PLEC DE PRESCRIPCIONS TÈCNIQUES DEL SUBMINISTRAMENT D'EQUIPS TALLAFOCS PER A LA XARXA INFORMÀTICA DE LA UNIVERSITAT DE BARCELONA (UB).

EXPEDIENT 2023/149

1 INTRODUCCIÓ

La solució tecnològica de seguretat actual de la Universitat de Barcelona (UB), pel que fa a equips tallafocs de nova generació (NGFW), està composta per diversos elements, físics i virtuals, del fabricant Palo Alto i gestionats centralitzadament amb la plataforma Panorama del mateix fabricant.

Aquests equips formen parelles configurades com a clúster, actiu-actiu o actiu-passiu depenent de les seves funcionalitats i àmbit de protecció (perimetral, CPD, entorns dedicats, etc.).

La UB vol renovar un d'aquests clústers, ja que properament quedarà sense suport per part del fabricant per considerar-se equips obsolets. El nous tallafocs hauran de reemplaçar els actuals i hauran d'assegurar la seva compatibilitat total amb els altres elements de la infraestructura pel que fa a la seva funcionalitat, gestió i monitorització.

En aquest plec es demana:

- 2 equips tallafocs idèntics que funcionaran com a una parella en alta disponibilitat.
- Transceptors òptics necessaris. (En funció de les primeres reunions d'inici i anàlisi del projecte amb l'adjudicatari es ratificarà el número exacte de transceptors a demanar. Al plec s'especifica el màxim que podrien ser necessaris.)
- Garanties del fabricant pels períodes definits.
- Llicenciament per les funcionalitats demanades pels equips durant els períodes definits.
- Serveis per a la substitució, claus en ma, segons s'especifica a aquest plec tècnic.

2 REQUISITS GENERALS

Els equips han de poder reconèixer i controlar totes les aplicacions (nivell 7 pila TCP) sobre qualsevol port TCP/UDP, tant per a IPv4 com a IPv6, de manera nativa, sense llicències ni mòduls addicionals que puguin impactar en el seu rendiment.

Els perfils de seguretat i filtratge han d'incloure totes les firmes o mecanismes actius sense degradació del rendiment pel nombre de firmes actives.

Les característiques funcionals que han de complir els equips objecte de la licitació són:

- Suport d'alta disponibilitat, tant actiu/passiu com actiu/actiu.

- Amb l'objectiu de poder garantir que una sobrecàrrega del maquinari destinat a donar el servei (tràfic de xarxa), no afecti la gestió d'aquest, els equips han de disposar de maquinari independent de gestió integrat a l'equip, fins i tot sistema operatiu diferent amb l'objectiu d'independitzar totalment els plànols de gestió i xarxa.
- Port de gestió dedicat fora de banda.
- Es necessiten ports específics de gestió d'alta disponibilitat dedicats a fi de garantir que no consumeixin interfícies de servei per a aquesta tasca
- Els equips han de poder ser completament gestionats tant des d'entorn web com des d'entorn CLI
- Suport per a sistemes virtuals per tal de crear entorns completament diferenciats
- Desplegaments de xarxa en mode sniffing (fora de línia, rebent un mirror del tràfic), cable (transparent), capa 2 i capa3 (routing). S'han de poder barrejar diferents tipus de topologies d'interfícies de xarxa simultàniament sobre el mateix equip.
- Suport de l'estàndard IEEE 802.1Q (encapsulat de diverses vlans sobre el mateix enllaç físic) i IEEE 802.3ad (agregació de diversos enllaços físics).
- Suport a Jumbo Frames (MTU 9192 bytes).
- Suport d'IPv6 tant en mode nivell 3 com en mode transparent.
- L'equip ha de suportar les següents característiques de VPN (Virtual Private Network) :
    - Suport a VPNs sobre IPSec (Internet Protocol Security).
    - Suport a VPNs sobre SSL (Secure Socket Layer).
    - Suport a x-auth a SSL-VPNs per a integració amb clients de tercers.
- Gestió d'esdeveniments dels equips mitjançant:
    - Enviament de logs a tercers sistemes via syslog.
    - Gestió via SNMP.
- Suport de protocols d'encaminament (routing):
    - Protocols dinàmics de routing: RIP, OSPF i BGP
    - Suport de routing per a tràfic multicast (PIM Sparse Mode)
    - Suport de Policy Routing.
- Suport de RBAC (Role Based Access Control - Perfils per a gestió diferenciada i gestió delegada).
- Capacitat de realitzar tasques de NAT i PAT, inclòs NAT transparent.
- Suport de HTTP2, sense cap configuració addicional. (Aquesta millora permet protegir els servidors web que presten serveis sobre HTTP/2 i permet beneficiar els usuaris de la velocitat i l'eficiència de consum de recursos d'aquest protocol).
- Capacitat de generació de certificats digitals, així com de importació de certificats emesos per tercers.
- Suport a OCSP (Online Certificate Status Protocol) i llistes de revocació de certificats (CRL).
- Suport a la integració amb mòduls HSM de tercers per emmagatzemar les claus criptogràfiques.
- Permetre aplicar QoS per aplicació, usuari o URL. Establiment d'amplada de banda màxima i garantida. (L'activació d'aquesta funcionalitat no ha de minvar la resta de capacitats exigides a la solució, ni en funcionalitat ni en rendiment).

