenclatura no estandarditzada i certificats obsolets.	Proposta de nomenclatura i pla de neteja.
VPN i accessos remots	VPN SSL, IPsec, accessos de proveïdors, MFA si escau, caducitat de comptes i còpies de seguretat d'accés.	Llistat de túnels, usuaris/perfils, riscos i mesures.
Encaminament i SD-WAN	Rutes estàtiques, policy routes, SD-WAN, balanceig de sortida, commutació per error, asimetries i dependències.	Mapa lògic i proves de commutació.
Seguretat avançada	IPS, antivirus, filtratge web, filtratge de correu, FortiGuard, signatures, polítiques d'inspecció i exclusions.	Estat dels perfils i recomanacions d'enduriment.

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486. Llibre 4.788. Foli 17. Full 62.254. Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

Fortianalyzer i registre	Recepció de registres, retenció, alertes, informes, correlació i cerques forenses bàsiques.	Captures/informes i proposta d'alertes.
Monitorització i ticketing	Integració d'alarmes, llindars, notificació, prioritat i traçabilitat.	Matriu alarma-severitat-tiquet-responsable.

L'auditoria inicial s'haurà de lliurar en un termini màxim de 30 dies naturals des de la reunió d'inici del Servei, sens perjudici del termini inferior que, si escau, hagi ofert l'empresa adjudicatària d'acord amb els criteris d'adjudicació establerts al PCAP.

El pla de millora haurà de classificar les accions per criticitat, esforç, risc, impacte, dependència i finestra requerida, indicant hores estimades i prioritat d'execució.

L'adjudicatari haurà d'executar les millores aprovades per l'entitat contractant amb control de canvis formal i amb evidències de validació posteriors.

5. REQUISITS DE MANTENIMENT DE FABRICANT, GARANTIES I RMA

El suport de fabricant és una peça essencial del servei i haurà de cobrir la totalitat dels equips inclosos durant tota la vigència contractual, incloses pròrrogues, ampliacions i substitucions. S'exigeix que l'adjudicatari actuï com a interlocutor únic davant del fabricant i assumeixi la gestió integral d'incidències, RMA i escalats.

L'adjudicatari haurà de tramitar directament els casos amb el fabricant, aportar diagnòstics, recollir evidències, fer seguiment diari dels casos crítics i mantenir informada l'entitat contractant fins al tancament.

En cas de substitució d'equip, l'adjudicatari haurà d'assistir en la preparació de l'RMA, la restauració de la configuració, la validació de connectivitat, la verificació de llicències, les proves d'HA/VDOM/VPN i la documentació del canvi.

6. MODEL DE SUPORT, ATENCIÓ I ESCALAT

El servei haurà de disposar d'un punt únic d'entrada per a incidències, peticions, consultes i canvis, amb registre automàtic, assignació d'identificador, classificació per severitat, assignació de tècnic responsable, traçabilitat de comunicacions i tancament validat.

Nivell	Responsabilitat mínima	Criteri d'intervenció
N1	Recepció, registre, categorització, recopilació inicial d'informació, execució de tasques de baixa complexitat i comunicació amb l'usuari autoritzat.	Incidències simples, consultes operatives, seguiment d'alarmes i verificació inicial.
N2	Diagnòstic tècnic, canvis controlats, resolució d'incidències de complexitat mitjana i coordinació amb N3.	Polítiques, VPN, perfils, registres, problemes recurrents i configuracions estàndard.
N3	Resolució d'incidències complexes, anàlisi avançada, coordinació amb fabricant, disseny de solucions i validació de canvis crítics.	Avaries de clúster, routing, VDOM, SD-WAN, rendiment, fallades de firmware o ciberincidents.
Fabricant	Suport especialitzat, anàlisi d'errors, substitució de maquinari, hotfix, recomanacions oficials i escalat intern.	Casos no resolubles per l'adjudicatari, RMA, defectes de producte o anàlisi d'enginyeria.
Director/Responsable de servei	Govern del contracte, control d'SLA, interlocució, reporting, escalat jeràrquic i millora contínua.	Incompliments, incidències greus, decisions de prioritat i comitès de seguiment.

