



INFORME EN EL QUE ES JUSTIFIQUEN ELS ASPECTES ESTABLERTS ALS ARTICLES 28, 100, 101 I 116.4 DE LA LLEI 9/2017 DE CONTRACTES DEL SECTOR PÚBLIC EN RELACIÓ AMB EL CONTRACTE DE SUBMINISTRAMENT RELATIU A L'ADQUISICIÓ O RENOVACIÓ DE LES SUBSCRIPCIONS DE SOLUCIONS INFORMÀTIQUES DE CIBERSEGURETAT I SERVEIS DE MANTENIMENT ASSOCIATS DE LA XARXA DE DADES DE LA FUNDACIÓ PRIVADA DE L'HOSPITAL DE LA SANTA CREU I SANT PAU.

EXP LICFP 26/03

Descripció del contracte

Subministrament de subscripcions de solucions informàtiques de ciberseguretat i serveis de manteniment associats de la xarxa de dades de la Fundació privada de l'hospital de la Santa Creu i Sant Pau.

De conformitat amb el previst als articles 28, 100, 101 i 116.4, de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (en endavant, LCSP), a l'expedient de contractació s'han de justificar els aspectes que es detallen en els referits preceptes de la norma abans esmentada. A tal efecte, el present informe té per finalitat donar compliment a allò establert als esmentats articles i s'emet, per tant, per tal de justificar els aspectes que s'estableixen a continuació en relació amb el contracte de **"Subministrament relatiu a l'adquisició o renovació de subscripcions de solucions informàtiques de ciberseguretat i serveis de manteniment associats de la xarxa de dades de la Fundació privada de l'hospital de la Santa Creu i Sant Pau"**.

- Objecte del contracte.
- Necessitats a satisfer i idoneïtat de l'objecte i contingut del contracte.
- Insuficiència de mitjans propis de l'entitat per a realitzar la prestació objecte del contracte.
- El pressupost de licitació, el valor estimat i la durada del contracte.
- Elecció del procediment de licitació.
- Els motius pels quals el contracte indicat es realitza sense dividir el seu objecte en diferents lots.
- Els criteris de solvència tècnica o professional, econòmica i financera i els criteris d'adjudicació.
- Condicions especials d'execució.

A continuació es procedeix a desenvolupar els conceptes exposats prèviament:

I) Objecte del Contracte:

L'objecte de la licitació és l'adquisició o renovació de subscripcions de solucions informàtiques de ciberseguretat i serveis de manteniment associats de la xarxa de dades de la Fundació privada de l'hospital de la Santa Creu i Sant Pau. La descripció i característiques dels béns i la forma de portar a terme la prestació per l'adjudicatari seran les estipulades en el Plec de Prescripcions Tècniques (d'ara en endavant, PPT).

Codis CPV:

48000000-8	Paquets de software i sistemes d'informació
48730000-4	Software de seguretat informàtica
72267000-4	Serveis de manteniment i suport de software



72267100-5	Serveis de manteniment de sistemes d'informació
72262000-9	Serveis de desenvolupament de software (actualitzacions i millores evolutives)
72253200-5	Serveis d'assistència tècnica

S'ha de tenir present que l'adquisició o renovació de subscripcions de solucions informàtiques de ciberseguretat, han de ser compatibles amb la infraestructura i els sistemes actuals que ja estan en funcionament. Els objectius principals són els següents:

- Comptar amb unes solucions informàtiques de ciberseguretat adequades per protegir la xarxa de dades de la Fundació.
- Comptar amb un entorn de ciberseguretat de la Fundació, amb les eines adequades que facilitin l'eficiència en la gestió:
 - Unificant venciments de solucions ja existents i les de nova adquisició mitjançant còterm.
 - Mantenint i millorant el nivell de ciberseguretat en els diferents vectors sensibles com el correu, els endpoints, cloud, etc.
- Acompanyament en la implantació d'eines avançades, amb interoperabilitat amb l'ecosistema existent Fortinet.
- Compliment normatiu (ENS, RGPD/LOPDGDD) i traçabilitat d'activitat.

II) Necessitats a satisfer:

Es requereix que una empresa informàtica externa, faciliti la subscripció de solucions informàtiques de ciberseguretat per la xarxa de dades de la Fundació i que també s'encarregui del seu manteniment, les efectes que l'Àrea de Sistemes d'Informació pugui desenvolupar correctament totes les tasques que li estan encomanades. Per tant, l'abast inclou:

- El subministrament de subscripcions de solucions informàtiques de ciberseguretat, ja sigui per la via de la renovació de solucions actualment existents o per la via de l'adquisició de noves solucions.
- En arreglar-se dels serveis de manteniment, així com dels serveis tècnics associats a les subscripcions renovades o adquirides de nou durant tota la vigència del contracte.

III) Idoneïtat de l'objecte i contingut del contracte:

La Fundació disposa d'una arquitectura de ciberseguretat amb equipaments i solucions de ciberseguretat de Fortinet sobre la qual es requereix continuïtat i evolució funcional com la gestió centralitzada, l'anàlisi de logs, MFA, ZTNA, MDR, CASB i protecció de correu. Es considera la renovació i adquisició de les diferents solucions informàtiques de ciberseguretat seguretat, com una mesura bàsica i essencial pel bon funcionament dels sistemes d'informació.

