



PLEC DE PRESCRIPCIONS TEQUQUES QUE REGEIXEN CONTRACTE DEL SERVEI D'ALLOTJAMENT WEB ADMINISTRAT PEL MUSEU PICASSO DE BARCELONA.

1. OBJECTE

El present contracte de serveis té per objecte la contractació del servei l'allotjament (hosting) del web administrat pel Museu Picasso (<https://museupicassobcn.cat>).

El present document defineix el **plec tècnic per a la infraestructura i plataforma del servei web del Museu Picasso de Barcelona**, amb l'objectiu de garantir un servei **estable, segur, escalable i altament disponible** per als visitants i usuaris. L'abast del projecte inclou la **modernització, optimització i seguretat de la plataforma web**, amb especial atenció, al **rendiment del lloc web** i la **protecció davant de ciberamenaces**.

El Museu Picasso de Barcelona és un dels espais culturals més visitats de la ciutat, amb **milions de visites anuals** tant presencials com a través del seu portal web. L'experiència digital és clau per **atraure visitants, facilitar la compra d'entrades, oferir informació sobre la col·lecció i sobre les exposicions temporals i millorar la interacció amb el públic**. Per això, la seva infraestructura tecnològica ha de garantir un servei **àgil, segur i accessible** per a tot tipus d'usuaris i dispositius.

En qualsevol cas, l'objecte d'aquest plec és garantir el servei descrit mantenint sempre la url del web del Museu Picasso: www.museupicassobcn.cat

L'**objectiu** principal d'aquest plec és **definir els requisits tècnics i operatius** per assegurar que el servei web del Museu Picasso sigui:

- **Altament disponible:** Arquitectura redundada i escalable per gestionar pics de trànsit.
- **Segur i conforme a normatives:** Compliment estricte del **RGPD, LOPD-GDD, ENS i NIS2**.
- **Escalable:** Adaptació a l'augment del trànsit i creixement del Museu a curt i mig termini.
- **Fàcil de gestionar i mantenir:** Plataforma robusta amb gestió eficient d'incidències i actualitzacions.

El projecte **inclou** la definició i implantació de millores en els següents àmbits:

1. Infraestructura tècnica i allotjament

- Migració i optimització del **hosting (Cloud VPS gestionat)** amb alta disponibilitat.
- Separació de serveis web i base de dades i arquitectura de preproducció per millorar rendiment.
- Balanceig de càrrega i CDN per optimització del trànsit web.

2. Arquitectura de la xarxa i seguretat

- Implementació de **WAF (Web Application Firewall) i protecció contra DDoS**.
- Xifratge avançat **TLS 1.3 i HTTP/3** per connexions segures.



- Protecció avançada del DNS.

3. Compliment normatiu i seguretat de dades

- **RGPD, LOPD-GDD, ENS i NIS2** per garantir la privacitat i seguretat.

5. Monitorització i gestió d'incidències

- **Supervisió 24/7** amb temps de resposta definit per SLA.
- **Sistema de detecció d'incidents i resposta automatitzada.**
- Pla de **recuperació davant de desastres** amb backups en temps real.

L'actual infraestructura del Museu Picasso consta de servidors virtuals gestionats actualment amb tecnologia Linux i base de dades PostgreSQL-SOLR. Aquesta configuració presenta limitacions en escalabilitat i rendiment, i no disposa de mecanismes avançats de protecció contra ciberamenaces.

Per això, es proposa una modernització de l'arquitectura tecnològica a curt i mig termini, incloent:

- **Infraestructura cloud escalable amb balanceig de càrrega.**
- **Integració d'un CDN i mecanismes de caché per optimització del rendiment.**
- **Implementació de polítiques de seguretat avançades i encriptació de dades.**

2. ANTECEDENTS. SOLUCIÓ ACTUAL DE QUE DISPOSA EL MUSEU PICASSO DE BARCELONA

Actualment el **Museu Picasso de Barcelona** disposa d'una infraestructura allotjada en un proveïdor de serveis **PaaS (Platform as a Service)**. Aquesta configuració consta de:

Per a la plataforma de producció:

- **1 servidor web** dedicat a allotjar el lloc web principal i gestionar continguts dinàmics i estàtics.
 - **2 vCPU** (Intel Xeon de 2.0 a 2.4 GHz)
 - **4 GB de RAM**
 - **50 GB de disc**
 - **Sistema operatiu: Linux**
- **1 servidor combinat per a serveis web, base de dades i SOLR** (cercador de continguts avançat).
 - **2 vCPU** (Intel Xeon de 2.0 a 2.4 GHz)
 - **4 GB de RAM**
 - **50 GB de disc**
 - **Sistema operatiu: Linux**

Per a la plataforma de preproducció:

- **1 servidor combinat per a serveis web, base de dades i SOLR**
 - **2 vCPU** (Intel Xeon de 2.0 a 2.4 GHz)



- **6 GB de RAM**
- **50 GB de disc**
- **Sistema operatiu: Linux**

L'actual infraestructura presenta **diversos punts destacables:**

- **Infraestructura en un ISP de confiança**
- **Presència a Internet ben configurada** (amb protecció SPF i DMARC per correu).
- **Xifratge SSL/TLS actualitzat** amb suport per **TLS 1.2 i TLS 1.3** (DigiCert - Thawte).

Es tracta d'una Infraestructura optimitzada basada en servidors Cloud gestionats

Limitacions detectades:

- **Infraestructura monolítica:** Un sol servidor per a web, base de dades i SOLR genera dependències i pot afectar el rendiment.
- **Escalabilitat limitada:** L'actual configuració no permet escalar fàcilment en cas de pics de trànsit.
- **Baixa tolerància a fallades:** No hi ha mecanismes de redundància ni balanceig de càrrega.
- **Recursos insuficients a mitjà termini:** 4GB de RAM pot ser insuficient per gestionar un volum elevat de consultes i continguts multimèdia.

Per garantir la compatibilitat del projecte, a continuació es detalla la tecnologia actual del web:

Plataforma de Gestió de Continguts (CMS)

- **Drupal (versió 9)**
 - CMS de codi obert robust i escalable, adequat per a la gestió de continguts dinàmics i gran volum de visites.
 - Permet la personalització i integració amb altres serveis externs.
 - Requereix manteniment regular i actualitzacions per seguretat i rendiment.

Llenguatges de programació

- **PHP**
 - Llenguatge principal per al back-end del CMS Drupal.
 - Necessita un servidor amb suport PHP actualitzat per seguretat i compatibilitat.

Frameworks

- **Bootstrap (versió 5.2.0)**
 - Utilitzat per al disseny responsiu i l'estructura del front-end.
 - Facilita la compatibilitat amb dispositius mòbils i millora l'experiència d'usuari (UX).
- **GSAP**
 - Llibreria d'animacions avançades per a una experiència d'usuari més dinàmica.

Biblioteques JavaScript

- **jQuery (versió 3.6.3)**
 - Llibreria per a la manipulació DOM i efectes visuals.
- **core-js (versió 3.21.1)**
 - Compatibilitat amb funcionalitats modernes de JavaScript.

- **DataTables (versió 1.11.3)**
 - Millora la presentació i interacció amb taules de dades.
- **ScrollMagic (versió 2.0.8)**
 - Control d'animacions i efectes en el desplaçament de la pàgina.
- **Tiny Slider**
 - Eina per a sliders i carrousels d'imatges.
- **Splide**
 - Llibreria lleugera per a la gestió de galeries i sliders d'imatges.
- **AOS (Animate On Scroll)**
 - Biblioteca per a efectes d'animació quan els elements es fan visibles en desplaçar-se.

Publicitat i Analítica Web

- **Google Ads**
 - Plataforma de publicitat en línia per a la promoció del museu.
- **Google Analytics (GA4)**
 - Monitorització i anàlisi del trànsit web i comportament d'usuaris.

Fonts i Tipografia Web

- **Google Font API**
 - Ús de fonts personalitzades mitjançant la plataforma de Google.

Certificació de Seguretat i Protocol HTTPS

- **SSL/TLS certificat per Thawte**
 - Proporciona seguretat en la transmissió de dades entre el servidor i els usuaris.
 - Necessari per garantir el xifratge de les comunicacions i el compliment normatiu (RGPD).

