Consorci
Administració Oberta
de Catalunya

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARE PARA LA CONTRATACIÓN DE UN SERVICIO DE ALOJAMIENTO CLOUD Y EXPLOTACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CONSORCI AOC
(EXPEDIENTE AOC-2022-64)

Índice de cláusulas y anexos

Se hace constar que se trata de una traducción automatizada y que, en caso de discrepancia, prevalece la versión catalana.

1. Introducción

El Consorci Administració Oberta de Catalunya (en adelante Consorci AOC), como organismo público enfocado a ofrecer servicios para la modernización y digitalización de las Administraciones Públicas catalanas, dispone de diferentes plataformas tecnológicas actualmente alojadas en diferentes Centros de Proceso de Datos (CPD) , con el objetivo de diversificar riesgos y disponer de mecanismos de contingencia en caso de incidencia en alguna de las plataformas.

Algunas de estas plataformas actuales, están basadas en hardware propiedad del Consorci AOC y están desplegadas en un CPD " *on-premise* " (en local). Otras plataformas están desplegadas en un cloud privado del Consorci AOC que funciona de acuerdo al modelo de " *Cloud computing* ". Finalmente se han iniciado algunas experiencias con proyectos puntuales para trasladar sus plataformas al cloud público para aprovechar la gran capacidad de éste en cuanto a escalabilidad, alta disponibilidad, facilidad de desarrollo, provisión y elevado nivel de servicio. Estos proyectos se han iniciado de manera individual, como primeros ensayos que deben servir al Consorci AOC para tomar experiencia en el funcionamiento del cloud público y poder definir una estrategia manifiesta de evolución de los servicios del Consorci AOC al cloud público.

Los contratos que actualmente están vigentes con los diferentes proveedores que ofrecen estos servicios de Centros de Proceso de Datos y cloud privado finalizan en septiembre de 2023. Estos contratos han agotado las posibilidades de crecimiento frente al aumento constante de nuevas plataformas e infraestructura tecnológica que ha requerido el Consorci AOC en los últimos años para poder desarrollar tanto los nuevos servicios que ha desarrollado, como especialmente para absorber el destacado incremento en la demanda que han presentado los servicios que ya ofrecía. Por otra parte, los contratos de las iniciativas en el cloud público finalizan a mediados de 2022, pero no disponen de la opción de ser prorrogados y tampoco permiten el despliegue de nuevos servicios o plataformas.

Por todas estas razones, el Consorci AOC ha decidido pujar un nuevo concurso que permita, por un lado, gestionar el incesante incremento de infraestructura tecnológica que requiere para poder continuar ofreciendo sus servicios con todas las garantías de disponibilidad y nivel de servicio, y en paralelo, que le permita definir y desarrollar una estrategia transversal de evolución en el cloud público de una parte cada vez más significativa de sus servicios.

El objetivo de esta nueva licitación es implantar un nuevo modelo de gestión global de sus plataformas y tecnologías TIC más eficiente, que aproveche las mejoras tecnológicas presentes y futuras que van apareciendo en el mercado TIC, y que permita una optimización de los recursos para conseguir soluciones flexibles, ágiles y sostenibles.

Esta transformación del modelo global de gestión TIC debe permitir al Consorci AOC implantar una estrategia transversal que se pueda utilizar como hoja de ruta para mejorar la eficiencia y la eficacia de sus servicios, a la vez que dar respuesta a nuevos requerimientos y necesidades de la organización, a través de distintos ejes:

- Aplicando economías de escala.
- Regularizando y racionalizando la demanda.
- Obteniendo sinergias y optimizando el uso de recursos de los proveedores de servicios.
- Homogeneizando y estandarizando los servicios.
- Alineando servicios TIC con las necesidades de la organización.
- Dotándose de instrumentos y prácticas de Gobernanza de los servicios que garanticen la consecución de los objetivos y respondan a las necesidades de la organización.
- Disponiendo de mecanismos innovadores y flexibles para la adquisición de servicios TIC.

Los objetivos a conseguir con la implantación del nuevo modelo TIC en lo que afecta a la contratación de los servicios de alojamiento de infraestructura tecnológica son:

- Obtener más y mejores prestaciones de servicios TIC por el Consorci AOC con los mismos recursos económicos.
- Aumentar la eficiencia operacional y la racionalización de los recursos.
- Homogeneizar, simplificar y mejorar la gestión de los servicios.
- Disponer de un mejor control de rendimiento de los servicios.
- Gestionar de forma más flexible la asignación de recursos TIC a los diferentes servicios en función de la demanda.
- Aumentar la velocidad y agilidad en la entrega de estos recursos TIC.
- Ofrecer niveles de adaptación inmediata, gracias a la escalabilidad en el crecimiento/decrecimiento de los recursos TIC en función de las necesidades de negocio.
- Garantizar la continuidad de sus servicios incrementando los niveles de disponibilidad, resistencia a caídas, resiliencia y seguridad.
- Adaptarse a un mundo digital en constante cambio y liderar los avances tecnológicos.

Para alcanzar los objetivos marcados será necesario aplicar soluciones de mercado a la prestación de los servicios, tanto desde el punto de vista de la tecnología como de los procesos de gestión y provisión del servicio, incorporando las mejores prácticas que se aplican a organizaciones con complejidad similar a la del Consorci AOC.

2. Objeto de la licitación

El presente pliego se divide en 2 bloques de tareas bien diferenciadas que se contratarán mediante 2 lotes independientes y no exclusivos. Los licitadores se podrán presentar a uno oa los 2 lotes, en función de lo que crean conveniente, sin que este hecho implique ningún beneficio o perjuicio en la valoración de las ofertas presentadas.

Este documento recoge los requerimientos para la valoración de los 2 lotes. El formato de las ofertas presentadas deberá ajustarse a la descripción realizada en este pliego.

El objeto de cada uno de los lotes es el siguiente:

- **Lote 1: Servicio de Definición e Implantación de la Estrategia de Migración en el Cloud (SDIEMC)** para la definición e implantación de la estrategia cloud del Consorci AOC que impulse la adopción del nuevo modelo TIC.

- **Lote 2: Servicios de provisión de infraestructura de cloud público, y administración, operación, mantenimiento y explotación cloud.** En este lote se incluye toda la colección de servicios y recursos de cloud público, necesarios para la ejecución de los servicios del Consorci AOC que se determinen que deben transformarse y desarrollarse a lo largo de la duración del contrato sobre un cloud público, así como la puesta en marcha, administración, gestión y explotación de estos servicios de cloud público.

La duración de cada uno de estos lotes irá desde el día siguiente a la formalización del contrato y hasta el 31 de diciembre de 2023, sin que exista la posibilidad de que se puedan prorrogar.

3. Lote 1: Servicio de Definición e Implantación de la Estrategia de Migración en el Cloud (SDIEMC)

Las tareas que forman parte del alcance del lote 1 son las siguientes:

- **Asesoramiento en la definición del plan de transformación estratégico** . Asesoramiento al equipo del Consorci AOC para definir el plan corporativo de transformación estratégica y de evolución hacia entornos cloud. Este plan debe ser global y de alcance en toda la organización, y debe determinar el camino por la adopción de la tecnología cloud a partir del nivel de madurez cloud del modelo TIC actual. Dentro del plan de transformación se tendrá que determinar la línea base con los resultados esperados y las decisiones estratégicas de cómo alcanzarlos con el menor tiempo posible, estableciendo los marcos de gobernanza y organización, e identificando las principales barreras de adopción. Otro punto clave será el soporte especializado y el acompañamiento al equipo del Consorci AOC en el uso de las tecnologías cloud a lo largo de todo el proceso de adopción al nuevo modelo TIC propuesto, con el objetivo de garantizar el éxito del proceso de transformación que se promueve.

- **Puesta en marcha de la estrategia cloud del Consorci AOC** . A partir de la información que se trasladará a la empresa adjudicataria, ésta deberá realizar un análisis exhaustivo de los diferentes CPDs del Consorci AOC, así como de las diferentes iniciativas de migración al cloud público que se estén llevando a cabo, con el objetivo de definir de forma detallada la arquitectura de CPDs futura del nuevo modelo TIC. Se deberá estudiar la estrategia de cloud público óptima para el Consorci AOC analizando la viabilidad de una solución multi-cloud hacia una solución single-cloud. El adjudicatario tendrá que definir detalladamente la situación final deseada en un contexto cloud después de racionalizar, reorganizar, y reestructurar los diferentes CPDs. El adjudicatario tendrá que determinar el plan de proyecto para ejecutar la transición, incluyendo las fases del proyecto de transición y sus plazos.

- **Definir las métricas e indicadores para evaluar el grado de avance de la adopción en el nuevo modelo TIC** . Precisar las métricas e indicadores que deben ayudar a medir la evolución del proceso de adopción del nuevo modelo TIC, el grado de madurez alcanzado en el nivel de aceptación de los sistemas cloud (según CMM) y los beneficios aportados por el nuevo modelo . Las métricas e indicadores de evaluación deben servir para detectar y prevenir retrasos en la adopción de la estrategia cloud definida identificando cuellos de botella, descoordinación o desalineamiento de prioridades entre los distintos equipos de trabajo internos. El objetivo de SDIEMC debe ser en todo momento reconducir este tipo de situaciones alineando los intereses de todos los equipos de trabajo con la estrategia del plan de transformación. Estas métricas e indicadores tendrán que reflejarse en un cuadro de mando y en un conjunto de informes de control que permitan conocer en todo momento el estado de situación y facilitar la toma de decisiones.

- **Análisis y catalogación de los servicios y plataformas actuales del Consorci AOC** . Catalogación exhaustiva de las principales plataformas y servicios del Consorci AOC para determinar la hoja de ruta óptima de adopción de las tecnologías cloud de acuerdo a sus condiciones y al grado de madurez de sus procesos tecnológicos. Deberá tenerse en cuenta especialmente las previsiones de crecimiento y los diferentes proyectos que ya estén llevando a cabo la transformación hacia el nuevo modelo TIC. La hoja de ruta definida deberá incluir para cada servicio y plataforma analizados, el modelo de cloud idóneo (público, privado o híbrido), el patrón de migración (Re-host, Re-platform, Re-architect, Re-build , ...), la propuesta de arquitectura (máquinas virtuales, contenedores, microservicios, desarrollos con tecnologías propietarias de cada cloud, etc.) con un enfoque " *cloud first* " y de pago por uso, la selección del/de los proveedor/ s cloud, así como la categoría de servicios (IaaS, PaaS o SaaS) recomendados, el detalle del catálogo de servicios cloud a utilizar, sus relaciones, el alineamiento

con la plataforma DevOps, la adecuación a la estrategia cloud definida, revisando el diseño de la red de comunicaciones, etc.

- **Estandarización cloud y catálogo de servicios comunes** . Derivado del punto anterior, se tendrán que determinar los requerimientos necesarios que debe cumplir cualquier solución de cloud público para poder ser utilizada y se tendrá que definir el catálogo de servicios cloud estándar, las diferentes plantillas base de recursos y el conjunto de servicios comunes que preferentemente tendrán que utilizar las plataformas y servicios del Consorci AOC que se vayan transformando y adaptando al nuevo modelo TIC. Este nuevo catálogo de servicios cloud estándar tendrá que ofrecer y priorizar el formato de pago por uso. Además, se tendrán que definir las directrices que tendrán que seguir todos los servicios y plataformas que se vayan transformando en el nuevo modelo TIC, destacando las actividades clave de adaptación de los procesos actuales. También se deberá incluir en este apartado el análisis de cualquier nuevo proyecto o iniciativa llevada a cabo por el Consorci AOC para encajarla y alinearla con el nuevo modelo TIC:

    - Definición de los modelos de buenas prácticas en el cloud.
    - Creación del marco de referencia de arquitecturas cloud.
    - Definición del modelo gobierno y roles.
    - Definición de la gestión de cuentas y accesos.
    - Definición del modelo de relación con sus proveedores.
    - Diseño del modelo de costes.
    - Diseño de la solución de almacenamiento.
    - Diseño de la solución de backup.
    - Diseño de la solución de monitoreo.
    - Diseño de la solución de cifrado y protección de los datos.
    - Diseño de la solución para el plan de continuidad de negocio o plan contingencia.
    - Definición de los requerimientos de seguridad y diseño de la solución de integración con las herramientas SIEM y/o SOAR.
    - Definición de los requerimientos de auditoría.
    - Definición de la nomenclatura de objetos.

- **Determinar el marco de gobernanza entre la solución cloud propuesta y el modelo actual de CPDs del Consorci AOC** . Definir, implementar y comunicar los modelos de gobernanza de la solución cloud propuesta con el objetivo de minimizar los riesgos de gestión y financieros del nuevo modelo TIC. Determinar las políticas, procedimientos, roles y herramientas de gobernanza, transversales a toda la organización, que permitirán la implementación de estos modelos o optimizando los esfuerzos de adopción del nuevo modelo TIC y amortiguando la complejidad creciente de los diferentes entornos de infraestructura y las tecnologías diversas que irán apareciendo a medida que se vaya desplegando el nuevo modelo TIC. El objetivo de este marco de gobernanza debe ser evitar abusos de autogestión por parte de los diferentes equipos de trabajo que puedan provocar un entorno caótico difícil de reconducir, pero a la vez debe conseguirse el difícil equilibrio de evitar también modelos cuya excesiva rigidez pueda dificultar la productividad. El marco de gobernanza deberá sentar las bases que permitan el crecimiento constante y la mejora continua del nivel de madurez cloud (según el modelo CMM) del Consorci AOC, adaptando las políticas, procedimientos y herramientas de gobernanza a medida que vaya aumentando el nivel de madurez del Consorci AOC y deberá definirse el modelo de competencias organizativas para desplegar la estrategia cloud y el impacto que supone sobre el modelo de gestión de proveedores. Es importante destacar que todas estas tareas se tendrán que llevar a cabo bajo la dirección y control de la Oficina de Gobernanza y Calidad (OGQ) del Consorci AOC y que conjuntamente con la OGQ se tendrán que adaptar los procesos actuales de gobierno, los modelos organizativos, los sistemas de control, la gestión de las cuentas de los diferentes entornos cloud y CPDs, o las políticas de seguridad en los requisitos del nuevo modelo TIC.

- **Selección de las herramientas de administración y gestión de entornos de cloud híbrido** . Proponer las herramientas de gestión de infraestructuras en la nube, p. ej. herramientas de tipo

Cloud Management Platform (CMP) y/o de tipo *Configuration Management DataBase* (CMDB), que permitan la administración de un inventario global, así como la gestión centralizada de las diferentes infraestructuras cloud (públicas y privadas) ofreciendo una visión de cloud híbrido con las siguientes funcionalidades y características mínimas:

- Integración y abstracción de todas las infraestructuras de cloud públicas y privadas seleccionadas en el nuevo modelo TIC.
- Compatible tanto con el mayor número posible de proveedores de cloud público como con el mayor número de tecnologías de cloud privado.
- Gestión unificada de identidades y seguridad de accesos.
- Gestión centralizada del inventario de todos los recursos cloud.
- Gestión centralizada de costes.
- Gestión centralizada de la seguridad y cumplimiento normativo.
- Gestión centralizada de las labores de automatización de las plataformas DevOps.

Estas herramientas tendrán que posibilitar la automatización de los procesos de aprovisionamiento de nuevos servicios cloud, reduciendo el tiempo de suministro y facilitando la toma de decisiones operativas. Es importante destacar que estas herramientas tendrán que permitir también la definición y configuración de la infraestructura y recursos cloud según el paradigma *Infraestructure as Code* (IaC) a través de scripts y archivos de definición en un lenguaje de alto nivel que permita su ejecución y despliegue en diferentes soluciones cloud.

- **Fijar y automatizar las políticas de control y supervisión** : selección, configuración y puesta en marcha de las herramientas necesarias que permitan automatizar las políticas de control para monitorizar el uso de los recursos y la actividad cloud con el objetivo de asegurar que la gestión sea óptima, que se respeten los modelos de gobernanza, que se minimicen los errores humanos en la interacción con los recursos cloud, que los costes facturados están alineados con los costes previstos inicialmente y que el crecimiento de estos costes está en todo momento bajo control .
  Se tendrán que definir también los roles responsables de llevar a cabo la supervisión de estas tareas de control, así como los cuadros de mando y los informes de control que periódicamente se tendrán que presentar en el Consorci AOC.

- **Definir el plan de seguridad** . Establecer las normas, procedimientos, políticas y requerimientos de seguridad, que garanticen el cumplimiento de la normativa vigente, evaluando el impacto que supone el nuevo modelo cloud y adoptando el principio de la seguridad por diseño. Adaptación de la gestión de seguridad del Consorci AOC para la incorporación de los servicios cloud, recopilando el inventario de activos, estableciendo la arquitectura de seguridad, el esquema de líneas de defensa y el perímetro de seguridad propuestos, la gestión de identidades y la seguridad de accesos, la fragmentación de redes y subredes, los requerimientos de auditoría y centralización de logs, la detección de amenazas, etc.
  El adjudicatario de este lote finalmente será responsable de definir los procedimientos y herramientas (SIEM, SOAR, etc.) que permitan ofrecer una visión y control generales de la seguridad, así como detectar y comunicar los incidentes de seguridad que puedan producirse , con el correspondiente análisis forense.