Actualment es compta amb les següents subscripcions de solucions informàtiques de ciberseguretat a la Fundació:

- FortiCASB (100 usuaris)
- FortiClient + EMS (100 endpoints)
- FortiEDR (100 endpoints)
- FortiAnalyzer
- FortiAuthenticator (fins 500 usuaris)
- FortiMail (100 bústies i 5 dominis)

Es considera per tant que es dona compliment al que es disposa en l'article 116.4.e), ja que hi ha una clara i proporcional vinculació entre l'objecte del contracte i les necessitats que es pretenen satisfer.

IV) Insuficiència de mitjans propis de l'entitat per a realitzar la prestació objecte del contracte

- *Insuficiència de mitjans materials:* L'entitat no pot fer directament la prestació objecte del contracte, atès es tracta de compra de subscripcions de programari específics a proveïdors, de forma que al no comptar amb els mitjans materials apropiats per poder donar compliment a l'objecte del contracte que precisa, és necessari la contractació d'una empresa distribuïdora que pugui subministrar la totalitat de les prestacions descrites en el PPT.

V) Pressupost de licitació:

S'entén per pressupost base de licitació, el límit màxim de despesa que, en virtut del contracte pot comprometre l'òrgan de contractació, inclòs l'Impost del Valor Afegit. Atinent a que el pressupost de licitació ha de ser adequat als preus de mercat, havent de tenir en consideració els costos directes i indirectes i altres eventuais despeses calculats per a la seva determinació, es fixa el següent pressupost de licitació:

Total pressupost base de licitació: **100.000.-€ (IVA exclòs)** per un període de 5 anys

Concepte	Import (IVA exclòs)	IVA (21%)	Import total (IVA inclòs)
Pressupost base de licitació	100.000.-€	21.000.-€	121.000.-€

VI) Valor estimat del contracte:

S'entén per valor estimat del contracte el valor l'import total, sense incloure l'Impost del Valor Afegit, pagador segons les estimacions realitzades. El mètode aplicat per calcular el valor estimat del contracte és, de conformitat amb l'article 101 de la LCSPS, el següent:

Concepte	Import (IVA exclòs)
Pressupost base de licitació total	100.000.-€ (5 anys)
Possibles modificacions	NO
Pròrrogues	NO
TOTAL	100.000.-€

VII) Durada del contracte:

El termini de durada del contracte serà de 5 anys, a comptar des de el dia següent a la formalització contractual. No es preveuen pròrrogues del contracte. Pel que respecta a la provisió de les subscripcions, el termini màxim és de 2 mesos, a excepció de la subscripció de Forti EDR que caldrà subministrar quan caduqui la subscripció actual (a gener de 2027).

El manteniment i servei tècnic associat a les subscripcions es realitzarà durant tota la durada del contracte. Aquest contracte s'executarà en La Fundació Privada Hospital de la Santa Creu i Sant Pau (veure plec de prescripcions tècniques).

VIII) Justificació del procediment utilitzat per l'adjudicació del contracte:

Considerant l'import del contracte, la seva durada i les prestacions que constitueix el seu objecte, així com el valor estimat del contracte i els criteris que serviran per a la seva adjudicació, es considera que el més adient és adjudicar aquest contracte mitjançant un procediment obert no subjecte a regulació harmonitzada de conformitat amb el que s'estableix a la LCSP, essent necessària la preparació dels plecs de clàusules particulars i de prescripcions tècniques que regeixin la corresponent licitació.

Es tracta d'un contracte de subministrament, d'acord amb el que es preveu en l'article 16 de la LCSP, definits com aquells l'objecte dels quals són objecte per l'adquisició, l'arrendament financer o l'arrendament amb o sense opció a compra de productes i bens mobles.

Amb la finalitat de garantir la major concurrència pública, el procediment més idoni per a la licitació i adjudicació del contracte de subministrament és la tramitació mitjançant procediment obert no harmonitzat, d'acord amb el contingut dels articles 156, 157 i 158 de l'actual LCSP; uns articles on es regulen les normes bàsiques sobre el procediment obert en la seva modalitat de tramitació ordinària.

Així mateix, i atenent al valor estimat del contracte a licitar per valor de 100.000.-€ IVA Exclòs (que no esdevé superior a la xifra de 221.000.-€ IVA exclòs), d'acord amb l'article 22.1.b) no estarà subjecte a regulació harmonitzada.

IX) Justificació de la no divisió en lots:

Aquesta licitació, té per objecte l'adquisició i la renovació de les subscripcions de solucions de ciberseguretat (licències i els seus serveis associats), així com els serveis de manteniment corresponents per a la xarxa de dades corporativa de l'entitat, incloent-hi el seu suport, les actualitzacions, la gestió de versions, l'assistència tècnica i, si escau, les substitucions o serveis professionals vinculats. Es tracta d'un conjunt de prestacions interdependents en què el subministrament que correspon a les subscripcions i el servei de manteniment formen una unitat funcional orientada a mantenir un nivell de seguretat informàtica i disponibilitat homogènia a tota la xarxa de dades.

