COORDINACIÓ SERVEIS DIGITALS
XG/mc

Exp. 902082 / 2025

PLEC DE PRESCRIPCIONS TÈCNIQUES

1. OBJECTE.

L'objecte del contracte es la subscripció d'un producte de ciberseguretat sobre el tràfic de xarxa informàtica, NDR, basat en intel·ligència artificial per a la monitorització, detecció, anàlisi i resposta en temps real a incidents de seguretat, així com dels serveis de suport SOC associats.

2. Requeriments tècnics.

2.1. Descripció del sistema.

El sistema de ciberseguretat haurà d'utilitzar tecnologies avançades d'intel·ligència artificial per desenvolupar les seves funcionalitats basant-se en el trànsit que circula per les xarxes informàtiques de l'ÀMB. Aquest sistema ha de proporcionar, en temps real, una visió exhaustiva i contínua de l'estat de la seguretat de la xarxa, identificant i responent a amenaces automàticament, garantint així la integritat i la confidencialitat de les dades corporatives.

El sistema requerit haurà de ser capaç d'integrar-se completament amb la infraestructura tecnològica existent de l'ÀMB, incloent-hi, però no limitant-se a, la xarxa LAN, connexions Wi-Fi, xarxes privades virtuals (VPN) i zones desmilitaritzades (DMZ). A més, ha de tenir la capacitat de monitoritzar i gestionar el trànsit de xarxa tant intern (Est-Oest) com extern (Nord-Sud) en els dos Centres de Processament de Dades (CPDs) de l'ÀMB, així com el trànsit entre tots els centres de treball.

La solució oferta haurà d'estar alineada amb els estàndards de seguretat vigents i d'acord amb les mesures i millors pràctiques de la indústria, assegurant la conformitat amb:

- ISO 27001 - Certificació de Seguretat de la Informació o equivalent.
- ISO 27018 - Protecció d'Informació Personal al Núvol o equivalent.

2.2. Objectius estratègics i operatius

L'objectiu de la implantació d'aquest sistema és enfortir la postura de seguretat de l'ÀMB, permetent anticipar-se i aturar les amenaces de ciberseguretat, facilitar una operativa més flexible durant una anàlisi d'un incident i una millor capacitat de resposta davant la varietat i sofisticació d'amenaces cibernètiques emergents. A més, es busca complir amb els més alts estàndards de protecció de dades i regulacions de ciberseguretat tant nacionals com internacionals.

El sistema ha de basar-se en l'aprenentatge continu a partir del comportament dels fluxos d'informació a la xarxa així com a partir de dades de ciberintel·ligència procedents d'una àmplia xarxa global d'amenaces.

2.3. Cobertura i funcionalitats

El sistema proporcionarà la cobertura integral de l'anàlisi del trànsit de xarxa per a un mínim de 2500 dispositius connectats, incloent almenys 1200 estacions de treball, 250 servidors, 800 dispositius mòbils i altres equips a la xarxa. Serà imprescindible que el sistema tingui la capacitat d'escalat per suportar increments significatius futurs en el nombre de dispositius sense degradar el seu rendiment.

El sistema sol·licitat ha de funcionar de manera proactiva i autònoma. Ha d'incloure algorismes d'autoaprenentatge i tècniques d'IA per realitzar anàlisis detallats del trànsit de xarxa, detectant no només amenaces conegudes a través de signatures i comportaments maliciosos predefinits, sinó també anàlisis dels metadades que ha d'extreure dels paquets de xarxa en circulació. Detectarà comportaments de trànsit anòmal, inesperat i inhabitual, així com la detecció, resposta i anàlisi davant amenaces emergents com ara atacs *zero-day* o anomalies en temps real.

La solució ha d'incloure el subministrament i instal·lació de maquinari i programari, la configuració i posada en marxa del sistema, i el suport i manteniment continu durant la vigència del contracte. A més, la solució requerida inclourà la formació del personal tècnic de l'ÀMB per a l'ús i gestió autònoma del sistema.

2.4. Capacitats de la plataforma

2.4.1. especificacions físiques

Els appliances es connectaran als equips de comunicacions de la xarxa informàtica de l'ÀMB de manera que tinguin visibilitat de tots els segments d'aquesta. La connexió es farà en alta disponibilitat i no representarà ni un coll d'ampolla ni un punt de fallida únic. En cap cas el tràfic existent es veurà limitat o alentit per la monitorització. Aquesta connectivitat haurà de permetre la ingesta de tràfic provenint d'enllaços funcionant, com a mínim, a 40Gbps amb un pic sostingut de 5Gbps. Igualment, els equips que actuïn com a *master* suportaran un mínim de 200.000 connexions per minut (CPM) i analitzaran un mínim de 500.000 esdeveniments per minut (EPM).

Els dispositius disposaran de redundància en tots els elements físics que ho permetin, com ara emmagatzematge local, connectivitat de xarxa o fonts d'alimentació. També hauran de redundar-se entre ells, de manera que en cas de fallida d'un dels appliances, l'altre assumeixi la seva càrrega sense pèrdues apreciables de rendiment.

Els dispositius disposaran d'una interfície de gestió separada que es connectarà als segments d'administració de seguretat de la xarxa de l'ÀMB.

2.4.2. Característiques i funcionalitats

El contracte objecte d'aquest plec inclou el subministrament d'un sistema de detecció i resposta a incidents de ciberseguretat basat en l'anàlisi del trànsit de xarxa amb intel·ligència artificial que disposi de capacitat d'autoaprenentatge i autogestió. Aquest sistema garantirà una monitorització exhaustiva, anàlisi avançat i resposta immediata davant amenaces, operant localment sense la necessitat de transferència externa de dades per a la seva funcionalitat.

Es requereix el subministrament de totes les llicències d'ús del sistema que cobreixin un mínim de 2500 dispositius IP per a totes les funcionalitats sol·licitades en el plec. Aquestes estaran incloses durant tota la durada del contracte a partir de la data de signatura de l'acta de recepció del sistema. Es prendrà aquesta data com d'inici de validesa de les llicències i serveis de subscripció i suport.

El sistema de ciberseguretat objecte d'aquest contracte ha de complir amb una sèrie d'especificacions tècniques, detallades a continuació, que assegurin la seva capacitat per protegir eficaçment la infraestructura de xarxa de l'ÀMB contra una àmplia gamma d'amenaces cibernètiques.