3. REQUISITS GENERALS DE LA PLATAFORMA

Ateses les limitacions referides, la solució a contractar haurà de complir amb els **requisits generals de la infraestructura i la plataforma tecnològica** del servei web del **Museu Picasso de Barcelona**, asseguraran que sigui escalable, segura i eficient per donar suport al volum de trànsit i a les transaccions de venda d'entrades.

L'allotjament web serà **administrat i gestionat per un proveïdor especialitzat**, amb un **alt nivell de disponibilitat, seguretat i redundància**, garantint així un **rendiment òptim i la protecció de les dades** dels visitants i usuaris.

L'allotjament web inclourà:

- **Infraestructura de centre de dades**
 - Ubicació **dins la Unió Europea**, complint amb la **Reglamentació General de Protecció de Dades (RGPD)**.
 - Provisió de **servidors, elements de xarxa i mecanismes de seguretat** per garantir un funcionament estable i segur.
 - Redundància i alta disponibilitat per evitar interrupcions del servei.
 - Connexió amb **amplada de banda garantida** per suportar alts volums de trànsit sense degradació del rendiment.
- **Gestió i monitorització**
 - Operació i administració de la infraestructura del centre de dades i els servidors.
 - **Monitorització 24/7 del rendiment i la seguretat** per detectar i mitigar incidències de manera proactiva.

- **Alertes i mecanismes de resposta ràpida** davant caigudes del servei o atacs de ciberseguretat.
- **Suport tècnic**
 - Servei d'atenció i suport tècnic especialitzat amb temps de resposta definits segons SLA.
 - Assistència en la resolució d'incidències, aplicació d'actualitzacions i optimització del servei.

La infraestructura del servidor web serà robusta i escalable, incorporant serveis essencials com **seguretat, comunicacions i còpies de seguretat**.

Per garantir un **servei estable i escalable**, s'han de considerar els següents requeriments de hardware:

- **Arquitectura del servidor**
 - Amb garanties **d'alta disponibilitat i distribució de càrrega**.
 - Amb **una arquitectura en cloud amb autoescalabilitat** segons el trànsit.
- **Emmagatzematge i continguts multimèdia**
 - **Integració amb un servei** per allotjar i servir continguts estàtics (imatges, vídeos, documents).
 - **L'espai actual utilitzat del disc dur és de 42,6GB**, però ha de permetre expansió segons el creixement del museu.
- **Sistema de backup i recuperació**
 - **Backups diaris automatitzats** amb capacitat mínima per assegurar la disponibilitat de dades en cas de fallida.
 - Els backups s'han de desar en **una ubicació externa xifrada** per garantir la seguretat i recuperació en cas de desastre.

El sistema ha d'implementar **mesures de seguretat avançades** per protegir-se d'amenaques cibernètiques i complir amb la normativa vigent.

- **Protecció contra atacs i seguretat web**
 - Firewall i sistemes de detecció d'intrusions (IDS/IPS).
 - Protecció contra **DDoS** per evitar interrupcions del servei.
 - Certificat **SSL/TLS** amb protocols que garanteixin una connexió segura.
 - **Autenticació de doble factor (2FA)** per als accessos administratius.
- **Compliment normatiu**
 - Adaptació a la **Reglamentació General de Protecció de Dades (RGPD)** i **LOPD-GDD** per la gestió de dades personals així com la l'ENS i NIS2.
- **Escalabilitat**
 - La infraestructura ha de permetre l'escalabilitat vertical i horitzontal per adaptar-se a pics de trànsit durant exposicions especials o campanyes de venda d'entrades.
 - Integració amb un servei **CDN (Content Delivery Network)** per millorar la velocitat de càrrega i rendiment global.
- **Optimització de rendiment**
 - ús de **caché a nivell de servidor** per reduir la càrrega del servidor de

bases de dades.

- Minificació de codi i compressió per optimitzar el temps de resposta de la web.

4. DISPONIBILITAT, ESCALABILITAT I REDUNDÀNCIA

La solució oferirà una infraestructura basada en **alta disponibilitat, escalabilitat automàtica i redundància** garantirà un servei web robust i eficient per al Museu Picasso. La combinació de **balanceig de càrrega, base de dades replicada, emmagatzematge segur i eines d'anàlisi** assegura que el sistema pugui créixer segons les necessitats futures sense interrupcions ni pèrdua de rendiment.