En aquest contracte, i atenent al contingut de l'article 99.3 de la LCSP, no s'ha optat per la seva divisió en lots per raons de tipus econòmic i de caràcter tècnic. La naturalesa dels subministraments i la seva execució de forma independent de suposaria una dificultat tècnica pels següents motius:



- Les de tipus econòmic, deriven del fet que el volum dels possibles lots que resultarien de dividir el pressupost total de licitació, serien de poc import econòmic, aspecte que faria que molts dels distribuïdors de material informàtic no estiguessin interessats en concorre per separat a cadascun dels diversos lots de material (degut a la seva escassa quantia), provocant-se en conseqüència l'efecte contrari al que es pretén amb una licitació dividida en lots, que es fomenta la màxima concurrència dels possibles licitadors, atès la majoria d'aquets "distribuïdors de llicències de programes informàtics" treballen amb tots els productes que es sol·liciten.
- Garantia i Suport: Amb un únic proveïdor, és més senzill gestionar les llicències i el suport tècnic. Això pot ser crucial per a l'èxit del projecte.
- Coordinació en l'execució de les prestacions: La pluralitat de contractistes diferents poden produir riscos associats a la compatibilitat entre diferents prestacions o a la coordinació entre diversos proveïdors, la no divisió en lots és una opció més òptima.
- En termes d'unitat funcional i per garantir la coherència de la plataforma de les llicències de ciberseguretat d'una forma segura i garantir la seva gestió centralitzada, es decideix configuren i governen de manera integrada; dividir-les en lots independents trencaria la coherència de polítiques (regles, signatures, llistes, objectes), així com dificultaria la segmentació consistent i multiplicaria punts de fallada en correlació i logging.
-
- La gestió centralitzada de llicències i de les subscripcions (co-terminació, entitlements, claus i tenants) requereix que siguin gestionades per un únic responsable per assegurar la seva traçabilitat i un mode de governança unificada (versions, calendari de patching, inventari i auditories).

X) Criteris de solvència:

Atenent a que l'objecte del contracte és el subministrament de subscripcions de programari de ciberseguretat, i en funció del valor estimat es proposen els següents criteris de solvència:

A) Solvència econòmica:

Justificació: Es tria aquest criteri com a mitjà d'acreditació de la solvència econòmica de l'empresari així com el seu llindar mínim és comprovar que l'empresa licitadora té capacitat suficient per a fer front financerament a aquest contracte, no essent l'únic encàrrec que pot assumir simultàniament amb altres possibles clients que pugui tenir. L'entitat que concorri al contracte, ha de ser una empresa amb implantació, amb un volum de negoci o un patrimoni significatiu reflex d'una important activitat empresarial, que contribueixi a garantir l'èxit del subministrament i d'altra banda, és proporcionat al no ser excessivament elevat per a assegurar que el contracte no quedi desert.

Declaració sobre el volum global de negocis en l'àmbit d'activitats corresponent a fi del contracte, referit com a màxim als tres últims exercicis disponibles en funció de la data de creació o d'inici de les activitats de l'empresari, en la mesura que es disposi de les referències d'aquest volum de negocis. El volum global de negoci mínim exigit no excedirà 1,5 vegades el valor del contracte, atès que el contracte té una duració superior a un any, esdevenint en aquets cas com a mínim l'import a acreditar serà **de 150.000.-€**.



Acreditació: *El licitador presentarà els seus comptes anuals aprovats i dipositats al Registre Mercantil corresponent, si l'empresari està inscrit i, en cas contrari, per les dipositades al registre oficial al qual hagi d'estar inscrit. Els empresaris individuals no inscrits en el Registre Mercantil han d'acreditar el seu volum anual de negocis mitjançant els seus llibres d'inventaris i comptes anuals legalitzats pel Registre Mercantil. Atenent al que es disposa en l'article 87.2 LCSP, els licitadors inscrits al RELI i/o ROLECE, podran acreditar aquest requisit sempre que els mateixos es troben reflectits en el seu certificat del RELI o ROLECE.*

B) Solvència tècnica i professional:

Justificació: Entre els mitjans d'acreditació de solvència tècnica que s'estableix a l'article 90 de la LCSP, s'han considerat un que es descriuran a continuació, atès és fonamental que l'empresa adjudicatària compti amb suficient experiència en subministraments informàtics de similars característiques donada l'especificitat tècnica dels mateixos, fomentant-se alhora un adequat nivell de competència. Es tracta d'obtenir un subministrament de material informàtic que ofereixi garanties suficients en el seu funcionament. L'exigència d'acreditació dels subministraments d'igual o similar naturalesa als d'aquest contracte, resulten ajustats al valor estimat i es té en compte la seva durada per tal que es pugui garantir la selecció d'operadors econòmics amb la necessària solvència tècnica sense establir cap barrera que artificialment restringeixi la concurrència.

b.1.) L'empresa licitadora aportarà una relació dels principals subministraments efectuats en els darrers 3 anys de naturalesa igual o similar, segons la descripció de l'objecte del contracte, que incloguin imports, dates i destinataris. A efectes d'acreditació de la solvència, es considerarà suficient la realització d'un o diversos contractes de subministrament i serveis de ciberseguretat i/o gestió de llicències de software, per un import acumulat igual o superior a **100.000.-€**, sense que sigui necessari que cap contracte individualment considerat assoleixi aquest import.