2.4.3. Gestió d'Incidents i Resposta

La gestió eficaç d'incidents és crucial per minimitzar l'impacte de les amenaces de seguretat en la infraestructura tecnològica de l'ÀMB. El sistema de ciberseguretat proposat ha d'incloure protocols de resposta a incidents ben definits i provats que permetin una resposta ràpida i coordinada a incidents de seguretat detectats. El sistema ha d'incloure:

- Anàlisi en Temps Real: El sistema ha de ser capaç d'analitzar el trànsit de xarxa en temps real, utilitzant tecnologies avançades d'intel·ligència artificial per detectar patrons anormals i possibles amenaces de forma instantània.
- Detecció i Alerta Primerenca: Implementació de sistemes de detecció que utilitzin tecnologia d'IA per identificar amenaces potencials en temps real i emetre alertes automàtiques als operadors.
- Avaluació i Classificació d'Incidents: Sistema per avaluar ràpidament la gravetat i l'impacte potencial d'un incident, classificant-lo segons la seva urgència i el tipus de resposta requerida.
- Contenció i Erradicació: El sistema proposarà estratègies per contenir un incident un cop detectat, minimitzant la seva propagació i eliminant l'amenaça de l'entorn de la xarxa. A més de proposar estratègies, el sistema ha de permetre una resposta automàtica i quirúrgica que permeti, per exemple, aïllar un sol equip/dispositiu o actuar sobre un grup d'ells si s'expandeix l'amenaça. Aquesta resposta també ha de poder executar-se de forma manual utilitzant la interfície de la solució proposada.
- Capacitats d'Anàlisi Forense: Eines que permetin realitzar anàlisis forenses detallades post-incident per determinar la causa arrel, els vectors d'atac, i els possibles punts d'entrada, amb la finalitat de reforçar els sistemes contra futurs atacs.
- Revisió i Aprenentatge Post-Incident: El sistema permetrà revisar i analitzar cada incident, ajustant els protocols, models de detecció i resposta així com altres defenses de seguretat en conseqüència de les lliçons apreses.

A més, el sistema proposat per l'adjudicatari haurà de proveir eines avançades i estratègies de gestió per donar suport a l'operativa contínua i la millora de la seguretat. Aquestes s'integraran amb els serveis SOC descrits més endavant.

- Eines de Gestió d'Incidents: Solucions de programari que facilitin la gestió integral d'incidents, des de la detecció fins a la resolució, incloent eines de ticketing, seguiment de l'estat i informes d'incidents.
- Automatització de Respostes: Implementació d'eines que permetin respostes automàtiques a incidents comuns o ben definits, reduint la càrrega sobre el personal humà i accelerant la resolució d'incidents.
- Integració amb Altres Plataformes de Seguretat: Capacitat d'integrar el sistema de gestió d'incidents amb altres plataformes de seguretat en ús a l'ÀMB, com MDR, sistemes de prevenció d'intrusions, tallafocs, *feeds* de ciberintel·ligència i solucions de detecció d'anomalies, per a una resposta més coordinada i efectiva.

2.4.3.1. Anàlisi de Trànsit en Temps Real

La solució ha de poder desplegar-se mitjançant l'ús combinat d'appliances físics i sondes virtuals instal·lats en els hosts de virtualització de manera que el desplegament tingui visibilitat completa de trànsit lateral a més de trànsit nord-sud.

En qualsevol cas, els appliances físics i sondes virtuals no han de requerir de forma obligatòria una connexió a internet o connexió amb la infraestructura del fabricant per dur a terme el seu anàlisi i acció autònoma. En tot moment, totes les dades de L'ÀMB han de romandre *on-premise* i en la infraestructura de xarxa i els CPDs. Qualsevol dada capturada i analitzada per la solució ha de ser encriptada tant en trànsit com en emmagatzematge.

El sistema a implantar ha d'estar dissenyat per dur a terme una captura i anàlisi exhaustiva del trànsit de xarxa en temps real mitjançant *port mirrors*, funcionant en les capes OSI 2 i 3. Per a això ha de ser capaç de processar una rèplica exacta del trànsit que travessa els *switch* o *routers* designats sense exercir càrrega addicional ni alterar el flux original de dades. L'anàlisi en temps real ha de proporcionar una visibilitat completa i una supervisió constant del trànsit, permetent detectar anomalies i possibles ciberamenaces a mesura que ocorren.

El sistema ha de ser capaç de tractar grans volums de dades de trànsit sense disminuir el seu rendiment ni l'eficiència de la xarxa. Per a això, s'utilitzaran tecnologies avançades de processament de dades que permetin l'anàlisi de paquets en brut (*raw packet data*) i l'extracció de metadades significatives, essencials per a la identificació de patrons sospitosos i per a la construcció d'un model de comportament de la xarxa que serveixi de base a l'aprenentatge automàtic de la IA.

A més, el sistema disposarà d'algoritmes intel·ligents capaços de realitzar una anàlisi tant basat en models d'IA com heurístic i estadístic de les dades capturades. Això inclou el reconeixement de signatures digitals que puguin correspondre a programari maliciós conegut, així com la detecció de patrons de comportament anòmal que puguin indicar la presència d'amenaces emergents o atacs *zero-day*. Aquest tipus

d'anàlisi ha de permetre al sistema no només reaccionar davant amenaces conegudes, sinó també anticipar i prevenir atacs desconeguts abans que puguin causar dany.

La infraestructura necessària per a l'anàlisi en temps real ha de ser robusta i escalable i permetre la integració i coordinació amb múltiples sondes i sensors que es distribuiran al llarg de la xarxa. Això és especialment important en un entorn divers com el de L'ÀMB, on s'ha de garantir la seguretat no només en la xarxa principal, sinó també en subxarxes, sistemes de Wi-Fi, connexions VPN i LAN, i altres punts d'accés que podrien ser vulnerables a intrusions.

El sistema proporcionarà a L'ÀMB la capacitat d'analitzar dades en brut exportant les dades en format .pcap així com realitzar cerques avançades en capçaleres de comunicació i captures de paquets des de la pròpia interfície de la solució, proporcionant una visió completa dels esdeveniments de seguretat.

2.4.3.2. Alertes en Temps Real

Per garantir una resposta ràpida i efectiva davant qualsevol incident, el sistema comptarà amb mecanismes d'alerta immediata que proporcionaran a l'equip de seguretat la informació rellevant sobre qualsevol esdeveniment sospitós. Aquestes alertes seran configurables i podran escalar-se segons la gravetat de l'incident, assegurant que l'equip de seguretat pugui prioritzar els seus esforços de manera efectiva.

2.4.3.3. Resposta Autònoma

El sistema proposat facilitarà a l'ÀMB la capacitat de resposta autònoma davant incidents en temps real, amb opcions d'actuació que vagin des del *spoofing* de xarxa fins a la creació d'ACL a través de tallafocs per interrompre comunicacions específiques.

La tecnologia ha de disposar d'una resposta autònoma que realitzi accions quirúrgiques contra atacs avançats de dia zero, moviments laterals, C2, i tot tipus d'activitat indicativa d'un possible atac. La solució ha de reaccionar en segons per aturar atacs ràpids i imprevisibles.

La decisió de prendre una acció o no s'ha d'originar des d'un context i autoaprenentatge de les comunicacions de l'ÀMB, aprofitant la IA en tot moment sense l'ús de regles, signatures i *playbooks*. La solució ha de poder determinar la millor acció que s'ha de realitzar en el menor temps possible per reaccionar eficaçment a un ciberatac, en qualsevol lloc i en qualsevol moment en què es produeixi. És important que la solució pugui realitzar aquestes accions de manera nativa sense la necessitat de cap integració amb tercers.

Per fer front a l'activitat maliciosa, el sistema ofert ha de realitzar accions autodirigides. El sistema ha d'estar preparat per transferir coneixements dels incidents a sistemes de seguretat existents de tercers com a mecanismo de resposta.