- **Definir el plan de backup** . Definir el plan de backup integral y automatizable que pueda cubrir todos los tipos de datos, infraestructura y recursos IT del catálogo de servicios del Consorci AOC independientemente del CPD o tipo de cloud donde estén desplegados. Este plan de backup deberá prestar especial atención al garantizar la coordinación de los distintos orígenes de datos que formen parte de un mismo servicio. El adjudicatario deberá determinar las políticas de cifrado y los requerimientos de la solución de backup para cumplir con la normativa vigente en el ámbito de los backups (al menos ENS nivel alto y RGPD). También se tendrán que establecer las diferentes políticas de retención de los backups, el RPO (*Recovery Point Objective*) y el RTO (Recovery Time Objective) de cada uno de los servicios, así como el soporte y la ubicación de las copias de seguridad. Por último, el adjudicatario deberá determinar también los planes de continuidad de negocio y/o de contingencia para cada uno de los servicios que los requieran,

incluyendo los nuevos Acuerdos de Nivel de Servicio (ANS) y el diseño de la solución de Disaster Recovery propuesta .

- **Establecer los modelos de cálculo de costes de los servicios y plataformas ofrecidos en modalidad de pago por uso** . Está obligado e implementado los modelos para calcular los costes económicos, en todas sus vertientes: infraestructura, servicios, operación, mantenimiento, monitorización, seguridad, etc., tanto de los servicios comunes de cloud, como de los elementos estandarizados con el objetivo de poder determinar los costes anuales de los diferentes servicios y plataformas que se desplieguen en el cloud público en modalidad de pago por uso. Estos modelos de cálculo de costes se tendrán que ir perfilando y ajustando a medida que vaya avanzando el plan de transformación y aumentando el grado de madurez cloud del Consorci AOC. El adjudicatario también deberá proponer las herramientas de gestión del presupuesto de la infraestructura cloud que permitan realizar el seguimiento y el control del gasto, así como el sistema de clasificación y categorización de los costes que permita un control granular por entorno, servicio, plataforma , etc. Además, tendrán que definirse los modelos de informes de control de costes periódicos que permitan contrastar los costes reales con los modelos previstos. Estos informes tendrán que poner el foco al intentar anticipar futuras desviaciones del gasto del modo de pago por uso, así como establecer patrones de gasto que puedan anticipar los gastos futuros.

- **Proponer la guía prescriptiva y adaptar el marco de referencia DevOps** . Proponer los cambios organizativos, los ajustes en la metodología o en la forma de trabajar, así como definir las nuevas herramientas que deben permitir la automatización de los procesos y el aprovisionamiento de las plataformas necesarias para la integración continua (CI) y el despliegue continuo (CD) a lo largo del ciclo de vida completo de los servicios del Consorci AOC según el modelo de gestión DevOps. Este nuevo marco de referencia DevOps propuesto deberá estar adaptado a las necesidades del contexto del nuevo modelo TIC y estar preparado para funcionar en entornos multi cloud.

- **Impulsar la transformación digital que requiere el nuevo modelo TIC** . Colaborar con el Consorci AOC en impulsar la transformación digital que requiere el nuevo modelo TIC, fomentando la implantación de un cambio cultural en la organización que permita una adopción progresiva de las tecnologías cloud sin provocar disrupciones abruptas tanto en el ámbito tecnológico , como operativo y económico. El SDIEMC por tanto tendrá que convertirse en un vector de impulso en la promoción y dinamización del nuevo modelo TIC, fomentando su aceptación por parte de toda la organización.

- **Definición del plan de capacitación necesario para acelerar la adopción del nuevo modelo TIC** . Definir los equipos de trabajo y planes de formación que el Consorci AOC deberá llevar a cabo para ejecutar la implantación del nuevo modelo TIC: se definirá cuál sería la organización interna del Consorci AOC y la organización de proveedores más adecuadas para llevar a cabo estrategia de transformación, indicando cuáles son las habilidades clave y las necesidades de formación para cada uno de los miembros del equipo (arquitectos, técnicos de sistemas, desarrolladores, gestor económico del cloud, etc.) tanto interno del Consorci AOC como de sus proveedores. Con esta información se diseñará el plan de capacitación que debe llevar a cabo el Consorci AOC, en el ámbito de las tecnologías cloud, y las necesidades formativas de los diferentes equipos de trabajo con los objetivos de facilitar la adopción paulatina del nuevo modelo TIC y la obtención de los beneficios intrínsecos de éste sin la necesidad de tener que esperar a la finalización del proceso de adopción.

- **Diseño de los entornos de ejecución de contenedores y plataformas PaaS.** Proporcionar al Consorci AOC el diseño de los entornos de ejecución de contenedores, plataformas PaaS y servicios SaaS que pueden ser consumidos bajo la modalidad de pago por uso, y que estén alineados con la estrategia cloud y la arquitectura de referencia. El licitador deberá determinar el modelo de entrega de los entornos de ejecución de contenedores, plataformas PaaS y servicios SaaS, y deberá fijar el catálogo de servicios ofrecidos, definiendo los aspectos de

comunicaciones, escalado, seguridad, operación y backup, monitorización o explotación . Por último el licitador deberá definir las políticas de uso de estos entornos de ejecución de contenedores, plataformas PaaS y servicios SaaS, y diseñar los modelos de costes de cada uno de ellos.

- **Documentación de la estrategia cloud propuesta** . Desarrollo de un espacio web donde se recoja y se organice de forma exhaustiva toda la documentación relativa a este lote: hojas de ruta con los estudios, análisis y definiciones de arquitectura propuestos, catálogo de servicios cloud estandarizados, planes de capacitación, modelos de costes económicos, métricas e indicadores del grado de adelanto, plantillas, etc.

Para poder llevar a cabo todas estas tareas, SDIEMC deberá estar formado por un equipo de trabajo multidisciplinar regido por un marco metodológico ágil. El adjudicatario deberá dotar al SDIEMC con una amplia oferta de expertos que puedan llevar a cabo con garantías las diferentes tareas descritas en este pliego: líder en transformación digital, consultor/asesor en estrategia cloud, arquitecto cloud, consultor cloud, consultor de infraestructura y experto en seguridad cloud. Aunque la mayoría de estos perfiles tendrán dedicación parcial, sí se requerirá como mínimo que 1 experto (el arquitecto cloud) esté asignado con dedicación completa para poder coordinar con éxito a los diferentes miembros del SDIEMC .

A nivel indicativo, las horas necesarias para llevar a cabo el servicio se estiman en 5,995 horas. Estas horas están calculadas en base al supuesto de que el contrato estará operativo el 1 de agosto de 2022 y que llegará hasta el 31 de diciembre de 2023. Aunque se pudiera retrasar la fecha de inicio del servicio, la fecha de finalización se mantendrá fija en el 31 de diciembre de 2023. Por este motivo es importante destacar que el alcance de este lote se mantendrá en todo momento y que el adjudicatario tendrá que incrementar la dedicación de los recursos asignados a fin de poder garantizar que se alcanza el alcance definido en este apartado en caso de que el inicio del contrato se demore más allá del 1 de agosto de 2022.

A continuación se enumera el conjunto mínimo de entregables que tendrán que entregarse dentro del alcance de este lote, aunque se deja la opción al licitador de ampliar este catálogo. Todos los entregables serán documentos vivos que se tendrán que ir actualizando continuamente a lo largo de la duración del contrato.

- Análisis de situación actual.
- Plan estratégico cloud.
- Requerimientos cloud y servicios comunes.
- Propuesta de arquitectura de CPDs y aplicaciones.
- Marco de gobernanza.
- Plan de control y supervisión.
- Informes de control y grado de avance del nuevo modelo TIC.
- Modelo de cálculo de costes.
- Plan de seguridad.
- Plan de backup.
- Diseño de los entornos PaaS y plataformas de ejecución de contenedores.
- Plan de capacitación.

Toda la documentación estará disponible y actualizada en una herramienta de gestión documental propiedad del Consorci AOC. A principios del proyecto se definirá el conjunto de herramientas que apoyarán estos aspectos documentales.

4. Lote 2: Servicios de provisión de infraestructura de cloud público, y administración, operación, mantenimiento y explotación

El objeto de este lote incluye 2 clases de servicios notoriamente diferenciados:

- Toda la colección de servicios, infraestructura, licencias y recursos de cloud público necesarios para la ejecución de los servicios del Consorci AOC que deben transformarse y desarrollarse a lo largo de la duración del contrato sobre un cloud público, y que más adelante se detallan.

  El adjudicatario tendrá que proporcionar la infraestructura y recursos necesarios para los entornos de integración, preproducción y producción. Estos 3 entornos se tendrán que segmentar y aislar para poder funcionar de forma totalmente autónoma e independiente.

  Es importante destacar que tanto las suscripciones como las cuentas e identidades del cloud público necesarios para la gestión de los entornos de integración, preproducción y producción, tendrán que ser de titularidad del Consorci AOC.
  En el apartado ***4.11 Servicios de provisión de infraestructura de cloud público*** se detallan los servicios que forman parte de esta clase.

- La puesta en marcha, administración, gestión y explotación de estos servicios, infraestructura y recursos de cloud público. Dentro de esta clase de servicios, se incluye el Mantenimiento, Administración, Despliegue de soluciones de infraestructura, Explotación y Monitorización, de las diferentes plataformas tecnológicas donde se soportan las aplicaciones de negocio del Consorci AOC con el objetivo de ofrecer las máximas garantías de capacidad y disponibilidad, así como la infraestructura actualizada en las versiones más recientes y óptimas para los citados servicios.

  En el apartado ***4.2 Servicios de puesta en marcha, administración, gestión y explotación*** se detallan los servicios que forman parte de esta clase.

Las 2 clases de servicios indicadas deben englobar y dar alcance a los siguientes servicios de negocio que el Consorci AOC ya está transformando para poder desplegarlos sobre el cloud público de Amazon Web Services (AWS en adelante) a lo largo del año 2022.

La transformación de estos servicios se está haciendo de acuerdo a los principios y buenas prácticas del patrón de diseño *Re-architect* para convertirlos en servicios cloud nativos. La nueva arquitectura tecnológica, así como la estimación de costes prevista de los diferentes entornos de integración, preproducción y producción, para cada uno de estos servicios la puede encontrar en el ***ANEXO1 Arquitectura tecnológica y estimación de costes inicial de infraestructura previstos*** :

- **DESALLO** (https://www.aoc.cat/serveis-aoc/desa-l/). El gestor documental corporativo del Consorci AOC que sirve como repositorio electrónico de los documentos que generan los diferentes servicios de administración electrónica que presta el Consorci AOC.

- **EACAT Trámites** (https://www.aoc.cat/serveis-aoc/eacat-tramits/). Servicio que permite la tramitación entre administraciones de forma rápida y segura, reduciendo los plazos y costes de gestión administrativa.

- **Validador (PSIS)** (https://www.aoc.cat/portal-suport/validador-base-conocimiento/). Servicio que permite la verificación de certificados, la creación y verificación de sellos de tiempo y firmas digitales, así como el archivado de las mismas.

- **VALID 2.0** (https://www.aoc.cat/serveis-aoc/valid/). El integrador de servicios de identidad digital de Cataluña para que los ciudadanos tengan todas sus opciones para tramitar fácilmente.

- **Decidim/Buzón Ética** (https://decidim.org/es/). El servicio de participación ciudadana que ayuda a ciudadanos, organizaciones e instituciones públicas a autoorganizarse democráticamente a todos los niveles.

- **Servicios corporativos** (https://aula.aoc.cat ; https://idcatmobil.cat) . Dentro de este apartado se incluye una amplia gama de funciones administrativas e internas como los entornos de laboratorio para implementar pruebas de concepto, la web del Área de Innovación, o la web del IdCAT Móvil, o los espacios de Formación en el Aula con los cursos de formación que ofrece el Consorci AOC.

4.1 Servicios de provisión de infraestructura de cloud público

A continuación se detallan los servicios, la infraestructura, licencias y los recursos de cloud público de AWS que se tendrán que proporcionar al Consorci AOC en el momento de la adjudicación del contrato :

- Servicios en modalidad IaaS para poder consumir infraestructura de computación, almacenamiento y comunicaciones. El licitador deberá proporcionar al Consorci AOC los mecanismos de automatización que soporten el modelo de entrega de la infraestructura como servicio y tendrá que orientar estos servicios bajo el paradigma " *Infraestructure as Code (IaC)* " haciendo uso de las tecnologías que determine el Consorci AOC en la ejecución del lote 1 (AWS CloudFormation, Terraform, Ansible, etc.)
  Los servicios IaaS se tendrán que poder ofrecer en diferentes clases y opciones para optimizar sus costes de acuerdo a las necesidades del Consorci AOC: bajo demanda (es decir sin compromiso), con reserva, o *Spot* (acceso puntual).

- Servicios en modalidad PaaS. Inicialmente el catálogo de servicios PaaS que deberá ofrecerse al Consorci AOC son:

  - **Redis** : almacén y caché de datos de alto rendimiento.
  - **PostgreSQL** : base de datos relacional.
  - **Dynamo DB** : Base datos NoSQL.
  - **MongoDB** : Base datos NoSQL.
  - **Amazon SQS** : servicio de colas de mensajes.
  - **Amazon SNS** : servicio de notificaciones push.
  - **Amazon QLDB** : registro de transacciones inmutable.
  - **Elasticsearch/Opensearch** : motor de búsqueda distribuido para todo tipo de datos.
  - EFS: servicio de archivos equivalente al NFS.

  Todos estos servicios PaaS tendrán que ser totalmente autogestionados y tendrán que ofrecer la alta disponibilidad desde un mínimo de 2 zonas de disponibilidad o regiones.

- Dotar al Consorci AOC de la plataforma y servicios estandarizados necesarios para la ejecución de contenedores Linux. La plataforma de contenedores proporcionada deberá permitir la automatización del aprovisionamiento, el despliegue, el escalado, la administración y la restauración de los servicios del Consorci AOC que se hayan implementado para ser ejecutados sobre contenedores, y deberá proporcionar un entorno de orquestación para la ejecución consistente y confiable de estos servicios. Esta plataforma de contenedores deberá estar equipada con todas las capacidades de computación, comunicaciones, almacenamiento y seguridad integradas para ofrecer una arquitectura de desarrollo basada en microservicios.

- Servicios de almacenamiento seguro de objetos (documentos) basado en la solución S3 de AWS con alta escalabilidad, disponibilidad de datos, durabilidad, seguridad y rendimiento. Este servicio de almacenamiento de objetos deberá poder ofrecerse en diferentes modalidades, variedades de clases y niveles de acceso para optimizar los costes en función de los patrones de acceso o de los diferentes casos de uso a implementar.

- Servicios para ejecutar *AWS Lambda* , el servicio de computación sin servidor basado en eventos de AWS que permite ejecutar código de backend con un nivel de escalabilidad muy alto sin necesidad de aprovisionamiento o administración de servidores.

- La infraestructura de comunicaciones que garantice a los usuarios de los servicios del Consorci AOC el acceso a las diferentes plataformas de negocio desde la red pública internet, así como el acceso a internet a los recursos del cloud público que lo puedan requerir. Se deberá proporcionar un direccionamiento IP público con un rango mínimo de 64 direcciones IP según estándar IPv4 disponibles permanentemente.
  Este acceso a internet deberá estar redundado mediante dos enlaces de datos independientes y deberá disponer de un caudal mínimo garantizado y permanente de 500 Mbps.

- Herramientas tipo SIEM y SOAR para la administración de eventos de información de seguridad y respuesta automatizada de seguridad. Estas herramientas tendrán que monitorizar de forma continua la actividad de la red, los patrones de acceso a los datos y el comportamiento del cloud público con el objetivo de permitir la detección integral y la priorización de todo tipo de actividad maliciosa (accesos indebidos, cambios en las políticas de seguridad, accesos inusuales de datos, etc.), pero también tendrán que realizar una búsqueda proactiva para dar respuesta a otros tipos de posibles amenazas y tendrán que proporcionar las alertas e informes de incidentes de seguridad.
  Las herramientas de tipo SIEM y SOAR seleccionadas tendrán que ingerir datos de diferentes orígenes y tendrán que analizar la correlación entre estos orígenes de datos para ofrecer una respuesta inteligente que permita una detección de amenazas proactiva.

- Herramientas de seguridad avanzadas que permitan establecer un perímetro de seguridad con varias líneas de defensa que protejan todos los recursos y servicios desplegados en el cloud público:

  - Protección perimetral frente a ataques para provocar indisponibilidad del servicio tipo DDoS con el servicio *AWS Shield Advanced* .
  - Protección con una solución de tipos IDS/IPS frente a intentos de intrusión en servicios frontales.
  - Protección con una solución de tipos Web Application Firewall que evite la explotación de vulnerabilidades de tipo inyección de SQL, Cross-site scripting, etc. recogidas en el conjunto de normas CRS 3 del OWASP (Open Web Application Security Project) con el servicio *AWS WAF* .

- Solución de antivirus y antimalware *bucketAV Antivirus for S3* integrada con el servicio de almacenamiento de objetos que ofrezca protección frente a virus, troyanos y otros tipos de software malicioso con respuesta automatizada para borrar, etiquetar o poner en cuarentena los documentos infectados. Esta solución de antivirus deberá estar permanentemente actualizada y deberá integrarse con las herramientas SIEM y SOAR para generar las correspondientes alertas.

- Sistema de monitorización que recoja los logs de los distintos sistemas, dispositivos, servicios y aplicaciones. Este sistema de monitorización permitirá el filtrado y ordenación de los registros de log por diferentes criterios o categorías y ofrecerá funcionalidades de análisis avanzadas.

El sistema de auditoría debe garantizar la integridad, inmutabilidad y la posibilidad de verificación mediante criptografía de todos los logs registrados.

- Sistema de backup integral y automatizable que pueda cubrir todos los tipos de datos, infraestructura, o cualquier elemento específico, incluidos en la solución de cloud público objeto de este lote. Todos los componentes de la solución de backup tendrán que estar cifrados y tendrán que cumplir los requerimientos que define el ENS en el ámbito de los backups. La solución de backup propuesta deberá poder ofrecer diferentes políticas de retención de acuerdo a las pautas determinadas por el SDIEMC del lote 1 (p. ej. backup diario incremental y backup completo semanal con 2 semanas de retención), pero en ningún caso el período de retención podrá ser inferior a los 15 días. Otro requerimiento de obligado cumplimiento será la necesidad de disponer de una solución de backup offilne y se valorará la posibilidad de hospedar esta solución de backup offline en un CPD alternativo (backup off-site).
  El adjudicatario deberá especificar el RPO (Recovery Point Objective) y el RTO (Recovery Time Objective) de cada uno de los componentes del backup. Se valorará que tanto la RPO como la RTO estén lo más cerca de 0 que sea posible.