S'acreditarà mitjançant certificats expedits o visats per l'òrgan competent, quan el destinatari sigui una entitat del sector públic o, quan el destinatari sigui un subjecte privat, mitjançant un certificat expedit per aquest o, a falta d'aquest certificat, mitjançant una declaració de l'empresari acompanyada dels documents en qüestió, en poder del mateix que acreditin la realització de les prestacions on es deixi constància de l'import dels treballs, l'objecte contractual, el nom del client i l'any d'execució. En cas que aquesta relació consti al RELI, no caldrà acreditar-ho, sempre i quan en el mateix, consti validat amb un SI per l'òrgan competent.

b.2.) Normes de qualitat:

A l'objecte d'assegurar la conformitat de l'empresa adjudicatària amb determinades normes de qualitat directament relacionades amb el servei demandat, i garantir la capacitat tècnica de la mateixa en relació amb la infraestructura actual instal·lada a la Fundació i la proposta en la seva oferta, l'empresa licitadora ha de disposar i acreditar les següents certificacions:

Sistemes de gestió de la qualitat i de la seguretat de la informació:

Justificació: L'article 74.2 de la LCSP estableix que els requisits mínims de solvència han d'estar vinculats a l'objecte del contracte i ser proporcionals al mateix. Els articles 89, 90 i 92 LCSP permeten a l'òrgan de contractació escollir els mitjans d'acreditació de la solvència tècnica entre els previstos a la Llei (experiència, mitjans personals, certificats de qualitat, etc.).



L'article 93 LCSP regula l'acreditació del compliment de normes de garantia de la qualitat i admet expressament l'ús de certificats expedits per organismes independents, amb obligació de reconèixer certificats equivalents i d'acceptar "*altres proves de mesures equivalents*" que aportï l'empresari.

El licitador haurà d'acreditar que disposa de sistemes de gestió implantats i operatius en matèria de qualitat, gestió de serveis TI i seguretat de la informació, vinculats a l'objecte del contracte. A aquest efecte, es considerarà mitjà adequat d'acreditació l'aportació dels certificats següents, vigents en el moment de finalitzar el termini de presentació d'ofertes:

1. Certificació "**UNE-EN ISO 9001**" relativa a sistemes de gestió de la qualitat aplicable a activitats de subministrament i serveis TIC:

Motivació: La ISO 9001 encaixa de ple en el concepte de "*normes de garantia de la qualitat*", ja que estableix requisits sobre el funcionament intern de l'empresa per garantir la qualitat dels seus productes i serveis, de forma que l'òrgan de contractació pot exigir-la com a solvència tècnica, d'acord amb el que preveuen els articles 74, 89, 92 i 93 de la LCSP, en tant que norma de garantia de la qualitat directament vinculada a l'objecte del contracte. Aquesta exigència es configura de manera proporcional, atesa la criticitat dels serveis i subministraments de ciberseguretat sobre la xarxa de dades, i respecta els principis de concurrència en reconèixer "*certificats equivalents*" i altres proves adequades que acreditin l'existència de mesures de gestió de la qualitat equivalents.

Disposar d'aquesta ISO, garanteix que el licitador disposa d'un sistema de gestió de la qualitat implantat i auditat, basat en processos, en el cicle PDCA i en el pensament basat en el risc, fet que permet assegurar la prestació consistent i controlada dels subministraments i serveis TIC objecte del contracte, la correcta gestió de les comandes i renovacions de llicències, així com la resolució sistemàtica d'incidències i la millora contínua. En un contracte de subministrament i serveis TIC (llicències de ciberseguretat + manteniment):

- Assegura que el proveïdor té procediments documentats per al tractament de comandes, gestió d'incidències, control de versions, atenció a l'usuari, etc.
- Redueix el risc d'errors en la gestió de subscripcions, terminis de renovació, assignació de llicències, i en la coordinació amb els serveis de manteniment de la xarxa de dades.
- Facilita el seguiment de nivells de servei i la traçabilitat de les no conformitats, aspectes crítics per a la continuïtat d'un servei de ciberseguretat.

2. Certificació **ISO/IEC 20.000-1** relativa a sistemes de gestió de serveis TI:

Motivació: Des del punt de vista de la LCSP, ISO 20000-1 és una norma específica de qualitat en la prestació de serveis TI, que encaixa als articles 89/90 (solvència tècnica en subministraments i serveis) i 93 (normes de garantia de la qualitat), quan el contracte té com a objecte serveis de tecnologia de la informació o serveis que depenen de manera directa d'aquests, i no en contractes on l'objecte no és TI. És a dir, es considera adequat exigir-la quan hi ha prestació de serveis TI a l'organització o a tercers.



