AMB Àrea Metropolitana de Barcelona

APROVAT

COORDINACIÓ SERVEIS DIGITALS
OL/mc

Exp.900435/2025
22/01/2025

PLEC DE CONDICIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL DESENVOLUPAMENT D'UNA APLICACIÓ DE GESTIÓ DE COMPRES I MAGATZEM

Índex

1 ANTECEDENTS

Serveis Interns, com a part de les seves funcions, porta a terme la gestió de les sol·licituds de material d'oficina, així com la gestió de l'inventari del magatzem corresponent. Fins ara aquestes tasques es duien a terme mitjançant una aplicació que el fabricant va discontinuar per decisió seva, un cop finalitzada la vigència de l'últim manteniment contractat. Això va fer que la gestió de compres i magatzem de material d'oficina quedés en una situació molt precària, ja que no tenim el suport del proveïdor en cas que es produeixi un error que impedeixi el bon funcionament de l'eina.

Davant d'aquesta situació, cal disposar d'una aplicació que tingui al menys les mateixes funcionalitats cobertes per l'aplicació que ha quedat obsoleta, i a les quals es puguin afegir nous requeriments relacionats amb la seguretat i l'adaptació a l'entorn tecnològic de l'AMB.

2 OBJECTE

L'objecte del present concurs és fixar les condicions tècniques a les quals s'ajustarà el procediment obert simplificat per a la contractació del desenvolupament i implementació d'una aplicació de gestió de compres i magatzem.

3 ABAST

L'eina de gestió de compres i magatzem proposada pels licitadors ha de donar cobertura, almenys, als següents àmbits:

- Gestió de l'estoc del magatzem de material d'oficina.
- Gestió dels articles de material d'oficina.
- Gestió de les comandes de material als proveïdors.
- Gestió dels albarans i factures.

4 DURADA

La durada del projecte serà d'un màxim de dotze (12) mesos un cop formalitzat el contracte.

5 DESCRIPCIÓ TÈCNICA DE LA SOLUCIÓ

L'AMB necessita disposar d'una eina de gestió de compres i magatzem de material d'oficina que doni cobertura a tota l'activitat relacionada: sol·licituds de material per part dels serveis, gestió de les comandes amb els proveïdors, i gestió de les entrades i sortides del magatzem.

5.1 Requeriments funcionals

A continuació s'indica la relació de funcionalitats que ha de tenir l'aplicació informàtica. Serà obligatori que la nova aplicació reculli totes les funcionalitats especificades, tot i que no és una relació exhaustiva i l'AMB pot introduir algun canvi (adició o modificació) durant l'etapa d'anàlisi i disseny tècnic.

Codi	Requeriment	Descripció
RF01	Multiexercici	La gestió de compres i magatzem ha de ser multiexercici. Els usuaris gestors han de poder activar / inactivar els exercicis.
RF02	Multientitat	La gestió ha de ser multientitat, tenint en compte que: • Cada entitat ha de disposar del seu magatzem diferenciat de material d'oficina o del tipus que gestioni. • Dins de la informació corresponent a l'entitat s'hi ha d'incloure el seu logotip, que apareixerà als documents generats per l'aplicació.
RF03	Alta i recepció de sol·licituds	L'eina ha de permetre l'alta i recepció de les sol·licituds de material d'oficina que han enviat els diferents serveis d'AMB a Serveis Interns (usuaris gestors). La sol·licitud és la unitat de procés bàsica i caldria mantenir un historial de les accions realitzades contra ella a mode d'auditoria.
RF04	Tramesa de sol·licituds a compres	Els serveis d'AMB han de poder enviar les sol·licituds en bloc a Serveis Interns.
RF05	Gestió de les sol·licituds des de Serveis Interns	Serveis Interns ha de disposar d'una funció per tal de veure de manera senzilla i clara quin és l'estat de les comandes, així com el detall de cadascuna d'elles.
RF06	Gestió dels albarans	L'eina ha d'incloure la gestió dels albarans