- Plan de soporte *AWS Support Business* que debe permitir el acceso a las herramientas y conocimiento especializado por parte de AWS.

- El adjudicatario tendrá que garantizar el acceso al portal de gestión y la disponibilidad de toda la infraestructura y servicios de cloud público que son objeto de este lote con un nivel de soporte 24 x 7.

Todos los servicios e infraestructura de computación de cloud público proporcionados tendrán que estar certificados de conformidad con el nivel alto del Esquema Nacional de Seguridad (ENS) y tendrán que estar ubicados en la Unión Europea, Islandia, Liechtenstein o Noruega. Además, deberán ofrecerse en todo momento soluciones multiregión o basadas en diversas zonas de disponibilidad.

Uno de los objetivos fundamentales que persigue el Consorci AOC con el nuevo modelo TIC es alcanzar un alto grado de agilidad, flexibilidad y adaptabilidad en el consumo de los recursos IT, pero sin tener que sobredimensionar estos recursos ni tener que aprovisionarlos con antelación . Es en este contexto que el cloud público se convierte en un factor clave para alcanzar los objetivos del nuevo modelo TIC.

Dentro del alcance de este lote debe incluirse toda la infraestructura, servicios y recursos de cloud público descritos anteriormente, pero a medida que se vaya avanzando en el proceso de transformación del nuevo modelo TIC será necesario incrementar este catálogo de servicios y recursos IT. De esta forma es importante resaltar que potencialmente el Consorci AOC podrá requerir y consumir cualquier servicio o recurso IT que el proveedor de cloud público ofrezca en su catálogo actual o futuro.

Los costes de este lote se facturarán con periodicidad mensual y en todos los casos el importe de la factura deberá emitirse exclusivamente en €.

Es muy importante destacar que la titularidad de la suscripción de cloud público, así como de la/s cuenta/s de acceso asociadas a ésta, será en todo momento del Consorci AOC para facilitar el plan de devolución que se detalla en el ***ANEXO2 Plan de devolución del servicio*** .

4.2 Servicios de puesta en marcha, administración, gestión y explotación

Los servicios que se engloban dentro de esta clase en cuanto a la infraestructura desplegada oa desplegar a lo largo del ciclo de vida del contrato son los de Mantenimiento, Administración,

Despliegue de soluciones de infraestructura, Explotación y Monitorización, de las diferentes plataformas tecnológicas donde se soportan las aplicaciones de negocio del Consorci AOC.

Aquí vamos a describir las tareas necesarias que el proveedor de los servicios deberá garantizar para mantener los servicios de negocio con las máximas garantías de capacidad y disponibilidad, así como la infraestructura actualizada en las versiones más recientes y óptimas para dichos servicios.

Se entiende como **Mantenimiento** de la plataforma todas aquellas tareas necesarias para garantizar la correcta operatividad de todos los elementos físicos o lógicos, aplicaciones y servicios asociados a la plataforma ya la continuidad de negocio del Consorci AOC asociada a la misma.

La tipología del servicio de Mantenimiento requerido puede dividirse en tres tipos independientes:

- **Mantenimiento preventivo** . El mantenimiento preventivo corresponde a aquellas actuaciones destinadas a solucionar potenciales sucesos que podrían acontecer como incidentes que afectaran al correcto funcionamiento de los elementos que conforman la plataforma del Consorcio AOC descrita o una degradación de su rendimiento o funcionamiento.

- **Mantenimiento correctivo** . El mantenimiento correctivo corresponde a aquellas actuaciones destinadas a la resolución de cualquier suceso con afectación al funcionamiento y disponibilidad del servicio que ofrezca con indiferencia de su afectación a la disponibilidad y continuación de negocio y servicios ofrecidos por cualquiera de los elementos que conforman la plataforma del Consorcio AUC.

- **Mantenimiento evolutivo.** El mantenimiento evolutivo corresponde a aquellas actuaciones destinadas a actualizar componentes de la infraestructura de la plataforma por cualquier necesidad operativa del Consorci AOC y que afecte a los elementos que la componen.

Se entiende como **Administración** todas las tareas necesarias para configurar, adaptar, consolidar y extraer información del comportamiento de todos los elementos de la plataforma que figuran en este pliego. El objetivo de este servicio es garantizar el buen funcionamiento de los elementos y de la plataforma en general para garantizar el cumplimiento del Acuerdo de Nivel de Servicio (ANS) del Consorci AOC.

Este acuerdo se encuentra publicado y accesible en el portal corporativo existente en Internet.

La **Administración** de los elementos de la plataforma implica, entre otros, las tareas de modificación fina de algunos componentes de elementos a administrar para mejorar el rendimiento del mismo, la configuración de los elementos en función del resto, realizar las actualizaciones de versión posibles y necesarias en materia de seguridad, cambios de versión informados por parte del fabricante y modificaciones de las versiones existentes.

Se entiende también que dentro de la administración de los diferentes sistemas se realizarán los procesos periódicos de copias de seguridad según la configuración acordada y la accesibilidad con la agilidad necesaria para realizar las tareas de recuperación e importación de estas copias en caso de incidencia.

Se pide la redacción de informes periódicos sobre el funcionamiento de la plataforma desde el punto de vista integral, continuidad de negocio, e individual, de cada uno de los elementos existentes en las diferentes capas.

Se entiende como **Despliegue** o aprovisionamiento de infraestructura todas las tareas necesarias para instalar, configurar, adaptar, comprobar y extraer información de evolutivos, modificaciones,

correcciones o versiones de productos residentes en el portfolio del proveedor de cloud y asociados a los servicios de negocio que figuran en este pliego. El proveedor tiene la responsabilidad de seguir los procedimientos consensuados con el Consorci AOC al respecto. Los despliegues se regirán por actuaciones llamadas Intervenciones Operativas Programadas, IOP's. La infraestructura donde el Consorci AOC puede solicitar los servicios de Despliegue son todas las indicadas en el presente pliego o futuras que el Consorci AOC requiera, así como en la construcción de la plataforma base donde residirá el resto de servicios de cloud.

Se entiende por **Explotación** cualquier actuación que deba realizarse sobre cualquier elemento de la plataforma bajo petición previa del personal del Consorcio AOC habilitado a tal efecto, o personal de terceras empresas a los que se haya dado permiso previo para realizar esta petición. El objeto de este servicio viene dado por el dinamismo propio del negocio del Consorci AOC y necesidades de operación asociadas sobre la plataforma.

En esta modalidad del servicio se pueden entender todas las actuaciones que vulgarmente se entiende como "el día a día" y dará respuesta a requerimientos propios del Área de Tecnología del Consorci AOC. Dentro de estos requerimientos se incluyen la ejecución de tareas que podrán ser gestionadas como proyectos teniendo una coordinación especial entre el proveedor y el Consorci AOC para garantizar el éxito del mismo.

Dentro de esta modalidad del servicio también se podrán incluir peticiones asociadas a afectaciones a la continuidad de negocio o degradación en el rendimiento o funcionamiento de cualquier elemento de la plataforma que, por cualquier motivo, no estén cubiertas por los elementos de monitorización y procedimientos de mantenimiento correctivo establecidos.

Se entiende por **Monitorización** como la capacidad de recepción de sucesos frente a un cambio de comportamiento, disponibilidad o accesibilidad de todos los elementos de la plataforma o de sus componentes individuales susceptibles de modificar la capacidad y funcionamiento del mismo. El licitador tendrá que implementar la herramienta o solución que el Consorci AOC determine, y de su propiedad o suscripción, para garantizar, la detección, recepción y tratamiento de los eventos informativos que se configuren para garantizar la observabilidad global de la infraestructura y servicios asociados.

La plataforma de monitorización podrá ser centralizada o distribuida. Tiene que poder garantizar tener una idea global del estado del funcionamiento de la plataforma y particular de todos los elementos que la forman, en cuanto a la capacidad existente, el consumo de servicios cloud, detección de malfuncionamientos o errores y proyección de impacto en las distintas capas de servicio.

La plataforma de monitorización debe comunicarse con los equipos o elementos a supervisar mediante los servicios propios del proveedor de cloud y/o una red exclusiva para tal función con el fin de no penalizar la seguridad, la disponibilidad de la parte operativa y realizar una gestión más eficiente de la misma. El diseño y despliegue de la solución será consensuado por el Consorci AOC y proporcionado al proveedor para su implementación.

El licitador deberá garantizar en todo momento la accesibilidad a esta solución, según el modelo y procedimientos que sean acordados, al personal de Consorci AOC y terceras partes que se consideren necesarias, implementando las medidas de seguridad y control adecuadas.

Durante el transcurso del contrato, a medida que se produzcan nuevas necesidades de ampliación de servicios de cloud desplegados, el Consorci AOC requiere al adjudicatario la realización de las tareas necesarias para ejecutar estas modificaciones siguiendo requerimientos de la ampliación o integración. Estas tareas se realizarán de forma automatizada en la medida de lo posible y se realizarán en el momento de la detección de las necesidades con los umbrales y requerimientos previamente establecidos.

Cualquier ampliación de los activos del Consorci AOC relacionados con este pliego o cualquier aumento de recursos disponibles en el *cloud* , deberá ser asumido por el proveedor como parte del inventario dentro del servicio, sin que ello implique un sobrecoste del máximo establecido en este contrato ni modificación de las condiciones del servicio.

El Consorci AOC requiere que el modelo de servicio sea completo y global por toda la infraestructura tecnológica de la que disponga a su alcance para poder alcanzar los objetivos indicados en la Introducción de este documento.

Dentro del alcance de este lote 2 también se incluirán todas las tareas de administración, operación, mantenimiento y explotación de los servicios desplegados en el cloud público hasta la finalización del contrato para dichos servicios de negocio.

Con independencia de los servicios requeridos en el apartado ***4.2.1 Construcción y despliegue de infraestructura*** , donde se hace mención de las tareas de construcción general de toda la base tecnológica primaria y su evolución posterior, se considera necesario describir las tareas de los servicios de cloud público que se esperan para los servicios de negocio a transformar. A continuación detallamos cuáles son estas tareas :

- Creación de los entornos de integración, preproducción y producción en el cloud público. Estos entornos tendrán que estar segmentados y aislados para poder funcionar de forma totalmente autónoma e independiente. El adjudicatario será el encargado de realizar la segmentación de redes/subredes de los diferentes entornos, establecer los puntos de acceso a los diferentes servicios del Consorci AOC y afinar la configuración de la infraestructura y de los servicios de cloud con el objetivo de optimizar tanto su rendimiento como el coste en un escenario de múltiples entornos.

- Implementación del plan de seguridad definido de forma conjunta por el SDIEMC del lote 1 y el Consorci AOC en cada uno de los entornos de trabajo de integración, preproducción y producción con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de estos entornos. El adjudicatario del lote 2 deberá establecer el perímetro de seguridad de cada uno de los entornos activando las distintas líneas de defensa (soluciones DDoS, IDS/IPS, WAF, etc.). También tendrá que implementar la arquitectura de seguridad creando las diferentes cuentas e identidades, delimitando la seguridad de accesos según el principio de mínimo acceso necesario, implementando las diferentes redes y subredes internas, definiendo las reglas de firewall, cifrando los discos, etc .

- Configuración, gestión y monitorización por un equipo experto en seguridad de las herramientas SIEM y SOAR. El adjudicatario tendrá que activar los registros de actividad y los logs de las diferentes cuentas del cloud público (habilitando la correspondiente política de cifrado en reposo), y deberá configurar y poner en marcha las herramientas SIEM y SOAR estableciendo una consola de seguridad donde se centralicen las alertas de actividad maliciosa, amenazas de seguridad e intentos de intrusión. Esta consola de seguridad deberá funcionar como cuadro de mando operativo que permita de forma rápida conocer el estado actual de la seguridad del cloud público, permitiendo la consulta de los intentos de acciones no autorizadas, la detección de alertas de actividad maliciosa , actividad inusual, amenazas, anomalías e intentos de intrusión.
  Las herramientas SIEM y SOAR tendrán que recopilar datos de diferentes orígenes, tendrán que realizar la correlación de datos entre estos orígenes y tendrán que aplicar analíticas inteligentes, basadas en el aprendizaje automático del comportamiento de la red, para detectar y dar respuesta a las amenazas, así como para prevenir y mitigar los ataques y/o intentos de intrusiones. También tendrán que permitir la realización de búsquedas proactivas y dar respuesta a todos estos tipos de amenazas y actividad maliciosa.
  El adjudicatario será el responsable de automatizar la orquestación de estas herramientas y realizar la monitorización y supervisión continua, así como de proponer las recomendaciones y políticas que puedan reforzar la seguridad.

El adjudicatario también será el responsable de comunicar al Consorci AOC los incidentes de seguridad que se hayan podido producir, así como investigar y realizar el análisis forense de las acciones llevadas a cabo por el atacante. El adjudicatario deberá realizar un informe detallado de cada uno de los incidentes de seguridad categorizados como graves por el Consorci AOC, indicando la descripción detallada del incidente, los resultados del análisis forense, incluyendo el inventario de activos afectado y el evaluación del daño provocado por el ataque, el plan de recuperación propuesto y el plan de respuesta sugerido.

- Configuración de las políticas de acceso condicional que determine el SDIEMC del lote 1 y el Consorci AOC en el acceso al portal de gestión del cloud público: acceso a través de VPN, restricciones de IP autorizadas, autenticación con multi factor (MFA), etc.

- Implementación del plan de backup definido por el SDIEMC del lote 1 para todos aquellos servicios y componentes desplegados en el cloud público garantizando el cumplimiento de todos los requerimientos determinados en este plan de backup. El adjudicatario deberá realizar de forma periódica, al menos 2 veces al año, un simulacro de restauración en un entorno no productivo de aquel servicio o componente que determine el Consorci AOC para validar la integridad del sistema de backup, así como el cumplimiento de los RPO y RTO previstos.
  De forma análoga, deberá realizarse de forma periódica, al menos 1 vez al año, un simulacro de restauración en un entorno no productivo de cada uno de los servicios que dispongan de uno de plan de continuidad de negocio o contingencia específicos.
  Por último, se tendrán que generar los informes de control correspondientes al plan de backup y activar el sistema de generación de alertas en caso de error.

- Durante la etapa de prestación del servicio el adjudicatario será el responsable de llevar a cabo de forma proactiva todas las tareas y actividades necesarias para garantizar el correcto funcionamiento de los entornos, plataformas y servicios que forman parte del alcance de este lote, así como asegurar el cumplimiento de los ANS acordados a nivel de disponibilidad y rendimiento: gestionando, configurando, automatizando, securizando y monitorizando meticulosamente los recursos de cloud público consumidos por los servicios del Consorci AOC a lo largo de su ciclo de vida.
  Se deberá monitorizar de forma continua el comportamiento de los diferentes servicios y plataformas, se tendrán que ajustar todos los parámetros de configuración de estos servicios, realizar los mantenimientos específicos de cada componente, gestionar sus dependencias, realizar el seguimiento, control y rotación de los registros de log, configurar las alertas del estado de los servicios y plataformas, etc.
  Para realizar la monitorización inteligente de todos estos elementos, así como para definir las alertas de comportamiento, el adjudicatario deberá poner en marcha, mantener y gestionar las herramientas de monitorización necesarias para obtener en tiempo real e información histórica las métricas, gráficas con las tendencias de uso y comportamiento, información analítica, etc. que permitan el seguimiento, control y toma de decisiones. El objetivo de esta monitorización continua será identificar malas tendencias o incidentes significativos. El equipo de operación asignado deberá actuar según los procedimientos documentados para resolver los incidentes detectados o escalarlos a los responsables correspondientes.

  Las herramientas de monitorización y control seleccionadas tendrán que permitir el acceso con diferentes roles y permisos, personalizar los cuadros de mando y las vistas con filtrado por componentes, notificaciones de alertas multicanal (mail, SMS, ...), establecer varios baselines para definir los umbrales de los comportamientos anómalos o extraordinarios, gestión de datos históricos para realizar el análisis temporal y las comparativas de evolución, disponer de funciones de análisis avanzado para determinar las causas de los incidentes, etc.
  De forma periódica (al menos 1 vez al mes), el adjudicatario deberá entregar al Consorci AOC los informes de actividad, seguimiento y explotación, destacando los indicadores de calidad, el cumplimiento de los ANS o las principales métricas de la monitorización.

El adjudicatario finalmente será también el responsable de realizar las actualizaciones de nuevas versiones del software de base, las instalaciones de correctivos o la aplicación de los parches de seguridad de acuerdo con el procedimiento de actualizaciones del Consorci AOC.

- El adjudicatario tendrá que elaborar y mantener actualizada toda la base documental técnica de los distintos entornos (integración, preproducción y producción), sistemas, componentes, servicios, procesos, etc. que son objeto del alcance de ese lote. También deberá encargarse de la documentación de los procedimientos y procesos operativos, así como del inventario de activos y el estado de los servicios.
  El proceso de documentación no será tarea aislada sino un proceso integrado con el resto de actividades que son objeto de este lote.
  La documentación deberá guardarse en el repositorio GIT corporativo del Consorci AOC para que pueda estar disponible en todo momento por el personal asignado y también para disponer de la opción de control de versiones.