En el nostre cas, l'objecte és clarament serveis TI de ciberseguretat i manteniment de xarxa, per la qual cosa la vinculació amb l'objecte és directa i el requisit es pot defensar com a proporcional i no discriminatori,

La ISO/IEC 20000-1:2018 especifica els requisits necessaris per establir, implantar, mantenir i millorar de forma contínua un sistema de gestió de serveis (SMS) de TI. Inclou el disseny, la transició, el lliurament i la millora dels serveis per complir els requeriments del servei i aportar valor de qualitat al client.

Aquesta norma proporciona un marc homologat (alineat amb bones pràctiques tipus ITIL) perquè els serveis TI estiguin orientats al negoci i al client, assegurant, uns processos formals de gestió d'incidències, problemes i canvis, una gestió de nivells de servei (SLAs) i disponibilitat i una coordinació entre diversos proveïdors i serveis. Aquest aspectes, resulten especialment rellevants per al contracte que ens ocupa, atès l'objecte inclou serveis de tant de manteniment com de suport sobre solucions de ciberseguretat i sobre la xarxa de dades corporativa.

La seva exigència es considera proporcionada i adequada per garantir un nivell mínim d'organització i maduresa en la gestió dels serveis de ciberseguretat i de manteniment de la xarxa de dades, admetent en tot cas certificats equivalents i altres proves adequades de mesures de gestió de serveis de qualitat.

Disposar d'aquesta certificació, garanteix que el proveïdor disposa d'una organització de servei TI madura, capaç de gestionar incidències de seguretat, actualitzacions de signatures, canvis de configuració i suport a usuaris de forma consistent. Redueix el risc de caigudes de servei o de respostes improvisades davant incidents de ciberseguretat, donat que tot el cicle de vida del servei està definit i controlat.

3. **Certificació ISO/IEC 27.001** relativa a sistemes de gestió de la seguretat de la informació.

Motiva tècnica i jurídica: Des d'una òptica tècnica, la certificació ISO/IEC 27001 acredita que el licitador disposa d'un sistema de gestió de la seguretat de la informació basat en l'anàlisi i tractament de riscos, amb controls específics sobre xarxes, sistemes i dades. Això és essencial per a un contracte que té per objecte solucions de ciberseguretat i serveis de manteniment d'una xarxa de dades, ja que garanteix un nivell mínim i verificat de maduresa en la gestió de la confidencialitat, integritat i disponibilitat de la informació

Aquesta certificació, en termes jurídics es justifica en el sentit que s'exigeix com a mitjà d'acreditació de la solvència tècnica en matèria de seguretat de la informació, en tant que es una norma de garantia de qualitat clarament vinculada a l'objecte del contracte de ciberseguretat i manteniment de la xarxa de dades. La seva exigència es fonamenta en els articles 74, 89, 90, 92 i 93 de la LCSP i es configura de forma proporcional a la criticitat dels riscos de seguretat que es pretenen evitar, admetent certificats equivalents i altres proves adequades que demostrin la implantació de mesures de seguretat de la informació equivalents.

El seu requeriment, es planteja en termes que pot afectar una capacitat organitzativa interna de l'empresa (com gestiona la seguretat dels seus serveis), i esdevé objectivament rellevant per la correcta execució del contracte (com serien la protecció de dades i els serveis crítics),

Aquesta ISO defineix els requisits per establir, implantar, mantenir i millorar de forma contínua un sistema de gestió de la seguretat de la informació (ISMS). Es basa en un enfocament de gestió

de riscos, amb controls orientats a garantir la confidencialitat, la integritat i la disponibilitat de la informació, mitjançant polítiques, controls tècnics i organitzatius, auditories i millora contínua.

En l'àmbit de la ciberseguretat, demostra que l'empresa té un marc sistemàtic per identificar, valorar i tractar riscos de seguretat. Inclou controls sobre xarxes, accessos, criptografia, continuïtat de negoci, gestió d'incidents, etc., tots ells directament relacionats amb la gestió d'una xarxa de dades corporativa i solucions de ciberseguretat.

A més, la norma ajuda les organitzacions a complir requeriments legals i contractuals en matèria de protecció de dades i seguretat de la informació.

Tal i com s'ha citat de forma individual per a cadascun dels certificats, es recorda que també s'admetran **certificats equivalents** expedits per organismes establerts en qualsevol Estat membre de la Unió Europea, així com altres proves adequades que acreditin de forma fefaent l'aplicació efectiva de mesures de garantia de la qualitat, la gestió de serveis TI i la seguretat de la informació equivalents a les ofertes pels certificats anteriors, d'acord amb l'article 93 de la LCSP.

4. Experiència i qualificació del personal adscrit al contracte en relació a la certificació Fortinet NSE 7 (Network Security Architect) o certificació equivalent.

Motivació: L'objecte del contracte inclou la prestació de serveis relacionats amb la configuració, l'administració i el manteniment de solucions de ciberseguretat basades en tecnologia Fortinet, així com la resolució d'incidències de seguretat que poden afectar la continuïtat del servei de xarxa de dades corporativa. Aquestes tasques requereixen un nivell alt de coneixement especialitzat sobre l'arquitectura, la configuració avançada i les funcionalitats de les solucions Fortinet, especialment pel que fa a la definició de polítiques de seguretat, la gestió de VPN, la segmentació de xarxa, la detecció i resposta davant amenaces i la integració amb altres components de seguretat.