2.1 Requisits de maquinari dels Tallafocs

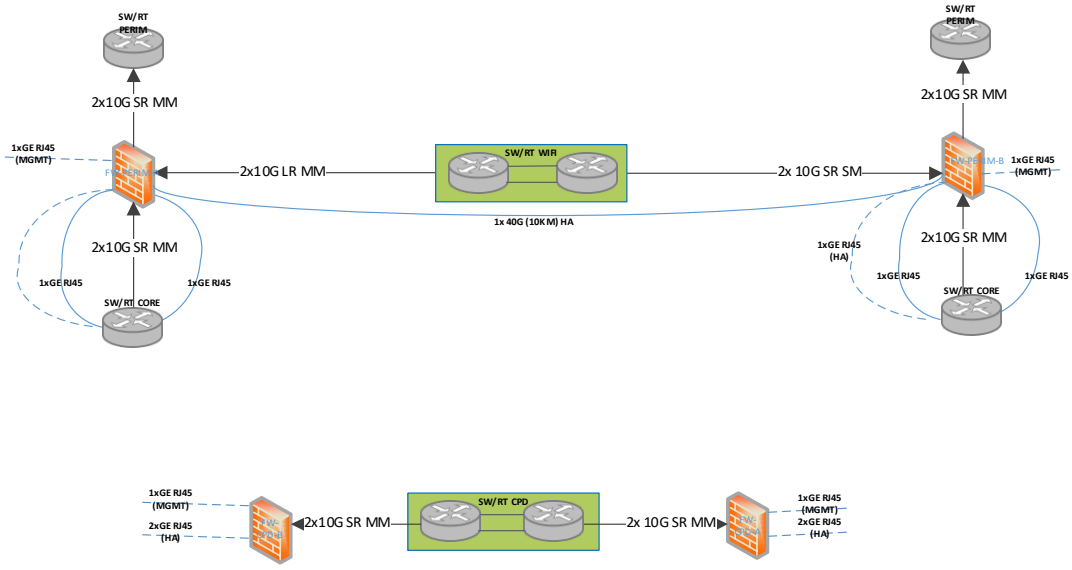
La proposta haurà d'incloure dos equips en format appliance, de les mateixes característiques, i que treballaran en alta disponibilitat (HA). Les característiques de capacitat mínima que ha de complir cadascun dels dos equips objecte de la licitació són:

- 8 ports Ethernet Coure 100/1000/10G.
- 12 ports 1G/10G SFP/SFP+.
- 4 ports 25G SFP28
- 4 ports 40G/100G QSFP+/QSFP28
- Disc dur redundat SSD per a Sistema Operatiu (Mínim 480GB)
- Port dedicat per a gestió fora de banda.
- Ports dedicats per a Alta Disponibilitat.
- Port de consola RJ45.
- Fonts d'alimentació redundants.