- Control de costes. Seguimiento del avance y control exhaustivo de los costes de la infraestructura de cloud público identificando los costes de los distintos recursos y servicios. Revisar que los costes estén alineados con los modelos previstos y que se adecúan a la estrategia cloud establecida, estableciendo patrones de gasto que permitan inferir y planificar los costes a futuro, así como anticipar futuras desviaciones.
  El adjudicatario deberá configurar las herramientas de gestión y control de presupuestos, y deberá proporcionar de forma periódica (como mínimo 1 vez al mes) los informes de control de costes cubriendo varios aspectos: costes por proveedor cloud, costes por servicio y plataforma, costes granulares por tipos de recurso IT, detección de costes superfluos por sobredimensionamiento, recursos infrautilizados, propuestas de ahorro, etc.
  Por último el adjudicatario deberá configurar y activar las alertas que permitan de forma proactiva conocer de inmediato cualquier desviación que pueda comprometer el presupuesto de cualquier servicio o plataforma y deberá establecer las medidas correctivas y las políticas restrictivas que el Consorci AOC determine sobre el uso de los recursos cloud de un determinado servicio o plataforma.
  El objetivo de todas estas tareas es mantener en todo momento bajo control los costes de la infraestructura de cloud público con una clara visibilidad del desglose del gasto.

- Puesta en marcha, configuración y administración de las herramientas de tipo CMP y/o CMDB que el SDIEMC del lote 1 determine para conseguir una solución de cloud híbrido que permita gestionar desde un único repositorio central el inventario de recursos de cloud público y privados necesarios para la ejecución de los servicios del Consorci AOC.
  El adjudicatario de este lote deberá administrar las suscripciones, cuentas de usuario e identidades necesarias para aprovisionar los servicios y recursos cloud llevando a cabo el control proactivo del inventario global de activos.

- Puesta en marcha y configuración de la plataforma de contenedores corporativa para entornos de integración, preproducción y producción. Además, el adjudicatario de este lote será el responsable de ejecutar las tareas operativas, de administración y configuración de las plataformas de contenedores, monitorizando y controlando de forma continua y proactiva a través de métricas y alertas el buen funcionamiento de estas plataformas. El adjudicatario será también el responsable de garantizar la fiabilidad, la escalabilidad y el rendimiento óptimo de la plataformas de contenedores, así como de coordinar las cargas de trabajo en ejecución, localizando, identificando, recuperando y restableciendo las interrupciones y los incidentes que se puedan producir.

- Creación, administración y custodia de los scripts y archivos de definición que permiten la gestión y aprovisionamiento de los servicios y recursos IT de cloud público según el paradigma " *Infraestructure as Code (IaC)* ". Estos scripts tendrán que estar implementados con las herramientas y lenguajes determinados por el SDIEMC del lote 1 (AWS CloudFormation,

Terraform, AWS CDK, Ansible, etc.) y se tendrán que guardar en el repositorio GIT corporativo del Consorci AOC.

- Integración y automatización de los procesos de despliegue continuo (CD) de las nuevas versiones de los servicios de la AOC según modelos de gestión basados en DevOps y en la mejora continua. Configuración de las herramientas y mecanismos para la automatización de procesos que permitan controlar y verificar de forma continua los despliegues a producción proporcionando estabilidad y seguridad en la aplicación de las nuevas versiones de los servicios y componentes.

A nivel indicativo, las horas necesarias para llevar a cabo el servicio se estiman en 8,669 horas. Estas horas están calculadas en base al supuesto de que el contrato estará operativo el 1 de agosto de 2022 y que llegará hasta el 31 de diciembre de 2023. Aunque se pudiera retrasar la fecha de inicio del servicio, la fecha de finalización se mantendrá fija en el 31 de diciembre de 2023. Por este motivo es importante destacar que el alcance de este lote se mantendrá en todo momento y que el adjudicatario tendrá que incrementar la dedicación de los recursos asignados a fin de poder garantizar que se alcanza el alcance definido en este apartado en caso de que el inicio del contrato se demore más allá del 1 de agosto de 2022.

El proveedor propondrá los perfiles del personal que considere adecuados para la ejecución y garantía de los servicios profesionales requeridos y descritos en este lote 2. De cualquier modo, se considera necesaria la participación mínima de los siguientes perfiles, roles y su dedicación en tareas constructivas, de desarrollo de la infraestructura y operación de la misma:

- Cloud Engineer. Perfil asociado a tareas de propósito general con dedicación a propuesta de los proveedores en función de los requerimientos del servicio y el número de personas necesarias para conseguir los objetivos acordados.
- Cloud Security Engineer. Perfil asociado a tareas relativas a la securización permanente y revisión del estado de las vulnerabilidades e incidencias asociadas a la seguridad. La dedicación y número de personas necesarias para conseguir los objetivos acordados será propuesto por el proveedor en función de los requerimientos del servicio.
- Cloud and on-premise Engineer. Perfil mixto que permitirá apoyar al Área de Tecnología del Consorci AOC, inicialmente en la Unidad de Sistemas, permanentemente en las tareas de transformación de los servicios de negocio y la preparación y/o adaptación de los sistemas que actualmente se encuentran en centros operativos on-premise o en cloud privado. Se considera necesaria una dedicación completa y diaria a lo largo del ciclo de vida del contrato.

4.2.1 Construcción y despliegue de infraestructura

El proveedor realizará todas las tareas de construcción de cualquier plataforma y entorno, así como la posible migración de servicios y elementos tecnológicos y datos que el Consorci AOC pueda solicitar a lo largo del contrato y relacionado con los objetivos y servicios objetos de este lote.

La construcción y evolución de la infraestructura se realizará con los elementos disponibles en el *Marketplace* del proveedor de cloud público, siendo éstos distribuidos en un esquema como el de la siguiente figura.

Las diferentes capas que se requieren desplegar inicialmente y evolucionar a lo largo del ciclo de vida de los servicios se pueden dividir en las siguientes:

- **VPC** : Conjunto de elementos de infraestructura y servicios del cloud público sobre los que se despliegan los servicios y productos de negocio del Consorci AOC, así como, los elementos y servicios necesarios para su gestión.

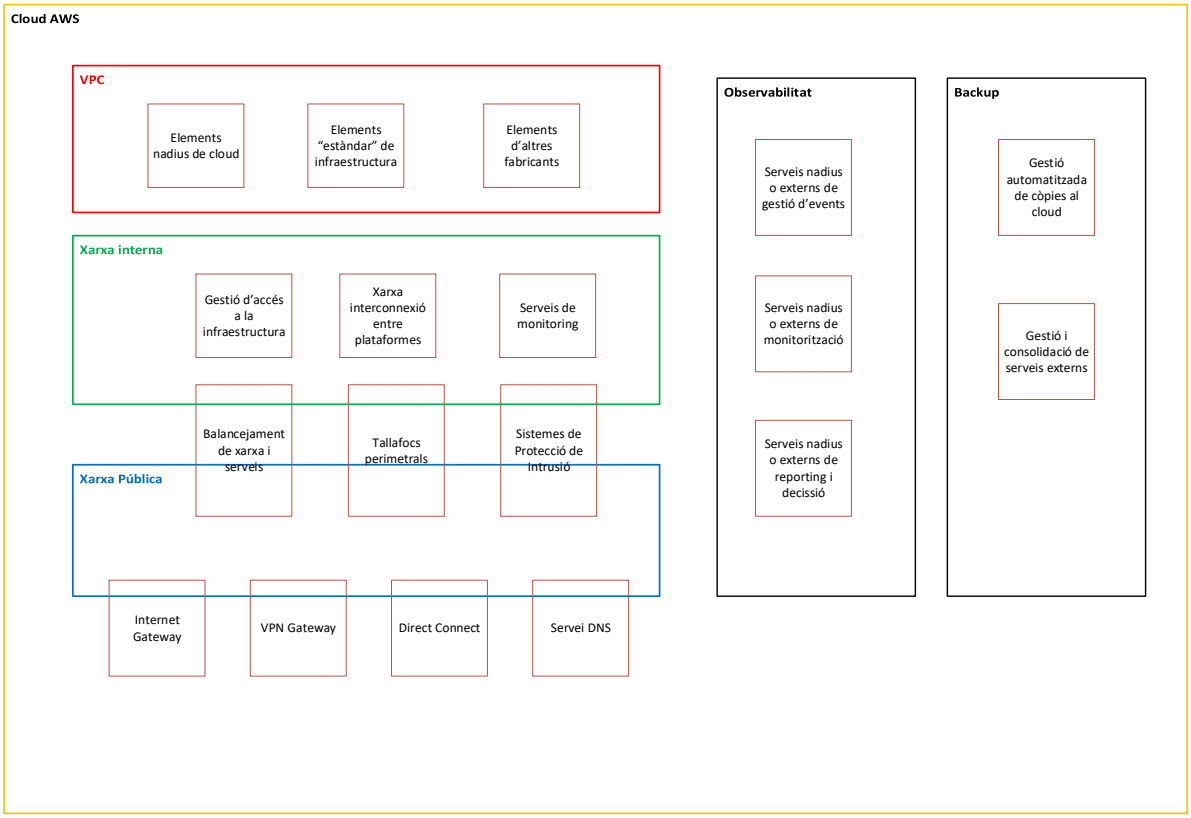
- **Red interna** : Conjunto de elementos de infraestructura y servicios del cloud público destinados al acceso, autorización, conectividad y control de los elementos desplegados en las VPC's necesarias, así como su interconexión y los elementos y servicios necesarios para su gestión ..

- **Red Pública** : Conjunto de elementos de infraestructura y servicios del cloud público destinados al acceso público y securización global de toda la arquitectura accesible desde la red Internet, así como, los elementos y servicios necesarios para su gestión . Se incluye el servicio de acceso a Internet de toda la infraestructura.

- **Observabilidad** : Conjunto de elementos de infraestructura y servicios del cloud público destinados a la recogida, almacenamiento, correlación e interpretación de los diferentes eventos configurados para conocer el estado operativo de todos los elementos y servicios, así como, la detección, adaptación y resolución de los incidentes que puedan producirse.

- **Backup** : Conjunto de elementos de infraestructura y servicios del cloud público destinados a almacenar todos los datos necesarios para restaurar un elemento o servicio en caso de incidencia del elemento o pérdida de información. Esta función permitiría aplicar todos los procesos asociados al concepto de recuperación en caso de desastre y continuidad de negocio.

La construcción y evolución de la infraestructura se realizará con los elementos disponibles en el *Marketplace* del proveedor de cloud público, siendo éstos distribuidos en un esquema como el de la siguiente figura.



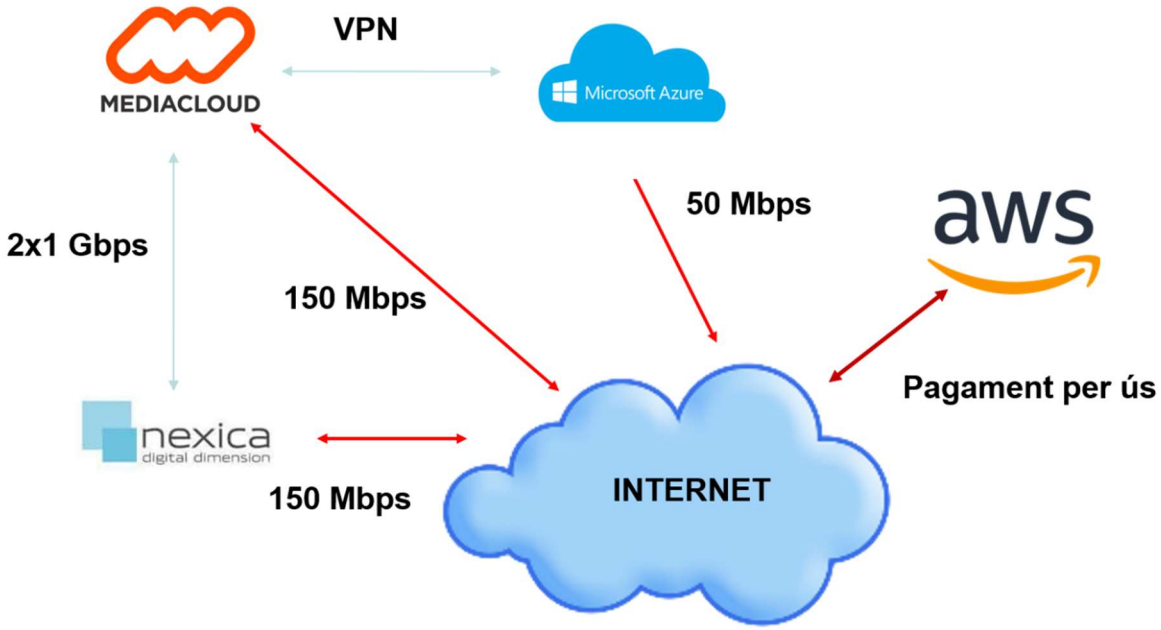
Se entiende que todos los productos, servicios y elementos susceptibles de ser necesarios para el desarrollo de la arquitectura tecnológica, y que el proveedor de cloud público ofrece u ofrecerá, pueden circunscribirse a estos cinco grupos. El Consorci AOC pedirá al proveedor el despliegue de cualquier elemento que considere necesario.

El Consorci AOC tiene el objetivo y el requerimiento en la ejecución de este contrato de que el proveedor realice todos los trabajos considerados dentro del concepto Gobernanza TIC desde un punto de vista técnico, dejando al personal del Consorci AOC las funciones de gestión de los servicios proporcionados por terceros, el análisis del cumplimiento de niveles de servicio, la gestión de todos los proyectos asociados, la definición del diseño y arquitectura de las soluciones relacionadas, la elaboración conjunta de procedimientos y protocolos y la interlocución y punto central de comunicación entre todos los proveedores y otras unidades internas del Consorci AOC o terceros.

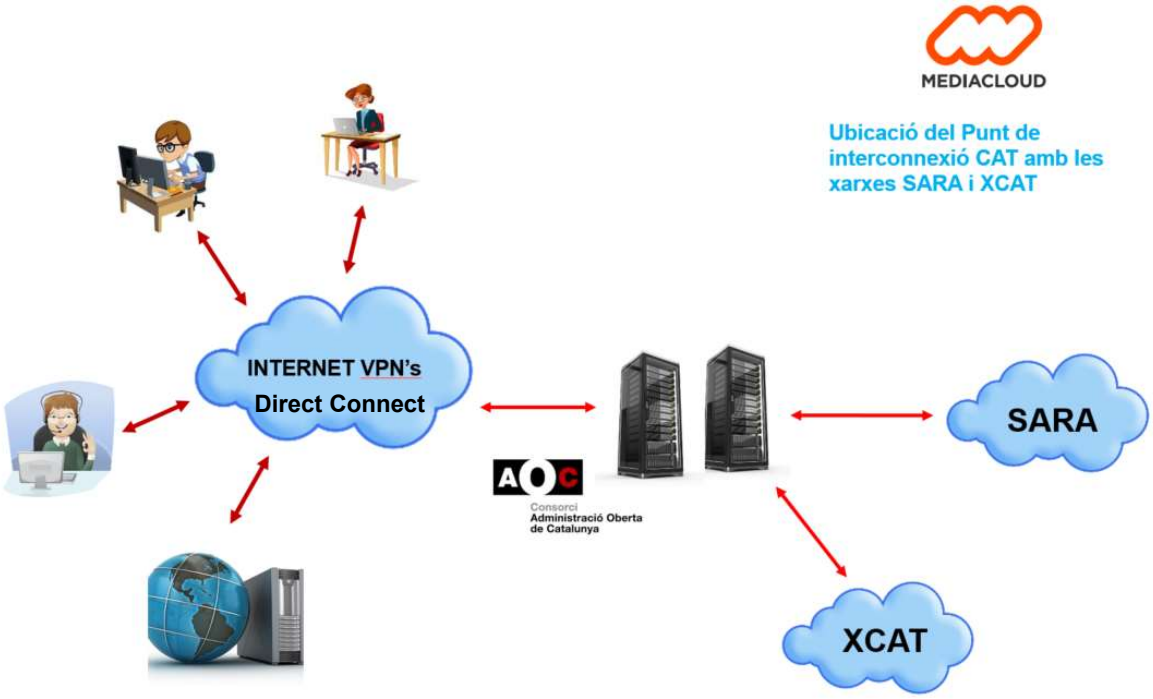
El proveedor deberá adaptar la provisión de servicios de cloud al aumento de la ejecución de tareas supeditada al volumen de sistemas a considerar. El conjunto de infraestructura bajo su responsabilidad es la suma de todos los elementos desplegados oa desplegar en el cloud. El proveedor debe considerar que uno de los objetivos estratégicos del Consorci AOC es la migración de sus servicios alojados en modo *housing* en el *cloud* y mencionados en el presente documento. Estos servicios podrán ser sustituidos por otros por necesidades estratégicas u operativas pero se mantendría la tecnología requerida o similar y con volumetrías comparables.

Como sistema complementario al servicio de resolución de dominios existente se requiere la puesta en producción de un sistema de resolución de dominios interno y externo en la plataforma. Se requiere que este sistema se encuentre redundado para garantizar la disponibilidad del mismo.

El Consorci AOC gestiona una serie de dominios internos y externos que tendrán que ser configurados en este sistema provisto por elementos del cloud público, u otros, para dar accesibilidad a los mismos en la red ya los servicios integrados en la plataforma.
El Consorci AOC es el nudo de interconexión entre las Administraciones Públicas de Cataluña y los servicios que la Administración General del Estado ofrece en la red privada Red SARA y en la red privada de la Generalidad de Cataluña XCAT. Diferentes aplicaciones del Consorci AOC requieren la accesibilidad a estas dos redes para ofrecer un servicio global e integral en ciertas funciones de los servicios de negocio. Dado que algunas de estas aplicaciones serán transformadas y desplegadas en el cloud público, se requiere que el proveedor despliegue, como servicio de cloud público y dentro del contrato al que se refiere esta licitación, la solución de comunicación entre centros que garantice esta accesibilidad. En el gráfico siguiente se presenta, de forma esquemática, la distribución de las comunicaciones de los diferentes centros de operación y su interconexión.