Codi	Requeriment	Descripció
		que els proveïdors envien a Serveis Interns.
RF07	Gestió de les factures	L'eina ha d'incloure la gestió (alta, modificació, baixa, consulta) de les factures que els proveïdors envien a Serveis Interns, així com el lligam amb els albarans corresponents a cadascuna.
RF08	Definició dels magatzems	L'eina ha de permetre definir les dades bàsiques d'un magatzem.
RF09	Gestió de les sol·licituds des del magatzem	L'eina ha de permetre cercar i gestionar les sol·licituds de material de magatzem. L'estat de les sol·licituds pot ser: a) enviada al magatzem, b) retornada al magatzem, c) lliurada totalment i d) lliurada parcialment.
RF10	Enviament automàtic de correus electrònics	L'eina ha de permetre enviar correus electrònics de manera automàtica als usuaris gestors i als usuaris de magatzem quan una sol·licitud de material canvia d'estat.
RF10	Material pendent de lliurar	L'eina ha de poder consultar la relació de sol·licituds de material que estan pendents de lliurar, indicant clarament la informació més rellevant de la sol·licitud perquè sigui fàcilment identificable.
RF11	Consulta de moviments d'articles	L'eina ha de permetre consultar els moviments d'articles per diferents criteris de cerca: família d'articles, subfamília, article concret, sol·licitud, interval de dates de sol·licitud, etc.
RF12	Consulta d'estocs	L'eina ha de permetre consultar de manera senzilla i entenedora l'estat de l'estoc per diferents criteris de cerca: família d'articles, subfamília, article concret, interval de preus, nom aproximat de l'article, etc. Ha de mostrar el codi i la descripció del magatzem, l'article, el nombre d'unitats i la localització.
RF13	Trencament d'estocs	L'eina ha de permetre detectar fàcilment quan s'ha produït un trencament d'estoc, definint quin és el nombre mínim i òptim de cadascun dels articles i avisant quan l'estoc d'un article sigui inferior al nombre mínim.
RF14	Consulta d'inventaris	L'eina ha de poder mostrar els diferents inventaris que s'han realitzat als magatzems i el detall dels articles.
RF15	Realitzar inventari	L'eina ha de permetre generar un inventari

Codi	Requeriment	Descripció
		per magatzem, carregant automàticament els articles amb el nombre d'existències anteriors, i permetent indicar el nombre d'unitats, el preu mitjà i la localització.
RF16	Altres moviments d'articles	L'eina ha de permetre gestionar els moviments d'articles aliens al circuit de compres: entrades, sortides i traspàs entre magatzems. Això permet afegir o restar a l'estoc articles que han tingut moviments per causes diverses: trencaments, pèrdues, donatius, etc. També es registren traspassos entre magatzems per a mantenir actualitzat l'estoc a cadascun d'ells.
RF17	Articles	L'eina ha de permetre definir la informació rellevant dels articles (material d'oficina), així com el lligam amb els proveïdors que els subministren.
RF18	Famílies d'articles	L'eina ha de permetre establir la següent jerarquia: 1. Famílies d'articles 2. Subfamílies d'articles 3. Articles
RF19	Canvi de referència d'articles	L'eina ha de poder permetre canviar la posició d'un article a la jerarquia de famílies i subfamílies.
RF20	Importació d'articles des de fitxer extern	L'eina ha de poder importar la informació bàsica dels articles des d'un fitxer tipus CSV o Excel.
RF20	Consulta de l'historial de preus d'un article	L'eina ha de permetre consultar quins preus ha tingut un article concret, així com els pressupostos on s'ha inclòs i els proveïdors que n'ha tingut.
RF21	Parametrització dels tipus d'IVA	L'eina ha d'incloure la parametrització dels diferents tipus d'IVA aplicables.
RF22	Gestió dels proveïdors	L'eina ha d'incorporar la informació bàsica dels proveïdors, com ara: nom, adreça completa, telèfon, web, correu electrònic, així com la vinculació d'una o més persones de contacte per a cadascú.
RF23	Gestió dels pressupostos	• Cal afegir la possibilitat de consultar, visualitzar, generar, modificar i eliminar la informació dels diferents pressupostos rebuts dels proveïdors. Aquests poden ser

Codi	Requeriment	Descripció
		els diferents filtres de cerca: número de sol·licitud, jerarquia d'articles, proveïdor, data de sol·licitud, etc. • Cal tenir la possibilitat d'enviar correus als proveïdors amb la sol·licitud dels pressupostos, incloent assumpte, text, capçalera, peu, persona de contacte i d'altres detalls personalitzats.
RF24	Gestió dels contractes	Ha de poder mantenir actualitzada la informació sobre els contractes amb els proveïdors, incloent informació sobre l'expedient de contractació corresponent i els articles inclosos al contracte.
RF25	Recàlcul d'estocs	L'aplicació ha de permetre arreglar l'estoc quan els serveis retornen material o Serveis Interns torna material que no és correcte. És necessari que l'aplicació permeti entrades i sortides del magatzem sense haver de fer una comanda o una sol·licitud.
RF26	Característiques generals de les consultes	L'aplicació ha de permetre fer consultes: • Obertes (fent servir caràcters de tipus comodí) • No sensibles a majúscules/minúscules • Exportables a formats com a Excel i PDF
RF27	Consultes de sol·licituds	L'eina ha de permetre consultar la informació principal i l'estat de les sol·licituds mitjançant un ampli conjunt de filtres: número de sol·licitud, data d'alta, data de comanda, nom del proveïdor, estat de la sol·licitud (lliurada pel magatzem, comanda feta, servei en curs). També ha de poder mostrar el detall si així es requereix.
RF28	Consulta dels articles oferts	L'eina ha d'incloure la possibilitat de consultar la jerarquia d'articles, tot indicant els proveïdors per a cadascun dels articles que compleixin el criteri de cerca.

