PLIEGO DE PRESCRIPCIONES TÉCNICAS

EXPEDIENTE NÚM.: 2024_EXP_F204_0001292- CDRB/2025/0034708

CONTRATO DE LOS *"SERVICIOS DE SOPORTE INFORMÁTICO DEL CONSORCI DE LES DRASSANES REIALS I MUSEU MARÍTIM DE BARCELONA, Y GESTIÓN Y SERVICIO DE COPIA DE SEGURIDAD REMOTA EN NUBE EXTERNA"*

CONTRATO	
Tipo	Tramitación ordinaria, procedimiento abierto.
Presupuesto de licitación IVA excluido	118.531,60 €, IVA incluido, dividido: - Parte fija: 75.020,00 € - Parte variable: 43.511,60 €
Descripción	Contrato de los ***"Servicios de soporte informático del Consorci de les Drassanes Reials i Museu Marítim de Barcelona, y gestión y servicio de copia de seguridad remota en nube externa".***

Consorci de les Drassanes Reials i Museu Marítim de Barcelona
DRASSANES REIALS
Av. de les Drassanes, s/n. 08001 Barcelona
Tel. 00 34 933 429 920
www.mmb.cat informacio@mmb.cat
CIF P5800029J

CONTRATO DE SERVICIOS DE LOS "*SERVICIOS DE SOPORTE INFORMÁTICO DEL CONSORCI DE LES DRASSANES REIALS I MUSEU MARÍTIM DE BARCELONA, Y GESTIÓN Y SERVICIO DE COPIA DE SEGURIDAD REMOTA EN NUBE EXTERNA*"

ÍNDICE

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL CONTRATO DE LOS "*SERVICIOS DE SOPORTE INFORMÁTICO DEL CONSORCI DE LES DRASSANES REIALS I MUSEU MARÍTIM DE BARCELONA, Y GESTIÓN Y SERVICIO DE COPIA DE SEGURIDAD REMOTA EN NUBE EXTERNA"*

Prescripción primera. – OBJETO Y ÁMBITO DE APLICACIÓN. SITUACIÓN ACTUAL.

A) Objeto y ámbito de aplicación.

El objeto de este contrato es dotar a la organización del Consorci de les Drassanes Reials i Museu Marítim de Barcelona (en adelante CDRiMMB) de los recursos necesarios para que sus sistemas informáticos presten los servicios para los que fueron adquiridos y evolucionen según sus necesidades.

Por ello, se ha realizado recientemente un estudio de necesidades y del estado actual que concluye que es necesario actuar de forma coordinada en tres ámbitos:

- **Control y mejora del servicio.** Existen más actividades susceptibles de un mejor soporte. Además, el teletrabajo ha generado nuevas necesidades. También es preciso implantar y supervisar más procedimientos de control.
- **Buen funcionamiento de los sistemas**. Los sistemas se han ampliado, son más complejos y las labores de administración han aumentado, y se prevé que continúen aumentando.
- **Gestión de copia de seguridad remota en nube externa.** En cumplimiento de los requisitos de seguridad del ENS (Esquema Nacional de Seguridad), y para garantizar la recuperación completa en caso de incidencias graves en los sistemas ubicados en la sala CPD y en las copias actuales situadas en salas técnicas del CDRiMMB.

Con el fin de llevar a cabo las actuaciones anteriores, y en consonancia con la dimensión del CDRiMMB, se considera oportuno iniciar la contratación de servicios externos especializados.

Esta contratación se desglosa en dos partes:

PARTE FIJA:

Los servicios solicitados bajo este contrato se describen en las siguientes categorías:

a) **Soporte de sistemas**

Por un lado, los servicios TIC al CDRiMMB se prestan con equipos y software ubicados en las propias instalaciones del CDRiMMB (la práctica totalidad de los servicios), además de otros en infraestructura de terceros (Microsoft 365, gestión de la red de puntos de

acceso Wi-Fi, servicios proporcionados por CSUC, etc.).

En ambos casos (equipos/software ubicados en el CDRiMMB o en instalaciones de terceros), es necesario realizar tareas de gestión y mantenimiento para mantenerlos actualizados y disponibles para los usuarios del CDRiMMB.

Este soporte incluye la gestión del equipamiento existente en cada momento durante la vigencia del contrato. Es decir, abarca tanto el equipamiento actual como la incorporación de nuevos equipos o sustitución de los existentes, sin que esto suponga modificación del contrato.

Se trata de un servicio que se prestará mayoritariamente en remoto y consistirá en apoyar los recursos TIC del CDRiMMB para facilitar el diagnóstico y la actuación sobre el terreno, minimizando la necesidad de desplazamientos.

b) **Gestión y servicio de copia de seguridad remota en nube externa**

El CDRiMMB dispone actualmente de una sala CPD local en sus instalaciones, y varias salas técnicas y cabinas de discos en el mismo edificio.