La infraestructura de interconexión se encuentra en una red privada dentro del Centro de Datos de MediaCloud, aunque también es accesible vía un enlace físico, ya existente, entre el cloud privado ubicado en Nexica y el Centro de Datos on-premisiones ubicado en Mediacloud. Para mantener y garantizar la accesibilidad de las aplicaciones a desplegar en el cloud público se requiere el despliegue de una solución de comunicaciones entre la infraestructura de red de este cloud y la infraestructura existente en el Centro de Datos on-premise y en el cloud privado, en una configuración de alta disponibilidad. Esta solución podrá ser implementada mediante redes privadas virtuales, con la máxima securización posible, entre los centros de operación, o bien, mediante la solución conocida como *Direct Conn* ect del cloud público, o cualquier otra que el cloud público ofrezca para tal fin . La elección de la solución más adecuada será consensuada entre el proveedor y el Consorci AOC. Dado que las soluciones de comunicaciones implican la intervención de los proveedores actuales tanto del centro on-premise como del cloud privado, se encuentra necesario que el proveedor gestione con éstos la mejor solución. Los servicios desplegados con este objetivo serán traspasados al Consorci AOC, como titular de los mismos, una vez finalice el contrato de los servicios.



El proveedor de servicios de cloud de este lote realizará toda la gestión de estas soluciones en coordinación con el proveedor de comunicaciones en caso de que sea necesario este tipo de solución, o con el proveedor responsable de la explotación de los elementos de comunicaciones donde finalicen los distintos túneles de las redes privadas que se desplieguen.

4.2.2 Servicios de soporte a la gestión global de los servicios de negocio

A lo largo del ciclo de vida del servicio se requerirá la ejecución de pruebas de alta disponibilidad o *failover* para comprobar que la solución implementada satisface los requerimientos del Consorci AOC al respecto.

Será responsabilidad del proveedor de servicios la ejecución de este tipo de pruebas en coordinación con el personal del Consorci AOC asociado a estas tareas y será éste último el que, después de recibir los informes resultantes de este plan de pruebas, validará las mismas y el correcto funcionamiento de la topología existente. Todos aquellos elementos que por cualquier motivo no se encuentren implementados con esta filosofía tendrán que ser configurados con la misma previa validación por el personal del Consorci AOC asociado al proyecto. En estas tareas podrán y tendrán que intervenir los perfiles profesionales necesarios para alcanzar los objetivos.

Las funciones principales a cumplir por el adjudicatario se describen a continuación.

Participación activa en el análisis de impacto, cuando el Consorci AOC lo solicite, el proveedor deberá participar activamente en el análisis del impacto y las tareas derivadas de este correspondiente a cualquier desarrollo sobre las plataformas junto con el empresa de desarrollo designada por el Consorci AOC a tal efecto.

Esta participación puede solicitarse tanto por nuevos desarrollos como por el diagnóstico y resolución de incidencias y problemas en aplicativos en funcionamiento.

Aplicar medidas de control de calidad sobre el desarrollo de sistemas que permitan asegurar la explotación de las aplicaciones del actual sistema de información.

Prestar soporte al equipo del Consorci AOC en la **gestión del ciclo de vida** de las aplicaciones.

Apoyo a las pruebas de carga, este servicio estará bajo la responsabilidad del proceso de validación del paso a operación existente en el Consorci AOC.

En este servicio el proveedor será el responsable de monitorizar los sistemas y servicios afectados por las distintas pruebas de carga que se le requieran.

Deberá entregar la información extraída de los sistemas y entregarla a los responsables del proceso de validación del paso a producción para que puedan realizar los correspondientes informes de resultado.

También tendrán que participar si se requiere en el análisis de estos resultados y en caso de que no sean satisfactorios participar en las pruebas más exhaustivas necesarias para buscar la solución tratándose en este caso como un incidente que requiere del servicio de ayuda al diagnóstico de incidentes y problemas.

Desde el inicio de la prestación del contrato uno de los objetivos prioritarios del adjudicatario debe garantizar la prestación de un servicio superior a la prestación actual.

Servicios de ayuda al diagnóstico de incidentes, problemas y cambios

Los desarrolladores deben poder acceder de forma controlada a los logs de ejecución y del sistema durante las tareas de diagnóstico de incidencias. Asimismo el proveedor será el responsable de:

- Preparar, ejecutar y analizar los resultados de las pruebas.
- Interpretar *dumps* , *heapdumps* , *logs* y otras herramientas de diagnóstico.
- Gestionar casos con los fabricantes para descartar problemas de software base, *middleware* o productos.
- Suministrar trazas, *logs* y otro material similar a los equipos de Desarrollo
- Habilitar opciones de *trace* y diagnóstico.
- Utilizar herramientas de diagnóstico específicas para cada plataforma.
- Colaborar con los equipos de desarrollo en el diagnóstico de los incidentes y problemas.

Servicio de apoyo a otras Unidades del Consorci AOC

El proveedor será el responsable de:

- Documentar las características de la arquitectura, implementación y uso de las distintas plataformas en los equipos de Desarrollo.
- Asesorar a nuevos proyectos sobre características específicas de las plataformas.
- Colaborar en el lanzamiento de las aplicaciones, planificación, incorporación de nueva infraestructura que pueda ser necesaria, dimensionado, etc.

El adjudicatario colaborará con el Consorci AOC en el lanzamiento de nuevos servicios TIC, planificación, incorporación de nueva infraestructura que pueda ser necesaria, dimensionado, y hará

las recomendaciones necesarias para garantizar una correcta alineación tecnológica de las necesidades de los servicios del Consorci AOC.

Modelo de relación

El modelo de relación que el licitador deberá incluir en su propuesta debe cumplir los requerimientos globales indicados en el apartado 4.2 de este documento y, en particular, debe contener, como mínimo, la estructura organizativa del servicio y los canales y herramientas de comunicación entre el proveedor y el Consorci AOC a todos los niveles. Es decir, debe incluir una propuesta de modelo de gestión del servicio y el modelo de comunicación que se crea adecuado a lo largo del ciclo de vida del servicio, poniendo énfasis en los circuitos de comunicación y escalado ante incidencias susceptibles de afectar o con afectación a los servicios bajo responsabilidad del proveedor, de forma directa o indirecta.

Se considera necesaria la figura de un responsable de servicio (*Service Manager*) que concentre las comunicaciones sobre la evolución del servicio y al que se pueda transmitir la visión de negocio y requerimientos transversales implícitos en la plataforma y en la propia esencia del Consorci AOC. Esta figura será el punto de contacto permanente sobre la evolución y desarrollo del servicio, así como, el rol de contacto, en modalidad 24x7, en caso de incidencia en la infraestructura tecnológica operada por el proveedor o por incidencia crítica de cualquier servicio de negocio y que requiera actuaciones de forma urgente.

Documentación

El licitador tendrá que cumplir los requerimientos globales indicados en el punto 1 de este documento y, en particular, debe contener, como mínimo, la tipología de documentación a generar y entregar en el ciclo de vida del servicio. Esta documentación generada y accesible por parte del personal del Consorci AOC y otros asociados al servicio deberá incluir, como mínimo, los siguientes tipos de informe:

- Informes de seguimiento. Entre los que debe figurar:
    - Informes periódicos sobre el funcionamiento global del servicio
    - Informes de incidencias y cumplimiento del nivel de servicio con periodicidad mensual
    - Informes del estado del servicio con periodicidad mensual.
    - Informes de desarrollo particular del servicio con periodicidad semanal, en caso de ser necesario en función de la solución propuesta.
- Documentación puntual. Documentación que se va a generar como resultado de una actuación o necesidad concreta y no estándar.
    - Propuestas de proyecto por actuaciones dentro de la operativa del servicio que así se crea conveniente por la complejidad a tratar o el impacto sobre los parámetros de disponibilidad y accesibilidad de elementos o servicios de la plataforma.
    - Informes explicativos de incidencias recurrentes o especialmente notables.
    - Propuesta de despliegues de nuevas soluciones o servicios que se puedan dar a lo largo del ciclo de vida del servicio

- Documentación de puesta en marcha del servicio. Plan de transición.
- Plan de devolución y entrega final del servicio

- Documentación de soporte al servicio **.** Se requerirá al adjudicatario la aportación de la siguiente documentación, en el formato que se determine:
  - Manual de procedimiento de peticiones y escalados
  - Manual de funcionamiento de las herramientas disponibles en el servicio
  - Planes de capacidad
  - Mapas topológicos y de arquitectura necesarios
  - Otra documentación que se considere necesaria para la evaluación del funcionamiento y rendimiento del servicio y elementos asociados.

Se requiere que la información resultante de la prestación del servicio que se ponga a disposición del personal del Consorci AOC se encuentre en lengua catalana y, en su caso, en otras lenguas.

4.2.3 Acuerdos de Nivel de Servicio

En este apartado se describe el marco contextual de aplicación de los Acuerdos de Nivel de Servicio para el lote 2. Para solucionar estas incidencias se establece el siguiente procedimiento de trabajo y Acuerdo de Nivel de Servicio (ANS):

Las posibles penalizaciones que se deriven del incumplimiento de los ANS, se aplicarán sobre descuento en la siguiente factura emitida después de la penalidad. La aplicación de penalidades será acumulativa.

Los Acuerdos de Nivel de Servicio se podrán revisar y modificar siempre y cuando exista mutuo acuerdo entre el adjudicatario del lote 2 y el Consorci AOC.

Requerimientos de nivel de servicio del Lote 2

Resolución de incidencias sin errores:

- Porcentaje de la resolución de incidencias sin errores en el plazo.
  - Cálculo: (A/B)*100

    A: Número total de incidencias resueltas sin error en el plazo

    B: Total de incidencias resueltas en el plazo
- Periodicidad: Diaria
- El porcentaje de incidencias sin error en el plazo establecido deberá ser al menos del 90%.
- El nivel ofrecido por quien resulte adjudicatario del lote constituirá un Acuerdo de Nivel de Servicio (ANS), cuyo cumplimiento se medirá durante toda la duración de la prestación del servicio.

ANS para la gestión de las incidencias

Este ANS aplica a la totalidad del servicio contratado.

Definiciones:

Nivel	Descripción
Bloqueando	Una incidencia se catalogará con criticidad bloqueando si impide la utilización total del servicio a todos los usuarios del mismo.
Alta	Una incidencia se catalogará con alta criticidad si impide la utilización de una parte concreta del servicio, a todos o algunos usuarios, y la afectación por el negocio es elevada.
Media	Una incidencia se catalogará con criticidad media si impide la utilización de una funcionalidad concreta de alguno de los servicios a todos o algunos usuarios externos a la plataforma y la afectación por el negocio es relativamente baja.
Baja	Una incidencia se catalogará con criticidad baja si no impide la utilización parcial ni total de alguno de los servicios a alguno de los usuarios.

El tiempo de respuesta y de resolución se establece según el tipo de incidencia:

- **Tiempo de respuesta** .

  Se define como tiempo de respuesta el tiempo que transcurre desde que la incidencia se comunica, y el usuario recibe el ticket de su incidencia. El tiempo de respuesta se cuenta sobre el horario de soporte de recepción de incidencias.

- **Tiempo de resolución** .

  Se define el tiempo de resolución de una incidencia como el número de horas que transcurren desde que el usuario recibe el tique de la incidencia hasta el momento en que la incidencia está solucionada. En el cálculo del tiempo de resolución de una incidencia no se tendrán en cuenta los posibles incrementos de tiempo provocados por la intervención inevitable de terceros en el proceso de resolución (por ejemplo, intervención de otros organismos).

El tiempo máximo permitido por la respuesta y resolución de una incidencia dependerá del nivel de criticidad de la incidencia. En la siguiente tabla se muestran los tiempos máximos permitidos por la resolución de una incidencia en función del nivel de criticidad:

Criticidad Incidencia	Tiempo de respuesta (horas)	Tiempo de resolución (horas)	% de resolución dentro del tiempo comprometido
0 Bloqueando	0,5	2	95%
1 Alta	1	16	95%
2 Media	1	40	95%

3 Baja	1	64	95%

Por el cálculo del tiempo de resolución de una incidencia se excluirán los posibles incrementos de tiempo provocados por la intervención inevitable en el proceso de resolución por parte de terceros.

En caso de que el adjudicatario no cumpla el acuerdo de nivel de servicio definido anteriormente al menos en el 95% de las de incidencias con criticidad 0 y 1 que hayan ocurrido dentro del mes se le aplicará las siguientes penalizaciones:

Porcentaje de incidencias con criticidad 0 y 1 en el mes que cumplen el ANS	Penalización sobre la cuota mensual de la factura
Superior al 95%	0%
Entre 95% y 80%	5%
Entre 80% y 70%	10%
Inferior al 70%	15%

En caso de que el adjudicatario no cumpla el acuerdo de nivel de servicio definido anteriormente por al menos el 90% de las de incidencias con criticidad 2 y 3 que hayan ocurrido al mes se le aplicará las siguientes penalizaciones:

Porcentaje de incidencias con criticidad 2 y 3 en el mes que cumplen el ANS	Penalización sobre la cuota mensual de la factura
Superior al 90%	0%
Entre 90% y 51%	5%
Inferior al 51%	10%

Requerimientos de nivel de servicio en la protección de datos

Se considerará incumplimiento del contrato la no aplicación de las medidas de seguridad impuestas al contratista. Aparte de las posibles responsabilidades que se puedan derivar de dicho incumplimiento, y que en función de la gravedad del mismo pueda comportar la resolución del contrato, se prevé la imposición de penalidades.

Las penalidades a imponer serán por cada incumplimiento que se produzca y con el tope máximo establecido en el artículo 192 de la Ley 9/2017, de Contratos del Sector Público:

- Medidas de seguridad de nivel bajo: 0,5% del precio de adjudicación del lote.
- Medidas de seguridad de nivel medio: 0,75% del precio de adjudicación del lote.
- Medidas de seguridad de nivel alto: 1% del precio de adjudicación del lote.

Incidentes de seguridad

Es importante destacar que cualquier incidente de Seguridad o de protección de datos personales que puedan afectar a los sistemas del Consorci AOC, deberá informarse en un tiempo inferior a las 24h.

En la fase inicial del proyecto deberá definirse un procedimiento de coordinación ante incidentes que puedan afectar a los sistemas del Consorci AOC. Este procedimiento tendrá que contemplar los flujos de información y las interacciones entre Consorci AOC y el adjudicatario durante la gestión del incidente.

A su vez el adjudicatario deberá informar periódicamente de los incidentes que hayan afectado a los sistemas o plataformas del Consorci AOC.

5. Condiciones de ejecución

El adjudicatario de cualquiera de los 2 lotes deberá cumplir las siguientes obligaciones básicas:

- Gestionar cualquier alteración del servicio en las condiciones expresadas en este pliego.
- Realizar reuniones periódicas con el Consorci AOC para exponer el cumplimiento del servicio y tratar los posibles problemas o mejoras del servicio.
- Establecer un marco metodológico de trabajo basado en Agile.
- Realizar la formación de los técnicos designados, en todos aquellos aspectos que el Consorci AOC crea oportunos y que sean de directa aplicación a los servicios requeridos.
- Toda la documentación generada por el equipo será en catalán y en el formato corporativo propuesto por Consorci AOC .
- Presentación de informes mensuales de presentación del servicio de acuerdo con los indicadores que el Consorci AOC considere apropiados:
    - Informe resumen de las actuaciones realizadas.
    - Informe de situación de las actuaciones en curso.
    - Informe resumen de las actuaciones pendientes.
    - Planificación de las actuaciones a realizar.
- Informe de fin del contrato con el resumen de las tareas realizadas.

6. Horario de ejecución del servicio

El licitador deberá incluir en su propuesta la disponibilidad horaria del personal asociado al servicio, aunque deberá garantizar su disponibilidad durante las siguientes franjas horarias:

- De lunes a viernes, excepto festivos, **de 08:00 a 19:00 horas** .

- El 90% de los trabajos se realizará en el horario indicado. En el 10% de los casos restantes se podrá solicitar previamente la realización de tareas fuera del horario anteriormente establecido sin coste adicional.

En caso de baja de cualquiera de los miembros del equipo, el adjudicatario deberá sustituirle en menos de 15 días laborables de acuerdo con los responsables del Consorci AOC.

Cualquier cambio en uno de los miembros del equipo a instancia del adjudicatario deberá ser pactado con el Consorci AOC. En estos casos, se fijará un tiempo de 2 semanas de formación/adaptación del nuevo miembro que serán a cargo del adjudicatario.

En el caso del lote 2, se requiere un servicio de disponibilidad permanente, denominado 24x7. Este nivel de soporte deberá estar disponible en la recepción de peticiones vía la herramienta asociada a la comunicación y gestión del servicio y deberá disponer de visibilidad permanente de la monitorización y sucesos que determinen el estado de los elementos que componen el servicio.

7. Infraestructura necesaria

Los adjudicatarios de cada uno de los lotes que son objeto de esta licitación tendrán que aportar la infraestructura técnica, licencias, y cualquier otro componente o medio técnico necesario para la realización de los trabajos. Los costes de esta infraestructura tecnológica correrán a cargo de los adjudicatarios. Es importante destacar que esta infraestructura tecnológica no podrá contener en ningún momento datos reales.

Las tareas se tendrán que llevar a cabo en las oficinas de cada una de las empresas adjudicatarias, aunque de forma puntual es posible que en alguna ocasión sea necesario el desplazamiento de alguno de los miembros de los adjudicatarios a las instalaciones del Consorci AOC o de terceros. Por este motivo, se recomienda que todos los miembros del equipo dispongan de ordenadores portátiles.