Codi	Requeriment	Descripció
		Possibles filtres de consulta: família, subfamília, article, entitat sol·licitant, interval de dates d'incorporació.
RF29	Consulta dels articles comprats	Permet consultar la jerarquia d'articles, tot indicant les sol·licituds on s'han demanat. Possibles filtres de consulta: família, subfamília, article, entitat sol·licitant, interval de dates de comanda.
RF30	Consulta dels articles rebuts pels serveis	Permet veure la relació d'articles rebuts per un servei concret. Possibles filtres addicionals de consulta: família, subfamília, article, interval de dates de sol·licitud.
RF31	Consulta dels articles rebuts per sol·licitant	Permet veure la relació d'articles rebuts per un sol·licitant (usuari). Possibles filtres addicionals de consulta: família, subfamília, article, interval de dates de comanda.
RF32	Consulta dels articles oferts per proveïdor	Permet veure la relació d'articles oferts per un proveïdor concret. Possibles filtres addicionals de consulta: família, subfamília, article, interval de dates de pressupost.
RF33	Consulta dels articles comprats per proveïdor	Permet veure la relació d'articles que s'han comprat a un proveïdor concret. Possibles filtres addicionals de consulta: família, subfamília, article, interval de dates de comanda, servei.
RF34	Consulta de l'inventari valorat	Permet veure la relació d'articles que hi ha al magatzem i veure el seu valor. Possibles filtres de consulta: família, subfamília, article.
RF35	Consulta d'aplicacions per tercer i servei	Permet veure les compres fetes per proveïdor i servei. Possibles filtres addicionals: import total, estat, exercici
RF36	Gestió de taules bàsiques i configuració	L'eina ha de permetre definir la següent informació bàsica (codi i descripció): • Països • Províncies • Municipis • Motius de rebuig de les sol·licituds.
RF37	Gestió de Serveis	L'eina ha de gestionar les dades bàsiques dels serveis que sol·liciten material, així com assignar els usuaris que hi pertanyen.
RF38	Gestió d'usuaris	L'eina ha de gestionar les dades bàsiques

Codi	Requeriment	Descripció
		dels usuaris, com per exemple: nom, correu electrònic, telèfon, observacions. Un usuari ha de pertànyer a un d'aquests perfils: a) Usuaris de serveis: sol·liciten i reben material. b) Usuari gestor: són els usuaris de Serveis Interns. Reben les sol·licituds de material, les centralitzen i adrecen al magatzem o inicien la tramitació de la compra. c) Usuari de magatzem: rep les sol·licituds de material de l'usuari gestor i lliura el material. d) Usuari administrador: encarregat de donar d'alta els usuaris de l'aplicació i d'altres tasques de configuració.

6 ETAPES I DOCUMENTACIÓ

L'adjudicatari lliurarà tota la documentació tècnica i de gestió del projecte, així com qualsevol altra documentació que l'AMB consideri necessària per satisfer l'objecte del contracte.

Durant l'execució del projecte es proposa seguir les etapes següents com a full de ruta general:

6.1 Llançament

L'objectiu de l'etapa de llançament és disposar d'un Pla de Projecte consensuat entre l'adjudicatari i l'AMB. El Pla de Projecte estarà basat amb el proposat per l'adjudicatari en la seva oferta i haurà de ser conforme als requisits especificats en aquest Plec.

El projecte es plantejarà per objectius, i hi haurà terminis de lliurament de les diverses tasques que s'hauran de desenvolupar.

Es formalitzarà un Comitè de Direcció de Projecte liderat per un responsable de l'AMB i format per responsables de l'AMB i de l'empresa adjudicatària.

Es formalitzarà una reunió tècnica de seguiment setmanal en la que es posarà en comú l'estat del projecte a nivell tècnic i econòmic. El cap d'equip de projecte de l'empresa adjudicatària reportarà l'estat de projecte, recolzat pels tècnics del seu equip que puguin aportar informació d'interès.

L'AMB es reserva el dret de variar aquest sistema de treball sempre que ho consideri necessari.

El Pla de Projecte ha d'incloure els següents apartats:

- Definició del projecte (objectius, abast, lliuraments...)
- Organització i gestió (Organigrama, equips de treball i requisits de gestió)
- Planificació (planificació i matriu de lliuraments): cal incloure un cronograma com a gràfic temporal de la durada del projecte per etapes i amb la descripció de les fases, ordre d'implantació, fites, punts crítics, proves que es duran a terme, etc.
- Pla de Gestió del Canvi: ha de contenir una descripció detallada de la gestió del procés de transformació i canvi que es durà a terme a AMB com a conseqüència de la implantació del projecte, amb l'objectiu de maximitzar els beneficis i minimitzar els impactes en els usuaris de l'aplicació.
- Recursos

També s'elaborarà el Pla de Riscos del projecte identificant els possibles riscos i problemes i proposant quan calgui accions correctives per a cadascun d'ells.

L'elaboració del Pla de Projecte i del Pla de Riscos serà responsabilitat de l'adjudicatari però es realitzarà conjuntament entre l'adjudicatari i l'AMB.

El Pla de Projecte i el Pla de Riscos hauran de ser aprovats pel Comitè de Direcció del Projecte. La formalització de la presentació del Pla de Projecte i del Pla de Riscos al personal involucrat en l'execució del projecte es farà en la Reunió de Llançament del projecte.