Para cumplir con los requisitos del ENS (Esquema Nacional de Seguridad) y garantizar la recuperación completa del sistema informático en caso de incidencias graves que afecten al edificio entero, ataque de virus como CryptoLocker o similar (de encriptación de archivos) u otros que impidan el acceso a equipos y a las copias de seguridad ubicadas dentro del recinto del CDRIMMB), es imprescindible y necesario disponer de una copia de seguridad actualizada en la nube y fuera del recinto físico del CDRiMMB.

B) Descripción de la situación actual

a) Soporte de sistemas

Actualmente, este servicio se realiza internamente por los profesionales TIC del CDRiMMB. Tradicionalmente, se ha acudido a la contratación de pocas horas de soporte externo para cubrir temas de especialización y diagnósticos complejos, lo cual mantenía los sistemas actualizados. Actualmente, la mayor complejidad y carga de trabajo derivadas de la nueva realidad del teletrabajo han incrementado considerablemente las necesidades de soporte externo. En consecuencia, es necesario contar con soporte externo continuo, por ejemplo para gestionar una red Wi-Fi global, el teletrabajo, mantenimiento y actualización de equipos, gestión, mantenimiento y actualización de equipos, gestión, mantenimiento y actualización de servidores corporativos, de los diferentes proyectos previstos respecto a la actualización de infraestructura, entre otros.

b) Gestión y servicio de copia de seguridad remota en nube extern

Actualmente, el CDRiMMB dispone de una sala CPD local en sus instalaciones, con dos entornos virtualizados con sistema VMWARE (uno para servidores corporativos con 2 hosts dedicados, y otro con VMWARE Horizon para la virtualización de escritorios con 2 hosts dedicados), un servidor físico con sistema NAGIOS (monitorización de sistemas), además de cabinas de datos y otro equipamiento tecnológico corporativo.

Dentro del protocolo de copias de seguridad corporativas, actualmente se realiza una copia completa del sistema informático —servidores y datos— utilizando el software especializado VEEAM (con dos licencias activas de VEEAM Essentials, una por entorno virtualizado), y se realiza sobre en cabinas ubicadas en otra sala técnica, lejos de la sala CPD pero dentro del mismo edificio y recinto.

Para cumplir las recomendaciones y requisitos del ENS (Esquema Nacional de Seguridad), y garantizar una recuperación completa alternativa en caso de desastre o incidencias graves que impidan el acceso o destruyan los datos (por ataques informáticos o destrucción del equipamiento local), es necesario disponer de una copia de seguridad actualizada en la nube, fuera del recinto físico del CDRiMMB.

Prescripción segunda – DESCRIPCIÓN DE LOS SERVICIOS SOLICITADOS.

1. **Alcance del Servicio**

A) Soporte de sistemas

Para garantizar el buen funcionamiento de los sistemas y una rápida gestión de incidencias y problemas, se requiere disponer de un servicio que, de forma orientativa y no exhaustiva, atienda:

- Gestión de incidencias con fabricantes en equipos bajo garantía.
- Inventario y control de configuración.
- Incidencias físicas y lógicas de las infraestructuras TIC.
- Administración y gestión de la red de datos del CDRiMMB, y de los elementos que la conforman, tanto de hardware como software, incluyendo switches, hubs, cortafuegos, armarios, y demás elementos que la conforman, y aplicación de actualizaciones de firmware o seguridad recomendadas por los fabricantes.
- Administración y gestión de los equipos de la red informática, como servidores, incluyendo gestión de bases de datos corporativas, dominios, entornos de virtualización, servicios comunes (archivos, impresión…) y demás elementos que la componen.
- Instalación, creación, despliegue, configuración, parametrización y actualización de los servidores host de los dos entornos de virtualización: vCenter, hipervisores ESXi, máquinas virtuales y appliances, así como instalación de parches de seguridad.

- Soporte puntual, a petición de los técnicos del museo, en la gestión de administración de usuarios (estos técnicos suelen encargarse, por su complejidad).
- Gestión y resolución de incidencias en servicios en la nube (Office 365 u otros).
- Gestión del software de protección perimetral (cortafuegos y antivirus).
- Ejecución y gestión integral de las copias de seguridad del sistema informático, tanto internas en el propio recinto, como las realizadas en la nube externa.
- Gestión del software de uso general del servidor instalado (servidores de archivos, bases de datos).
- En caso de ser requerido por los técnicos del museo, redacción de protocolos y guías de uso de hardware y software del que dispone el CDRiMMB.
- Habilitación ocasional de servicios de acceso a internet para eventos.
- Gestión de la monitorización del sistema informático usando NAGIOS (vigilante del sistema), instalado y configurado en un servidor local independiente, incluyendo actualización de software, mantenimiento de la configuración y agregación de nuevos parámetros para equipos recién incorporados.
- Recopilación y análisis de logs.
- Realizar soporte al sistema de virtualización de escritorios corporativos con VMWARE.
- Atención directa a consultas de los técnicos del museo relacionadas con el objeto de este contrato.
- Gestión de renovación de servicios clave del sistema, y que requieran actuaciones directas sobre los sistemas y equipos informáticos corporativos internos, especificados a continuación:

Periodicidad anual:

- Renovación anual de certificados digitales de servidor seguro, actualmente con la entidad certificadora DIGICERT (un SSL de validación extendida y otro tipo Wildcard).