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486. Llibre 4.788. Foli 17. Full 62.254. Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

El licitador haurà de proporcionar com a mínim dues vies d'obertura de tiquet: correu electrònic i telèfon. El servei de suport i atenció d'incidències haurà d'estar disponible les 24 hores del dia, els 365 dies de l'any (24x7), inclosos dissabtes, diumenges i festius.

L'adjudicatari haurà de garantir la disponibilitat dels recursos tècnics necessaris per atendre i gestionar les incidències durant tot aquest període, amb independència del nivell de suport requerit, i assegurar el compliment dels temps de resposta i escalat establerts en aquest plec.
Aquesta cobertura inclourà l'atenció remota i, quan sigui tècnicament necessari, la intervenció presencial, sense cap cost addicional per a ICB.

El sistema de suport haurà d'enviar notificacions d'obertura, canvis d'estat, sol·licitud d'informació, escalat i tancament.
Tota incidència haurà de contenir, com a mínim: data/hora d'obertura, sol·licitant, actiu afectat, servei afectat, severitat, causa estimada, accions realitzades, tècnic responsable, estat, propers passos, evidències i validació de tancament.

L'adjudicatari haurà de prestar assistència remota il·limitada per a incidències i consultes dins de l'abast, sense que el nombre de contactes pugui limitar l'obligació de restablir el servei.

7. SLA, CLASSIFICACIÓ D'INCIDÈNCIES I PENALITZACIONS

Els acords de nivell de servei es mesuraran des de l'obertura del tiquet o des de la detecció automàtica de l'alarma, el que succeeixi abans. Els temps de resposta impliquen una primera actuació efectiva documentada per personal competent, no només un acusament de recepció.

Severitat	Definició	Resposta remota	Resposta presencial	Actualització mínima	Objectiu de restauració
S1 - Crítica	Caiguda total o degradació severa del clúster principal, pèrdua de sortida a Internet corporativa, indisponibilitat de VPN crítica, afectació a més del 50% de la xarxa, risc de seguretat actiu o compromís en curs.	30 minuts	2 hores si escau	Cada 30 min	Treball continu fins a la restauració o workaround acceptat.
S2 - Alta	Afectació parcial rellevant, fallada d'un node HA sense pèrdua total, degradació de rendiment, problema en seu crítica, pèrdua de visibilitat de registres o bloqueig operatiu d'una àrea.	1 hora	4 hores si escau	Cada 2 hores	Restauració o workaround en jornada, excepte dependència del fabricant.
S3 - Mitjana	Incidència sense indisponibilitat crítica, consulta tècnica complexa, ajust de política, problema d'usuari/grup/VPN no generalitzat.	2 hores	N/A excepte necessitat tècnica	Diària o segons acord	Planificació segons prioritat i finestra autoritzada.

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486, Llibre 4.788, Foli 17, Full 62.254, Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

S4 - Baixa / Canvi	Consulta, petició d'informació, canvi menor, documentació, ajust evolutiu o tasca preventiva planificada.	2 hores	N/A	Segons planificació	Segons el pla de treball aprovat.

Els temps de resposta establerts en aquest apartat seran exigibles les 24 hores del dia, els 365 dies de l'any, inclosos dissabtes, diumenges i festius, d'acord amb el règim de cobertura del servei establert a l'apartat 6 d'aquest plec.

L'adjudicatari haurà de complir un mínim del 99% mensual dels SLA de resposta compromesos. Quan la resolució depengui del fabricant, operador o tercer, l'adjudicatari continuarà sent responsable del seguiment, coordinació, escalat i reporting fins a la recuperació del servei.

Es considerarà incompliment la manca d'actualització en incidències crítiques, l'absència d'evidències al tiquet, el tancament sense validació de l'entitat contractant o la classificació injustificada a una severitat inferior.

Les penalitzacions contractuals hauran de vincular-se a l'incompliment dels SLA de resposta, l'absència de reporting, la manca d'execució de tasques preventives, la reiteració d'errors de configuració i la manca de disponibilitat de suport de fabricant.

El compliment dels nivells de servei (SLA) establerts en aquest plec tindrà caràcter obligatori durant tota la vigència del contracte.

El compliment dels temps de resposta, actualització i seguiment de les incidències es verificarà mitjançant el sistema de gestió de tiquets, que haurà de permetre acreditar de manera objectiva les dates i hores de registre, les actuacions realitzades i els terminis de resposta.