La tecnologia ha de proporcionar diferents modes de bloqueig en funció de la severitat de l'activitat observada. L'ÀMB i els seus equips de seguretat han de tenir l'opció de configurar modes de confirmació davant certa activitat mentre que deteccions més crítiques siguin en un mode autònom amb una resposta immediata.

Les funcionalitats de resposta i sistemes de bloqueig de la plataforma proposada han de poder-se executar en tot moment fins i tot sense cap connexió a internet des de la plataforma.

2.4.3.4. Capacitats d'Autoaprenentatge i Autogestió

Per a la detecció proactiva d'amenaces emergents, anomalies i comportaments sospitosos abans que es materialitzin en incidents de seguretat, el sistema ha d'implementar tecnologies d'Intel·ligència Artificial (IA) i *Machine Learning* per analitzar predicativament patrons de trànsit i comportaments d'usuaris i dispositius en temps real.

El sistema ha de tenir capacitat per no només detectar, sinó també respondre automàticament a incidents detectats mitjançant accions preconfigurades, com l'aïllament de dispositius compromesos o la modificació de regles de tallafocs, minimitzant així l'impacte potencial de les amenaces.

La solució s'adaptarà contínuament al perfil únic i canviant de l'entorn de TIC de l'ÀMB, mitjançant perfilat dinàmic de l'entorn, aprenent dels patrons normals de trànsit i comportament de dispositius per ajustar dinàmicament els llindars de detecció i resposta.

La solució permetrà la configuració de models de detecció i respostes a mida basats en les necessitats específiques de seguretat de l'ÀMB, facilitant una protecció més granular i ajustada als riscos i polítiques de l'organització.

El sistema implementarà automatització de processos i tasques de seguretat rutinàries, com actualitzacions de signatures i anàlisis de vulnerabilitats, alliberant recursos valuosos de l'equip de seguretat per a tasques més estratègiques.

El sistema ha de ser autoexplicatiu, intuïtiu i guiat per a l'operador, implementant algun tipus d'assistent virtual que el guiï durant el procés d'investigació i mostrant les evidències correlacionades que han determinat una alerta així com guiant l'operador sobre les vulnerabilitats aplicables i els següents passos a seguir.

El sistema rebrà i aplicarà actualitzacions de manera autònoma per assegurar la protecció contra les últimes amenaces sense requerir intervenció manual, garantint així una defensa sempre actualitzada. La solució ha de tenir capacitat per automatitzar respostes i tasques de seguretat rutinàries, com l'actualització de signatures de virus o IOCs, per millorar l'eficiència operativa.

A través de l'aprenentatge continu i la retroalimentació operativa, el sistema es perfeccionarà constantment, millorant la seva precisió i eficàcia en la detecció i resposta a amenaces.

2.4.3.5. Escalabilitat del Sistema

El sistema ha de ser dissenyat amb una arquitectura escalable que permeti a l'ÀMB adaptar-se als canvis en la seva infraestructura tecnològica i respondre a un augment en les demandes operatives o de seguretat. Això inclou:

- Capacitat d'Expansió: El sistema ha de permetre l'addició fàcil de nous mòduls de programari, increments en la capacitat de processament o emmagatzematge, i la integració de nous dispositius de seguretat sense la necessitat d'una revisió completa del sistema.
- Flexibilitat per a Augment de Càrrega: El sistema ha d'estar preparat per suportar increments en el volum de trànsit de xarxa i el nombre de dispositius connectats, assegurant que el rendiment no es degradi amb el creixement de la xarxa de l'ÀMB.
- Adaptabilitat a Noves Tecnologies: Garantir que el sistema pugui adaptar-se a noves tecnologies i estàndards emergents en ciberseguretat, facilitant la integració amb altres plataformes i l'adopció de noves pràctiques de seguretat.
- El sistema ha d'oferir la capacitat d'integració futura en la mateixa interfície amb plataformes a serveis de núvol públics i privats, entre altres, i correlacionant totes elles, ja que es considera fonamental per assegurar una protecció integral en l'actual panorama de TI híbrid entre *On-Premise* i *Cloud*.

2.4.3.6. Integració i Compatibilitat

El sistema ha de ser compatible amb la infraestructura de TI existent a l'ÀMB, incloent-hi maquinari, programari i protocols de xarxa, per assegurar una integració sense fissures.

Ha de poder configurar-se per comunicar-se amb sistemes SIEM, eines d'anàlisi de vulnerabilitats, llistes d'IOCs externes i altres components de la infraestructura de seguretat, integrant-se amb noves tecnologies i adaptant-se a futures expansions de la xarxa o canvis en la infraestructura tecnològica.

El sistema ha de permetre la seva integració amb solucions SIEM/SOAR.

La solució ha de disposar d'una multitud de possibles integracions, incloent-hi:

- Integracions natives amb solucions SIEM/SOAR estàndards del mercat: Splunk, Cortex, XSOAR, Swimlane, FortiSOAR, etc.
- Poder enviar alertes a sistemes externs via diversos formats de SYSLOG: LEEF, CEF, JSON.
- Ha de disposar d'una API extensiva amb la qual l'equip de seguretat de l'ÀMB pugui fer integracions utilitzant HTTPS GET i POST per a integracions ad-hoc.
- La solució ha de disposar d'integracions ja preparades amb solucions externes incloent-hi les considerades estàndard del mercat: LogRythm, Splunk, Sentinel, Teams, JIRA, Slack, ServiceNow, etc.
- La tecnologia ha d'oferir integració amb LDAP, Entra ID i SSO per facilitar un accés simplificat a la solució a més d'enriquiment de dades a la interfície.

- La solució pot rebre *logs* i alertes de solucions externes per proporcionar més profunditat i context a les deteccions. L'ÀMB ha de poder crear models de detecció que combinin esdeveniments de sistemes externs a més de la solució guanyadora.

- La solució ha d'oferir una integració activa (incloent l'enviament de telemetria) a més de la seva pròpia resposta autònoma, amb fabricants com MS Defender, Sophos i Fortinet

- El fabricant ha de disposar d'un portal de clients en el qual està documentat en profunditat totes les possibles integracions i que disposa d'un servei de suport 24/7.

2.4.4. Elements de xarxa

La infraestructura de monitoratge de xarxa que s'implementarà com a part del sistema de ciberseguretat basat en IA sol·licitat, ha d'incloure components de maquinari i programari dissenyats per a una integració i funcionament òptims dins de la xarxa existent de l'ÀMB. Això previsiblement inclourà equips concentradors mestres, sondes de xarxa físiques i virtuals, sensors, i altres dispositius necessaris per al monitoratge efectiu del trànsit en temps real, tant als CPDs com als enllaços de xarxa que connecten diferents ubicacions i serveis de l'entitat. Les característiques de que haurien de disposar aquests equips són les següents:

- Sondes de Xarxa: Dispositius dedicats que s'instal·laran en punts estratègics de la xarxa per capturar i analitzar el trànsit. Aquestes sondes seran capaces de realitzar inspeccions profundes dels paquets (*Deep Packet Inspection* o DPI) per identificar patrons de trànsit anòmals i possibles amenaces sense afectar el rendiment de la xarxa.
- Sondes de Xarxa Virtuals: Components programari en forma de màquines virtuals que s'instal·laran en punts estratègics de la infraestructura per capturar i analitzar el trànsit entre màquines virtuals. Aquestes sondes seran capaces de realitzar inspeccions dels paquets per identificar patrons de trànsit anòmals i possibles amenaces sense afectar el rendiment de la xarxa.
- Concentrador Mestre: Equip que centralitzarà l'operació, rebent les dades de les sondes físiques i virtuals.