- Renovación anual del servicio de *mail gateway* (pasarela de correo corporativo), el utilizado actualmente por el CDRiMMB es con DuoCircle.

- Renovación de soporte de licencias VEEAM Essentials (Backup vCenter granja VDI con 2 hosts (4 sockets)) (Contrato VEEAM: #01528650).

- Renovación de soporte de licencias VEEAM Essentials (Backup vCenter granja Servidores con 2 hosts (4 sockets)) (Contrato VEEAM: #01493044).

- Renovación anual del servicio de soporte de cabina HUAWEI OceanStor 2600 V5 (s/n 2102354CMKTUM6900061) —Onsite Standard 8x5xNBD + Basic Software License.

- Renovación anual del servicio FortiCare y FortiGuard Unified Threat Protection (UTP) para los 2 equipos FortiGate F100 actualmente existentes.

- Renovación anual del servicio Fortinet FortiGate Cloud Management, y el servicio Analysis and 1 Year Log Retention para FortiGate 100F.

- Renovación anual del servicio de consola de gestión Aruba Central y soporte de los 65 equipos AP que componen la infraestructura Wi-Fi corporativa.

Periodicidad puntual, siempre que la fecha de renovación esté comprendida dentro del período de vigencia del contrato, concretamente:

- Renovación por 5 años del dominio complementario existente con CDMON, cuya próxima renovación será en junio de 2026.

Las intervenciones se refieren al mantenimiento preventivo, correctivo, adaptativo y perfeccionador de servidores, redes, comunicaciones, sistemas de almacenamiento y copias de seguridad.

Los recursos TIC del CDRiMMB facilitarán el diagnóstico inicial de las incidencias y ofrecerán servicio de asistencia remota para aquellas actuaciones que lo permitan.

Los ámbitos implicados en la resolución de incidencias físicas y lógicas y la actualización de la documentación son los siguientes:

- Servidores Windows: controladores de dominio, servidores SQL, de aplicaciones, archivos e impresión, así como su periférico asociado (cabinas de discos, racks, monitores, etc.), y los elementos NAS y SAN.
- Servidores Linux: Centos.
- Servidores Vmware.
- Sistemas de almacenamiento.
- Sistemas de gestión de bases de datos.
- Electrónica de red.
- Conectividad externa.
- Software propietario (directo del fabricante o a través de distribuidor).
- Virtualización de escritorios.
- Licencias de uso.
- Control y movimiento de material.
- Sistemas de impresión.
- Correo electrónico.
- Sistemas corporativos y departamentales de aplicación.
- Aplicaciones como servicios internos y externos.
- Software en la nube.

- Equipos cortafuegos corporativos FortiGate

Para garantizar la calidad del servicio en la gestión del Sistema de Gestión de Seguridad de la Información (SGSI), el contratista deberá contar con la siguiente certificación de norma ISO:

- ISO 27001

B) Gestión y servicio de copia de seguridad remota en nube externa

Este servicio incluye la contratación de una copia de seguridad remota completa del sistema informático y datos en la nube externa, proporcionando todos los elementos necesarios (almacenamiento y software complementario) para gestionar de forma integral y centralizada a través del portal de copias VEEAM actualmente utilizado en el CDRiMMB.

La copia en la nube deberá ser **inmutable** y **cifrada**, facilitando las credenciales utilizadas al equipo técnico del CDRiMMB.

El servicio en la nube se prestará desde instalaciones ubicadas en **territorio nacional** por las siguientes razones:

- Evitar posibles conflictos de acceso a la información derivados de tensiones geopolíticas.
- Garantizar el cumplimiento de las normativas estatales y del ENS (Esquema Nacional de Seguridad) en materia de protección de datos.
- En caso de desastre total, facilitar y agilizar la recuperación de datos y backups mediante acceso y descarga presencial desde dichas instalaciones.

Los CPD deben ubicarse en instalaciones que cumplan con la certificación TIER III Compliance.

Para asegurar la operatividad, seguridad y resiliencia del servicio, la entidad operadora de las instalaciones debe disponer de las siguientes normas ISO:

- ISO 27001
- ISO 9001
- ISO 22301
- ENS Medio

En caso de que la entidad operadora sea diferente al contratista, el adjudicatario deberá demostrar la relación contractual existente con la misma.

Con objeto de garantizar el correcto funcionamiento y permitir el cálculo del alcance del servicio, se detallan los requerimientos iniciales y necesidades actuales:

- 50 TB de espacio mínimo en nube

- 50 equipos/MV para copias

El servicio deberá proporcionarse en la modalidad de “VEEAM Cloud Provider”, e incluirá tanto el coste del espacio en la nube, la suscripción del software necesario de VEEAM Cloud Connector por equipo, así como la gestión y seguimiento de su correcta ejecución, integración y sincronización con el portal interno de gestión de las respectivas copias.