2.2 Transceptors òptics

La proposta haurà d'incloure transceptors òptics propis del fabricant de tallafocs proposat, indicats també amb el seu preu unitari, ja què és desig de UB el reaprofitar tots els transceptors actualment en us que es puguin. Per això, la compra exacta del número de transceptors es definirà entre UB i l'adjudicatari en funció de les primeres reunions d'inici i anàlisi del projecte, on es ratificarà el número exacte a demanar. Al plec s'especifica el número màxim* que podrien ser necessaris, i es vol el preu unitari per a realitzar la compra i pagament dels que s'acordin, que seran com a màxim els oferts i requerits al plec:

- 14 transceptors 10G FO SR MM
- 2 transceptors 10G FO LR SM



**Aquests números són els que UB ha extret de l'anàlisi dels ports actuals en us:*

FW-Perimetrals, entre els 2 equips ja existents, tenen tots aquests transceptors:

Servei en A:
Total 4 ports 10G FO SR MM
Total 2 ports 10G FO LR SM
Total 2 ports 1G RJ45
Servei en B:
Total 6 ports 10G FO SR MM
Total 2 ports 1G RJ45
Ambdós FW:
Un link 40G entre els dos per HA
HA1 dedicat = ja es GE RJ45
Mgmt dedicat = ja es GE RJ45

FW-CPD, entre els 2 equips ja existents, tenen tots aquests transceptors:

Servei en A:
Total 4 ports 10G FO SR MM
Ambos FW:
HA1 + HA2 + MGMT dedicats = ja són GE RJ45

2.3 Requisits de Capacitat i Rendiment

REQUERIMENTS	VALOR MÍNIM
Throughput (tassa de transferència efectiva) amb inspecció a nivell 7, identificació d'aplicacions y logging activat utilitzant paquets de 64 KB amb tràfic mixt.	56,0 Gbps

Throughput activant la prevenció d'amenaces i tots els serveis següents (Control d'aplicaciones, IPS, Antivirus conegut, Antispyware, AntiMalware desconegut (SandBoxing), logging activat fent servir paquets de 64 KB amb tràfic mixt, control d'URL, seguretat DNS, i File blocking)	32,0 Gbps
IPSEC VPN throughput	28,7 Gbps
Capacitat total de sessions	5.000.000
Noves sessions per segon	370.000
Sistemes virtuals	15, ampliable a 65 amb llicència

2.4 Requisits de Seguretat

Respecte de les funcionalitats de seguretat, aquestes s'han de poder activar de manera concurrent en tots els sistemes de seguretat tant virtuals com físics. Per tant, els equips han d'incorporar les llicències actives adequades.

2.4.1 Visibilitat i control d'aplicacions

- El motor de classificació que s'utilitzarà per identificar el tràfic de dades serà segons l'aplicació (nivell 7 de la pila TCP), i no només el port. Així, doncs, l'aplicació no ha de formar part d'un filtre que s'apliqui posteriorment, sinó que ha de ser l'element d'identificació inicial i basar la resta de l'anàlisi en el seu context.
- Capacitat per identificar i controlar, de manera nativa, sense llicències ni mòduls addicionals que puguin impactar en el rendiment, un mínim de 2.000 aplicacions actives actuals (com ara Sharepoint, Whatsapp, Facebook, Spotify, SAP, Oracle, Skype, etc.).
- Reconeixement i filtratge de qualsevol aplicació sobre qualsevol port TCP/UDP, i no només sobre els ports estàndard.
- Possibilitat de crear signatures personalitzades per a la identificació d'aplicacions propietàries.
- Utilització d'una política de seguretat unificada, que contempli les aplicacions com a part integral de la mateixa.

- Reconeixement i control de les subfuncions dins d'una aplicació, com ara transferències de fitxers, correu electrònic, xat, etc.
- Identificar, classificar i gestionar sistemàticament el tràfic desconegut. La solució ha de ser capaç d'identificar el tràfic desconegut, categoritzar-lo pel seu anàlisi i gestionar-lo en base a polítiques. A més, ha de ser possible prendre captures (PCAPs) automàticament del tràfic desconegut, així com generar firmes personalitzades per identificar-lo en cas que sigui tràfic desitjat.

2.4.2 Integració i identificació d'usuaris

- Identificació d'usuaris de forma transparent mitjançant la integració amb directoris LDAP inclòs l'Active Directory de Microsoft.
- Capacitat d'identificar i confirmar usuaris en entorns Microsoft mitjançant l'ús del Windows Management Instrumentation (WMI).
- API XML per a la identificació d'usuaris, que permetrà injectar usuaris apresos des d'altres sistemes, facilitant així la integració amb altres mecanismes d'autenticació via scripting (com ara sistemes 802.1x, Radius, …).
- El Sistema de Seguretat integrarà un recol·lector de syslog (tant TCP com UDP) per poder aprendre usuaris que han estat validats en altres sistemes d'autenticació.
- Serveis d'autenticació basada en LDAP (incloent-hi NTLM), Kerberos (inclòs Single Sign On), Radius i base de dades local al Sistema de Seguretat per als accessos VPN i per a l'accés a aplicacions.
- Capacitat per crear grups dinàmics els membres dels quals s'actualitzin mitjançant una API XML.