L'AMB haurà de validar i acceptar formalment la següent documentació abans de poder donar per tancada l'etapa de llançament del projecte:

- Pla de projecte
- Pla de riscos
- Acta de la reunió de llançament

6.2 Anàlisi i disseny

L'objectiu de l'etapa d'anàlisi i disseny és la identificació de tots els requisits tant funcionals com no funcionals del sistema, com de gestió documental, així com la definició de l'arquitectura tècnica sobre la qual es construirà el sistema.

En aquesta etapa del projecte és especialment rellevant l'elaboració d'una maqueta que inclogui les funcionalitats més importants del sistema per tal que l'usuari pugui validar-les.

Al finalitzar l'Etapa d'anàlisi i disseny es presentaran els següents productes i documentació per validar i acceptar formalment:

- Document de Requisits del sistema
- Document Glossari amb les definicions de tots aquells termes que cal que siguin detallats
- Document de Casos d'Ús del sistema i el seu flux d'esdeveniments
- Document d'Especificacions o requisits no funcionals del sistema
- Maqueta
- Document de l'Arquitectura del sistema
- Pla de Proves incloent-hi com a mínim les dels tipus:
    - Proves unitàries: Un cas de prova unitària per a classe de cas d'ús crític/principal
    - Proves d'integració: Un cas de prova d'integració per a cada requeriment d' integració
    - Proves de rendiment: Un cas de prova, com a mínim, per a cada requeriment de rendiment
    - Proves de qualitat de codi: Un cas de prova, com a mínim, per a cada requeriment de qualitat de codi

- Proves d'usabilitat: Un cas de prova, com a mínim, per a cada requeriment d'usabilitat
- Proves d'accessibilitat: Un cas de prova, com a mínim, per a cada requeriment d'accessibilitat
- Proves documentals: Un cas de prova, com a mínim, per a cada requeriment de gestió documental
- Proves de seguretat: S'hauran de dur a terme les proves de seguretat descrites a l'apartat de Seguretat inclòs en aquest plec
- Proves funcionals: Un cas de prova per a cada cas d'ús com a mínim. Cada escenari d'èxit ha de tenir associada, com a mínim, una prova, i cada escenari alternatiu, com a mínim, una prova
- Proves d'acceptació d'usuari (UAT): Un cas de prova per a cada requeriment funcional

A partir del Pla de Proves, durant l'etapa de construcció s'han de definir els casos de prova, executar i informar dels resultats.

Com a resultat de l'execució de les proves, es realitzarà un informe del resultat de l'execució de les proves i es presentarà a l'AMB per a la seva consideració i validació en cas que ho consideri necessari.

És responsabilitat de l'adjudicatari la generació de jocs de dades de proves per tal de realitzar proves en entorns de proves i desenvolupament i de preproducció.

6.3 Construcció

L'objectiu d'aquesta etapa és la construcció del sistema. En aquesta etapa es realitzarà un desenvolupament iteratiu. Les duracions de les iteracions s'establiran a la fase de llançament.

S'haurà d'elaborar el document de disseny tècnic que inclogui els dissenys de base de dades. Aquesta documentació ha d'incloure el lliurament de diagrames en fitxer (format estàndard importable des d'eines de modelatge).

Amb cada iteració s'actualitzarà el Pla de Proves, tot incloent la definició dels casos de prova corresponents a les funcionalitats afegides. Es realitzarà l'informe del resultat de l'execució juntament amb l'enregistrament dels resultats obtinguts. Com a prova d'aquest enregistrament es pot utilitzar:

- Fitxer de resultats generat per l'aplicació d'execució de proves
- Fitxer log de l'aplicació
- Captura de finestres amb el resultat de les proves

Aquests resultats es presentaran després de cada iteració a l'AMB per a la seva avaluació i validació. Aquesta validació serà necessària per a poder donar per tancada cada iteració i poder començar l'execució de la següent.

Abans de tancar cada iteració es presentarà la documentació tècnica de cada iteració:

- Document de Disseny Tècnic

L'adjudicatari serà responsable del disseny del Pla de Proves i de l'execució d'aquestes. Per a la validació de cada etapa d'iteració del projecte caldrà que l'adjudicatari lliuri el document amb el resultat d'haver passat de forma satisfactòria les proves realitzades sobre l'aplicació.

Al finalitzar l'etapa de construcció l'adjudicatari presentarà a l'AMB els següents productes i documentació per a la seva validació i acceptació formal abans de passar a l'Etapa de Transició:

- Disseny Tècnic
- Pla de Proves actualitzat amb el resultat de els següents tipus de proves:
    - Unitàries
    - D'integració
    - Funcionals
    - De càrrega (estrès)
- Programari corresponent a l'aplicació
- Programari corresponent als casos de prova (unitàries i integració)

El programari dels casos de proves unitàries ha de lliurar-se separadament del corresponent a l'aplicació i s'ha de poder executar de manera independent.