Durante la vigencia del contrato se contempla la posibilidad de necesidades derivadas de variaciones en el aumento del espacio de almacenamiento o del número de equipos/MV para realizar copia (que incluirá la licencia necesaria de software para su realización), según los siguientes conceptos:

Coste mensual por cada Terabyte de espacio extra en la nube externa que exceda del número contratado inicialmente.
Coste mensual por cada Equipo/MV extra que exceda del número contratado inicialmente.

Se solicitará al licitador que presente junto a su oferta el coste extra mensual por unidad de cada uno de estos dos conceptos en la base presupuestaria como parte variable, según se indica y en la forma que se define en la cláusula 1.3 del PCAP.

2. Cualificación de la empresa

La empresa deberá disponer de los siguientes certificados, y como mínimo del nivel especificado o superior:

- “Expert Partner de FORTINET”
  (Para la criticidad de la solución implantada de FortiGate como cortafuegos corporativo, gestionar configuración y posibilitar la tramitación de la renovación anual de soporte de licencias incluida en el presente pliego.

- “Silver Partner de VEEAM Backup”
  (Para la correcta gestión integral del sistema de copias de seguridad corporativo, y posibilitar la tramitación de la renovación anual de soporte de licencias incluida en el presente pliego).

- “Solutions Partner de Microsoft”
  - (Para dar soporte a los sistemas Windows y Office 365)

- “Silver Partner de Huawei”
  - (Para dar soporte a la cabina de discos de fondos digitalizados y datos, y posibilitar la tramitación de la renovación anual de soporte de licencias incluida en el presente pliego)

- “Business Partner de Aruba”
  (Para la correcta gestión integral del sistema Wi-Fi corporativo, y posibilitar la

tramitación de la renovación anual del servicio de gestión de la consola Aruba Central y soporte de los 65 equipos AP incluidos en el presente pliego)

3. Carga estimada de trabajo

Actualmente, los sistemas del CDRiMMB se componen, principalmente, de:

- Dos hosts para un entorno vSphere de VMware con 30 servidores virtuales Windows y Linux.
- Dos hosts para un entorno Horizon de VMware con 10 servidores virtuales Windows y Linux, y 80 escritorios virtuales derivados de 6 plantillas.
- Cuatro PC físicos.
- 30 portátiles para teletrabajo y equipos Zero Client locales para conexión a escritorios virtuales.
- Dos cabinas de almacenamiento principales (PURE Storage y HUAWEI), y tres para copias de seguridad (SYNOLOGY y THECUS) en salas técnicas del propio edificio.
- Núcleo de la red con equipos redundantes en el CPD con un total de 3 conmutadores NETGEAR gestionables.
- 6 salas técnicas con 13 conmutadores NETGEAR gestionables, conectados al núcleo con fibras ópticas redundantes.
- 5 salas técnicas secundarias con 9 conmutadores NETGEAR gestionables, conectados al núcleo con fibra óptica.
- Dos cortafuegos FortiGate 100F configurados en alta disponibilidad.
- 65 puntos de acceso ARUBA de Wi-Fi de altas prestaciones (Wi-Fi 6) con gestión centralizada de Aruba Central.
- 2 SAIs SOCOMEC gestionados, y 4 individuales montados en racks.

Además de la lista anterior, hay una serie de equipos complementarios de menor importancia.

Se estima que la prestación podrá llevarse a cabo de forma remota en más del 95 % de los casos.

Adicionalmente, se ha estimado que la participación del personal propio del CDRiMMB reducirá en un 5 % la carga de trabajo al eliminar algunos desplazamientos y mejorar el diagnóstico inicial de las incidencias.

4. Horario del servicio

La prestación del servicio de soporte de sistemas y de gestión y servicio de copia de seguridad remota en nube externa estará disponible en horario de 8 a 18 horas durante los días laborables del CDRiMMB.

El servicio estará disponible los 12 meses del año.

Todas las incidencias que requieran una intervención especial por parte de un coordinador estratégico se valorarán por precio/hora (no se encuentra incluida en la parte

fija), y deberán diferenciarse si se prestan en el horario laboral de 8 a 18 horas o bien fuera de este horario o en festivos y fines de semana. Estas intervenciones se valorarán como parte variable del presente contrato.

5. Canales de comunicación de incidencias.

Se establecen como canales de contacto y comunicación de incidencias los siguientes:

- Telefónico y/o dirección electrónica:
  El contratista facilitará los teléfonos y direcciones electrónicas de contacto de sus interlocutores en cada momento, así como los nuevos que puedan surgir durante la vigencia del contrato.

- Plataforma de soporte y seguimiento de incidencias:
  El contratista se compromete a facilitar el uso de una plataforma de “tickets” de servicio y seguimiento de incidencias

Prescripción tercera.- CALENDARIO LABORAL. RECURSOS PROPIOS.

CALENDARIO

Se seguirá el calendario laboral del CDRiMMB. Los horarios de cada servicio se han descrito en su apartado correspondiente, dado que cada uno tiene sus particularidades propias.
En caso necesario, el CDRiMMB podrá solicitar que se preste servicio fuera del horario habitual, lo cual se facturará según precios unitarios establecidos en la cláusula 1.3 del Pliego de Cláusulas Administrativas Particulares.