La solució ha d'utilitzar un disseny de *'master-probe'*, en el qual, si es requereix, el trànsit local de les seus remotes pugui ser capturat localment sense necessitat d'enviar tot l'ample de banda a un equip local. L'enviament de trànsit entre la sonda i el mestre ha de ser inferior al 5% del trànsit ingerit. La comunicació entre el mestre i la sonda ha de ser mitjançant HTTPS 443 de forma segura.

Les propostes han d'incloure una proposta detallada del desplegament a implantar per a l'ÀMB amb diagrames de connexió.

2.4.5. Programari de gestió del trànsit a la xarxa.

El sistema de ciberseguretat ha d'incloure un programari avançat de gestió de trànsit que permeti la visualització en temps real de l'estat de la xarxa, la detecció

d'anomalies i la resposta automàtica a incidents. Aquest programari haurà d'oferir les següents capacitats:

- Anàlisi de Trànsit en Temps Real: Utilització d'algorismes avançats per analitzar el flux de dades i detectar comportaments sospitosos o no autoritzats. Això inclou la identificació d'intents d'intrusió, noms d'arxius, programari maliciós, i altres formes de ciberatac.
- Visualització de Dades: Interfícies gràfiques que permetin als operadors de seguretat visualitzar l'activitat de la xarxa en temps real, amb eines per a l'anàlisi detallada d'esdeveniments i alertes.
- Automatització de Respostes: La solució proposada ha de permetre als administradors configurar accions automàtiques per la pròpia tecnologia de forma autònoma, en resposta a incidents detectats, com, però no limitat a, l'aïllament de dispositius compromesos o la modificació de regles de tallafocs per bloquejar trànsit maliciós.

La infraestructura de monitoratge de xarxa haurà d'estar dissenyada per ser escalable, permetent futures expansions o modificacions sense comprometre la seguretat ni el rendiment. També haurà de ser capaç d'integrar-se amb els serveis MDR i entorns de seguretat presents a l'ÀMB.

Independentment del nombre d'appliances/sondes instal·lats, l'ÀMB ha de comptar amb una interfície unificada que mostri totes les alertes de la solució i les funcionalitats de gestió.

El sistema proposat ha de comptar amb capacitat d'emmagatzematge mínim per a:

- Una setmana de captures en format estandarditzat PCAP (captures de trànsit realitzades, en brut, sense processar del trànsit de tots els equips)
- Un mes per a metadades de les connexions (origen, destinació, protocol, nom màquina, arxiu, etc.)
- 9 mesos per als logs de connexions dels equips.

La proposta haurà d'incloure una relació exhaustiva de les capacitats de gestió de trànsit incloses així com exemples.

3. Requeriments d'execució.

3.1. Serveis a realitzar

L'adjudicatari haurà d'incloure en la seva proposta una descripció detallada, clara i sense ambigüitats de cadascun dels serveis i cobertures oferts, que hauran de donar cobertura completa als requeriments sol·licitats en el present plec, demostrant la seva capacitat per complir amb les expectatives i necessitats específiques i assegurant una protecció completa i efectiva davant les amenaces cibernètiques.

Es diferencien les tasques inicials de desplegament dels serveis de SOC posteriors amb els que es vol complementar la plataforma.

3.1.1. Desplegament.

3.1.1.1. Equipament i Programari

L'adjudicació del contracte implica el subministrament complet i implementació d'un sistema de ciberseguretat basat en intel·ligència artificial, que inclourà tots els components de maquinari i programari necessaris per al seu funcionament i operació efectiva. L'adjudicatari haurà de proporcionar almenys dos appliances físics de seguretat cadascun a instal·lar en un els dos CPDs de l'ÀMB. Aquests appliances actuaran com els nodes centrals per al monitoratge, anàlisi i gestió del trànsit de xarxa.

Tant el maquinari com el programari del sistema a subministrar i integrar per part de l'adjudicatari ha de ser capaç d'integrar-se sense conflictes amb la infraestructura tecnològica actual de l'ÀMB, i ha d'incloure capacitats avançades d'aprenentatge automàtic i processament heurístic per detectar i respondre a amenaces de manera proactiva. A més, ha de permetre configuracions personalitzades segons les necessitats específiques de l'ÀMB, incloent però no limitant-se a, la creació de polítiques de seguretat, configuració d'alertes, investigació d'incidents de seguretat i generació d'informes detallats.

3.1.1.2. Instal·lació i Configuració

Els equips a desplegar inclouran, com a mínim:

- Equips mestres centrals.
- Sondes en format appliance en cada CPD dels edificis A i B.
- Sondes virtuals en els entorns de virtualització de l'ÀMB

Aquestes sondes s'ubicaran per tal de permetre l'anàlisi de tots els segments de xarxa, tant de l'àmbit client (segments d'accés per cable i WiFi) com del de servidors (*core*). Cal tenir en compte que tots els segments travessen els tallafocs de segmentació (diferents dels perimetrals)

El sistema es configurarà en alta disponibilitat on cap component pugui representar un punt de fallida únic. També haurà de poder continuar operant amb normalitat en cas de fallida de qualsevol component de la xarxa ÀMB que disposi de redundància i havent de continuar estant operatiu fins i tot en el cas d'indisponiblitat d'un CPD complet. Igualment el sistema tindrà previst la tornada a la normalitat des d'una situació de funcionament amb indisponiblitats. Totes aquestes transicions es realitzaran de manera automàtica sense intervenció humana.

La implementació del sistema ha de ser realitzada per personal tècnic qualificat de l'adjudicatari, que garanteixi una instal·lació i configuració òptimes de tots els components. Aquest procés inclourà:

- Instal·lació Física: Col·locació i connexió dels appliances als racks corresponents dins dels CPDs, connexió a la infraestructura de xarxa existent, i assegurament del seu correcte funcionament energètic i de xarxa.
- Configuració del Sistema: Ajustos inicials del programari per integrar-se amb la xarxa de l'ÀMB, configuració dels mòduls d'anàlisi de trànsit, establiment

de paràmetres de seguretat i proves de la funcionalitat d'autoaprenentatge i detecció proactiva.

- Proves d'Acceptació: Un cop instal·lat i configurat el sistema, es realitzaran proves exhaustives per verificar que tots els components funcionen segons les especificacions tècniques i compleixen amb els objectius de ciberseguretat establerts. Això inclou proves de càrrega i resistència, simulacres d'atac i avaluació de la resposta del sistema davant incidents de seguretat simulats.