La certificació Fortinet NSE7 (Network Security Architect) acredita que el tècnic ha assolit un nivell avançat de competència en el disseny, desplegament i administració de solucions de seguretat de xarxa Fortinet en entorns complexos, incloent-hi la capacitat per diagnosticar i resoldre incidències crítiques. Per aquest motiu, es considera tècnicament necessari exigir que el licitador disposi d'un nombre mínim de tècnics amb certificació Fortinet NSE7 o superior, o bé amb certificacions i experiència equivalents, com a mitjà per garantir que l'empresa adjudicatària disposa de personal qualificat per prestar amb garanties les prestacions de ciberseguretat i manteniment de la xarxa de dades objecte del contracte, reduint el risc de configuracions inadequades, temps d'inactivitat prolongats i incidents de seguretat no gestionats correctament.

D'acord amb el que estableix l'article 74.2 de la Llei 9/2017, de 8 de novembre, de contractes del sector públic (LCSP), els requisits mínims de solvència han d'estar vinculats a l'objecte del contracte i ser proporcionals al mateix. En el present contracte, l'objecte consisteix en la prestació de serveis de ciberseguretat i manteniment de la xarxa de dades basats en solucions Fortinet, la qual cosa fa que la qualificació tècnica del personal encarregat de la seva execució sigui un element essencial per garantir-ne l'adequada prestació.

L'article 90.1.e) LCSP preveu expressament com a mitjà d'acreditació de la solvència tècnica, en els contractes de serveis, la titulació acadèmica i professional del personal responsable de l'execució, i, per extensió, la seva qualificació tècnica específica. En aquest sentit, la certificació



Fortinet NSE7 s'utilitza com a referència objectiva i verificable de la competència avançada del personal en l'àmbit concret de la seguretat de xarxa sobre tecnologia Fortinet.

El requisit es configura, a més, de forma proporcional, atès que:

- Es limita a un nombre determinat de tècnics adscrits al contracte (no a tota la plantilla de l'empresa),
- Es circumscriu a funcions directament vinculades a l'objecte del contracte (disseny, administració i suport de les solucions de ciberseguretat sobre la xarxa de dades), i
- S'admeten certificacions i proves equivalents, és a dir, no s'exigeix de manera excloent una única certificació de marca, sinó que es permet acreditar un nivell de coneixement i experiència equiparable mitjançant altres certificacions professionals en seguretat de xarxa i documentació acreditativa de l'experiència.

D'aquesta manera, el requisit de comptar amb tècnics amb certificació Fortinet NSE7 o equivalent es presenta com un mitjà adequat i necessari d'acreditació de la solvència tècnica del licitador, d'acord amb els articles 74 i 90 LCSP, i respecta els principis de lliure concurrència, igualtat de tracte i no discriminació, en la mesura que no tanca el mercat a un únic esquema de certificació i es limita a garantir un nivell mínim de competència tècnica coherent amb la complexitat i criticitat de l'objecte contractual.

El licitador haurà d'acreditar que disposa de personal tècnic amb qualificació avançada en el disseny, configuració, administració i manteniment de solucions de ciberseguretat de xarxa basades en tecnologia Fortinet o equivalent. A aquests efectes, es requereix que el licitador disposi, com a mínim:

- La disponibilitat, en plantilla o mitjançant vinculació contractual estable, d'almenys 1 tècnic que s'adscriurà a l'execució del contracte, que compleixin els requisits següents:
 - o Tinguin experiència acreditada en la implantació i administració de solucions de ciberseguretat sobre infraestructures de xarxa de dades corporatives.
 - o Estiguin en possessió de la certificació Fortinet NSE 7 (Network Security Architect) o superior.
 - o o bé, alternativament, acreditin un nivell de coneixements i experiència equivalent mitjançant altres certificacions professionals avançades en l'àmbit de la seguretat de xarxa i/o de la tecnologia Fortinet, i documentació acreditativa de l'experiència en projectes de característiques similars a l'objecte del contracte.

Aquesta solvència tècnica es podrà acreditar mitjançant la presentació, com a mínim, de la documentació següent:

- Relació nominativa del tècnic que el licitador preveu adscriure al contracte per al compliment del requisit anterior, indicant-ne el perfil professional, funcions i grau d'adscripció.
- Currículum vitae o fitxa tècnica de cadascun dels professionals, on constin de manera clara: la formació acadèmica, les certificacions professionals en l'àmbit de la



ciberseguretat i de la tecnologia Fortinet, i l'experiència prèvia rellevant en serveis de característiques semblants a l'objecte del contracte.

- Còpia de les certificacions Fortinet NSE7 o superiors i, si escau, de la resta de certificacions professionals que s'al·leguin com a equivalents, així como qualsevol altra documentació acreditativa de l'experiència i competència tècnica.