RECURSOS PROPIOS DEL CDRIMMB

El equipo técnico TIC del CDRiMMB se compone actualmente de una única persona para la gestión TIC a nivel corporativo, a tiempo completo, asignada al servicio de atención al usuario, al control administrativo de la ejecución y otras tareas que no puedan ser delegadas a personal externo al CDRiMMB.

El equipo técnico TIC del CDRiMMB efectuará tareas presenciales de soporte al usuario, y en caso de necesidad y ser requerido, de forma integrada con los recursos del contratista del servicio.

También actuará como facilitador de los diagnósticos iniciales y como manos remotas para el soporte de sistemas.

El CDRiMMB pondrá a disposición del contratista un espacio de trabajo con las herramientas informáticas necesarias para que se puedan llevar a cabo los servicios contratados.

Asimismo, el CDRiMMB suministrará toda la información relacionada con el servicio y todas las contraseñas de usuario administrador para la realización de las tareas solicitadas.

Prescripción cuarta.- LUGAR DE PRESTACIÓN DE LOS SERVICIOS

- Presencial: Sede central del CDRiMMB en Av. de les Drassanes, s/n. (Barcelona).
- Virtual: Acceso remoto vía VPN proporcionada por el CDRiMMB y/o telefónicamente con el personal del CDRiMMB.

Prescripción quinta.- ADQUISICIÓN, DEVOLUCIÓN, EQUIPO TÉCNICO Y SEGUIMIENTO DEL SERVICIO

A) Adquisición del Servicio

El contratista dispondrá de un período de dos semanas en el que podrá estudiar toda la información facilitada para la realización de las tareas solicitadas, y realizar cuantas consultas considere necesarias al equipo técnico del CDRiMMB.

Durante este período de adquisición del servicio se podrá reducir el ritmo de los trabajos dedicados a la prestación del servicio, excepto en lo relativo a la resolución de incidencias, en que se deberá, en todo momento, mantener el SLA descrito en el apartado "Acuerdos de nivel de servicio", descritos en el apartado de Penalizaciones de la cláusula 2.6 del Pliego de Cláusulas Administrativas Particulares (PCAP).

B) Plan de retorno del servicio

El contratista deberá mantener en todo momento la documentación necesaria para la prestación del servicio totalmente actualizada, y deberá entregarla al CDRiMMB siempre que sea solicitada por el equipo técnico del museo o en caso de no continuar prestando sus servicios al finalizar el contrato.

Al finalizar el servicio, por cualquiera de las causas que pudieran determinarlo, el CDRiMMB establece un plazo transitorio de ejecución de las prestaciones del contrato en condiciones especiales, de forma que se garantice la prestación del servicio de forma ininterrumpida, comprometiéndose el contratista saliente a colaborar, si procede, con el nuevo contratista en las actividades detalladas, encaminadas a la planificación y ejecución del cambio.

El contratista se compromete a garantizar la completa y correcta operatividad de todos los servicios prestados en virtud del contrato durante el posible período de transición requerido al finalizar el contrato, que permita el cambio de contrato y de proveedor de servicios.

Los técnicos encargados de la prestación del servicio deberán colaborar con la nueva empresa realizando la transferencia a los nuevos responsables en las mismas ubicaciones del CDRiMMB.

Se establece que el tiempo necesario para llevar a cabo esta fase de transición será como mínimo de 15 días laborables, ejecutándose, siempre que sea posible, el período indicado en los días inmediatamente previos a la finalización del contrato.

Una vez finalizado el contrato, deberán estar un mínimo de una semana más a total disposición para evacuar dudas y/o realizar nuevas transferencias.

Pasado este tiempo, el nuevo contratista elaborará una lista de lo que considere que no ha sido transferido o lo ha sido de forma deficiente. El CDRiMMB arbitraría la forma de finalizar dicha transferencia.

C) EQUIPO TÉCNICO

Tanto el responsable del servicio como los profesionales que presten el servicio deben estar familiarizados con los equipos, procedimientos y tecnologías descritas en estos pliegos y que se utilizan en el CDRiMMB, ya que se requiere eficacia desde el primer día.

La composición del soporte técnico que se precisa según las tareas a desarrollar es la que se relaciona a continuación y que, de acuerdo con la naturaleza del contrato, los servicios de soporte a la explotación de los sistemas y su evolución conllevan tareas muy interrelacionadas entre sí, hasta el punto de que una misma persona puede realizar tareas de diferentes bloques:

a) Responsable del servicio:

   El responsable del servicio debe disponer de un título de grado superior en informática o ingeniería, con una experiencia de 10 años en servicios similares al objeto del contrato, quien además ejercerá las funciones de coordinador estratégico.

b) 2 Técnicos:

   a) 1 técnico de Soporte de sistemas

      El técnico asignado, con titulación mínima de formación profesional de grado medio de la familia profesional de Informática y Comunicaciones, debe poder justificar conocimientos y una experiencia mínima de dos años en la dirección de este tipo de servicio.