2.4.3 Protecció davant d'atacs de denegació de servei

- Reconeixement i prevenció d'escaneigs de xarxa.
- Detecció i mitigació d'atacs de DoS. S'haurà de comptar almenys amb els següents tipus de protecció: SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, protecció davant inundacions per noves sessions, o protecció per atacs de desbordament per límits de sessions establertes, sent capaç d'establir, en cada cas, els llindars necessaris per activar aquestes proteccions.

2.4.4 Protecció davant de vulnerabilitats

Quant a protecció davant de vulnerabilitats, el tallafocs ofert haurà de comptar amb la possibilitat d'aplicar polítiques de protecció davant de vulnerabilitats i exploits tant al tràfic entrant com al sortint, havent de complir amb les següents funcionalitats:

- S'han de poder aplicar polítiques tant de detecció com de prevenció (mode IDS o IPS) davant de possibles exploits de vulnerabilitats que es detectin en el tràfic entrant o sortint d'Internet efectuant l'anàlisi en una única passada per a tot tipus d'amenaces.
- En la protecció davant de vulnerabilitats el criteri a utilitzar és la identificació de l'aplicació per poder aplicar perfils de vulnerabilitats ajustats a aquesta aplicació, de manera que no es vegi afectat el rendiment de l'equip.
- Els perfils de detecció i protecció davant de vulnerabilitats han de permetre ser aplicats tant per al tràfic originat des de la xarxa interna com per al tràfic originat des d'Internet, havent de ser possible l'aplicació de detecció i protecció davant de vulnerabilitats especificant si són vulnerabilitats que apliquen als clients , els servidors o tots dos indistintament.
- Les vulnerabilitats han d'estar categoritzades per tipus i per nivells de risc, de manera que l'aplicació de perfils de protecció al tràfic es pugui fer sobre la base d'aquestes categories.
- S'ha de poder permetre utilitzar la identificació CVE de vulnerabilitats per poder utilitzar aquesta identificació a l'aplicació de perfils de protecció específics.
- Utilització de la identificació d'aplicacions com a criteri per seleccionar els perfils de protecció de vulnerabilitats, de manera que només s'apliquin aquelles firmes específiques segons l'aplicació que s'està utilitzant.

2.4.5 Antivirus

El tallafoc proposat ha de tenir la capacitat de definir polítiques d'antivirus, de manera que les descàrregues de fitxers realitzades en sentit Internet xarxa Interna o viceversa siguin inspeccionades i bloquejades si el contingut és maliciós.

- S'han de poder aplicar polítiques que permetin aplicar el motor d'antivirus sobre protocols com ftp, http, imap, pop3, smb o smtp, definint per a cadascun d'aquests protocols l'acció a realitzar (permetre els fitxers, descartar els fitxers, desconnectar la sessió o registrar mitjançant logs) davant la detecció del fitxer maliciós pel motor d'antivirus.
- El tallafoc ha de permetre l'aplicació de polítiques d'antivirus de forma granular, permetent, per exemple, l'aplicació d'aquestes polítiques a certs usuaris de determinats grups, a certs segments de xarxa amb encaminament determinat o a certes aplicacions.
- El mòdul d'antimalware haurà de disposar d'un motor d'anàlisi estàtic basat en algorismes de Machine Learning que permetin identificar mostres malicioses

desconegudes en temps real sense haver d'esperar el veredicte del mòdul de Sandboxing.

2.4.6 Filtratge d'URLs

- Els equips han de suportar la creació de categories d'URL i la inspecció o no del trànsit xifrat SSL segons aquestes categories. Desxifrat de trànsit SSL i SSH sobre qualsevol port. Capacitat per identificar les aplicacions reals dins dels túnels SSL. Ha de tenir la possibilitat de bloquejar les sessions SSL que no poden ser desxifrades o aquelles amb certificats de servidor no fiables.
    - Valoració extra subjectiva:
        - Suport de desxifrat de trànsit TLS1.3 i HTTP/2, incloent un log dedicat per a aquest trànsit.
        - El desxifrat SSL haurà de fer-se en maquinari/asics dedicat específicament per a això.
- Possibilitat de detectar l'enviament de credencials corporatives (usuaris i contrasenyes de la xarxa corporativa) cap a les webs que es visiten, de manera que es pugui advertir, bloquejar o permetre aquest enviament de credencials en funció de les categories de web visitades.
- Capacitat de fer filtratge per URL o per categoria d'URL. S'oferirà un sistema de filtratge que inclogui la categorització d'URLs per part del fabricant, així com la seva actualització automàtica. Així mateix, s'inclourà un mecanisme per poder sol·licitar canvis en la categorització de les URLs.