L'adjudicatari serà responsable de dur a terme les adequacions necessàries en els sistemes presents a l'ÀMB i haurà de disposar de l'acceptació per part d'aquesta per a realitzar-les. En aquest sentit es proporcionarà, abans de realitzar el desplegament, tota la informació de l'arquitectura de xarxa resultant, els canvis requerits i l'impacte que aquests impliquen. En cas que l'ÀMB jutgi que les modificacions proposades poden ocasionar efectes negatius en la disponibilitat o rendiment dels sistemes en producció, l'adjudicatari haurà de modificar la seva proposta fins a que l'ÀMB la consideri acceptable. En cap cas aquestes modificacions suposaran un cost addicional per l'ÀMB.

L'adjudicatari ha de justificar i assegurar que el sistema implementat sigui completament compatible amb les polítiques de seguretat de l'ÀMB i que el seu funcionament no introdueixi vulnerabilitats a la xarxa existent.

Després de la instal·lació, l'adjudicatari haurà de proporcionar un informe detallat de la instal·lació i implementació que inclogui *as-built*, documentació tècnica, esquema de l'arquitectura, registres de configuració i resultats de les proves d'acceptació.

3.1.1.3. Metodologia del projecte

L'adjudicatari haurà de presentar una planificació del projecte detallant les diferents activitats, amb els seus fites associades i posterior servei, per a cadascuna de les fases previstes en la metodologia aportada.

L'adjudicatari efectuarà la implantació segons la seqüència de fases especificades en la seva proposta, respectant el detall d'activitats presentades, liderades pel responsable de cadascuna d'elles.

A continuació, es descriuen les tasques que com a mínim s'han de contemplar:

1. Anàlisi de la situació inicial: L'adjudicatari iniciarà el projecte amb una revisió dels requeriments establerts a l'ÀMB.
2. Estratègia d'implantació i calendari: Tenint en compte les capacitats de l'Entitat, l'adjudicatari elaborarà una estratègia de gestió que contempli el descrit en apartats previs sobre aquest particular.
3. Revisió de la configuració de la plataforma: L'adjudicatari ha de subministrar la subscripció a la plataforma i, de la mà de l'equip de Tecnologia de l'Entitat, configurar l'arquitectura tècnica adequada per al seu correcte funcionament.
4. Anàlisi periòdic: L'adjudicatari ha de proporcionar una metodologia per analitzar, durant el cicle de vida del servei contractat, els nivells de servei i el funcionament del sistema.

3.1.2. Serveis de SOC.

De forma complementària a les eines d'anàlisi del transit que el personal de l'ÀMB podrà analitzar i interpretar, el servei de subscripció comptarà amb un servei complementari amb personal especialitzat que facilitarà i ajudarà en la gestió del sistema.

Es objecte del contracte realitzar un servei de monitoratge operatiu 24x7x365, que ha de permetre identificar les incidències i vulnerabilitats de seguretat més crítiques per tal de poder actuar en conseqüència de forma activa. Aquest servei s'oferirà des d'un Centre d'Operacions de Seguretat (SOC), qui en la modalitat de serveis i centrant-se en l'explotació de l'eina NDR aportada, proporcionarà:

- Servei de prevenció: Anàlisi de les vulnerabilitats de la seguretat dels Sistemes d'Informació.
- Servei de detecció: Detecció dels esdeveniments de seguretat i permeti una detecció ràpida dels incidents i les amenaces.
- Servei d'anàlisi i resposta: Un servei que ajudi en l'anàlisi dels incidents i pugui col·laborar en donar una resposta adequada i ajustada.

3.1.2.1. Tasques i protocols d'actuació.

El Centre d'Operacions de Seguretat (SOC) ha de realitzar un servei de revisió/supervisió/anàlisi continu de la pròpia plataforma de monitorització, sobre la qual haurà de realitzar les següents tasques:

- Classificar els diferents elements, investigar-los per tal de determinar si són incidents que poden afectar a la seguretat corporativa, o si no són rellevants.
- Coordinar els serveis necessaris per a la resolució de la incidència partint de la urgència i nivells de servei contractats.
- Notificar/avisar als responsables de l'ÀMB de la incidència esdevinguda, detallant l'impacte de la mateixa i el pla per a la seva resolució.
- Realitzar propostes de millores a tots els nivells (organitzatius, operacionals, etc.), que es presentaran als informes de seguiment mensuals.

El contracte inclou l'elaboració d'un protocol d'actuació en el cas d'incidències, que s'anirà adaptant de forma progressiva per ajustar-se a les necessitats de l'ÀMB. Serà objecte del contracte disposar d'aquest document de protocol actualitzat i ajustat.

3.1.2.2. Adaptació a noves amenaces.

El servei SOC vetllarà per que la plataforma NDR estigui preparada per a fer front a noves amenaces. Això inclourà tant l'actualització de tots els components que la integrin com la realització d'accions a mida específiques que es requereixin.

3.1.2.3. Informes de seguiment.

El contracte inclou la realització de diferents informes on es reculli tota la informació i els resultats del servei de monitorització i anàlisi de la xarxa IP. Inclourà diferents informes:

- Un Informe/auditoria general trimestral indicant a nivell general els punts de millora en l'àmbit de la seguretat corporativa. Aquest informe serà de caràcter executiu, fent les recomanacions de seguretat general.
- Un Informe resum mensual de les accions realitzades, la descripció i anàlisi dels esdeveniments crítics ocorreguts durant el període, així com la descripció de les accions i/o recomanacions realitzades.

La periodicitat dels informes es podrà revisar ajustant-la a les necessitats de l'ÀMB. Igualment, en cas d'ocórrer algun esdeveniment d'especial rellevància a judici de l'ÀMB, es podrà sol·licitar la realització d'un informe extraordinari.

3.1.2.4. Requeriments del SOC.

El Centre d'Operacions de Seguretat (SOC) aportat realitzarà les tasques de monitoratge, ajudant i assessorant al personal del Servei d'Informàtica i Telecomunicacions. Els requeriments mínims que ha de complir són:

- El SOC ha d'estar format per un equip de treball altament qualificat i amb coneixements de les eines d'anàlisi de xarxa proposades.
- Disponibilitat 24x7 amb diferents canals de contacte (telefònic, web, correu electrònic).
- El SOC haurà d'establir un mecanisme segur d'accés a l'eina NDR.
- S'haurà de poder realitzar una auditoria de les tasques realitzades pels diferents tècnics que hagin actuat amb la plataforma.

3.1.2.5. Integració servei MDR Advanced de Sophos.

Actualment l'ÀMB té contractat el servei MDR Advanced ofert per l'empresa Sophos. Aquest servei realitza operacions assimilables a un SOC però delimitades als equipaments i entorns que gestiona (*Endpoints* a plataforma client i servidor, tallafocs de segmentació XGS, entorns Microsoft 365) i dels que rep telemetria (tallafocs perimetrals). El servei SOC inclòs en aquest contracte haurà de funcionar en paral·lel amb l'ofert pel MDR sense dificultar o afectar aquest. MDR retindrà la capacitat d'actuar sobre els equipaments que gestiona mentre que el SOC podrà actuar sobre l'NDR.