Els tècnics que s'hagin utilitzat per acreditar la solvència tècnica es consideraran adscrits al contracte, d'acord amb l'article 76 de la LCSP, i l'òrgan de contractació podrà exigir, durant l'execució, que l'adjudicatari mantingui un nivell de qualificació i dedicació del personal igual o superior al declarat en la fase de licitació, sense perjudici de les substitucions que es puguin autoritzar sempre que es garanteixi un nivell de capacitat equivalent.

En relació a la proporcionalitat del requisit del criteri de solvència, així com en relació a l'admissibilitat de les seves equivalències, d'acord amb els articles 74 i 90 de la LCSP, atenent la naturalesa i complexitat de l'objecte del contracte, i es considera proporcional en limitar-se a un nombre determinat de tècnics directament vinculats a l'execució i que en cap cas aquest requisit tindrà caràcter exclouent respecte d'una única certificació de marca, atès que es reconeixeran certificacions i proves equivalents que acreditin un nivell de competència tècnica igual o superior en l'àmbit de la seguretat de xarxa i de les solucions de ciberseguretat aplicables a l'objecte del contracte.

XI) Criteris d'adjudicació:

De conformitat amb l'article 145.1 de la LCSP i en el marc del compromís de l'òrgan de contractació amb la sostenibilitat ambiental, s'estableixen els següents criteris d'adjudicació ambientals, vinculats a l'objecte del contracte i valorables mitjançant fórmula. Tots els criteris ambientals són vinculants amb l'objecte del contracte i tenen una incidència directa sobre la qualitat i sostenibilitat del subministrament.

Tots aquest criteris de tipus automàtic, estan clarament vinculats amb la naturalesa del subministrament informàtic. La seva quantificació es objectiva, atès es poden puntuar amb barems clars. La seva evidència es durà terme mitjançant certificacions, declaracions tècniques o proves documentals.

Oferta econòmica (100 punts)

S'haurà d'ofertar un preu únic per a totes les subscripcions a subministrar que consten detallades en el PPT.

La fórmula aplicable es la següent:

(preu ofertat per la millor oferta, la més baixa) / (preu de l'oferta avaluada) x (puntuació màxima d'aquest apartat).

En cap cas la suma del preu ofertat pot superar els 100.000,00.-€.

Baixa temerària: Es considera baixa temerària aquells preus que siguin inferiors en 20% a la mitjana de les ofertes presentades.

La puntuació final serà la resultat de valorar la fórmula anterior (màxim de 100 punts).

XIII) Condicions especials d'execució:

S'estableixen per aquest contracte les següents condicions especials d'execució:

1. **Condicció d'especial execució "Esquema Nacional de Seguretat (ENS)":**

Motivació: Disposar de la certificació del "ENS" determina la política de seguretat que s'ha d'aplicar en la utilització dels mitjans electrònics, per a complir amb les exigències de seguretat dels sistemes, dades, comunicacions i serveis electrònics. La finalitat de l'Esquema Nacional de Seguretat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, que permeti als ciutadans i a les Administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans"; que de conformitat amb l'article 1 d'aquest Reial decret 3/2010, l'ENS "serà aplicat per les Administracions públiques per assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en mitjans electrònics que gestionin en l'exercici de les seves competències.

En definitiva, l'ENS persegueix fonamentar la confiança en què els sistemes d'informació prestaran els seus serveis i custodiaran la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control, i sense que la informació pugui arribar al coneixement de persones no autoritzades" –en paraules del preàmbul del Reial decret 3/2010– i s'aplica a sistemes, dades, comunicacions i serveis electrònics que gestionen les Administracions Públiques –o, si s'escau, operadors que prestin serveis o proveeixin solucions a les entitats públiques– en l'exercici de les seves competències o funcions.

El Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat - previst en l'article 156.2 de la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic-, estableix en el paràgraf tercer del seu article 2.3 que: *"Els plecs de prescripcions administratives o tècniques dels contractes que celebrin les entitats del sector públic incloses en l'àmbit d'aplicació d'aquest reial decret contemplaran tots aquells requisits necessaris per a assegurar la conformitat amb el ENS dels sistemes d'informació en els quals se sustentin els serveis prestats pels contractistes, com ara la presentació de les corresponents Declaracions o Certificacions de conformitat amb el ENS.*

D'acord amb l'article 202 de la LCSP, constitueix una condició especial d'execució del contracte el compliment de l'Esquema Nacional de Seguretat (ENS) en la categoria que resulti d'aplicació als sistemes d'informació afectats pels serveis objecte del contracte. L'empresa adjudicatària haurà d'acreditar, abans de la formalització del contracte i durant tota la seva vigència:

a) El compliment de l'ENS mitjançant la presentació d'un certificat vigent expedit per una entitat de certificació degudament acreditada. Els distintius de Conformitat hauran de ser exhibits pel contractista en el seu lloc web i hauran d'enllaçar amb les corresponents certificacions de Conformitat, que romandran sempre accessibles en el lloc web del contractista. A més, la "Fundació Privada de l'Hospital de la Santa creu i Sant Pau" podrà sol·licitar en tot moment al



contractista els corresponents informes d'autoavaluació o auditoria, a fi de verificar l'adequació i la idoneïtat de les certificacions, o bé

b) Mitjançant altres proves o evidències acceptades per l'òrgan de contractació que demostrin el compliment dels requisits de seguretat establerts per l'ENS en la categoria corresponent.