2.4.7 Bloqueig de fitxers i dades sensibles

- Cal que els tallafocs tinguin, de manera nativa, capacitat de controlar quin tipus de fitxers circulen per la xarxa, inclosos els fitxers comprimits. La solució ha de diferenciar entre upload/download.

2.4.8 Sandboxing

Capacitat de detecció de codi maliciós desconegut en base a tecnologia de sandboxing al núvol.

- El sistema d'anàlisi d'amenaces al núvol ha d'estar ubicat a la Unió Europea, i que pugui acreditar el compliment de les normatives Europees en matèria de protecció de dades.
- El sistema de detecció del núvol ha d'executar el fitxer que ha estat enviat utilitzant una sandbox virtual per determinar qualsevol comportament maliciós. El sistema ha de

ser capaç de generar signatures automàticament en base a l'activitat observada i distribuir-les als tallafocs.

- L'administrador del Sistema de Seguretat ha de ser capaç d'accedir a aquesta sandbox per veure l'estat dels fitxers inspeccionats, així com també pujar-hi fitxers de manera manual.
- Cal inspeccionar almenys fitxers EXE, DLL, PDF, APK, Java, Office de Microsoft, Mach-O i DMG d'OS-X.

2.4.9 Seguretat DNS

Capacitat per detectar i prevenir de manera automàtica i dinàmica les peticions de DNS malicioses associades amb dominis de codi maliciós (malware), a les quals el tallafocs ha de respondre automàticament amb una IP falsa en lloc del servidor autoritatiu (DNS sinkholing). La base de dades de dominis maliciosos ha de ser nodrida per les fonts següents:

- Sistema de sandbox per trobar nous dominis C2
- DNS passius i telemetries
- Fast-flux domains
    - Prevenció d'amenaces de DNS en l'ús de servidors intermediaris de Botnets basats en DNS
- Dictionary DGA
    - Detecció i prevenció d'atacs basats en dominis maliciosos que usen paraules conegudes
- Ultra-slow DNS tunneling
    - Detecció i prevenció de túnels C2 basats en DNS amb moviment lent
- Dangling DNS attacks
    - Detecció i prevenció d'amenaces en atacs basats en dominis DNS oblidats
- NRD Maliciós
    - Detecció d'atacs basats en l'ús de dominis DNS de nova creació

2.5 Requisits de Gestió i Administració

Els requeriments de gestió de l'equip són:

- Tant les capacitats de gestió, administració, gestió de logs i informes, han de ser components nadius al tallafocs, sense necessitat d'adquirir altres elements maquinari o programari per disposar d'aquestes funcionalitats
- Auditoria de configuracions, incloent la cerca de diferències entre diferents fitxers de configuració.
- La solució de gestió ha de ser capaç de correlar automàticament esdeveniments disjunts que, quan s'uneixen al llarg d'un període de temps per a un mateix equip o usuari, indiquen que aquest equip ha estat probablement compromès. Per exemple,

una vulnerabilitat des d'un exploit kit, juntament amb un accés posterior a un domini maliciós que acaba finalment amb una descàrrega de codi maliciós (malware) ha de generar un esdeveniment correlat indicant compromís, a més dels tres esdeveniments individuals.

- La solució ha de suportar informes totalment personalitzats per a tots els logs sobre el propi equip (sense necessitat per tant utilitzar un equip secundari per a aquestes tasques). A més, ha de ser possible extreure tant els informes predefinits com els personalitzats mitjançant una API XML, que permetrà la integració amb sistemes externs.
- La solució serà capaç de realitzar de manera automàtica una anàlisi de comportament diari, en base a tots els logs, a la recerca d'equips que puguin formar part de botnets desconegudes. El resultat serà un informe que inclourà totes les màquines susceptibles d'haver estat reclutades per botnets noves, així com els comportaments que han tingut pels quals se les considera infectades.
- Disponibilitat de mapa geogràfic per identificar l'origen i la destinació dels fluxos i amenaces que entren i surten de la xarxa.
- Capacitat per consumir indicadors de compromís de tercers i incorporar-los automàticament als tallafocs. Cal consumir almenys llistes d'IPs, URLs i DNS.
- Actualitzacions automàtiques, programables, per a les firmes d'Aplicació, IPS, Antivirus i AntiSpyware. Cal llicència corresponent a la prevenció d'amenaces.