      Los miembros asignados al servicio deben poder justificar la prestación de servicios similares a los sistemas básicos del CDRiMMB mencionados en el apartado 2.

b) 1 técnico de Gestión de cortafuegos FortiGate (de Fortinet)

Un técnico de soporte asignado para la gestión especializada de cortafuegos FortiGate, con titulación mínima de formación profesional de grado medio de la familia profesional de Informática y Comunicaciones. Dado el nivel de criticidad y grado de complejidad en la configuración de los equipos de seguridad FortiGate existentes, es requisito que la empresa cuente en su plantilla con un técnico que posea el certificado Fortinet de nivel NSE 7.

Gestión de proyectos y cambios futuros

Se valorará la disponibilidad de un perfil técnico por parte del licitador, certificado en metodologías ITIL (con nivel mínimo ITIL v.3 o superior), y con experiencia demostrable como Project Manager (gestión de proyectos), y formará parte del criterio de adjudicación según se describe en la cláusula 1.11 del PCAP.

D) Seguimiento del contrato.

Se prevé la siguiente organización de seguimiento de la ejecución del contrato:

a) Representantes del CDRiMMB y del contratista

El CDRiMMB designará un responsable del contrato.

El contratista designará un responsable de los servicios a prestar de acuerdo con los servicios definidos en el objeto del contrato, que será el interlocutor único de la empresa adjudicataria del contrato ante el CDRiMMB para la dirección de los trabajos y gestión del contrato.

Este interlocutor se encargará de dar las instrucciones oportunas al personal de la empresa con periodicidad diaria según las necesidades del servicio.

b) Comité de Dirección

Trimestralmente se realizará una reunión entre los responsables del CDRiMMB y de la empresa adjudicataria. A la misma asistirán, además, las personas que las partes consideren oportunas.

Los objetivos de la reunión serán:

- Revisar si el servicio se está desarrollando tal como estaba previsto.
- Revisar si el servicio se puede desarrollar mejor.
- Revisar si tal como está planteado sigue siendo lo que necesita el CDRiMMB.
- Revisar si está generando los efectos deseados.

- En caso de ser necesario, elaboración de un plan de acción

c) Comité de Seguimiento

Mensualmente y siempre que sea requerido por los responsables del CDRiMMB se realizará una reunión de seguimiento entre los responsables del CDRiMMB, del contratista y las personas que ellos consideren necesarias.
El contratista presentará los informes preceptivos y se revisará:

- Trabajo realizado.
- Indicadores de calidad.
- Análisis de los riesgos gestionados y avance de las medidas a tomar.
- Próximos trabajos a desarrollar.
- Análisis de nuevos riesgos detectados.
- Plan de acción y de gestión.

PARTE VARIABLE:

Se contemplan como parte variable los siguientes conceptos:

a) Coste por horas realizadas fuera del horario laboral, festivos y fines de semana, en remoto o presencial, ya sea por parte de técnicos y/o coordinador estratégico.
b) Coste por horas realizadas por soporte de un técnico (presencial), laborables de 8 a 18 horas.
c) Coste por horas de soporte de sistemas, del coordinador estratégico, laborables de 8 a 18 horas, en remoto o presencial.
d) Coste mensual por cada TeraByte de espacio extra en la nube externa que exceda del número contratado inicialmente.
e) Coste mensual por cada Equipo/MV extra que exceda del número contratado inicialmente.

El contratista deberá presentar la oferta de cada uno de estos conceptos en la forma que se describe en el Anexo 1 del PCAP.

Prescripción sexta.- PROPIEDAD DE LOS DATOS Y CONFIDENCIALIDAD

a) Confidencialidad.

Toda la información calificada de confidencial a la que el CDRiMMB tenga que dar acceso al contratista con motivo de la prestación del servicio contratado, solo podrá ser utilizada por este para el fin indicado, respondiendo, en consecuencia, de los perjuicios que el incumplimiento pudiera ocasionar al CDRiMMB.

El contratista informará al CDRiMMB de todas las alteraciones que proponga realizar en la estructura de archivos que contengan datos de carácter personal, antes de llevarlas a cabo, así como de la intención de suprimir o crear archivos que contengan este tipo de datos, con el fin de que el CDRiMMB, como titular de dichos archivos, pueda notificar con la debida antelación a la Agencia de Protección de Datos estas variaciones. En todo caso, cualquier variación estará sujeta al acuerdo expreso previo del CDRiMMB.

b) Deber de secreto profesional.

El contratista deberá incluir en los contratos que tenga establecidos con sus trabajadores una cláusula de confidencialidad por la que estos se comprometen a no revelar ni utilizar en beneficio propio o de terceros la información que conozcan en función de su cometido, tanto durante el tiempo que dure el contrato, ya sea laboral o de cualquier otro tipo admitido en derecho, como posteriormente a la finalización de dicha relación.

Se cumplirán íntegramente los mandatos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Prescripción séptima.- SEGURIDAD, AUDITORÍAS Y MEDIDAS MÍNIMAS DE SEGURIDAD.