Igualment l'eina NDR es configurarà per a subministrar telemetria a l'MDR per tal que es pugui incloure la informació recollida pels equips NDR en els casos gestionats pel MDR.

En tot moment es buscarà la creació de sinèrgies entre ambdós serveis de manera que la col·laboració redundi en una millor protecció dels sistemes de l'ÀMB.

3.2. Suport i Manteniment

3.2.1. Suport Tècnic

El contracte inclourà un servei de suport tècnic disponible les 24 hores del dia, els 7 dies de la setmana, per assegurar la contínua operativitat i eficiència del sistema de ciberseguretat. Aquest suport tècnic ha d'oferir:

- Accés Directe a Experts: L'ÀMB tindrà accés directe a experts en ciberseguretat que poden assistir en la resolució de problemes, ajustos de configuració, i consultes tècniques generals.
- Actualitzacions i Pegats de Seguretat: El suport tècnic inclourà la gestió i aplicació d'actualitzacions de programari i pegats de seguretat necessaris per protegir contra vulnerabilitats conegudes. L'adjudicatari proporcionarà totes les peces i materials necessaris per mantenir el maquinari en bon estat de funcionament.

Les peces de recanvi proporcionades sota el suport de maquinari hauran de ser equivalents o superiors en funcionalitat, rendiment i fiabilitat.

3.2.2. Manteniment Preventiu, Correctiu i Actualitzacions

El contracte inclourà tant el manteniment preventiu com el correctiu per assegurar l'eficiència, durabilitat i seguretat del sistema. Això inclourà, com a mínim:

- Manteniment Preventiu: Revisions i actualitzacions planificades que es realitzaran periòdicament per garantir que el sistema funcioni de forma òptima i per evitar possibles avaries. El sistema ha de ser capaç de fer-se un autodiagnòstic que permeti detectar i anticipar-se a incidents de manteniment a través d'alertes en la interfície i per enviament de correus electrònics.

- Manteniment Correctiu: Solució ràpida i efectiva de qualsevol fallada o problema que ocorri en el sistema, incloent la solució de vulnerabilitats crítiques en el sistema, minimitzant així el temps d'aturada i mantenint la integritat de les operacions de seguretat.

Pel que fa a les actualitzacions, el sistema permetrà fer-les sense connexió a internet. L'ÀMB ha de poder actualitzar la solució, si així ho sol·licités durant el període del contracte, sense que la plataforma tingui accés en línia. Ha de ser possible descarregar qualsevol arxiu d'actualització des d'un portal central de clients que tingui totes les actualitzacions disponibles permetent a l'ÀMB fer una instal·lació sense connexió. El fabricant ha de proporcionar un portal que detalli tot l'historial d'actualitzacions, noves funcionalitats/millores en totes les versions.

És essencial, per tal de mantenir la integritat i efectivitat del sistema de ciberseguretat davant amenaces emergents i evolucionar amb el panorama canviant de la ciberseguretat, implementar actualitzacions de seguretat de forma regular i sistemàtica. L'adjudicatari serà responsable de:

- Provisió Contínua d'Actualitzacions: S'inclourà en l'oferta el subministrament regular d'actualitzacions per al programari i maquinari del sistema,

assegurant que totes les eines i sistemes estan actualitzats amb les últimes defenses contra amenaces conegudes.

- Gestió de Pegats de Seguretat: S'oferirà un sistema de gestió de pegats que asseguri l'aplicació ràpida de correccions a vulnerabilitats identificades en el programari o maquinari que forma part del sistema de ciberseguretat.
- Notificació i Documentació d'Actualitzacions: S'informarà a l'ÀMB sobre cada actualització o canvi realitzat amb antelació, proporcionant detalls sobre la millora o la necessitat de l'actualització i la documentació pertinent sobre com afecta al sistema i als procediments operatius estàndard.

Qualsevol actualització del programari ha de ser realitzada per un usuari autenticat amb accés limitat a la consola/consoles dels dispositius. No ha de ser possible actualitzar la solució des de la interfície principal, per raons de seguretat s'obligarà a fer-se amb un usuari específic a tal efecte i a través d'una interfície específica.

Les propostes hauran d'incloure una descripció del compliment d'aquests punts així com un pla de manteniment que detalli les freqüències dels manteniments, els procediments per a proves de sistemes i components, i les estratègies per a l'actualització de la infraestructura tecnològica associada al sistema proposat.

3.3. Capacitació, Formació i Transferència de Coneixements

3.3.1. Programes de Capacitació

La implementació d'un sistema de ciberseguretat avançat requereix no només eines d'alta tecnologia, sinó també que el personal de l'ÀMB estigui adequadament capacitat per utilitzar aquestes eines de manera efectiva. L'adjudicatari haurà de proporcionar i descriure un programa de capacitació exhaustiu que inclogui:

- Capacitació Tècnica Inicial: Sessió o sessions detallades per al personal tècnic sobre l'operació, administració i manteniment del sistema. Això inclourà formació sobre la configuració del sistema, monitoratge diari, resposta davant incidents i procediments de recuperació. Temps mínim de la sessió: 8 hores.

- Capacitació en el sistema: Programes sobre com utilitzar les eines de seguretat tant de manera reactiva com proactiva per detectar, respondre i investigar amenaces. Temps mínim de la sessió: 16 hores.

- Seminaris i Tallers: S'oferiran sessions periòdiques que s'actualitzaran amb les últimes tendències i avenços en ciberseguretat per assegurar que el personal de l'ÀMB es mantingui al dia amb les noves tecnologies i estratègies de defensa. S'especificarà el nombre de Seminaris i Tallers inclosos, que no serà inferior a 10. Aquests inclouran la realització d'un mínim d'un simulacre anual.

- Recursos en Línia i Suport Continu: Accés a una biblioteca de recursos en línia del fabricant del sistema, incloent FAQs, tutorials en vídeo i documentació actualitzada, que el personal de l'ÀMB pugui consultar per aclarir dubtes o aprofundir en aspectes específics del sistema. S'especificarà en les ofertes els continguts de recursos en línia.

- Capacitació Continuada: S'oferiran programes d'actualització i cursos de refresc que s'oferiran periòdicament per assegurar que el personal de l'ÀMB es mantingui actualitzat respecte als canvis en la tecnologia i les pràctiques de seguretat.

La capacitació serà adaptada a diversos nivells d'habilitat tècnica i s'oferirà en diversos formats, incloent sessions presencials, tallers pràctics i mòduls en línia, per garantir una comprensió integral i la flexibilitat en la formació.

Els continguts formatius seran lliurats o posats a disposició de l'ÀMB després de la formació per a la seva posterior consulta que haurà de romandre accessible fins i tot més enllà de la finalització del contracte.

3.3.2. Transferència de Coneixements i Documentació

Per assegurar que l'ÀMB pugui gestionar i operar el sistema de ciberseguretat de manera autònoma i efectiva, l'adjudicatari haurà de descriure un pla de transferència de coneixements, que inclourà, com a mínim, la següent documentació tècnica completa:

- Manuals d'operació
- Guies d'usuari
- Esquema as-built de la instal·lació
- Documentació de configuració i manteniment
- Procediments estàndard d'operació
- Usuaris i contrasenyes

Aquests documents seran lliurats a l'ÀMB i estarà disponible en formats accessibles, estàndards de mercat (ex: .pdf, .docx, .pptx) hauran de ser fàcilment comprensibles i estar redactats en català.