6.4 Proves

Les proves de validació es realitzaran sobre l'entorn de proves de

preproducció, on posteriorment les validarà l'usuari. Serà responsabilitat de l'adjudicatari la preparació dels jocs de prova i habilitar els entorns corresponents per a les proves funcionals, així com els perfils i usuaris necessaris per executar aquests plans de proves.

No es passarà a les proves d'usuari fins que l'AMB no validi en la seva totalitat el seu correcte funcionament com a usuari pilot.

Les activitats de proves definides en aquest apartat s'hauran d'ajustar a les re-planificacions que puguin esdevenir-se en el projecte, reajustant els equips dedicats sempre que sigui necessari per a canvis o imprevistos en el calendari d'implantació.

Abans de l'execució de les proves s'hauran de realitzar com a mínim les següents activitats:

- El coneixement dels requeriments d'usuari és de vital importància per una correcta planificació del Pla de proves. En l'etapa de requeriments s'inicia l'elaboració del model jeràrquic de requeriments de prova partint dels processos funcionals als quals donen cobertura els diferents actius de programari a avaluar.

- En l'etapa d'elaboració, l'adjudicatari realitzarà el disseny del Pla de proves funcionals, identificant, acordant i especificant els atributs i característiques de qualitat que s'han de provar. L'objectiu és dissenyar les proves amb la probabilitat de trobar un major nombre de defectes amb la mínima quantitat d'esforç i temps, demostrant que les funcionalitats són operatives, que l'entrada de dades s'accepta de forma correcta i que els resultats esperats són els correctes.

- Verificarà que s'han identificat i definit els casos de prova necessaris per a garantir les funcionalitats dels processos funcionals definits, pels quals es detallaran accions a realitzar i per a cadascun dels casos s'associarà el seu resultat esperat que podrà ser verificat. Durant aquesta mateixa etapa, s'especifiquen també les dades d'entrada necessàries perquè els casos de prova definits puguin ser executats, ja sigui buscant l'èxit del resultat o bé l'error.

- Es realitzarà l'execució dels casos de prova anteriorment dissenyats de forma manual seguint el detall del guió establert. L'analista que executi les proves ha de disposar de certa llibertat i autonomia per detectar situacions anòmales no contemplades.

- Es guardarà un llistat detallat dels errors trobats en l'execució dels casos de prova i de la seva correcció.

- Es repetirà la bateria de proves tantes vegades com s'estimi necessari fins a l'obtenció del resultat correcte.

- La gestió d'incidències és una part implícita de l'etapa d'execució i de rellevant importància en les proves funcionals essent el canal de comunicació amb l'equip de desenvolupament.

Quan al realitzar una prova no s'obtingui el resultat esperat s'haurà d'obrir o reportar una incidència perquè l'equip de desenvolupament tingui constància de l'error. La comunicació d'incidències ha de ser amb un grau elevat de detall perquè l'equip de desenvolupament tingui prou informació per comprendre l'error, reproduir-lo, localitzar-lo i poder solucionar-lo.

S'haurà de mantenir un continu canal de comunicació obert amb l'equip de desenvolupament per conèixer l'estat dels defectes i poder realitzar novament les proves necessàries pel seu tancament.

L'adjudicatari haurà de proposar una aplicació, com a sistema de test per a les proves funcionals garantint la qualitat del programari desenvolupat.

Descriurà les propostes tècniques en quant a eines de treball pels Serveis de Qualitat respecte a l'execució de plans de proves, verificació de qualitat de productes i gestió d'incidències.

Sempre, i en tot cas, s'haurà de lliurar un Informe del Resultat de l'Execució de les proves, juntament amb l'enregistrament dels resultats de cada prova (possibles opcions: fitxer de resultats generat per una aplicació de testing, lliurament d'un fitxer log, captura de finestres amb el resultat de les proves...).

Aquestes tasques seran supervisades i validades en primera instància per AMB.

La definició i execució del Pla de proves serà validat definitivament pel Comitè de direcció del projecte i requerirà de la seva aprovació per a ser admès.

L'informe contindrà, com a mínim, els següents elements:

- Identificació i descripció de la prova

- Identificació i especificació dels atributs i característiques de qualitat que composen la prova

- Resultat de la prova, especificant si aquest és satisfactori o no, incloent les observacions que es considerin necessàries per justificar el resultat

- Informe d'incidències en què haurà d'especificar-se com a mínim descripció de la incidència, data d'obertura, data resolució, responsable. Aquest informe haurà d'estar actualitzat diàriament i s'utilitzarà per al seguiment d'iteracions de les proves

Abans de passar a l'etapa d'implantació, per tant com a mínim a l'última iteració prevista del producte, caldrà que l'AMB validi el sistema construït amb la verificació dels resultats obtinguts en l'execució de totes les proves previstes al Pla de Proves.

6.5 Migració

Abans de la implantació de cadascun del mòduls funcionals es procedirà a la migració de les dades actualment existents amb l'objectiu de donar continuïtat al servei.