Els incompliments dels nivells de servei, quan siguin imputables a l'adjudicatari, podran donar lloc a l'aplicació de les penalitats establertes al Plec de clàusules administratives particulars (PCAP), sens perjudici de les altres conseqüències contractuals legalment procedents.

8. MANTENIMENT PREVENTIU, CORRECTIU I EVOLUTIU

8.1 Manteniment preventiu

- Revisió de registres, esdeveniments, gràfiques i alarmes que puguin indicar anomalies.
- Comprovació de l'estat del clúster HA i de la sincronització entre nodes.
- Comprovació de còpies de configuració, desament correcte i restaurabilitat.
- Verificació de notificacions, integració amb monitorització i escalat d'alertes.
- Revisió de l'estat dels serveis FortiGuard o equivalents i vigència de llicències.
- Revisió de firmware, recomanacions del fabricant i necessitat d'actualització.
- Comprovació del funcionament entre cada tallafocs i Fortianalyzer.
- Revisió de VPN, certificats, objectes no utilitzats, regles genèriques i polítiques sense registre.
- Anàlisi de tendències: CPU, memòria, sessions, throughput, registres, atacs bloquejats i esdeveniments recurrents.

8.2 Manteniment correctiu

- Atenció remota d'incidències de maquinari, programari, configuració, llicències, registres, encaminament, VPN, polítiques o integració amb directori.
- Desplaçament in situ quan el diagnòstic remot determini una necessitat tècnica o quan la severitat ho requereixi.
- Restauració de configuracions, validació de serveis, proves de connectivitat i documentació de la resolució.
- Tramitació de RMA i coordinació amb el fabricant, incloent-hi seguiment, comunicació i validació de la substitució.
- Escalat a N2/N3/fabricant amb retenció de responsabilitat per part de l'adjudicatari.

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486, Llibre 4.788, Foli 17, Full 62.254, Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

L'adjudicatari haurà de documentar la causa arrel quan hi hagi una incidència repetitiva, una incidència crítica o una intervenció del fabricant.
Tota solució temporal haurà de registrar-se com a workaround, amb risc acceptat, data objectiu de solució definitiva i responsable assignat.

8.3 Manteniment evolutiu i millores

L'adjudicatari haurà de proposar millores de configuració, seguretat, rendiment, estandardització i operació, especialment sobre regles, VPN, SD-WAN, objectes, certificats, perfils de seguretat, registre i reporting.
Les millores aprovades s'executaran mitjançant control de canvis, prioritzant el baix risc, la reducció de la superfície d'atac i la continuïtat operativa.

8.4. Abast del servei de manteniment

Totes les actuacions de manteniment preventiu, correctiu i evolutiu descrites en aquest plec, així com les tasques de configuració, actualització, optimització, resolució d'incidències i millora contínua de la infraestructura de seguretat perimetral Fortinet de betevé, es consideren incloses en el preu d'adjudicació.
La prestació del servei tindrà caràcter integral i no estarà subjecta a una limitació del nombre d'hores d'intervenció, tant remotes com presencials, sempre que les actuacions estiguin compreses en l'objecte i l'abast del contracte.
L'adjudicatari no podrà excloure unilateralment cap actuació de les prestacions contractades ni exigir-ne una remuneració addicional. Qualsevol discrepància sobre l'abast de les obligacions contractuals haurà de ser comunicada i justificada davant d'ICB, que la resoldrà d'acord amb el que estableixen els plecs i el contracte, sens perjudici dels drets que legalment corresponguin a l'adjudicatari.

9. GESTIÓ DE CANVIS, CONFIGURACIÓ I DOCUMENTACIÓ

L'adjudicatari haurà de mantenir una CMDB o inventari tècnic actualitzat dels actius de seguretat, relacions, ubicacions, rols, llicències, versions, dependències, contactes i criticitat.

Abans de qualsevol canvi s'haurà de fer una còpia de seguretat de la configuració i haurà de quedar registrada la versió prèvia, la versió posterior i el motiu del canvi.

El licitador haurà d'aportar un procediment de canvis que inclogui sol·licitud, avaluació, aprovació, execució, validació, reversió i tancament documental.