Todos los trabajos desarrollados, y en particular los entregables entregados, tendrán que seguir las guías de estilo definidas por el Consorci AOC. El Consorci AOC facilitará a todos los adjudicatarios estas guías de estilo y su cumplimiento deberá ser obligatorio para la aceptación de los trabajos.

8. Lugar de prestación de los servicios del lote 2 en territorio español

El Consorci AOC provee, por encargo de la Generalidad de Cataluña, el servicio de identificación y firma idCAT Móvil . El idCAT Móvil es un sistema de identificación y firma de los previstos en la letra c de los artículos 9 y 10 de Ley 39/2015 del procedimiento administrativo común.

Para la provisión del idCAT Móvil el Consorci AOC, tal y como se prevé el AIPD que elaboró el Departamento de Vicepresidencia y de Economía y Hacienda de la Generalidad de Cataluña en fecha 17 de diciembre 2020, recoge el dato biométrica imagen que tiene la consideración de categoría especial de datos de conformidad con lo establecido en el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos y por lo que se deroga la Directiva 95/46/CE.

Los artículos 9 y 10 de la Ley 39/2015 en su apartado tercero dispone, en relación a los sistemas de identificación y firma previstos en la letra c de los artículos 9 y 10, que como se ha dicho comprende el idCAT Móvil, la *obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estas datos y por lo que se deroga la Directiva 95/46/CE, en territorio español."*

Los datos que se traten por parte del Consorcio para expedir el idCAT Móvil, entre ellos los datos biométricos, estarán en la región de AWS de España a contratar.

Por otra parte, los servicios objeto de licitación en el Lote 2 tienen la consideración de *"recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas"* puesto que el adjudicatario de este lote deberá encargarse , entre otros, del mantenimiento, gestión

y explotación del servicio DESA'L en el que se almacenarán y custodiarán los datos de carácter especial indicados del idCAT Móvil. Dentro de los servicios de mantenimiento, gestión y explotación que son objeto del Lote 2, de forma excepcional puede existir la necesidad de que el adjudicatario tenga que acceder, previa autorización explícita del Consorci AOC y mediante la grabación de los correspondientes eventos de auditoría, a los datos de cualquiera de los servicios que son objeto de este Lote 2. Para dar cumplimiento a los artículos 9 y 10 de la Ley 39/2015, todos los recursos técnicos proporcionados por el adjudicatario del Lote 2 tendrán que prestar sus servicios desde unas oficinas ubicadas en territorio español.

9. Propiedad intelectual

Los adjudicatarios de cada uno de los lotes aceptan expresamente que la propiedad intelectual de todos los entregables, independientemente de su naturaleza y resultados de los trabajos realizados, y en particular los productos y servicios objetos del contrato, corresponden únicamente al Consorci AOC con exclusividad y con carácter general, sin que los adjudicatarios puedan conservar, ni obtener copia de los mismos o facilitarlo a terceros.

Las empresas adjudicatarias no podrán hacer uso o divulgación de los estudios y documentos utilizados o elaborados como resultado de la prestación del servicio objeto del contrato, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa del Consorcio AOC, que la daría, en su caso, previa petición formal del adjudicatario con expresión del fin.

10. Garantía

Todas las tareas objeto de los 2 lotes que forman parte del alcance del contrato tendrán una garantía de 6 meses. Durante este período, cada uno de los adjudicatarios deberá comprometerse a resolver satisfactoriamente todas aquellas incidencias o defectos detectados en cualquiera de las actividades llevadas a cabo por sus equipos de trabajo que le sean imputables con él por acción u omisión.

11. Normativa aplicable

El adjudicatario del lote 2 se compromete a cumplir los requerimientos de seguridad y continuidad aplicables al objeto del contrato especificados en:

- La legislación vigente en general y, en particular, cuando se traten datos de carácter personal, el Reglamento UE 2106/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Además de lo establecido en el Pliego de cláusulas administrativas particulares por cada evolutivo que implique el tratamiento de datos de carácter personal habrá que aportar un informe justificativo del análisis del impacto del mismo sobre los datos afectados y la justificación de las medidas implantadas para dar cumplimiento a la normativa vigente.

- El ***Anexo3 Requerimientos de seguridad (ENS) por los proveedores*** basado en las medidas de seguridad del Anexo II del Esquema Nacional de Seguridad.

12. Protección de datos

El adjudicatario del lote 2 deberá aportar informe justificativo de las medidas de privacidad desde el diseño y por defecto implantadas, incluidas las medidas de seguridad de nivel alto previstas en el Esquema Nacional de Seguridad, para dar cumplimiento a la normativa vigente en materia de protección de datos de carácter personal y por remisión de ésta al Esquema Nacional de Seguridad. El adjudicatario del lote 2 por tanto, deberá disponer de un perfil (p. ej. alguno de los *técnicos de seguridad cloud*) con conocimientos suficientes del RGPD y la LLOPiDGDD para garantizar el cumplimiento de dicha normativa.

Además, el adjudicatario del lote 2 deberá cumplir con lo establecido en el PCAP en cuanto a protección de datos de carácter personal y seguridad de la información, y debe mantener la confidencialidad en el tratamiento de la información del Consorcio, y no divulgar o acceder indebidamente a la información sin la autorización expresa del Consorci. El adjudicatario quedará obligado a no acceder ni utilizar la información a la que tenga acceso para fin alguno que no esté explicitado en el contrato o se autorice expresamente por escrito con posterioridad a la firma del contrato ya cumplir lo establecido al respecto PCAP

El proveedor deberá cumplir con lo establecido en el PCAP y sólo podrá subcontratar empresas previa autorización expresa por escrito del Consorci AOC, que cumplan las mismas obligaciones en materia de protección de datos y seguridad que el propio adjudicatario.

13. Gobernanza de Seguridad del servicio

Medidas de seguridad por el adjudicatario del Lote 2.

Por el tipo de tratamientos que el adjudicatario del Lote 2 deberá realizar, las medidas de seguridad que deberá aplicar son las siguientes.

La seguridad de los datos y servicios se convierte en un aspecto esencial del servicio objeto del contrato y el adjudicatario deberá llevar a cabo todas las actuaciones necesarias, validadas previamente con el Consorci AOC, para garantizar unos elevados niveles de protección de los servicios, establecer los mecanismos de coordinación y seguir las directrices fijadas por el Consorci AOC como máximo responsable de la ciberseguridad de los servicios objeto del contrato. Entre otros, es fundamental que el adjudicatario alcance los siguientes objetivos:

- La incorporación al modelo de cumplimiento normativo de Ciberseguridad de la Generalitat, desarrollado por la Agencia de Ciberseguridad, del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y del Reglamento (UE) 2016/679 del Parlamento y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas, en cuanto al tratamiento de datos personales , y el seguimiento de los mismos.
- La implantación de los controles de seguridad acordados con el Consorci AOC, que permitan mitigar los riesgos a los que están expuestos los activos del CPD y procesos objeto del contrato, así como la adopción del modelo de arquitectura de ciberseguridad y el despliegue del perímetro de ciberseguridad definidos por el Consorci AOC.
- Coordinación con los órganos establecidos por el Consorci AOC para garantizar el alineamiento con la estrategia de ciberseguridad definida por el Consorci AOC.
- Que el adjudicatario sea conocedor en todo momento de las principales amenazas de seguridad que pueden afectar a los servicios de almacenamiento contratado, con la finalidad

de acordar con el Consorci AOC e implantar las medidas pertinentes para hacer frente y reducir el nivel de exposición y de riesgo a un nivel aceptable por el negocio.

Dada la naturaleza cambiante de las amenazas de seguridad, la propia evolución tecnológica y los cambios que se puedan producir en la prestación del servicio, el adjudicatario deberá adecuar los controles, medidas de seguridad y el servicio prestado para hacer frente a las mismas nuevas amenazas, a los cambios tecnológicos ya los cambios en la forma de desplegar el servicio que puedan ocurrir durante la ejecución del contrato. De forma general, es fundamental que las medidas de seguridad a desplegar por el adjudicatario permitan hacer frente a, al menos, amenazas del tipo:

- Robo de información, con el posterior impacto en el negocio y legal (como la RGPD).
- Intrusión a los equipos, cambios de configuración/seguridad para tomar el control.
- Robo de credenciales de los administradores/operadores/usuarios.
- Explotación de las vulnerabilidades.
- Acceso no autorizado y/o uso no autorizado de recursos del CPD. Los atacantes podrían aprovechar las vulnerabilidades de los equipos (servidores, equipos de comunicaciones del CPD, etc.) con el fin de llevar a cabo un ataque informático de mayor envergadura.
- Interceptar el tráfico de red por la captura de información.
- Incumplimiento normativo. Por ejemplo, incumplimiento del ENS y el RGPD.
- Provocar una denegación del servicio.
- Acceso por parte de administradores/desarrolladores no autorizados o por un uso ilegítimo. Uso no autorizado de recursos.
- Errores de los administradores/desarrolladores del servicio. Por ejemplo, configuraciones erróneas, medidas de seguridad mal aplicadas, etc.
- Accesos remotos no controlados. Los atacantes podrían aprovechar mecanismos de acceso remoto débiles.
- Ingeniería social para acceder a información confidencial del personal que presta el servicio ,

El Consorci AOC será el máximo responsable de garantizar que los servicios den cumplimiento al marco normativo vigente.
El adjudicatario tendrá que proponer e implementar los controles de seguridad necesarios para dar cumplimiento al marco normativo. El Consorci AOC aprobará todas las medidas de seguridad a implantar en función de su coste y funcionalidades aportadas.

Requerimientos transversales de seguridad

Los requerimientos transversales de seguridad son los siguientes:

Cumplimiento Normativo

- Los servicios del Consorci AOC amparados por el objeto del contrato, tendrán que cumplir con todos los requerimientos que sean de aplicación de acuerdo al marco normativo de seguridad de la información vigente que sea de aplicación y de todas las actualizaciones posteriores que se produzcan, por ejemplo el marco normativo de la Generalidad, el Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD.
- En los casos que el Consorci AOC determine, el adjudicatario instalará herramientas automáticas indicadas por la Agencia de Ciberseguridad, para auditar el grado de cumplimiento normativo de forma continua y automática.
- El adjudicatario tendrá que garantizar que los equipos cumplen con los estándares de protección aprobados por el Consorci AOC.
- El adjudicatario deberá garantizar el acceso del personal autorizado de la AOC y de aquellos que la AOC autorice, a la información de seguridad (procedimientos, registro de incidentes, trazas, etc.). Toda la información de seguridad deberá estar siempre disponible para ese personal, autorizado y previamente identificado. AOC, y el adjudicatario establecerán conjuntamente los mecanismos para facilitar el acceso del personal autorizado a esta información, estableciendo los controles de seguridad necesarios.

- En caso de ejecución de auditorías y seguimiento de los planes de acción, el adjudicatario deberá participar activamente tanto en la entrega de evidencias, como en las sesiones que sea requerido por el auditor, así como adaptar sus propios sistemas cuando éstos se consideren parte del Sistema de Información.

Seguimiento del Servicio

- El adjudicatario facilitará al Consorci AOC, los datos de contacto del Responsable de Seguridad del Proveedor (RSP) y un teléfono de contacto 24x7 por coordinación en caso de incidentes. Estos datos deberán mantenerse durante el período de vigencia del contrato.
- Periódicamente, se realizarán reuniones de seguimiento de seguridad con el Consorci AOC a las que podrá asistir la Agencia de Ciberseguridad de Cataluña donde se presentarán entre otros:
    - Cuadro de mando de ciberseguridad: que incluya el nivel de ciberseguridad, el nivel de riesgo y otros indicadores de relevancia.
    - Evolución del plan de despliegue de servicios de seguridad
    - Estado del plan de mitigación de riesgos
    - Evolución del grado de implantación controles transversales
    - Seguimiento de vulnerabilidades
    - Seguimiento de excepciones
    - Evolución de plan de cumplimiento normativo.
    - Plan de evolución e innovación en ciberseguridad

Formación y concienciación:

- El adjudicatario tendrá que impartir formación específica en seguridad a sus equipos de trabajo para garantizar que se les trasladan directrices adecuadas en materia de seguridad (la importancia de usar contraseñas robustas, el bloqueo automático de los dispositivos por inactividad, uso del cifrado en las comunicaciones, prudencia cuando se reciben correos de origen desconocido, etc.). Habrá que dejar evidencia formal de estas formaciones.
- Esta tarea es esencial para concienciar a los equipos de CPD sobre un buen uso de los dispositivos y el cumplimiento del marco normativo aplicable.

Modelo de seguridad de los servicios

Para garantizar un adecuado nivel de seguridad de los servicios objeto del contrato, el adjudicatario tendrá que contemplar la seguridad en los distintos momentos del ciclo de vida de un servicio. Estas actuaciones permitirán gestionar los riesgos de seguridad de cualquier servicio en todo momento, tomando las decisiones que se consideren oportunas.
El adjudicatario deberá:

- De forma periódica, el Consorci AOC revisará la clasificación de seguridad de los datos y servicios, y en su caso, el adjudicatario deberá participar en la reevaluación de los controles de seguridad aplicados. También se tendrán que revaluar los controles de seguridad en caso de cambios en la infraestructura del sistema.

En la fase de despliegue de los servicios:

- Actualizar toda la información de los activos de la infraestructura en la herramienta de inventario de la AOC.
- Desarrollar e implantar todas aquellas medidas de seguridad definidas en la Declaración de Aplicabilidad (DA).
- Por todos los entornos (DES, PRE), el adjudicatario utilizará la herramienta de análisis de vulnerabilidades configurada según las indicaciones de la Agencia de Ciberseguridad para revisar la infraestructura previamente al paso a preproducción. El proveedor entregará al Consorci AOC el informe resultante del análisis proporcionado por la herramienta y planificará las correcciones correspondientes.

- Será un requisito para desarrollar los servicios que la información aportada en los apartados de seguridad del DA sea completa y de calidad, y que el resultado de las pruebas realizadas por el adjudicatario esté dentro de los umbrales permitidos.
- Corregir todas aquellas vulnerabilidades de seguridad para cumplir con los umbrales solicitados por el Consorci AOC. El Consorci AOC establecerá los umbrales de aceptación a partir de los cuales se podrá proceder formalmente al despliegue del servicio.

En la fase de servicio (producción)

- Dar todo el soporte e información necesarios al Consorci AOC para poder ejecutar los análisis técnicos de seguridad que el Consorci AOC considere adecuados.
- El Consorci AOC podrá ejecutar cualquier tipo de análisis que considere oportuno en cualquier momento y podrá exigir la corrección de aquellas vulnerabilidades que se consideren graves del sistema de información, según el criterio del Consorci AOC. La corrección de estas vulnerabilidades deberá realizarse en base a lo que establece la norma de gestión de vulnerabilidades.
- Corregir todas aquellas vulnerabilidades de seguridad para cumplir con los umbrales solicitados por el Consorci AOC.

Operación y gestión de la seguridad

Tal y como se ha indicado anteriormente, la operación y gestión de la seguridad por parte de los equipos que prestan los servicios del Consorci AOC, es una de las líneas de servicio clave del contrato. En este sentido, todos los servicios objeto del contrato tendrán que desplegar las medidas de seguridad establecidas por los diferentes marcos normativos y seguir las directrices marcadas por el Consorci AOC.

El adjudicatario será responsable de la operación y gestión de la seguridad de todos los servicios objeto del contrato, así como de su integración con las herramientas, casos de uso y metodologías del Consorci AOC.

Se describen a continuación las principales líneas de trabajo que tendrán que llevar a cabo los equipos del adjudicatario en materia de ciberseguridad:

Coordinación :

- Los equipos se tendrán que coordinar de forma continua con el Consorci AOC, que hará el seguimiento del correcto despliegue de todas las medidas de seguridad requeridas por el marco normativo
- Los equipos operativos y de gestión de la seguridad tendrán que desplegar todos los servicios de seguridad pactados en el plan director de seguridad presentado al inicio del servicio y que será revisado anualmente. De forma periódica, se evaluará el grado de consecución por parte del Consorci AOC para determinar acciones correctoras.

Inventario:

- Mantener actualizada la CMDB (en su caso) con la información vinculada a los elementos y activos objeto del contrato, como por ejemplo: ubicación del activo, hardware, SO, software, versiones, direccionamiento IP, nombres de los equipos, antivirus instalado lat, códigos de servicio, código aplicación, entorno al que pertenecen, y otros atributos que se puedan requerir a futuro por necesidades. En definitiva, será el responsable de la provisión, gestión y control del inventario (A/B/M) de todo el hardware y software del servicio prestado.
- Poner a disposición del Consorci AOC las IPs de las aplicaciones, desde CPD hasta su publicación (relación IPs internas, con IPs de Nateo, e IPs públicas)
- Garantizar que toda la información del inventario esté a disposición y accesible por parte de la AOC, la Oficina QA transversal de protección del servicio y la Agencia de Ciberseguridad, y que en su defecto, se entregue esta información en un formato explotable con una periodicidad que se determinará o cuando haya cambios.

Clasificación de la información:

- El adjudicatario deberá conocer (y solicitarlo si no se tiene ese conocimiento) el nivel de clasificación de la información de las aplicaciones y sistemas de información para garantizar la correcta aplicación del marco normativo y legal en materia de seguridad. El adjudicatario tendrá que cumplir la norma de clasificación de la información.

Gestión de Trazas:

- El adjudicatario deberá garantizar que las trazas de todos los servicios prestados se guardan en un repositorio único y asegurar que almacena todos los trazos que le son de aplicación de acuerdo con el marco normativo y legal aplicable.
- Este conjunto de trazas recopilará:
    - Trazas necesarias para la detección/solución de incidencias.
    - Trazas necesarias para la detección y gestión de amenazas e incidentes de seguridad.