Serà responsabilitat de l'adjudicatari confeccionar i lliurar el Pla de migració per la seva aprovació. S'analitzaran totes les dades disponibles en origen amb l'objectiu de migrar-les totes i minimitzar la pèrdua d'informació. Aquelles dades que no es requereixin per a la pròpia gestió del servei amb la nova aplicació es consideraran posar-les disponibles en un mòdul de consulta de l'històric. Les dades corresponents a procediments i actes administratius s'han de conservar d'acord als requeriments de gestió documental, segons l'etapa del cicle de vida, i s'han de valorar i conservar d'acord a les taules d'avaluació documental.

L'abast de les dades que s'hauran de migrar son les emmagatzemades a la base de dades de l'aplicació actual, SCAP Compres, a més de totes aquelles dades que es disposen en altres suports com fulls de càlculs, fitxers ASCII i altres contenidors de dades.

L'equip tècnic d'AMB es comprometrà a lliurar en un format d'intercanvi estàndard les dades del projecte que s'acordin migrar per a ser carregades a la nova plataforma abans de l'etapa d'implantació. Les dades de l'aplicació actual que es considera imprescindible migrar són:

- Proveïdors
- Famílies / Subfamílies / Articles
- Estoc del(s) magatzem(s)
- Moviments "vius" de material

Serà responsabilitat de l'adjudicatari desenvolupar els procediments de carrega de les dades al nou entorn.

6.6 Implantació

L'objectiu d'aquesta etapa és la finalització del projecte. Prèviament al seu tancament i dins d'aquesta darrera etapa, es realitzaran les següents tasques:

- Validació de tot el sistema per part de l'usuari
- Execució del Pla de Gestió del Canvi previst i aprovat a l'etapa anterior:
    - Comunicació del calendari de desplegament del sistema
    - Formació del personal: el pla de formació sobre l'ús de l'aplicació informàtica ha de ser prou detallat per a valorar la seva adequació als diferents tipus d'usuari de l'aplicació (sol·licitants de material, usuaris gestors de Serveis Interns, usuari tècnic informàtic / administrador) i les funcions que corresponen a cadascun d'ells.
    - Desplegament a Producció
    - Suport a Usuaris
- Lliurament de la documentació del sistema:
    - Descripció funcional
    - Descripció tècnica
    - Manual d'usuari
    - Manual tècnic o d'administració

6.7 Lliuraments

A continuació es fa un llistat exhaustiu de tots els lliuraments que s'hauran de tenir en compte durant el projecte i que seran requerits per part de l'AMB:

- Document de llançament del projecte
- Pla de projecte
- Acta de constitució del projecte

- Actes de seguiment de projecte
- Acta de certificació i acceptació dels lliurables
- Acta de tancament de projecte
- Document de planificació del projecte
- Documents d'anàlisi funcional
- Documents de disseny tècnic
- Anàlisi i seguiment de riscos
- Codi font de les personalitzacions del producte
- Pla de proves complert
- Informe de grau de cobertura de proves automàtiques
- Proves d'integració amb altres components/sistemes
- Proves de càrrega, concurrència i rendiment
- Informe de revisió de les proves
- Document d'anàlisi de vulnerabilitats
- Pla de qualitat del projecte
- Pla de migració de les dades
- Pla de gestió del canvi
- Pla de desplegament
- Pla de comunicació del projecte
- Pla de formació
- Pla de suport a usuaris
- Document de valoració d'impacte sobre privacitat
- Manual d'explotació
- Manual d'usuari

- Diccionari de dades

7 REQUERIMENTS TECNOLÒGICS

7.1 Seguretat de l'aplicació

7.1.1 Compliment normatiu

Atès que AMB desenvolupa la seva activitat amb informació que pot ser de caràcter confidencial i es tractaran dades personals, s'haurà d'acomplir amb les mesures definides a l'Esquema Nacional de Seguretat, les guies del CCN-CERT i les establertes a l'inici del projecte segons el nivell de risc sobre les dades personals i segons l'avaluació d'impacte que l'adjudicatari haurà de realitzar de forma prèvia al desenvolupament amb el recolzament d'AMB.

S'hauran de tenir en compte entre altres els següents punts:

- Alta d'usuaris: la creació d'usuaris ha de ser nominal i individual, i no hi ha d'haver usuaris genèrics amb accés a dades.

- Identificació i autenticació d'usuaris: S'haurà de fer mitjançant al menys identificador i contrasenya, d'acord amb la política de contrasenyes definida per l'AMB (de qualitat, conservació xifrada, etc.) amb la previsió d'autenticació per doble factor d'autenticació o certificat digital i/o contrasenya temporal generada per a cada accés concret.

- Perfils d'usuari: Cal establir els perfils (consulta/modificació) o jerarquies d'accés necessàries que garanteixin que els usuaris tenen accés estrictament a la informació que correspon al seu lloc de treball.

- Entorns de desenvolupament: En els entorns de desenvolupament/ integració/preproducció que puguin ser alimentats amb dades reals, caldrà aplicar un procés de dissociació de dades personals (opció recomanable) o bé – prèvia autorització – fer ús de dades reals aplicant les mateixes mesures tècniques que a l'entorn productiu.