La documentació mínima haurà d'incloure diagrames lògics, mapa de zones, matriu de regles crítiques, matriu de VPN, matriu de perfils, guia d'operació, guia d'escalat, inventari de certificats i pla de contingència.

Tota la documentació tècnica generada o actualitzada en execució del contracte, inclosos els inventaris, les configuracions, els procediments, els diagrames i els informes, haurà de quedar a disposició d'ICB en formats accessibles i editables, tant durant la vigència del contracte com a la seva finalització, sense cap cost addicional.

10. MONITORITZACIÓ, TICKETING, REPORTING I QUADRES DE COMANDAMENT

El servei haurà d'integrar-se amb eines de monitorització existents o proposades, incloent-hi alarmes crítiques, pèrdua de connectivitat, estat HA, expiració de llicències, ús de CPU/memòria, saturació de sessions, caiguda de VPN, absència de registres i esdeveniments de seguretat crítics.

L'eina de ticketing haurà de suportar processos ITIL d'incidències, peticions, problemes, canvis, configuració, versions i desplegaments, o aportar funcionalitat equivalent.

El client haurà de disposar d'accés en línia a l'estat dels tiquets, cues, prioritats, SLA, històrics i evidències, amb vistes executives i operatives.

L'adjudicatari haurà d'habilitar un quadre de comandament mensual amb indicadors operatius i executius, actualitzat com a mínim amb periodicitat diària per a tiquets i alarmes.

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486. Llibre 4.788. Foli 17. Full 62.254. Data 23/12/83 — CIF A08862997

KPI mínim	Descripció	Periodicitat
Disponibilitat lògica del servei	Estat del clúster, VPN crítiques, sortida a Internet i recepció de registres.	Mensual / esdeveniment
Compliment SLA	Resposta remota, resposta presencial, actualitzacions i restauració/workaround.	Mensual
Volumetria de tiquets	Nombre per severitat, categoria, actiu, estat i antiguitat.	Mensual
Causa arrel i recurrència	Incidències repetitives, problemes oberts i accions preventives.	Mensual
Canvis executats	Canvis aprovats, rebutjats, ajornats, reeixits i revertits.	Mensual
Estat de llicències i suport	Expiracions, modalitat, casos amb fabricant i RMA.	Mensual
Seguretat	Atacs bloquejats, malware, IPS, filtratge web, anomalies i recomanacions.	Mensual

11. EQUIP HUMÀ, CERTIFICACIONS I PARTNER DEL FABRICANT

El servei requereix coneixement especialitzat en seguretat perimetral, tecnologia Fortinet, operació en entorns productius crítics, gestió d'incidències i govern de serveis gestionats.

L'adjudicatari haurà de garantir, durant tota la vigència del contracte, l'accés efectiu al suport tècnic avançat de nivell N3 del fabricant Fortinet, mitjançant l'acreditació Engage Tech Support Partner (ETSP) o un mecanisme equivalent que permeti garantir el mateix nivell d'accés i escalat, sense demores incompatibles amb els nivells de servei establerts en aquest plec.

L'equip assignat al servei haurà de disposar de les capacitats tècniques necessàries per cobrir els nivells de suport N1, N2 i N3, així com les funcions de responsable de suport i director de servei, amb responsabilitats clarament definides i canals d'escalat establerts.

Els professionals que assumeixin funcions de nivell N2 hauran de disposar d'una experiència mínima de dos anys i de les certificacions tècniques del fabricant corresponents a les funcions que hagin de desenvolupar.

Els professionals que assumeixin funcions de nivell N3 hauran d'acreditar una experiència superior a cinc anys en solucions Fortinet o equivalents i capacitat d'interlocució tècnica amb el fabricant.
Una mateixa persona podrà assumir diferents funcions o nivells de suport, sempre que compleixi els requisits de qualificació i experiència corresponents al nivell més exigent i que aquesta acumulació de funcions no comprometi la disponibilitat ni la qualitat del servei.

L'adjudicatari haurà de garantir la disponibilitat permanent dels recursos tècnics necessaris per assegurar la cobertura del servei les 24 hores del dia, els 365 dies de l'any, i el compliment dels temps de resposta establerts en aquest plec.

L'adjudicatari haurà de garantir la continuïtat del coneixement mitjançant una base de coneixement, documentació de procediments, traspàs intern i cobertura durant vacances, baixes o rotació de personal.