- El adjudicatario deberá aprovisionar y operar la infraestructura de recolección y gestión de trazas, garantizando su integración con las herramientas de visibilidad y correlación de la Agencia.
- Habilitar el acceso online y vía web a la consulta de los logs de los servicios de plataforma en el Consorci AOC,
- Configurar la infraestructura de recolección de trazas para recibir y almacenar los logs de los servicios objeto de este contrato.
- Disponer de capacidad de análisis sobre la información recolectada que permita la detección de máquinas comprometidas/infectadas y sea una herramienta de apoyo a la gestión y resolución de incidencias.
- Integrar la herramienta de gestión de trazas con el resto de herramientas de observabilidad y/o de correlación de trazas que tenga el Consorci AOC con el objetivo de ampliar el espectro en la identificación de aspectos a tener en cuenta en la posible identificación de futuras incidencias.

Gestión de usuarios y control de acceso:

- Todas las identidades con acceso a redes o sistemas de información tendrán que estar dadas de alta en el Directorio Corporativo. El adjudicatario deberá estructurar los roles de los usuarios conforme al principio de mínimo privilegio y manteniendo en todo momento la vigencia de las cuentas y privilegios otorgados.

Gestión de identidades de máquinas:

- El adjudicatario deberá gestionar y gobernar las identidades de los workloads bajo su responsabilidad (contenedores, máquinas virtuales, aplicaciones, servicios, microservicios, RPA bots) y velar por la custodia segura de las credenciales/claves asociadas, de acuerdo con las indicaciones del Consorci AOC. Habrá que dotar de herramientas o servicios de gestión de secretos/claves para que los equipos de cloud, desarrollo y mantenimiento de aplicaciones puedan gestionar sus secretos.

Gestión de usuarios privilegiados:

- El Consorcio dispone de una herramienta PAM (Privileged Acces Management) para la custodia de los secretos de administración. El adjudicatario deberá:
- Mantener un inventario actualizado de cuentas privilegiadas en la herramienta PAM del Consorci AOC.
- Segmentar los privilegios en base a la necesidad de acceso a los recursos, aplicando siempre que sea posible mecanismos de elevación delegación JIT.
- Registrar (logging), monitorear y controlar los accesos privilegiados

- Los administradores dispondrán de cuentas personales productivas para las tareas operativas habituales, correo electrónico, sistema de tiqueting, etc. diferenciadas de las cuentas de administración.
- Habrá que limitar al máximo los usuarios con elevados privilegios, garantizando la trazabilidad de su uso en todo momento.
- Recertificar a los usuarios con acceso a cuentas privilegiadas de forma semestral, y presentar semestralmente el resultado del proceso de certificación llevado a cabo y las acciones mitigadoras planificadas o puestas en marcha.

Seguridad del prestamista del servicio:

- El adjudicatario, tanto sus propios sistemas de información como su personal, serán un activo más del sistema y por tanto también estarán obligados a cumplir las medidas de seguridad organizativas, operaciones y de protección que marca el ENS. El adjudicatario deberá cumplir con las medidas indicadas en el ***Anexo3 Requerimientos de seguridad (ENS) por los proveedores*** .
- El Consorci AOC auditará en un plazo no superior a 6 meses, que el adjudicatario cumple con los requerimientos del ***Anexo3 Requerimientos de seguridad (ENS) para los proveedores*** . La auditoría se realizará mediante la entrega de evidencias indicadas en el anexo al Consorci AOC para que éste determine el grado de cumplimiento.
- El adjudicatario estará exento de la auditoría si aporta una certificación vigente del Esquema Nacional de Seguridad de nivel bajo o superior, expedido por una empresa certificadora independiente y homologada.
- En caso de que haya partes del servicio que estén subcontratadas, el adjudicatario debe comprometerse a que sus subcontratistas ofrecen las garantías equivalentes en materia de seguridad a las que él mismo asuma.

Principales funciones operativas del servicio

Prevención :

- Aplicación de las reglas de seguridad que desde el Consorci AOC se determinen.
- Velar por que las configuraciones de las máquinas sean seguras.
- Despliegue de los parches de seguridad de los fabricantes de dispositivos por la corrección de vulnerabilidades detectadas sobre los dispositivos objeto de la licitación, de acuerdo a los plazos fijados por el Marco Normativo, a los niveles de servicio solicitados en el contrato y al grado de exposición que suponen estas vulnerabilidades. El Consorci AOC deberá tener visibilidad permanente de la actualización de los sistemas y software base, y poder consultar online el estado de los parches concretos aplicados.
- Borrado seguro de todos los dispositivos que sean reutilizados o que quieran darse de baja. En caso de baja definitiva, aplicación de los procedimientos de destrucción segura corporativos, así como la entrega de un certificado que lo certifique.
- Todos los servidores y estaciones de trabajo, físicos o virtuales, deben disponer de las capacidades de protección, detección y respuesta más adecuadas con independencia del sistema operativo o software específico que tengan instalados. Las herramientas propuestas se gestionarán desde una consola central.
- Garantizar la inclusión de los requerimientos aplicables a los diferentes proyectos o iniciativas existente en el CPD, siguiendo la metodología descrita en el presente pliego, garantizando en todo caso el modelo operativo de ciberseguridad, su viabilidad económica, y su evolución.
- El adjudicatario deberá disponer, y poner a disposición del Consorci AOC, información actualizada y exacta referente a la topología de red completa del CPD, incluyendo direccionamientos de equipos, direccionamiento & relación con dominios, nombres y versiones de los diferentes elementos de red, seguridad o servidores, SO de los servidores, aplicaciones que corren, etc.
- Gestión de vulnerabilidades:
    - Todos los sistemas serán escaneados al menos con periodicidad mensual. Los escaneos serán ejecutados por la Agencia de Ciberseguridad de Catalunya,

siguiendo los procedimientos establecidos en la gestión de cambios y peticiones definidos por la AOC.
    - El Consorci AOC podrá auditar las máquinas para verificar el cumplimiento y corrección siempre que lo considere necesario.
    - Corregir las vulnerabilidades identificadas dando cumplimiento a los ANS establecidos en este pliego y al marco normativo de seguridad vigente por la gestión de vulnerabilidades, ajustándose a los plazos de corrección requeridos en el marco normativo.
    - El adjudicatario deberá realizar una gestión proactiva de las vulnerabilidades de los sistemas, productos y protocolos y coordinar con el lote de aplicaciones y los ámbitos las potenciales afectaciones y limitaciones que puedan existir.
    - Todos los resultados de los análisis de vulnerabilidades y software de base serán volcados en el Portal de Seguridad de la Agencia de Ciberseguridad, desde donde el adjudicatario podrá realizar el seguimiento.
- Entrega de informes vinculados a las medidas de prevención, como:
    - Plan de acción por la gestión de las vulnerabilidades.
    - Controles compensatorios por las vulnerabilidades que no pueden ser resueltas de forma directa.
    - Coordinación con los ámbitos y proveedores de aplicaciones para la gestión de las vulnerabilidades.
    - Excepciones tramitadas por aquellas vulnerabilidades cuya resolución no podrá llevarse a cabo de forma justificada.

Detección y protección:

- Cualquier incidente de seguridad deberá ser reportado en el Consorci AOC, siguiendo los procedimientos de gestión de incidentes y notificación de vulneraciones de seguridad establecidos.
- El adjudicatario deberá facilitar toda la información y accesos (a las máquinas afectadas) para facilitar las labores de investigación del equipo de gestión de amenazas y el equipo de gestión de incidentes de seguridad del Consorci AOC.
- Apoyar de forma inmediata por la gestión de cualquier ciber ataque relevante.
- Integrarse con los procedimientos operativos de gestión de amenazas del Consorci AOC. En este sentido, será necesario que el adjudicatario participe de forma activa en las sesiones de orquestación cuando sea requerido por el Consorci AOC.
- Establecer planes de acción para hacer frente a las principales amenazas aplicables ya los vectores de ataques asociados, que tendrán que ser validados por el Consorci AOC
- Será responsabilidad del adjudicatario la instalación, gestión y mantenimiento de aquellas capacidades de protección, tal y como describe el marco normativo de seguridad.

Respuesta:

Por la correcta gestión de potenciales amenazas o de incidentes de seguridad, el proveedor deberá:

- Ejecutar las principales acciones de contención determinadas por el Consorci AOC, ya sea mediante herramientas automáticas tipo SOAR, o bien acciones ad hoc requeridas.
- Ejecutar las acciones de erradicación y recuperación de todos los puntos afectados por el incidente para poder volver a la normalidad, así como la protección de un futuro impacto.
- Documentar y mantener la bitácora de las acciones realizadas durante la gestión del incidente.
- Disponer de una matriz de escalado 24x7 para la gestión de incidentes de seguridad, así como de un procedimiento de actuación frente a ciberataques.
- En el caso de gestión de crisis de incidentes de nivel crítico o especialmente relevantes, El Consorci AOC podrá establecer períodos excepcionales que requieran la generación de informes de estado periódicos, así como la presencia del responsable de seguridad del adjudicatario en las diferentes reuniones que se puedan realizar (disponibilidad 24x7)
- Disponer de un procedimiento de extracción y entrega de evidencias de forma segura (trazas, eventos de sistema y/o aplicación, clonado de activos, etc.) el cual deberá ser validado por

AOC y la Agencia de Ciberseguridad durante el inicio de la prestación del servicio. Este procedimiento deberá ser ejecutado siempre que AOC y la Agencia de Ciberseguridad lo requieran por la gestión de incidentes de seguridad y para atender requerimientos de la norma de uso de las TIC.

- Preservar las evidencias según normativa vigente y con la calidad necesaria para dar respuesta a la información necesaria para la resolución de un incidente de seguridad, garantizando su cadena de custodia para asegurar su validez jurídica.
- Documentar formalmente en informes cualquier actividad realizada dentro de la gestión de incidentes, que podrán ser solicitados por la AOC en cualquier momento.
- Cuando sea requerido por el Consorci AOC, el adjudicatario deberá ejecutar las acciones de Troubleshooting específicas en el ámbito de seguridad, con la entrega del correspondiente informe de finalización.
- Disponer de soluciones completas para dotar al servicio de capacidad de análisis forense a los activos incluidos dentro del alcance de la presente licitación que sean compatibles con las soluciones actualmente disponibles en la Agencia de Ciberseguridad.
- El adjudicatario deberá suministrar los accesos remotos necesarios a los interlocutores del Consorci AOC para poder acceder a las herramientas desplegadas en caso de incidente de seguridad.
- Participar periódicamente o bajo demanda en simulaciones de incidentes de ciberseguridad coordinadamente con el Consorci AOC y la Agencia de Ciberseguridad de Cataluña, mediante la preparación y definición de planes de actuación en función del tipo de amenaza simulado.
- Habrá que identificar los roles y responsabilidades en las diferentes funciones de seguridad del contrato así como la gestión bajo circunstancias excepcionales, tales como incidentes de seguridad. Se definirá conjuntamente con el adjudicatario un procedimiento por el que, en situaciones de crisis, el control y operación de elementos seguridad podrían pasar a ser gestionados por un grupo específico.

Resiliencia y continuidad de los servicios:

El adjudicatario tendrá que garantizar que el diseño de la arquitectura de la solución/aplicación permite alcanzar los requerimientos de disponibilidad/continuidad requeridos.

- Ejecutar, al menos una vez al año, pruebas de recuperación de desastres (PRDs), de aquellos sistemas de información dentro del alcance del contrato. Por orden de prioridades:
  - Pruebas de los sistemas considerados críticos por parte del Consorci AOC.
  - Pruebas de aquellos sistemas que dispongan de una infraestructura dedicada a todas las capas.
- Ejecutar, al menos anualmente, pruebas de restauración de backups de todas las tipologías utilizadas para demostrar su efectividad. El resultado de las pruebas se tendrán que entregar al Consorci AOC para validar su alcance y resultados.
- Entregar al Consorci AOC, una planificación del servicio, especificando el tipo de pruebas a realizar durante un período no inferior a 6 meses. Se evaluará anualmente la consecución de los objetivos planificados y acordados cada año entre las partes.
- Toda la información vinculada a los planes de recuperación de desastres, a las pruebas de recuperación de backups y los informes de las pruebas realizadas deberá estar siempre a disposición del Consorci AOC y la Agencia de Ciberseguridad de Catalunya.
- El proveedor deberá desarrollar e implantar un plan de continuidad para su personal y para las instalaciones desde las que opera. Este plan deberá:
  - Incluir la ubicación alternativa, los puestos de trabajo y el equipamiento necesario para garantizar la prestación del servicio desde un sitio alternativo para dar cumplimiento a los niveles de servicio fijados por el Consorci AOC.
  - Ejecutar una prueba anual para validar su efectividad.
- El adjudicatario deberá utilizar el repositorio de información que le indique el Consorci AOC, toda la información vinculada a la seguridad (incidentes, PRDs, evidencias de auditorías, procedimientos, pruebas, informes, reporting del servicio, documento de explotación del servicio).

Además, el adjudicatario del lote 2 deberá subencargar el tratamiento de almacenamiento de los datos al proveedor AWS.

- El adjudicatario deberá garantizar que en el tratamiento realizado por el subencargado, se cumplen las medidas de seguridad correspondientes al Anexo II del Esquema Nacional de Seguridad.
- El adjudicatario revisará que los servicios del subencargado que sean activos del sistema estén certificados en el nivel Alto del ENS. En el caso de algún componente no lo esté, lo devengará al Consorci AOC para buscar una alternativa.

14. Responsabilidades y obligaciones

El adjudicatario de cada uno de los 2 lotes tendrá que identificar claramente los roles de las personas involucradas en la prestación del servicio (no es necesario que haya una persona por cada rol). El Consorci AOC también definirá por su parte a los interlocutores que propone. Ambas partes tendrán que definir a sus relativos interlocutores como mínimo para los siguientes roles:

- Responsable de la seguridad.
- Persona de contacto para incidentes de seguridad.
- Persona de contacto para cambios y mantenimiento de sistemas.
- Persona de contacto para incidencias relativas a los indicadores de servicio (SLA).
- Persona de contacto para aspectos contractuales.
- Persona de contacto para temas jurídicos y reguladores, en particular en cuanto a datos de carácter personal (si existe el DPD).

Barcelona, 11 de mayo de 2022

Sergio Gutiérrez Palomino
Jefe de proyectos del Consorci AOC

ANEXO 1 Arquitectura tecnológica y estimación de costes de infraestructura inicial previstos

En este apartado encontrará los documentos de referencia que describen la nueva arquitectura tecnológica, así como la estimación de costes prevista de los diferentes entornos de integración, preproducción y producción, para cada uno de los servicios que inicialmente serán objeto del ***Lote 2: Servicios de provisión de infraestructura de cloud público, y administración, operación, mantenimiento y explotación cloud*** . El objetivo de estos documentos es facilitar y ayudar a comprender el alcance de ese lote.

Todos estos anexos se pueden consultar en el siguiente enlace:

https://llicenciesaoc-my.sharepoint.com/:f:/g/personal/sgutierrez_aoc_cat/ElqX_kM3fzFJl-k9Jgi8jQ0BWWqddCC1x3gqbtddbLyK3A?e=bhKTEE

- ***ANEXO 1.1 Diseño técnico DESÁLGALO***
- ***ANEXO 1.2 Estimación de costes DESAL***
- ***ANEXO 1.3 Diseño técnico EACAT Trámites***
- ***ANEXO 1.4 Estimación de costes EACAT Trámites***
- ***ANEXO 1.5 Diseño técnico Validador (PSIS)***
- ***ANEXO 1.6 Estimación de costes Validador (PSIS)***
- ***ANEXO 1.7 Diseño técnico VALID 2.0***
- ***ANEXO 1.8 Estimación de costes VALID 2.0***
- ***ANEXO 1.9 Diseño técnico Decidim***
- ***ANEXO 1.10 Estimación de costes Decidim***

Cabe destacar que toda la información relativa a estos servicios es susceptible de adaptaciones en tanto los servicios se tendrán que acabar de ajustar a la estrategia cloud que se vaya definiendo a lo largo de la ejecución del lote 1.

ANEXO2 Plan de devolución del servicio

El proveedor incluirá un plan de devolución del servicio detallado que describa las obligaciones y tareas que tendrán que ser desarrolladas por cada una de las partes en relación con la devolución, y que incluya los términos y condiciones en que se realizará.

En caso de cese o finalización del contrato, el proveedor estará obligado a devolver el control de los servicios objeto del contrato, debiendo realizar en paralelo los trabajos de devolución con los de prestación del servicio, sin coste adicional por el consorcio de la AOC .

Dado que en la plataforma tecnológica del Consorci AOC, que será ubicada en los servicios objeto del contrato, existen servicios de negocio considerados como críticos por el Consorci AOC y por la Generalitat de Catalunya y otros entes como consumidores de los mismos, y debido al potencial impacto sobre la continuidad de estos servicios de negocio que tienen las transiciones de proveedor, infraestructura y configuración, el Consorci AOC requiere que el contratista que resulte adjudicatario del presente contrato deberá avenirse a prestar los servicios al nuevo adjudicatario durante el período de transición establecido a los mismos precios ofrecidos en el Consorci AOC.