Objectius de disponibilitat:

- **Disponibilitat mínima del 99,95%** anual per assegurar un servei ininterromput.
- Reducció de **temps d'inactivitat no planificat** mitjançant mesures preventives.
- **Monitorització 24/7** per detectar i solucionar incidències de manera proactiva.
- Definició d'un **SLA (Service Level Agreement)** amb temps nivell de resposta mínim segons el següent quadre:

Tipus d'incidència	Nivell de resposta mínim
Crítica (Caiguda del servei web, fallada del servidor, atac de ciberseguretat actiu amb afectació a la venda d'entrades)	RTO: 12h, RPO: 30 dies
Alta (Ralentització significativa del servei, fallada en la base de dades, problema greu de seguretat que no afecta a la venda d'entrades)	RTO: 48h, RPO: 30 dies
Mitjana (Error parcial en el funcionament web que no afecta la venda d'entrades)	RTO: 72h, RPO: 30 dies
Baixa (Peticions de millora, ajustaments no urgents que no afecten a la venda d'entrades)	RTO: 1 setmana, RPO: 30 dies

Estratègies per garantir la disponibilitat:

- Implementació d'un **balanceig de càrrega** entre diversos servidors per distribuir el trànsit i evitar sobrecàrregues.
- Utilització d'un **sistema de failover** per garantir la continuïtat del servei en cas de fallada d'un servidor.
- Còpies de seguretat automatitzades i testades periòdicament per garantir una recuperació ràpida.
- Integració amb un **sistema de CDN (Content Delivery Network)** per distribuir continguts estàtics i reduir la càrrega del servidor principal.
- Plans de **recuperació davant de desastres (DRP - Disaster Recovery Plan)** per minimitzar l'impacte d'incidències crítiques.

El nombre de visitants del Museu Picasso és elevat i varia segons la temporada, amb pics durant **exposicions especials, promocions i esdeveniments culturals**. Per aquest motiu, la infraestructura ha de ser **escalable**, permetent ajustar els recursos segons la demanda.

Requisits d'escalabilitat:

- **Escalabilitat vertical:**
 - Augment de recursos (CPU, RAM, emmagatzematge) segons les necessitats puntuals.
 - Configuració de servidors en cloud que permetin l'escalabilitat automàtica.
- **Utilització d'una base de dades escalable:**
 - PostgreSQL/PostGIS ha de permetre la replicació i distribució de càrrega per evitar colls d'ampolla.
 - Implementació de tècniques de particionament de bases de dades per millorar el rendiment en consultes de gran volum.
- **Ús de tecnologies de caché (Redis o Memcached)** per reduir càrrega de peticions al servidor i millorar la velocitat de resposta.

La redundància garanteix que, **en cas de fallida d'un component**, el servei es mantingui operatiu. Això inclou mecanismes de **redundància de servidors, xarxa i emmagatzematge**.

Estratègies de redundància:

- **Infraestructura multi-regió:**
 - Hosting amb servidors en **diferents centres de dades** dins la Unió Europea per assegurar recuperació en cas de fallida regional.
- **Redundància de servidors:**
 - Implementació d'una arquitectura **multi-node** amb **almenys dos servidors VPS balancejats**.
 - Sincronització constant entre els nodes per replicar dades i sessions d'usuaris.
- **Redundància en l'emmagatzematge:**
 - **Espai Cloud** amb replicació de dades en temps real en diferents ubicacions geogràfiques.
 - Mecanismes de **snapshotting i backups incrementals** per assegurar la recuperació de dades en cas de corrupció.

5. COMPLIMENT DE NORMATIVES

El servei web del **Museu Picasso de Barcelona** gestiona **dades personals**, a través de formularis i de "calls to actions" de subscripció al butlletí, fet que implica el compliment estricte de diverses normatives europees i espanyoles en matèria de **protecció de dades i de seguretat de la informació**.

Per garantir la seguretat jurídica i la protecció dels usuaris, el **proveïdor adjudicatari haurà de demostrar documentalment el compliment de totes les normatives aplicables** abans de la posada en producció del servei. Aquesta documentació podrà ser exigida al licitador que resulti proposat com adjudicatari, en el requeriment de documentació previst en els articles 140 i 150.2 de la LCSP.