- Registre d'accessos: s'haurà de poder registrar els accessos d'usuaris amb, com a mínim la següent informació: usuari, data/hora, registre accedit, si l'accés ha estat autoritzat o no i el tipus d'accés (consulta, modificació, supressió). El format del registre serà marcat per part d'AMB per integrar-lo dins del sistema d'anàlisi disponible.

7.1.2 Control d'accés

Es detallen a continuació els requisits mínims de seguretat que cal considerar en la confecció del control d'accés:

- Ocultació de missatges d'error: per tal d'exposar el mínim d'informació a possibles atacants es recomana:
    - No mostrar els errors per defecte que pugui generar el servidor, ja que proporciona informació valuosa per als atacants sobre la tecnologia utilitzada.
    - En cas d'intent de login fallit, no indiqueu si falla el nom d'usuari o contrasenya, per no donar confirmació d'un nom d'usuari vàlid sobre el qual efectuar atacs per força bruta.
- Complexitat de contrasenyes: cal exigir una longitud mínima de contrasenya de 12 posicions, que imposi certs requisits de complexitat, com l'obligatorietat d'utilitzar com a mínim majúscules/minúscules/dígits/caràcters. No es podran repetir les darreres contrasenyes segons el valor màxim permès pel sistema operatiu.
- Modificació de contrasenyes: l'usuari haurà de poder modificar la contrasenya en qualsevol moment un cop hagi accedit al sistema.
- Recuperació de contrasenyes: utilitzar un mecanisme de recuperació segura de contrasenyes, per exemple, afegint preguntes de seguretat al moment del registre, de manera que s'eviti la intervenció del personal administrador en la majoria de casos.
- Notificació del canvi de contrasenya: a través del correu electrònic amb l'objectiu que l'usuari detecti qualsevol anomalia amb l'accés al seu compte.
- Tancament de sessió: Cal tancar les sessions per inactivitat de més de 60 minuts.

7.1.3 Desenvolupament segur

La construcció de l'aplicació garantirà el desenvolupament segur, segons el cicle de vida model "Secure SDLC", per trobar i corregir les vulnerabilitats potencials el més aviat possible.

Com a mínim haurà de centrar-se a cobrir les vulnerabilitats recollides al top 10

d'OWASP (Open Web Application Security Project):

- **Fallades al control d'accés**

Les API tendeixen a exposar punts finals que tracten identificadors d´objectes, creant un problema de control d'accés de nivell de superfície d'atac ampli. Les verificacions d'autorització a nivell d'objecte s'han de considerar a cada funció que accedeix a una font de dades utilitzant una entrada de l'usuari.

- **Falles criptogràfiques**

Aquesta categoria sistematitza les fallades vinculades amb la criptografia, que poden arribar a exposar dades sensibles i comprometre els sistemes en la seva totalitat.

Es tracten, doncs, de vulnerabilitats vinculades a l'absència de protocols de comunicacions segurs. És a dir, xifrats. L'arrel d'aquest problema es troba en la utilització de:

- Esquemes de xifratge obsolets i/o insegurs
- Claus de xifratge febles
- Usar algorismes de xifrat forts i plenament actualitzats

- **Injecció**

Les falles d'injecció, com SQL, NoSQL, injecció d'ordres, etc., ocorren quan s'envien dades que no són de confiança a un intèrpret com a part d'una ordre o consulta. Les dades malicioses de l'atacant poden enganyar l'intèrpret perquè executi ordres no desitjades o accedeixi a dades sense la deguda autorització.

La millor manera de mitigar aquest tipus de debilitats és seguint els consells següents:

- Fer ús de les funcions incloses a la pròpia API o al framework de l'aplicació. Per, així, vincular de manera segura els paràmetres d´entrada proporcionats per l´usuari.
- Si l'opció 1 no es pot implementar, cal implementar del costat del servidor els filtres adequats als valors proporcionats pels usuaris. De

manera que es garanteixi que no poden alterar de manera inesperada el comportament de les accions dutes a terme per l'aplicació.

- **Disseny insegur**

Engloba els diferents riscos associats als defectes de disseny i arquitectura web o el que és el mateix, aplega el conjunt de debilitats derivades de l'absència de l'aplicació de metodologies de disseny segur.

- **Configuració de seguretat incorrecta**

La configuració incorrecta de la seguretat sol ser el resultat de configuracions predeterminades no segures, configuracions incompletes o ad-hoc, emmagatzematge al núvol obert, encapçalats HTTP mal configurats, mètodes HTTP innecessaris, ús compartit de recursos d'origen creuat (CORS) permissiu i missatges d´error detallats que contenen informació confidencial.