El Plan de devolución deberá cumplir, como mínimo, los siguientes principios y contenidos:

- El plazo de ejecución será el determinado por la AOC dentro del contrato en vigor.
- Incluirá la metodología de transferencia de conocimiento de los aspectos fundamentales de operación y, como mínimo, describirá:
    - Apoyo al nuevo adjudicatario, formación y documentación sobre los procedimientos del servicio.
    - El acceso a los elementos, servicios, software, información, documentación y otro material utilizado por el adjudicatario en la provisión del servicio.
    - La formación práctica tutelada, en la que el personal designado por el consorcio de la AOC realice los trabajos propios de cada proceso o funcionalidad tutelados por el personal del adjudicatario.
- El adjudicatario deberá entregar las cuentas del cloud público, adscritas de forma exclusiva a los servicios objeto del contrato, al consorcio de la AOC oa terceras partes nombradas por éste.
- El Consorcio de la AOC será el propietario de todas las licencias que se hayan requerido de uso sobre los sistemas del Consorci AOC y que fueran necesarias para asegurar la continuidad del servicio.
- El adjudicatario tendrá que ofrecer un plan para definir las responsabilidades y gestionar la resolución de problemas entre el nuevo adjudicatario, el Consorci AOC y/u otros adjudicatarios.
- Durante el período de devolución del servicio, el adjudicatario debe cumplir los acuerdos de nivel de servicio. El plan de devolución no debe causar discontinuidad alguna en el servicio.
- El consorcio de la AOC no asumirá una dedicación significativa de recursos propios en las actividades de devolución.
- El proveedor deberá prestar al Consorci AOC servicios de asistencia adicionales durante al menos los 3 meses posteriores a la devolución del servicio, en caso de ser solicitados.

Transición del servicio

Dado que en la plataforma tecnológica del Consorci AOC, que será ubicada en los servicios objeto del contrato, existen servicios de negocio considerados como críticos por el Consorci AOC y por la Generalitat de Catalunya y otros entes como consumidores de los mismos, y debido al potencial impacto sobre la continuidad de estos servicios de negocio que tienen las transiciones de proveedor, infraestructura y configuración, el Consorci AOC requiere que todos los elementos y soluciones que el licitador proponga a su oferta se encuentren disponibles, en las condiciones y niveles de servicio, el mismo día de la formalización del contrato.

La solución a entregar deberá ser aceptada previamente por personal del Consorci AOC antes de realizar la migración asociada a la transición del servicio.

Todas las acciones derivadas de la puesta en operación de los servicios asociados a este contrato corren a cargo del proveedor resultante de la licitación del mismo bajo la supervisión, validación y aceptación del personal del Consorci AOC relacionado al servicio.

La transición del servicio se propone que siga el siguiente esquema:

- **Prestación actual** : en esta fase opera únicamente el adjudicatario.
- **Due Diligence** : El nuevo adjudicatario, conjuntamente con el consorcio de la AOC, revisa la información que se ha entregado al adjudicatario durante la fase de licitación para comprobarla, completarla o corregirla.
- **Transición** : es el período que va desde el inicio de ejecución del contrato la toma de control del servicio por parte del nuevo adjudicatario.

  Durante la transición se llevarán a cabo las siguientes actividades:

  - **Transferencia** : El nuevo adjudicatario recibirá soporte del proveedor, que facilitará y colaborará en el traspaso de conocimiento así como en la habilitación de la operación. En ese momento, el adjudicatario actual sigue realizando la prestación del servicio y alcanzando los ANS actuales.
  - **Prestación en transición** : El nuevo adjudicatario comienza a prestar el servicio con sus propios medios, aunque los ANS siguen siendo los de la prestación actual. Durante esta fase, el nuevo adjudicatario será el único responsable de la prestación del servicio.

  El nuevo adjudicatario tendrá que alcanzar los valores objetivos requeridos en los indicadores, aunque el modelo de penalizaciones no será aplicado en el transcurso de esta fase.

  - **Nueva prestación** : una vez finalice la fase de transición, el adjudicatario deberá prestar el servicio, en tres tipos de actividad principal.
  - **Mantenimiento de sistemas en modalidad actual** : asegurar que los clientes de la AOC siguen recibiendo un servicio sobre los sistemas en su configuración actual
  - **Transformación** : realizar aquellos cambios para migrar los servicios necesarios al nuevo adjudicatario
  - **Nuevo servicio** : prestación de servicios en las nuevas modalidades

En caso de no poder completar la transición del servicio en el período contractual, el Consorci AOC podrá requerir prolongar el período de transición del servicio en cuestión hasta su correcta finalización.

En este último caso, el adjudicatario asumirá los gastos necesarios para la continuidad del servicio por parte del actual contratista hasta su correcta transición.

Plan de transición del servicio

El Plan de Transición del Servicio, deberá tener los siguientes contenidos:

- Planificación detallada de actividades del proceso de transferencia del conocimiento.
- Plan de metas principales de la transición.
- Plan de activación del servicio.
  El plan indicará la secuencia de actividades a realizar para tomar el control efectivo del servicio, así como la lista de control que se va a utilizar para comprobar que todos los elementos computables pueden ser gestionados correctamente. Esta lista de control se utilizará los días en que se ejecuten las metas de transferencia de responsabilidad como secuencia de acciones necesarias para asumir el control del servicio.

  Además, el plan de activación del servicio deberá incluir un plan de contingencia para garantizar la continuidad del servicio en caso de problemas durante la transferencia.
- Planificación de la incorporación de recursos en el servicio.
- Plan de riesgos de la transición, incluyendo la identificación de principales riesgos y las acciones asociadas.
- Identificación de recursos de principal importancia para la correcta prestación del servicio, si los hubiere.
- Método de gestión de trabajos en curso, entendidos como aquellas actividades o tareas que están iniciadas o previstas en el momento en que el proveedor entrante asume la responsabilidad del servicio.

Hitos y calendario

Los principales hitos de la transición deben incluir, al menos, para cada una de las tareas a llevar a cabo en el proceso de transición, las fechas de inicio y fin de cada una de ellas, la distribución de responsabilidades, los criterios aplicables de aceptación y cualquier otro detalle adicional que se estime pertinente.

En cualquier caso, se espera la participación activa del proveedor adjudicatario para garantizar la correcta alineación de las planificaciones de los distintos contratos, independientemente de cuál sea el proveedor responsable.

El consorcio de la AOC identificará dependencias y condicionantes entre contratos que el proveedor deberá respetar, a fin de minimizar el impacto de la transición en los ámbitos y realizar la transición de forma coordinada.

Transferencia del Servicio

La transferencia de servicios entre proveedores será responsabilidad del proveedor entrante, aunque el proveedor saliente colabore en el proceso para que, en ningún caso, esta transferencia afecte al

funcionamiento, disponibilidad y nivel del servicio. Para garantizar esta colaboración, el consorcio de la AOC supervisará los procesos de transferencia.

El proceso de transferencia del conocimiento debe incluir, al menos:

- Formación específica y formal por la asunción del servicio. Esta formación será proporcionada por el proveedor saliente según las condiciones que haya acordado con el proveedor adjudicatario del servicio y bajo la supervisión de la AOC.
- Documentación necesaria por la asunción del servicio a ser proporcionada por el proveedor saliente. Es responsabilidad del proveedor adjudicatario identificar y recopilar toda la información necesaria para la correcta prestación del servicio (documentación de sistemas y aplicaciones, documentación técnica, procedimientos de actuación, etc.). En aquellos casos en los que no exista documentación previa necesaria para prestar el servicio, el proveedor adjudicatario deberá planificar y ejecutar su elaboración, de acuerdo con el consorcio de la AOC y sin coste adicional para el consorcio de la AOC.

Al inicio de la fase de transferencia, el proveedor entrante deberá realizar las siguientes tareas:

- Coordinación con el proveedor saliente del proceso de transferencia del conocimiento y de la formación formal que haya considerado necesaria.
- Presentación de un plan de calidad, que debe aprobar el consorcio de la AOC.
- Presentación de un plan de contingencia para asegurar la continuidad del servicio.
- Cualquier otro condicionante necesario para la ejecución del proceso de transferencia del conocimiento y de la transferencia de responsabilidad.

Adicionalmente, el proveedor entrante debe comunicar al consorcio de la AOC la organización con la que proporcionará el servicio, así como la asignación de recursos y confirmación de roles, tareas y responsabilidades necesarias para la prestación del servicio.

La transferencia del servicio tendrá asociada una fase de toma de contacto y una fase de desarrollo de la transferencia.

ANEXO 3 Requerimientos de seguridad (ENS) por los proveedores

ID 1. Política de Seguridad
Se dispone de una Política de Seguridad que incluye:

1- Objetivos de la organización
2- Marco legal y regulador
3- Roles relacionados con la seguridad, así como sus responsabilidades y procedimiento de designación.
4- Estructura del comité de gestión y coordinación de seguridad.
5- Criterio para la clasificación de la documentación.
6- Referencia a la legislación aplicable en materia de tratamientos de datos de carácter personal.
7- La Política de Seguridad debe ser un documento en papel o soporte electrónico.
8- La Política de Seguridad incluye la especificación del plazo y condiciones de su revisión y que debe estar aprobada por un órgano superior.
9- La Política de Seguridad incluye un apartado específico de gestión de los usuarios y sus privilegios, así como la persona responsable.
10- La Política de Seguridad incluye un apartado específico indicando a los responsables de la información gestionada por el sistema.

ID 3. Procedimiento de revisión de la Política de Seguridad
Documento conteniendo el Procedimiento de revisión y aprobación de la Política de Seguridad o en su defecto, apartado de la Política de Seguridad donde se especifique el período de revisión y aprobación.

ID 4. Evidencia de la difusión de la Política de Seguridad
Evidencia de que la Política de Seguridad es accesible por el personal afectado en la Intranet, página web, portal, repositorio o ha sido distribuida a todos cuyos usuarios son responsables mediante el correo electrónico.

ID 10. Evidencia de la difusión de la Normativa de Seguridad
Evidencia de que la Normativa de Seguridad - ya sea propia o se utilice el Marco Normativo de la Agencia de Ciberseguridad de Cataluña - está disponible en la Intranet, página web, portal, repositorio, librería o en cualquier otro medio accesible para todos los usuarios implicados o que les ha sido distribuida a través del correo electrónico.

ID 11. Procedimientos de Seguridad
Se dispone de procedimientos de seguridad para la realización de las tareas rutinarias.
Éstos deben incluir como mínimo:
1- Cómo llevar a cabo las tareas habituales.
2- Quien debe hacer cada tarea.
3- Cómo identificar y reportar comportamientos anómalos.

ID 13. Evidencia de la difusión de los procedimientos de seguridad o de la posibilidad de acceso por parte de los usuarios.
Evidencia de que los Procedimientos de Seguridad - sean propios o se empleen los del Marco Normativo de la Agencia de Ciberseguridad de Cataluña - están disponibles en la Intranet, página web, portal, repositorio, librería o en cualquier otro medio accesible para todos los usuarios implicados.

ID 40. Documento de Identificación del Control de Acceso al sistema
Se dispone de un procedimiento formalizado de gestión de usuarios debidamente aprobado y actualizado que se indique:
- Cómo se realiza la gestión de los usuarios y de sus privilegios así como la persona responsable de la gestión de los usuarios.
- Que los identificadores de los usuarios deben ser nominales y no se pueden compartir.
- El período de retención de los usuarios.

ID 43. Procedimiento de Autenticación del Sistema
Se dispone de un procedimiento debidamente aprobado y actualizado en el que se describen los mecanismos de autenticación de los usuarios o se especifica dentro del procedimiento formalizado de gestión de usuarios los siguientes puntos:
1- Se detalla los sistemas de autenticación de los usuarios con la obligación de tener al menos un factor de autenticación.
2- Se detalla y se obtiene la evidencia de que el usuario confirma la recepción del identificador, conoce y acepta las obligaciones.
3- Se explica cómo gestionar las bajas de usuarios y el vínculo con RRHH que permita avisar a los responsables de gestión de usuarios del cambio en las relaciones con éstos.
4- Se indica que se utilicen al menos dos factores de autenticación en los sistemas categorizados como nivel medio y alto.
5- En caso de que se utilicen tokens, que éstos utilizan un algoritmo autorizado por el CCN, por ejemplo AES.

ID 46. Documento de Requerimientos de Acceso al sistema
Se dispone de un procedimiento formalizado de gestión de usuarios debidamente aprobado y actualizado que se indique:
- Cómo se realiza la gestión de los usuarios y de sus privilegios así como la persona responsable de la gestión de los usuarios.
- Que los identificadores de los usuarios deben ser nominales y no se pueden compartir.
- El período de retención de los usuarios.

ID 50. Herramienta corporativa específica para la gestión de los propios usuarios
Se dispone de una herramienta corporativa específica para la gestión de usuarios.

ID 54. Procedimiento de Gestión de Derechos de Acceso al Sistema
Se dispone de un procedimiento o se incluye dentro del procedimiento formalizado de usuarios del sistema los siguientes puntos:
- Se asignará el rol adecuado a cada usuario con los mínimos privilegios posibles y revisándose los mismos periódicamente.
- Se incluirá la relación entre los permisos que debe tener cada usuario en función de su rol.
- Se especificará cuáles son los responsables de los recursos de los sistemas (físicos y lógicos) y quién tiene la responsabilidad delegada de conceder, alterar o anular el acceso a los mismos.

ID 62 Evidencia de que el usuario confirma la recepción del identificador, conoce y acepta las obligaciones
Se dispone de la evidencia que demuestra que los nuevos usuarios confirman la recepción del identificador, conocen y aceptan sus obligaciones. Esta evidencia puede tomar diversas formas:
1- Evidencia de que al crear su identificador se informa al usuario por correo electrónico, y al acceder por primera vez debe aceptar los derechos y deberes de acceso al aplicativo.
2- Que el personal de un proveedor firme un documento de obligaciones el primer día, así como un acuerdo de confidencialidad y queda constancia de la entrega del identificador.
3- Que en la parte inferior de la pantalla de acceso se indiquen los términos y condiciones, por lo que los usuarios están implícitamente aceptándolas para acceder al sistema.

ID 63. Acuerdo de confidencialidad donde se hace constar la entrega del identificador
Se dispone del documento conteniendo el Acuerdo de Confidencialidad firmado por el usuario haciendo constar la recepción de su identificador. Debe existir un registro de cada usuario confirmando la recepción del identificador.

ID 64. Evidencia del último usuario propio dado de baja
Se dispone de la evidencia mostrando la baja de un usuario con fecha efectiva de la baja.

ID 67. Procedimiento de Acceso en Local

Se dispone de un Procedimiento de Acceso en Local que especifique que:
1- Los sistemas antes de entrar en explotación o los ya existentes han sido configurados de forma que no revelen información del sistema antes de un acceso autorizado.
2- Los diálogos de acceso (en el puesto de trabajo, dentro de las propias instalaciones de la organización, en el servidor, en el dominio de red, etc.) no revelen información sobre el sistema al que se está accediendo.
3- Haga constar que se debe informar siempre a los usuarios de sus obligaciones una vez han accedido dentro del sistema.
4- Se debe informar al usuario de su último acceso al sistema.
5- Defina unos horarios en los que es posible la conexión al sistema y otros en los que no lo es.
6- No se puede acceder al sistema fuera de las horas autorizadas.
7- Indique puntos de renovación de autenticación durante la sesión de un usuario.

ID 107. Evidencia de qué se dispone de antivirus en los sistemas de información
Se dispone de la evidencia del uso de mecanismos de prevención frente a código perjudicial (antivirus) para todos los equipos (Servidores y puestos de trabajo) del sistema y también en las maquetas, así como de su configuración.

ID 111. Evidencia de que el programa antivirus se encuentra actualizado
Se dispone de la evidencia de que las opciones de configuración aplicadas a los antivirus son las recomendadas por los fabricantes (p.ej. Análisis de ejecución de programas, análisis de correo entrante y saliente, bloqueo automático de código nocivo, etc.), así como las referentes a la frecuencia de actualización.

ID 172. Evidencias de la difusión del contenido del Plan de Concienciación
Se dispone de evidencia de la difusión del contenido del plan de concienciación (en la intranet o por algún otro medio se lanzan mensajes de concienciación (p.ej. correos, comunicados internos,…)).

ID 174. Evidencias de la difusión del contenido del Plan de Formación
Se dispone de evidencia con la difusión del contenido del plan de formación en los últimos 3 años.

ID 241. Documento donde se indica el mecanismo de autenticación e identificación
Se dispone de una política o normativa documentada respecto al diseño de un sistema que contemple los mecanismos de identificación y autenticación y además contempla los mecanismos de protección de la información tratada.
Asimismo no debe ser posible acceder a información del sistema que pueda ser utilizada para la escalada de privilegios, ni ejecutar acciones haciéndose pasar por otro usuario, etc.

ID 244. Procedimiento para la elaboración y ejecución del plan de pruebas de la aplicación
Se dispone de un procedimiento de Aceptación y Puesta en Servicio de Protección de las Aplicaciones Informáticas. Antes de pasar a producción debe comprobarse el correcto funcionamiento de la aplicación. Se debe comprobar que:
1- Se cumplen los criterios de aceptación en materia de seguridad.
2- No se deteriora la seguridad de otros componentes del servicio.
3- Las pruebas deben realizarse en un entorno aislado (preproducción).
4- Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
5- Se realizan análisis de vulnerabilidades.
6- Se realizan análisis de coherencia y código fuente.

ID 273. Procedimiento de configuración segura del correo.
Se dispone de un procedimiento que se detalla cómo se configura el correo para disponer de un sistema seguro.

ID 276. Evidencia de la herramienta monitorización de los elementos de seguridad

Se dispone de la evidencia en la que se observa que se dispone de una herramienta para monitorizar los elementos de seguridad tales como los virus o el spam debidamente configurado y mantenido.

ID 330. Normativa documentada que especifica los deberes y obligaciones del personal contratado a través de un tercero.

Se dispone de normativa en la que se especifican los deberes y obligaciones del personal contratado a través de un tercero.

ID 460. Protocolo de actuación respecto al incumplimiento de las obligaciones por parte del personal tercero
Se dispone de un procedimiento que define la resolución de incidentes relacionados con el incumplimiento de las obligaciones por parte del personal del tercero, además de identificar a la persona de contacto con el tercero para la resolución de este tipo de incidentes.