1. Compliment del Reglament General de Protecció de Dades (RGPD - UE 2016/679) i la Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals (LOPD-GDD - Llei 3/2018)

El proveïdor haurà de garantir el **compliment íntegre del RGPD**, assegurant que, com encarregat del tractament de les dades, sigui segur, transparent i legítim.

1.1. Requisits específics de compliment

- **Protecció de dades des del disseny i per defecte (Privacy by Design & by Default):** Aplicació de mesures proactives per garantir la seguretat i privacitat de les dades.
- **Xifratge de dades:** Implementació de tècniques de xifratge per a la protecció de la informació emmagatzemada i en trànsit.
- **Transferències internacionals de dades:** Assegurar que no existeix cap transferència de dades fora de la UE.

Documentació requerida:

- Informe de compliment del RGPD per part del Delegat de Protecció de Dades.
- Política de privacitat i termes d'ús alineats amb el RGPD.
- Registre d'activitats de tractament de dades on s'identifiqui com encarregat del tractament.
- Informe d'anàlisi de riscos i mesures de seguretat aplicades al tractament de dades personals.

2. Compliment de l'Esquema Nacional de Seguretat (ENS - Reial Decret 311/2022)
L'ENS estableix les mesures necessàries per garantir la **seguretat dels sistemes d'informació en entorns públics i privats que col·laboren amb l'Administració**.

2.1. Requisits específics de compliment

- **Classificació del sistema segons ENS:** El servei web ha de complir almenys amb el nivell **MIG** de seguretat.
- **Identificació i autenticació segures:** Implementació de sistemes d'autenticació robustos, incloent **dobles factors d'autenticació (2FA)** per accés administratiu.
- **Protecció contra ciberamenaces:** Implementació de mecanismes per a la detecció, resposta i recuperació davant d'atacs informàtics.
- **Gestió d'incidents de seguretat:** Obligació de notificar incidents greus al client i a l'autoritat competent (CCN-CERT).

Documentació requerida:

- Informe de certificació ENS – Nivell Mig .
- Resum executiu favorable de l'auditoria de seguretat dels serveis ofertats.

3. Compliment de la Directiva Europea NIS2 sobre Ciberseguretat (Directiva UE 2022/2555)

Aquesta normativa amplia els requeriments de seguretat per a **infraestructures digitals crítiques**.

3.1. Requisits específics de compliment

- **Gestió de riscos de ciberseguretat:** Implementació de controls de seguretat per protegir el servei contra atacs dirigits.

- **Supervisió contínua:** Monitorització activa per detectar vulnerabilitats i atacs.
- **Pla de resposta a incidents:** Definició de procediments per contenir i recuperar-se d'atacs cibernètics.
- **Notificació d'incidents:** Obligació de comunicar incidents greus a les autoritats corresponents.

Documentació requerida:

- Pla de resposta a incidents cibernètics
- Pla de continuïtat de les activitats i gestió de crisis.
- Política i/o procediment per avaluar l'eficàcia de les mesures de gestió dels riscos de seguretat.
- Política i/o procediment per a la seguretat de la cadena de subministrament, inclosos els aspectes de seguretat relatius a les relacions entre cada entitat i els seus proveïdors o prestadors de serveis directes.
- Política i/o procediment per a la seguretat en l'adquisició, el desenvolupament i el manteniment de sistemes de xarxes i d'informació, inclosa la gestió i divulgació de les vulnerabilitats.
- Acreditació d'ús de solucions d'autenticació multifactorial o d'autenticació contínua, comunicacions de veu, vídeos i text segures i sistemes segurs de comunicacions d'emergència, quan escaigui.
- Protocol de notificació d'incidents de seguretat.

A més, el proveïdor haurà de sotmetre's a **auditories periòdiques de seguretat i privacitat** per verificar el manteniment del compliment normatiu durant tot el període del contracte.

6. INFRAESTRUCTURA TÈCNICA. SERVIDORS I HOSTING (CLOUD)

La solució ofertada garantirà una **infraestructura optimitzada** basada en **servidors Cloud gestionats**.