El manteniment del compliment de l'ENS durant tota la vigència del contracte tindrà la consideració d'obligació essencial, la inobservança de la qual podrà donar lloc a la imposició de penalitats i, si escau, a la resolució del contracte, d'acord amb el que es preveu al present Plec i a la LCSP.

2. Condició d'execució essencial: Partnership amb fabricants d'“Authorized/Expert Partner” de Fortinet.

Motivació: D'acord amb l'article 74.2 de la LCSP, els requisits de participació i condicions d'execució han d'estar vinculats a l'objecte del contracte i ser proporcionals al mateix. En el present cas, l'objecte contractual se centra en la renovació de subscripcions i en el manteniment de solucions de ciberseguretat d'un fabricant concret (Fortinet), la qual cosa fa necessari que l'empresa adjudicatària pugui actuar com a interlocutor autoritzat davant del fabricant per a l'obtenció de les llicències, dels serveis de suport i de les garanties oficials.

L'actual doctrina administrativa, ha reconegut la possibilitat d'exigir aquesta condició com a exigència vinculada a la correcta execució del contracte, especialment en contractes de manteniment de components o solucions d'una marca determinada, quan és necessari per mantenir garanties i accedir a recanvis o serveis de suport oficial.

En conseqüència, en un contracte de manteniment de components d'una marca concreta, és legítim exigir que l'adjudicatari sigui partner autoritzat del fabricant, atès pot ser necessari per mantenir garanties, obtenir recanvis, suport oficial, etc. En cap moment es planteja com una condició de solvència o habilitació empresarial, formulant-se de forma proporcional i respectuosa amb la lliure concurrència, així com s'admeten fórmules d'autorització equivalents que no exclouen operadores que puguin acreditar per altres vies la seva habilitació directa per subministrar i mantenir les solucions Fortinet objecte del contracte.

L'empresa adjudicatària haurà d'acreditar, abans de la formalització del contracte, que disposa de l'autorització necessària per part del fabricant Fortinet per subministrar les subscripcions i prestar els serveis de manteniment i suport oficial de les solucions de ciberseguretat objecte del contracte, mitjançant la possessió d'un nivell de partenariat amb el fabricant o equivalent que garanteixi l'accés al suport tècnic i a les actualitzacions de producte. En el cas que no s'acrediti dins d'aquest termini, es considerarà que el licitador ha incorregut en causa de resolució de l'adjudicació amb les conseqüències previstes a la LCSP.

S'acreditarà de la següent forma:

- La condició de Fortinet Expert Partner dins del programa oficial de partners de Fortinet,
- o bé la condició d'un altre nivell de partnership de Fortinet que, d'acord amb la documentació oficial del fabricant, habiliti per a la venda i manteniment de les solucions objecte del contracte,



- o bé un document d'autorització expressa emès per Fortinet on es reconegui l'empresa adjudicatària com a entitat autoritzada per subministrar i mantenir les solucions i serveis objecte del contracte.

Aquesta exigència tindrà la condició de condició especial d'execució, d'acord amb l'article 202 de la LCSP. La manca d'acreditació dins del termini atorgat per l'òrgan de contractació podrà donar lloc a la no formalització del contracte per causa imputable a l'adjudicatari, amb les conseqüències previstes a la LCSP, així com, si escau, a la resolució del contracte i a la imposició de penalitats.

- **Consideracions de tipus econòmic:**

- o Els pagaments de les subscripcions es farà en el moment de la seva adquisició.
- o Els pagaments s'efectuen mitjançant transferència bancària.

- **Causes d'exclusió derivades de l'avaluació de les ofertes:**

- o No es valoraran les propostes dels licitadors i, per tant, s'exclouran del procediment, si es dona algun dels supòsits següents:
 - Quan el/s preu/s ofert/s pel/s licitador/s supera/en el/s preu/s màxim/s establert/s.
 - Quan l'objecte de la valoració no compleixi els requeriments mínims establerts en el Plec de prescripcions tècniques (PPT).

Barcelona, a 7 de gener de 2026.

Sr. Jordi Grau Hernández
Director de Sistemes d'Informació
de la Fundació Privada de l'Hospital
de la Santa Creu i Sant Pau

"NOTA 1: Aquest document s'incorpora per duplicat a l'expedient de contractació, d'una banda s'incorpora el document signat per la persona competent i, d'altra banda en atenció al que es disposa a l'article 5.1.c del Reglament General de Protecció de Dades, el document anonimitzat per tal que amb la seva publicació no es vulneri el dret a la protecció de les dades de caràcter personal que hi pugui contenir".

NOTA 2: A tots els efectes, es considera que la data d'aquest document és la que figura al final del mateix.

NOTA 3: Amb la signatura del present document, el/s la sotasignat/s declara/en que no existeix conflicte d'interès en la pròpia actuació professional. Així mateix, declara que coneix les seves obligacions, segons consta el Codi de Bon govern aprovat per la Fundació Privada de l'Hospital de la Santa Creu i Sant Pau.