2.6 Altres requeriments

- Es requereix que el fabricant proposat, figuri a l'apartat de líders del quadrant màgic de gartner d'Enterprise Firewalls, durant els darrers 10 anys.
- El fabricant ha de tenir publicades les guies de configuració recomanades del Centre Criptològic de Seguretat, CCN-STIC.
- El producte ofert ha d'aparèixer al Catàleg de Productes de Seguretat TIC, CPSTIC, recomanats pel Centre Criptològic Nacional.
- La solució proposada haurà de disposar de mecanismes que, injectin als tallafocs de manera automàtica, llistes dinàmiques provinents de bases de dades de tercers (per exemple serveis anti phishing, llistes de dominis maliciosos, serveis antispam, serveis d'identificació de nodes TOR, avisos de CERTs etc). Aquestes fonts hauran de ser rebudes de manera automàtica, processades i injectades als tallafocs a través de STIX, TAXI, JSON, llistes dinàmiques, etc. sense intervenció humana.

3 SERVEIS DE DIRECCIÓ i EXCUCIÓ DEL PROJECTE

El projecte és claus en mà, per tant, l'adjudicatari haurà de proporcionar tots els recursos de personal i petits materials necessaris per a la seva execució.

- El dimensionament de l'equip de treball ha de ser el necessari per complir amb les tasques demanades en aquest plec.
- L'equip de treball ha d'estar configurat per persones amb coneixements i experiència suficient per garantir l'execució i la qualitat de les tasques contractades.
- Es requereix que o bé el cap de projecte o algun membre de l'equip de treball acrediti titulació Cisco CCIE Enterprise Infraestructure activa.
- Tots els perfils tindran la formació i el bagatge necessari per executar la seva funció.
- Per cada un dels membres de l'equip de treball ha de poder acreditar-se el nivell de coneixements y experiència adequats a les funcions que realitza.

3.1 Tasques a realitzar

La instal·lació / substitució / migració dels tallafocs es realitzarà en dues fases:

- Fase1: substitució dels actuals tallafocs perimetrals PaloAlto que estan en un punt entremig del seu període de vida, pels nous tallafocs objecte d'aquest projecte. Es fa això per què és l'entorn perimetral el que més rendiment i funcionalitats requereix. Aquest entorn es mantindrà en el model actual Actiu-Actiu, i es mantindrà la ubicació dels tallafocs.

- Fase2: amb els anteriors equips tallafocs PaloAlto que feien el servei de control perimetral, farem la substitució dels actuals tallafocs de CPD PaloAlto, que estan arribant al seu final de vida. Aquest entorn es mantindrà en el model actual Actiu-Passiu, i es podria redefinir la ubicació dels tallafocs, sempre mantenint-los dintre dels racks del CPD a Pavelló Rosa.

Per a ambdues fases, és desig de la UB el realitzar el canvi amb les màximes garanties d'èxit i el mínim impacte als serveis. Els canvis amb afectació es realitzaran en horari nocturn o en l'horari més convenient per a la UB. Es vol pre-instal·lar tots els equipaments que després substituiran els actuals en paral·lel, i garantir prèviament al canvi que l'element nou ja ha estat correctament integrat per l'adjudicatari en les plataformes de gestió de UB (Centreon, Panorama).

Caldrà documentar els canvis i facilitar tota la documentació pròpia del projecte.

4 GARANTIES DE FABRICANT

Per tots els equips es obligatori que l'adjudicatari subcontracti al fabricant dels mateixos les corresponents "garanties hardware i software de fabricant" en règim 24x7x4 per un període mínim de 4 anys. Aquestes garanties, així com les llicències necessàries, s'activaran a partir de la posada en producció del projecte.

Els licitadors hauran d'incloure, dins de les seves propostes tècniques, una/es carta/es del fabricant/s garantint que poden contractar aquestes garanties. La no presentació d'aquest documents, o la seva presentació amb posterioritat a l'obertura del sobre amb la documentació tècnica, serà motiu d'exclusió de la licitació.