La infraestructura complirà amb les expectatives immediates següents:

1. **Separació de serveis web, bases de dades i reproducció:**
 - Creació d'un **servidor exclusiu per a la base de dades i SOLR** per reduir càrrega sobre el servidor web.
 - Millora del rendiment i escalabilitat en consultar informació.
- **Augment dels recursos actuals fins arribar al mínim de:**
 - Servidors web: (i) un processador (vCPU) de 6 vCPU, (ii) memòria RAM de 16 GB; (iii) emmagatzematge de 200 GB SSD.
 - Servidors de cerca: i) un processador (vCPU) de 4 vCPU, (ii) memòria RAM de 8 GB; (iii) emmagatzematge de 200 GB SSD.
 - Servidors de reproducció: i) un processador (vCPU) de 2 vCPU, (ii) memòria RAM de 6 GB; (iii) emmagatzematge de 150 GB SSD.
- Possibilitat d'afegir més recursos segons necessitats de creixement.

- **Implementació d'un sistema de balanceig de càrrega (Load Balancer)**
 - Per millorar l'escalabilitat i tolerància a fallades.
- **Ús d'un CDN (Content Delivery Network)**
 - Per reduir el temps de càrrega i protegir contra atacs DDoS.
- **Implementació de backups remots en temps real**
 - Còpies de seguretat diàries en **una ubicació separada**.

En tot cas, la solució ofertada haurà de complir amb els següents requeriments mínims:

Component	Configuració Mínima	Objectiu
Servidor Web	6 vCPU, 16GB RAM, 200GB SSD	Optimitzar rendiment
Base de Dades	Instància gestionada en Cloud	Escalabilitat automàtica
Servidor de Cerca	4 vCPU, 8GB RAM, 200 GB SSD	Millorar velocitat de consulta
Servidor preproducció	2 vCPU, 6GB RAM, 150 GB SSD	Garantia disposició entorn de proves
Balancejador de càrrega	LB en Cloud	Distribució eficient de tràfic
CDN i WAF	CDN i WAF integrada	Millorar seguretat i rendiment
Còpies de seguretat i Recuperació de Desastres	Còpies de seguretat en temps real	Protecció davant de fallades
Monitorització Avançada	Plataforma de monitorització i gestió remota	Detecció proactiva de problemes

7. TREBALLS DE MIGRACIÓ

L'adjudicatari serà el responsable de realitzar la migració al nou portal de tota la informació actual continguda a la web del Museu Picasso, amb termini màxim de 15 dies. La migració cap a aquesta nova infraestructura haurà de ser **gradual** i **planificada**, seguint una planificació personalitzada per fases.

El proveïdor garantirà una migració sense interrupcions

- Es faran testos previs i caldrà un cronograma documentat amb les fases de desplegament que inclourà:

- **Proves de funcionalitat i rendiment:** Validació prèvia en un entorn de preproducció simulant la càrrega real.
- **Testos de compatibilitat:** Garantia que la migració no afectarà serveis existents ni integracions crítiques.
- **Fases de desplegament:** Documentació clara del calendari de migració, incloent una fase inicial per preparació, una fase de desplegament i una fase de monitorització, posterior al desplegament.
- **Pla de mitigació de riscos:** Identificació de possibles punts crítics i estratègies de contenció per minimitzar l'impacte.
- **Acceptació final:** Validació per part dels responsables tècnics abans de la posada en producció definitiva.

El procés de migració ha de garantir la continuïtat del servei en cas de fallida i ha de preveure:

La migració ha de garantir que la web del Museu Picasso continuï funcionant al 100% durant tot el procés de la migració. Només en el moment de traspàs hi podrà haver una interrupció menor a 2 hores, i caldrà fer-ho en horari nocturn. A més, haurà de garantir el següent pla de reversió i restauració automàtica en cas d'errors documentats.

- **Temps de detecció i resposta:** Identificació automàtica d'errors crítics amb temps màxim de resposta de **15 minuts**.
- **Procés de reversió automàtica:** Restauració automàtica del sistema en **màxim 1 hora** en cas de fallada de la migració.
- **Còpies de seguretat garantides:** Recuperació des del backup més recent amb un **RPO (Recovery Point Objective) ≤ 15 minuts**.
- **Validació post-restauració:** Verificació del correcte funcionament del sistema en un període màxim de **1 hora** després de la restauració.