Hu ha quatre accions bàsiques per mitigar les vulnerabilitats de configuració incorrecta de la seguretat:

- Posar en marxa un procés de maquinari. Mitjançant aquest es poden aplicar configuracions adequades sobre tots els components de l'arquitectura.
- Realitzar, tant com sigui possible, una segmentació entre els diferents components de l'arquitectura web. Així es pot evitar que una vulnerabilitat que s'origina en un pugui donar lloc a moviments laterals dels atacants i afectar altres components.
- Aplicar directives de seguretat que apostin per una defensa en profunditat dels components.
- Revisar tota la documentació sobre bones pràctiques de seguretat relacionada amb els diferents elements que componen l'arquitectura.

- **Components vulnerables i obsolets**

Aquest tipus de vulnerabilitats s'origina per la utilització de programari o components dins d'una aplicació o infraestructura web obsolets o amb vulnerabilitats conegudes.

Per mitigar aquesta vulnerabilitat, una organització pot apostar per DevSecOps, un enfocament de gestió centrat a monitoritzar, analitzar i aplicar mesures de seguretat a totes les etapes de la vida útil d'un programari.

D'aquesta manera es garantiria que, de manera permanent, s'avaluen els components que conformen la infraestructura de l'aplicació web i s'implementen les mesures de seguretat necessàries per evitar que siguin vulnerables o quedin obsolets.

- **Fallades d'identificació i autenticació.**

Aquesta categoria tan important engloba les vulnerabilitats que permetrien o facilitarien la suplantació de la identitat dels usuaris, com a conseqüència d'una gestió incorrecta dels identificadors de sessió, o dels elements vinculats amb l'autenticació a l'aplicació. Entre les fallades d'identificació i autenticació més rellevants podem destacar:

- L'absència o implementació incorrecta de múltiples factors d'autenticació
- Processos insegurs de recuperació de credencials
- Escasses mesures contra atacs de força bruta
- Incorrecta renovació dels identificadors de sessió per a cada autenticació vàlida

S'evitarà que el servidor permeti l'accés a la informació i els documents per vies alternatives al protocol determinat.

- **Errors en el programari i la integritat de dades**

Aquest tipus de fallades estan vinculades amb la manca de protecció del codi i la infraestructura davant de les violacions de la integritat i serveix per posar el focus en debilitats relacionades amb:

- Atacs maliciosos a les supply chains de programari
- Plugins, biblioteques, repositoris i xarxes de lliurament de contingut no fiables

- Canals CI/CD insegurs, a través dels quals es poden introduir codis maliciosos o comprometre el sistema
- Funcionalitats d'auto-actualització en què les actualitzacions es descarreguen sense comptar prèviament amb un sistema segur de verificació de la integritat. A través d'aquesta via d'accés, els ciberdelinqüents poden pujar les pròpies actualitzacions malicioses per distribuir-les i executar-les a totes les instal·lacions

- **Errors en el registre i la supervisió de la seguretat**

La traçabilitat dels esdeveniments que tenen lloc a l'aplicació és essencial. En primer lloc, per bloquejar amenaces i, en segon lloc, per investigar incidents de seguretat que hagin tingut lloc i, així, evitar que es tornin a produir i poder concretar quins possibles actius s'han vist compromesos.

Les fallades al registre, la detecció, la supervisió i la resposta activa davant dels atacs es poden produir quan:

- Els esdeveniments auditables, com ara els inicis de sessió o les transaccions d'alt valor, no es registren
- Els advertiments i els errors no generen missatges de registre o són inadequats
- Els registres de les aplicacions i les API no se supervisen
- Els registres només s'emmagatzemen localment
- Les proves de penetració no activen les alertes de seguretat
- L'aplicació web és incapaç de detectar, escalar i alertar atacs a temps real

- **Falsificació de sol·licituds del costat del servidor**

Aquest tipus de vulnerabilitats es produeixen quan un atacant té la possibilitat de forçar el servidor a fer connexions cap a objectius que no estaven previstos inicialment. D'aquesta manera, l'atacant aprofita la posició privilegiada del servidor a la infraestructura per a:

- Evadir tallafocs
- Forçar connexions a elements de la xarxa interna

- Interactuar amb recursos que inicialment eren restringits

Per prevenir aquest tipus de riscos de seguretat, els desenvolupadors han de posar en marxa controls de defensa a les capes de xarxa i d'aplicació. Pel que fa a la primera es pot:

- Segmentar l'accés a recursos remots a les xarxes separades
- Aplicar polítiques de tallafocs de denegació per defecte o regles de control d'accés per bloquejar el trànsit de la intranet que no sigui essencial
- Es previndran intents d'escalada de privilegis

Mentre que pel que fa a la capa d'aplicació cal:

- Sanejar i validar les dades d'entrada subministrades pel client
- Fer complir l'esquema, el port i el domini amb una llista blanca de valors permesos
- Impedir l'enviament de respostes als clients sense un tractament previ de la informació
- Desactivar les redireccions HTTP
- Garantir la consistència de la URL per evitar atacs, entre altres, els atacs de manipulació de la URL
- Es previndran atacs per manipulació de fragments d'informació (cookies) emmagatzemats als navegadors
- Impedir els atacs per injecció de codi
- Es previndran atacs de "cross site scripting"