Els mitjans personals necessaris per a la prestació del servei quedaran subjectes al compromís d'adscripció de mitjans establert al Plec de clàusules administratives particulars (PCAP).

12. SEGURETAT DE LA INFORMACIÓ, COMPLIMENT NORMATIU I CONFIDENCIALITAT

L'adjudicatari haurà de complir la normativa aplicable en protecció de dades, confidencialitat, prevenció de riscos laborals, seguretat de la informació i obligacions sociolaborals exigibles en la contractació pública.

Tot accés remot de l'adjudicatari haurà d'estar justificat, autoritzat, traçat, limitat al mínim privilegi i

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486, Llibre 4.788, Foli 17, Full 62.254, Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

protegit mitjançant mecanismes robustos d'autenticació.

En cas que, per raó de la prestació del servei, l'adjudicatari hagi d'accedir o tractar dades personals per compte d'ICB, aquest tractament quedarà subjecte a les disposicions del Reglament (UE) 2016/679 i de la Llei orgànica 3/2018, així com a les condicions establertes al corresponent acord d'encàrrec del tractament, que s'haurà de formalitzar abans de permetre l'accés a les dades.

L'adjudicatari haurà de garantir que els accessos als sistemes i als registres de seguretat es limitin a la informació estrictament necessària per a la prestació del servei, amb les mesures adequades de control d'accés, autenticació i traçabilitat.

L'adjudicatari haurà de mantenir la confidencialitat sobre configuracions, adreçaments, regles, credencials, registres, vulnerabilitats i qualsevol informació obtinguda durant el contracte.

L'adjudicatari haurà de notificar immediatament qualsevol incident de seguretat que afecti la infraestructura, el servei prestat, les seves eines de suport o la informació de l'entitat contractant.

La comunicació dels incidents de seguretat que afectin els sistemes o la informació d'ICB es realitzarà de manera immediata des que l'adjudicatari en tingui coneixement, sense esperar a la resolució de la incidència ni al tancament del tiquet.

Aquesta comunicació haurà d'incloure la informació disponible sobre la naturalesa de l'incident, els sistemes afectats, les possibles conseqüències i les mesures de contenció adoptades, i s'haurà d'actualitzar a mesura que es disposi de nova informació. Les credencials compartides estaran prohibides llevat d'impossibilitat tècnica justificada i aprovada.

S'hauran d'emprar comptes nominatius, rols, MFA quan sigui possible i revocació després de la finalització del servei.

13. GOVERNANÇA, REUNIONS I MILLORA CONTÍNUA

Se celebrarà una reunió d'arrencada durant els primers 10 dies hàbils del contracte per validar l'abast, els contactes, les eines, les prioritats, l'inventari inicial, els accessos i el calendari d'auditoria.

Se celebraran reunions quadrimestrals de seguiment, sense perjudici de reunions extraordinàries per incidències greus o canvis rellevants.

L'adjudicatari serà responsable de convocar les reunions, preparar els indicadors, emetre actes, registrar acords, assignar responsables i fer el seguiment de les accions pendents.

El seguiment i la supervisió tècnica del servei correspondran a la persona designada per ICB, que serà l'interlocutor tècnic amb l'adjudicatari i s'encarregarà de validar els informes, els lliurables i les actuacions realitzades, així com de fer el seguiment del compliment dels nivells de servei establerts en aquest plec.

El model de govern haurà d'incorporar la gestió d'incidències, problemes, canvis, esdeveniments, coneixement, qualitat i millora contínua.

Comitè / reunió	Freqüència	Contingut mínim
Arrencada del servei	Una vegada	Abast, inventari, accessos, contactes, matriu de severitat, auditoria i calendari inicial.
Seguiment operatiu	Mensual o sota demanda	Tiquets, incidències obertes, canvis, llicències, riscos i properes accions.
Comitè de servei	Quadrimestral	KPIs, SLAs, penalitzacions, millores, full de ruta, riscos i decisions de govern.
Postincident crític	Després d'un S1	Cronologia, causa arrel, impacte, mesures preventives, canvis i responsables.