Els contractes de garantia amb el fabricant seran gestionats per l'adjudicatari però aniran a nom de la Universitat de Barcelona que, entre d'altres, podrà obrir, directament o a través de tercers, casos il·limitats al fabricant i fer seguiment dels mateixos.

Important

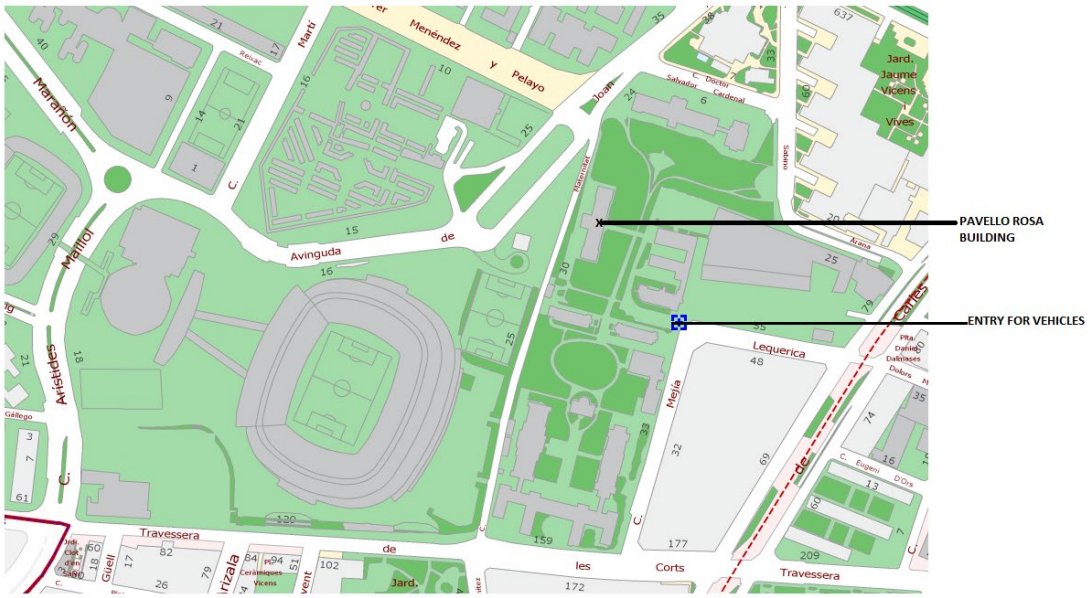
L'adjudicatari haurà d'acreditar i demostrar davant la UB, abans de 30 dies naturals des de la data de signatura del contracte, que ha realitzat les corresponents contractacions amb els fabricants.

Cas que aquesta certificació no s'hagi fet durant aquest període, la UB es reserva el dret a adquirir les garanties de fabricant pel seu compte. La UB, si és el cas, comunicarà a l'adjudicatari que procedeix a tramitar aquesta contractació l'import total de la qual, més un 20% de penalització, serà descomptat de l'import total d'adjudicació de la present licitació.

ANNEX I : LLIURAMENT DEL MATERIAL

El subministrament de tot el material es realitzarà a la següent adreça:

Àrea de Tecnologies de la Informació i la Comunicació de la Universitat de Barcelona
Pavelló Rosa (Recinte de la Maternitat)
Travessera de les Corts 131-159
08028 Barcelona



Es mostra la ubicació del Pavelló Rosa dins del recinte de la Maternitat.
L'entrada de vehicles per a càrrega i descàrrega és al carrer Mejía Lequerica nº 1-33



Per accedir a la planta baixa del Pavelló Rosa cal pujar 9 esglaons tal com es pot veure a la fotografia. No existeix muntacàrregues.

A la planta baixa hi ha un ascensor de càrrega màxima 300 kg que porta al soterrani, amb una porta d'accés de 69 cm d'amplada i 196 cm d'alçada. Les mides interiors de la cabina són 84 cm de fondària per 100 cm d'amplada. Des de la sortida de l'ascensor al soterrani fins a arribar al magatzem hi ha 30 metres en pla.

L'adjudicatari contractarà els mitjans necessaris per lliurar tot l'equipament demanat als magatzems de l'Àrea de Tecnologies situats al soterrani.

Barcelona,

Montserrat Bachs Castaño
Directora Àrea de Tecnologies de la
Informació i la Comunicació