Durant el procés es garantirà un suport tècnic especialitzat durant la transició, amb resposta garantida.

- **Disponibilitat 24/7:** Equip tècnic operatiu durant tota la fase de migració i post-migració immediata.
- **Temps màxim de resposta:** Resolució inicial d'incidències en **menys de 30 minuts** per errors crítics.
- **Canal de comunicació directe:** Línia exclusiva amb responsables tècnics per gestionar incidències en temps real.
- **Supervisió post-migració:** Seguiment actiu durant **7 dies després de la migració** per detectar i corregir possibles errors.

8. REQUERIMENTS D'ARQUITECTURA DE LA XARXA I SEGURETAT

L'arquitectura de xarxa i la seguretat del servei web del **Museu Picasso de Barcelona** han de garantir la **disponibilitat, rendiment i protecció davant de ciberamenaces**. Actualment, la infraestructura es troba **allotjada en un ISP (Arsys, IONOS SE, AS8560) a Espanya**, amb resolució DNS gestionada per **CDmon** i mecanismes de protecció com **SPF i DMARC per correu electrònic**.

Adreçament IP i serveis exposats

- **IP pública:** 82.223.132.37 (servidor web principal).



- **Proveïdor de hosting: Arsys (IONOS SE, AS8560)**, amb ubicació física a **Madrid (Espanya)**.
- **Ports oberts:**
 - **80/TCP (HTTP)** – Redirigit a HTTPS (301 Moved Permanently).
 - **443/TCP (HTTPS)** – Certificat SSL/TLS vàlid emès per **DigiCert (Thawte TLS RSA CA G1)**.

Resolució DNS i protecció de correu electrònic

- **Gestió DNS:** CDmon, amb servidors primaris i secundaris.
- **Protecció del correu:**
 - **SPF (Sender Policy Framework)** actiu: permet només servidors autoritzats enviar correu per museupicassobcn.cat.
 - **DMARC (Domain-based Message Authentication, Reporting & Conformance):** configurat en mode **quarantine** (p=quarantine), protegint contra spoofing i phishing.

Xifratge i compatibilitat SSL/TLS

- **Suport per TLS 1.2 i TLS 1.3** (versions segures).
- **Paràmetres Diffie-Hellman de 2048 bits** per establir connexions segures.

Limitacions i riscos detectats:

- **Manca de protecció avançada contra DDoS:** No s'observa la implementació d'un **WAF (Web Application Firewall)** ni **protecció CDN**.
- **Infraestructura centralitzada:** Actualment, no hi ha balanceig de càrrega ni distribució de tràfic entre diversos nodes.
- **Exposició directa de la IP del servidor web:** Augmenta el risc d'atacs dirigits a la infraestructura.

Per protegir la infraestructura davant de **ciberatacs i vulnerabilitats**, s'han d'implementar les següents mesures de seguretat:

Protecció del trànsit web

Implementació d'un WAF (Web Application Firewall)

- Filtratge de peticions sospitoses per evitar atacs SQL Injection, XSS i exploits de Drupal.
- Restricció d'accés a URL sensibles o d'administració.

Activació d'una CDN per reduir riscos

- Servei CDN per accelerar la càrrega i bloquejar tràfic maliciós.

Protecció contra atacs (força bruta, explotacions de vulnerabilitats, intents d'intrusions, etc.)

- Disposar d'un Centre d'Operacions de Seguretat 24x7 per detectar i contenir alertes. Per exemple, bloquejar IPs sospitoses.
- **Límits de connexions a l'administració i accés restringit per IP** origen escollides pel museu.

Autenticació i control d'accessos

- **Implementació d'autenticació de doble factor (2FA)** per administradors.
- **Registre de logs d'accés i monitorització** d'activitat sospitosa. Traçabilitat dels accessos i detecció d'activitat anòmla en cas d'una investigació per part de l'equip de resposta a incidents (CSIRT) del proveïdor.