3.4. Requisits de Seguretat, Confidencialitat i Protecció de Dades

El procés d'implantació del servei, així com la configuració de la plataforma, s'ha de dur a terme per part de l'adjudicatari tenint en compte les millors pràctiques de seguretat.

L'empresa contractista o les persones físiques, actuant directament o indirectament sota la seva responsabilitat, no podran realitzar cap acció que comprometi la seguretat o la integritat dels sistemes d'informació i comunicacions de l'ÀMB o la seva accessibilitat durant l'execució dels treballs.

L'empresa contractada s'obliga a no difondre i a guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte, i a subministrar-la només a personal autoritzar per l'Àrea Metropolitana de Barcelona.

Qualsevol comunicat de premsa o inserció als mitjans de comunicació que el proveïdor realitzi referent al servei que presta haurà de ser aprovat prèviament pel client.

3.4.1. Requeriments generals de seguretat

L'adjudicatari ha de garantir a l'ÀMB la seguretat de la informació a la qual tingui accés durant el desenvolupament del servei, observant les següents normes:

- Complir amb els estàndards i polítiques de seguretat de l'Entitat.
- Garantir la confidencialitat, integritat i disponibilitat de la informació emmagatzemada i transmesa per la seva xarxa.
- Informar sobre la política de seguretat pròpia, així com de la seva implementació i seguiment per part de la seva organització.
- Informar per escrit, tan aviat com detecti riscos reals o potencials de seguretat a la seva pròpia xarxa, o en l'equipament del client.
- Garantir que la informació, en la seva totalitat, no s'emmagatzema, duplica o intercepta, mentre circula per la seva xarxa.
- Establir un control d'accés lògic als equipaments de xarxa i/o sistemes d'informació, garantint-lo únicament als usuaris autoritzats.
- Garantir que el seu equip de treball aplica de forma estricta les normes de seguretat.
- Detallar els mecanismes i protocols d'encriptació de dades que utilitzaran en les transmissions.

El personal de l'adjudicatari que requereixi accés físic a les instal·lacions de l'ÀMB serà identificat i haurà de portar visible en tot moment l'acreditació assignada.

3.4.2. Requeriments de la seguretat per a l'execució del servei

En cas que l'adjudicatari detecti un incident de seguretat durant la prestació del servei, ha de notificar-ho immediatament al personal responsable del servei designat per l'ÀMB. Per tant, l'adjudicatari ha d'habilitar un canal de comunicació per a potencials incidents de seguretat i presentar, en el termini que s'estableixi, un informe de situació i un pla de reparació o mitigació, si escau. Addicionalment, qualsevol notificació d'incident que tingui una potencial transcendència pública anirà acompanyada d'una proposta de pla de comunicació a seguir per part de l'ÀMB.

3.4.3. Intercanvi segur d'informació

L'adjudicatari del servei ha de subministrar les eines necessàries per a un intercanvi segur d'informació entre ambdues parts que no requereixi la instal·lació d'aplicacions a l'ÀMB, assegurant l'ús d'un protocol de xifrat robust i de mercat. En cas que el protocol utilitzat per al xifrat es vegi públicament compromès al llarg de l'execució del servei, l'adjudicatari haurà de proporcionar una alternativa segura amb la qual treballar a partir d'aquest moment.

3.4.4. Registres de traçabilitat

Qualsevol acció sobre la plataforma ha de quedar registrada, identificant, com a mínim, l'usuari que la realitza, les dades o registres accedits/modificats, la data i hora en què es produeix, i si ha estat autoritzada o no. Els registres han de ser emmagatzemables i exportables a un format electrònic de mercat. A més, han de disposar dels adequats controls d'integritat que permetin identificar qualsevol potencial alteració.

3.4.5. Protecció de Dades i Privacitat

Totes les dades sensibles manejades pel sistema han de ser encriptades tant en trànsit com en repòs per protegir contra l'accés no autoritzat i les filtracions de dades.

El sistema ha de complir amb les normatives vigents a Espanya de protecció de dades, incloent el GDPR.

3.4.6. Propietat i utilització de les dades

L'empresa adjudicatària i el personal encarregat de la realització de les tasques, han de guardar secret professional sobre totes les informacions, documents i assumptes als quals tinguin accés o coneixement durant la vigència del contracte, estant obligats a no fer-los públics o alienar quants dades coneguin com a conseqüència o amb ocasió de la seva execució, per temps indefinit després de la finalització del contracte. L'adjudicatari es compromet a mantenir estricta confidencialitat i a no revelar o cedir dades, ni tan sols per a la seva conservació, o documents proporcionats per l'ÀMB, a tercers, per a qualsevol altre ús no previst com a necessari per al desenvolupament de la prestació objecte d'aquest contracte, especialment les dades de caràcter personal. Encara que no estigui previst en l'objecte d'aquest contracte, si personal a càrrec de l'empresa adjudicatària autoritzat a la realització de la prestació objecte de contractació tingués accés a dades de caràcter personal dels quals és titular l'ÀMB, comunicarà aquest fet a personal de l'ÀMB, havent de complir amb les obligacions de discreció que, respecte a les dades de caràcter personal, disposa la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, així com el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament que desenvolupa aquesta Llei. L'empresa adjudicatària serà responsable de tots els danys i perjudicis directes o indirectes soferts per l'ÀMB com a resultat de l'incompliment de la present obligació de confidencialitat i de protecció de dades.

3.4.7. Incidències en matèria de protecció de dades

L'adjudicatari del servei haurà de notificar en un termini màxim d'una hora des del seu coneixement qualsevol incidència que pugui afectar, potencialment o de manera confirmada, dades de caràcter personal de l'ÀMB. En un termini no superior a un dia, haurà de presentar un informe en el qual es descrigui l'impacte de la incidència, els motius que l'han causat, els procediments adoptats per protegir-se de noves ocurrències, així com la totalitat de requisits establerts en el RLOPD.

3.5. Metodologia de treball

Caldrà garantir que les actuacions es realitzin minimitzant l'impacte en els processos productius i els llocs de treball dels usuaris finals. Es planificaran les actuacions amb major afectació per ser dutes a terme en moments d'ús més baix i aprofitant tots els mecanismes de redundància per garantir en el possible la continuïtat del servei.

Caldrà tenir sempre en compte els criteris d'alta disponibilitat, optimització del rendiment i aprofitament de recursos en aquest ordre de prioritat. En cas de decisions crítiques o que no permetin un canvi assequible de criteri posterior respecte a qualsevol d'aquests aspectes caldrà disposar de l'aprovació del Servei TIC.

En cap cas es desplegarà un producte de programari o maquinari sense el consentiment del Servei TIC. Tot producte instal·lat quedarà sota el control d'aquest. Tot producte temporal es desintal·larà un cop finalitzat el seu ús. Tot producte que romangui instal·lat un cop finalitzat el desplegament haurà d'estar en les mateixes condicions de llicenciament d'ús i suport que la resta de la plataforma.