1.-Seguridad.

El contratista seguirá los procedimientos establecidos en el CDRiMMB relativos a las operaciones de sus Sistemas de Información.

2.- Sistemas de copias de seguridad.

El contratista se compromete a seguir los procedimientos descritos tanto en lo que respecta a la salvaguarda de datos como a su restauración en caso de que sea necesario.

3.- Datos de carácter personal.

El contratista se compromete, respecto a los archivos de datos de carácter personal, a cumplir las normas de seguridad que establece el documento de seguridad del CDRiMMB, de acuerdo con la legislación vigente.

4.- Disponibilidad de los datos.

El contratista solucionará, en el menor tiempo posible, las incidencias que eventualmente se puedan producir, especialmente aquellas que pongan en riesgo la disponibilidad de los datos para alguno de los procesos del CDRiMMB.

5.- Integridad de los datos.

El contratista velará por la preservación de la integridad de los datos del CDRiMMB.

El contratista se compromete a informar de las hipotéticas carencias de integración observadas en su día a día, con el fin de que los proveedores de las aplicaciones puedan gestionarlas o, si el problema se origina en una arquitectura de aplicaciones deficiente, se pueda proceder a su modificación.

6.- Acceso de usuarios.

El CDRiMMB tiene previsto establecer una política, así como los procedimientos asociados, para la gestión de identidades y autenticación de los usuarios de sus Sistemas de Información.

El contratista deberá conocer y aplicar los procedimientos descritos cuando estos comiencen a ser operativos.

7.- Plan de contingencia.

El CDRiMMB tiene previsto desarrollar un Plan de Contingencias.

El contratista deberá conocer y comprender su rol dentro del mismo y ejecutar dicho Plan en caso de activación de los procedimientos de contingencia.

8.- Auditoría de los Sistemas de Información.

El CDRiMMB podrá, si lo considera necesario, ordenar la realización de una auditoría de los sistemas de seguridad del CDRiMMB una vez al año, y el contratista deberá permitir el acceso de los auditores informáticos y facilitarles las pruebas que soliciten para cumplir el objetivo de la auditoría.

Asimismo, los auditores informáticos podrán verificar si se cumplen los estándares de calidad.

Si los resultados de la auditoría determinan que el CDRiMMB debe modificar los procedimientos relativos a la operación de los Sistemas de Información, el contratista deberá seguir los nuevos procedimientos.

Prescripción octava.- TIEMPOS DE RESPUESTA Y RESOLUCIÓN DE INCIDENCIAS. PENALIZACIONES ASOCIADAS POR INCUMPLIMIENTO

El contratista adquiere el compromiso de responder y resolver los problemas o incidencias que se presenten respecto a la asistencia técnica y soporte, al servicio de mantenimiento correctivo, a las actualizaciones de firmware y paquetes de seguridad recomendados por los fabricantes de los diferentes elementos que conforman el sistema

informático, y en general todos aquellos que puedan ocasionar un perjuicio al CDRiMMB de las Atarazanas Reales y Museu Marítim de Barcelona.

Definiciones

Definición de "Tiempo de respuesta": Es el tiempo transcurrido entre la comunicación de la incidencia al contratista por el canal previsto y el momento en que este asume la responsabilidad de la resolución de la incidencia, asignando los recursos necesarios para cumplir el tiempo de resolución.

Definición de "Tiempo de resolución": Es el tiempo transcurrido desde la comunicación al contratista de la incidencia por los canales previstos (indicado en la Prescripción segunda) hasta que la incidencia queda resuelta y documentada por el contratista. No se contabilizan los períodos en que el contratista esté a la espera de respuesta por parte de los técnicos o usuarios del CDRiMMB o de terceros proveedores.

Definición de "Día laborable": Jornada de lunes a viernes no festivo (según el calendario oficial de la autoridad laboral correspondiente), de 0 a 24 horas.

Definición de "Horario de servicio": Es el intervalo horario en que se atienden peticiones, consultas y se comunican las incidencias. Para este contrato, el horario de servicio será los días laborables no festivos en la ciudad de Barcelona, de lunes a viernes de 8 a 18 horas.

Nivel de cumplimiento: De manera general, se prevé que se cumplan los tiempos de resolución establecidos en la mayoría de incidencias. No obstante, en casos de incidencias de nivel crítico y alto se contempla que puedan darse situaciones excepcionales que requieran más tiempo del estipulado, siempre que estén plenamente justificadas. Estos casos específicos deberán ser validados y aprobados por el equipo técnico TIC del Museo.

El equipo técnico TIC del Museo evaluará el nivel de cumplimiento del tiempo de resolución de forma individual para cada incidencia, a efectos de aplicar la penalización correspondiente en casos de incidencias de nivel crítico y alto.