9. MONITORITZACIÓ I GESTIÓ D'INCIDENTS

La correcta operació i manteniment del servei web del **Museu Picasso de Barcelona** requereix un sistema de **monitorització proactiva i una gestió d'incidents eficient**, capaç de detectar problemes abans que afectin el rendiment i disponibilitat del sistema. Això inclou **supervisió 24/7, temps de resposta garantits i plans de recuperació davant de desastres**, assegurant un funcionament ininterromput i segur.

El proveïdor adjudicatari haurà de garantir un servei de **monitorització proactiva 24x7**, amb mecanismes automatitzats per identificar **problemes de rendiment, errors de seguretat i caigudes del servei**. Com a mínim amb les següents característiques:

- **Supervisió 24/7** de la infraestructura.
- **Alertes automatitzades i sistema d'avisos immediats**.
- **Plataforma de monitorització en temps real** accessible per l'equip tècnic del Museu, amb quadres de comandament que permetin consultar l'estat dels serveis i incidents detectats.
- **Generació d'informes periòdics** amb mètriques de rendiment i anàlisi d'incidències, incloent recomanacions de millora.

El servei d'allotjament web haurà d'incorporar **un sistema de gestió d'incidències amb resposta ràpida**, establint, com a requeriment mínim, els següents **temps de resposta màxims** segons la gravetat de cada incidència:

Tipus d'incidència	Descripció	Temps màxim de resposta (RTO)	Temps màxim de resolució (RPO)
Crítica	Caiguda del servei web, fallida del servidor, atac de ciberseguretat actiu amb afectació a la venda d'entrades.	12 h	30 dies
Alta	Ralentització significativa del servei, fallada en la base de dades, problema greu de seguretat que no afecta a la venda d'entrades.	48 h	30 dies
Mitjana	Error parcial en el funcionament de la web, problemes amb pagaments o formularis que no afecta a la venda d'entrades.	72 h	30 dies

Baixa	Peticions de millora, ajustaments de configuració no urgents que no afecta a la venda d'entrades.	1 setmana	30 dies
--------------	---	------------------	----------------

- **Servei d'atenció telefònica i correu electrònic** en horari de 8:00 a 18:00 en dies laborables.
- **Servei d'atenció per a incidències crítiques 24/7** via telèfon
- **Intervenció presencial en un màxim de 24 hores** en cas de requerir actuacions *in situ*.

El servei web haurà de comptar amb **un pla de recuperació davant de desastres (DRP - Disaster Recovery Plan)** que garanteixi **una restauració ràpida i segura en cas de fallida catastròfica**.

- **Temps màxim de recuperació (RTO): 30 minuts per serveis crítics.**
- **Temps màxim de pèrdua de dades (RPO): 1 hora**, garantint mínimes pèrdues d'informació.
- **Recuperació automatitzada** mitjançant snapshots i backups en entorns segregats.

L'adjudicatari serà responsable de realitzar **millores contínues del sistema** per garantir la seva **seguretat, eficiència i escalabilitat**.

- **Actualitzacions del sistema operatiu i software base** per motius de seguretat i rendiment.
- **Optimització de la base de dades i rendiment web** per reduir temps de càrrega.
- **Integració de millores tecnològiques** que permetin una gestió més eficient del servei.
- Servei de **consultoria tècnica permanent** per proposar millores tecnològiques.
- Acompanyament en processos de migració o ampliació de la infraestructura.

Consideracions per al plec tècnic

- 1. Actualització i manteniment del CMS Drupal**
 - Especificar la necessitat d'actualitzacions periòdiques per mantenir la seguretat i el rendiment.
- 2. Seguretat i Protecció de Dades**
 - Certificat SSL/TLS actualitzat per garantir transmissions segures.
 - Revisió de llibreries i frameworks per detectar vulnerabilitats.
- 3. Escalabilitat i Optimització**
 - Garantir el bon funcionament amb grans volums de trànsit.
 - Configuració adequada de la CDN per millorar la velocitat de càrrega.
- 4. Integració amb eines d'anàlisi i publicitat**
 - Assegurar la compatibilitat i correcte funcionament amb Google Analytics i Google Ads.



5. Disseny responsiu i accessibilitat

- Confirmar que el disseny compleix els estàndards WCAG per a l'accessibilitat web.

Barcelona, a data de la signatura electrònica