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486. Llibre 4.788. Foli 17. Full 62.254. Data 23/12/83 — CIF A08862997

14. LLIURABLES MÍNIMS I ACCEPTACIÓ DEL SERVEI

Lliurable	Termini / freqüència	Criteri d'acceptació
Pla de transició i arrencada	10 dies hàbils	Inclou abast, contactes, accessos, calendari, riscos inicials i procediment de tiquets.
Inventari tècnic i matriu de llicències	30 dies naturals	Tots els actius inclosos, suport vigent, firmware, criticitat i rols.
Auditoria inicial i pla de millora	30 dies naturals	Troballes prioritzades, evidències, impacte, esforç, riscos i proposta d'execució.
Acta de comitè quadrimestral	Quadrimestral	Acords, decisions, responsables, dates i accions pendents.
Documentació de canvis	Per canvi	Sol·licitud, aprovació, còpia prèvia, execució, validació i reversió si escau.
Informe postincident crític	5 dies hàbils després del tancament	Cronologia, impacte, causa arrel, accions correctives i preventives.
Informe final de reversibilitat	Final del contracte	Estat dels actius, documentació, llicències, accessos, pendents i traspàs.

L'acceptació del servei estarà condicionada al lliurament complet i validació per part de l'entitat contractant dels lliurables obligatoris.
La manca de documentació actualitzada serà considerada defecte de prestació encara que el servei tècnic es trobi operatiu.

14.1. Reversibilitat i traspàs del servei

A la finalització del contracte, qualsevol que sigui la seva causa, l'adjudicatari haurà de garantir la reversibilitat del servei i facilitar la transició ordenada a ICB o, si escau, a un nou prestador, sense comprometre la continuïtat operativa ni la seguretat de la infraestructura.
A aquest efecte, l'adjudicatari haurà de lliurar a ICB tota la documentació tècnica actualitzada relativa al servei, inclosos els inventaris, les configuracions, els diagrames, els procediments, les llicències, els informes, les incidències pendents i qualsevol altra informació necessària per garantir-ne la continuïtat.
L'adjudicatari haurà de prestar la col·laboració tècnica necessària per facilitar el traspàs del coneixement i la informació, incloent-hi les reunions de coordinació que siguin necessàries durant el període de transició.
La reversibilitat i el traspàs de la informació i documentació generada en execució del contracte es consideren obligacions incloses en el preu d'adjudicació i no podran comportar cap cost addicional per a ICB.
Un cop finalitzat el traspàs, l'adjudicatari haurà de retornar o eliminar, segons les instruccions d'ICB i la normativa aplicable, els accessos, les credencials i les còpies de la informació que conservi, sens perjudici de les obligacions legals de conservació que resultin exigibles.

Annex I. Model d'informe mensual de servei

L'informe i/o acta quadrimestral haurà de ser executiu i operatiu, amb un annex tècnic suficient per auditar-ne el compliment. Es proposa l'estructura mínima següent:

- Resum executiu: situació general del servei, riscos principals i decisions requerides.
- Inventari i llicències: altes, baixes, canvis, expiracions i casos amb el fabricant.
- Disponibilitat i estat de salut: clúster, seus, VPN, Fortianalyzer, registres i serveis FortiGuard.
- Tiquets: volumetria, severitat, estat, antiguitat, incompliments i tendències.
- SLA: compliment de resposta remota, presencial, actualitzacions i restauració/workaround.

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486, Llibre 4.788, Foli 17, Full 62.254, Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat

- Canvis: executats, pendents, rebutjats, revertits i propers canvis planificats.
- Seguretat: esdeveniments rellevants, atacs bloquejats, malware, IPS, filtratge web/correu i anomalies.
- Manteniment preventiu: tasques realitzades, evidències, troballes i accions correctives.
- Problemes i causa arrel: recurrències, accions preventives, propietari i data objectiu.
- Pla de millora: avanç, bloquejos, prioritats i decisions sol·licitades.
- Annexos tècnics: captures, registres, exportació de tiquets, configuració no sensible i evidències.

Joan Bussé i Artigas
Director tècnic d'ICB

Inscrita en el Registre Mercantil de Barcelona. Tom 5.486. Llibre 4.788. Foli 17. Full 62.254. Data 23/12/83 — CIF A08862997

Informació i Comunicació de Barcelona SA spm
plaça Tísner, 1
08018 Barcelona
beteve.cat
@beteve
(+34) 935 064 200
info@beteve.cat