Procedimiento de evaluación de incidencias:

Si el contratista considera que no podrá resolver una incidencia dentro del tiempo de resolución estimado, estará obligado a comunicarlo al equipo técnico TIC del Museo dentro del primer 50 % del tiempo de resolución asignado (es decir, dentro de las primeras 4 horas para nivel crítico, y las primeras 12 horas para nivel alto), exponiendo los motivos del posible retraso. Una vez evaluado, el equipo técnico del Museo decidirá si aplica una excepción a la penalización para dicha incidencia.

La resolución de incidencias será gestionada de forma continua hasta su cierre y no estará sujeta al horario de servicio.

Las incidencias se clasifican en tres niveles, con tiempos de resolución máximos en horario de servicio según su nivel (crítico, alto o bajo). El cumplimiento de estos tiempos para niveles crítico y alto estará sujeto a penalizaciones individuales por incidencia, de acuerdo con las condiciones mencionadas en el apartado “Nivel de cumplimiento” y según los detalles para cada nivel especificados a continuación:

A) Nivel CRÍTICO:

Tiempo máximo de respuesta: 1 hora en horario de servicio
Tiempo máximo de resolución: 8 horas en horario de servicio
Penalización: 50 € por hora de retraso.

Descripción:
Incidencias de nivel crítico que afectan de forma global y que impiden la operativa de los sistemas contemplados, provocando una completa inoperatividad del sistema. Se incluyen, entre otras:

- Parada o incidencias en cualquiera de los equipos HOST físicos que soportan los sistemas de virtualización de servidores corporativos y VDI (escritorios remotos).
- Parada de servidores corporativos.
- Incidencias que impiden la conexión de los equipos de trabajo o teletrabajo.
- Actuación en caso de sospecha de intrusión en bases de datos o información protegida.
- Actuación para limpieza o desinfección en caso de ataque por código malicioso o malware.
- Actuación ante incidencias que afectan a la integridad, confidencialidad y disponibilidad de la información.

B) Nivel ALTO:

Tiempo máximo de respuesta: 2 horas en horario de servicio
Tiempo máximo de resolución: 24 horas en horario de servicio
Penalización: 40 € por hora de retraso.

Descripción:
Incidencias de nivel alto que, aunque no impiden la operativa de los sistemas contemplados, suponen un modo degradado que afecta a la calidad del servicio o a algún proceso específico no crítico. Se incluyen, entre otras:

- Solicitud de información o verificación por parte del Museo sobre el funcionamiento de cualquier servicio.
- Incidencias relacionadas con el servicio de correo corporativo.
- Actuación frente a problemas de saturación o rendimiento de un servidor o servicio.

- Actuación ante una alarma crítica emitida por el software de vigilancia automatizada de los sistemas.
- Gestión y eliminación de entradas en listas negras.
- Actuación en solicitudes urgentes de modificaciones en las reglas de filtrado del firewall.
- Actuación en creación, asignación o cambio de permisos de usuarios, en solicitudes urgentes.

C) Nivel BAJO:

Descripción:
Incidencias de nivel bajo no incluidas en los supuestos anteriores y que no afectan al funcionamiento habitual, ni a las funcionalidades imprescindibles, ni a la calidad del servicio; o bien, por razones técnicas, deben programarse en fechas específicas acordadas para su ejecución.

Se incluyen, entre otras:

- Instalación, configuración y renovación de certificados de seguridad programada con antelación.
- Asesoramiento general al equipo técnico TIC del Museo.
- Elaboración de informes especiales y específicos requeridos por el Museo.
- Instalación de actualizaciones de firmware, complementos (plugins) del sistema y/o nuevas versiones de bibliotecas o programas, previa programación conjunta con el equipo técnico TIC del Museo.

No se aplicará el cómputo del ANS (Acuerdo de Nivel de Servicio) sobre este tipo de incidencias, excepto en los siguientes supuestos:

- Se permitirá un único cambio de técnico responsable del contrato/coordinador estratégico durante la vigencia del contrato (salvo sustituciones puntuales por enfermedad u otras causas justificadas). Su incumplimiento llevará aparejada una penalización de 500 € por infracción.

- La reiteración en no adoptar las medidas de seguridad mínimas definidas en la cláusula 7ª del PPTP implicará una penalización de 250 € por infracción.

CLASIFICACIÓN	TIEMPO DE RESOLUCIÓN
Crítica	8 horas durante el horario de servicio
Alta	24 horas durante el horario de servicio
Baja	De forma general no se aplicará el cómputo del ANS sobre este tipo de incidencias, salvo en los casos de incumplimiento especificados, en cuyo caso serán de aplicación las penalizaciones consignadas.

Barcelona,

Eva M. Carralero Zabala
Auxiliar informática

Maria José Fajardo Garcia
Gerente

Metadades del document

Núm. expedient	CDRB/2025/0034708
Tipus documental	Plica
Títol	PPPT TIC_CASTELLÀ

Signatures

Signatari	Acte	Data acte
Eva Maria Carralero Zabala (TCAT)	Signa	30/07/2025 07:56
Maria José Fajardo Garcia (TCAT)	Signa	30/07/2025 09:01

Validació Electrònica del document

Codi (CSV)	Adreça de validació	QR
b031ecfa23c9629db371	https://seuelectronica.diba.cat	