3.6. Avaluació de la plataforma aportada.

Es preveu la realització de diversos jocs de proves tant durant l'execució com a la finalització de les actuacions. Aquestes proves hauran de superar-se per tal que l'ÀMB accepti signar l'acta de recepció i comencin a comptar els terminis de suport i garantia.

3.6.1. Pla de proves.

L'adjudicatari presentarà un pla de proves per a cada sistema, en el qual s'establiran les validacions que s'hauran de basar en funció de les normatives de control de les instal·lacions i les normes establertes pels fabricants. En cas de no superar-se l'adjudicatari aportarà els mitjans i actuacions necessàries per esmenar-ne les causes i poder repetir les proves fins a superar-les sense cap cost addicional per l'ÀMB. Aquestes correccions s'aplicaran seguint els mateixos requeriments ja indicats en aquest plec.

Si bé el temps emprat pel fabricant o l'ÀMB en la realització d'aquestes proves no computarà en el termini màxim d'implantació, si ho farà l'emprat per l'adjudicatari per a corregir les mancances que puguin detectar-se en aquestes.

3.6.2. Acta de recepció

En superar-se les proves indicades i al finalitzar les tasques de migració l'ÀMB signarà una acta de recepció indicant la seva acceptació dels treballs efectuats. El termini de suport i garantia s'iniciarà l'endemà de l'esmentada signatura.

3.7. Altres consideracions.

Caldrà preveure el màxim nivell de serveis professionals que assegurin la correcta configuració i posada en funcionament del sistema, així com una resposta ràpida i eficaç davant de qualsevol eventualitat, error o anomalia.

4. Model de relació

L'equip de treball de l'empresa adjudicatària durà a terme la gestió operativa del servei i serà l'encarregat d'establir els mecanismes de seguiment, avanç, coordinació i control de qualitat de tots els lliuraments i de vetllar pel compliment dels estàndards d'execució. Aquest equip reportarà a la Direcció de l'ÀMB els avenços globals i individuals del servei.

L'adjudicatari haurà de presentar una proposta de comitè de coordinació i seguiment d'acord amb l'equip del servei, de manera que es permeti l'establiment d'un diàleg fluid a tots els nivells, i entre tots els implicats.

4.1. Seguiment del servei

L'ÀMB exigeix a l'adjudicatari el compliment i seguiment d'uns mecanismes globals de coordinació. Per a això, a través de l'equip de persones assignat al servei, establirà els mecanismes de seguiment i coordinació durant tot el cicle de vida del servei. Mitjançant aquests mecanismes es vetllarà per:

- Definició d'estàndards de treball de *reporting* i del projecte global.
- La coherència en el disseny global de l'estratègia de gestió de vulnerabilitats i implantació de la plataforma requerida.
- El compliment de totes les condicions d'execució descrites en aquest Plec.

Per donar suport a la metodologia de gestió del servei, l'empresa adjudicatària ha d'utilitzar les eines que s'indiquin des de l'equip per al seguiment, control i qualitat dels projectes (informes de seguiment, actes de reunions, informes de riscos per a l'avanç del projecte, etc.). L'equip designat per l'adjudicatari assumirà les següents funcions de seguiment i *reporting*:

- Seguiment mensual de la qualitat global del servei.
- Seguiment continuat de l'evolució del servei mitjançant la convocatòria de reunions mensuals amb la finalitat de revisar el grau de compliment dels objectius, la planificació d'activitats i altres aspectes de gestió.
- *Reporting* al responsable del servei per part de l'ÀMB.

El cap de projecte de l'adjudicatari haurà d'assistir a les reunions a les que sigui convocat per l'ÀMB.

4.2. *Reporting* del servei

Mensualment, l'adjudicatari ha de lliurar un informe, en el format que es defineixi en formalitzar el contracte corresponent, amb els següents continguts:

- Situació Global del Servei.
- Anàlisi de desviacions del servei.
- Informe de gestió d'incidències.
- Actes de reunió.

En la proposta s'haurà d'incloure una proposta de calendari preliminar i de processos per al *reporting* al llarg del servei.

5. Presa de requeriments i dades de la infraestructura actual.

   Serà responsabilitat de l'adjudicatari la correcta presa de requeriments i l'obtenció de dades de la situació de les infraestructures presents per l'elaboració de la seva proposta. Qualsevol adquisició, ampliació o adaptació de recursos de maquinari o programari, així com la contractació de serveis addicionals de tercers que es requereixin per la implantació anirà a càrrec d'aquest. En cap cas l'adopció de la solució presentada haurà de suposar per l'ÀMB un cost no contemplat a l'oferta.

   L'ús en aquesta instal·lació de recursos prèviament presents a l'ÀMB es farà seguint criteri d'aquesta. En /cas que l'ÀMB consideri que aquests recursos no s'hi poden destinar per incompatibilitat amb altres usos, pèrdues de rendiment o altres factors tècnics, l'adjudicatari haurà de proveir-los com si no es disposés d'ells.

6. Acords de nivell de servei (ANS o SLA).

   Al llarg d'aquest apartat es fixa els ANS per a la prestació del servei demanat. Aquests es podran revisar anualment.

   A efectes d'aquest apartat es defineixen les següents prioritats que s'aplicaran a incidències en els processos de còpia. En qualsevol cas l'ÀMB es reserva la capacitat determinar la prioritat d'una incidència segons el seu propi criteri.

   Per cada ANS incomplert es demanarà un informe de justificació analitzant les causes del mateix. En cas de justificar-se satisfactòriament als responsables del servei de AMB aquest trencament, no s'aplicarà la corresponent penalització.

Prioritat	Impacte	Incidència	Petició de servei
1	**Crític** Si afecta al servei	Interrupció total del servei: el servei manca per complet de disponibilitat. Hi ha un incident crític de seguretat.	Es requereix un canvi per mantenir la solució en funcionament.
2	**Greu** Si afecta al servei	Es pot fer part del treball diari però l'activitat es veu afectada. Moltes funcionalitats no estan disponibles. El risc de seguretat del servei és elevat	Es requereix un canvi per mantenir un element principal de la solució.
3	**Moderat** No afecta al servei	El servei està disponible però les activitats diàries poden veure's afectades moderadament. Una o més funcionalitats no poden funcionar a ple rendiment. Problema de maquinari afectant a un únic equip que disposi de redundància. Realització d'una anàlisi forènsic d'un incident de seguretat. El risc de seguretat del servei és moderat	Es requereix un canvi per millorar l'element de la solució.
4	**Baix** No afecta al servei	El servei està disponible i la majoria o totes les tasques diàries es poden seguir realitzant. El risc de seguretat del servei és baix.	Es requereix un canvi superficial d'un element de la solució.

Els ANS aplicables seran els següents:

Criticitat	*Temps de resposta*	*Temps de resolució*	*Percentil a assolir*	*Tipus*
1	30 min	4 hores	95%	Crític
2	30 min	6 hores	90%	No crític
3	1 hora	24 hores	90%	No crític
4	12 hores	5 dies	90%	No crític