Pliego de prescripciones técnicas particulares para la contratación del servicio impulso evolución tecnológica servicios AOC trans. Dig. AAPP (expediente AOC-2024-50)

Índice de cláusulas y anexos

1. Introducción

El Consorcio Administración Abierta de Cataluña (en adelante Consorci AOC) es un organismo público con uno misión estratégica clara: impulsar la transformación digital de las administraciones públicas catalanas para promover gobiernos ágiles, lógicos y colaborativos, con el objetivo que las personas puedan beneficiarse y disfrutar de servicios públicos de calidad.

Para poder cumplir con este mandato, el Consorci AOC trabaja en diferentes ejes clave como pueden ser facilitar la interoperabilidad de los sistemas de información, la prestación de servicios comunes de administración electrónica o garantizar la identidad, confidencialidad y el no repudio de las comunicaciones electrónicas. El compromiso firme del Consorci AOC es prestar estos servicios con los niveles más altos de disponibilidad, calidad y seguridad.

Hace unos años, el Consorci AOC tomó la decisión estratégica de acelerar la incorporación de las innovaciones que ofrece el sector TIC explorando e incorporando tecnologías como el cloud computing, el aprendizaje automático o la inteligencia artificial. Esta decisión está permitiendo modernizar el catálogo de servicios que ofrece el Consorci AOC y proporcionar un mayor valor añadido a la ciudadanía. Con esta iniciativa, el Consorci AOC busca por una parte garantizar la disponibilidad de sus servicios, asegurar la integridad y seguridad de los datos, y enriquecer su catálogo de servicios incorporando las tendencias tecnológicas emergentes.

La presente licitación representa por lo tanto una oportunidad excepcional y ocurrirá una pieza clave para dar un fuerte empuje a esta iniciativa de renovación de los servicios de administración digital del Consorci AOC, contribuyendo a la creación de una administración pública catalana más eficiente, transparente y de calidad.

El Consorci AOC entiende, sin embargo, que la transformación digital no es sólo una cuestión de tecnología, sino también de personas. Por este motivo dentro de esta licitación se trabaja también para garantizar que todos los ciudadanos tengan acceso a los servicios que el Consorci AOC ofrece, independientemente de su edad, ubicación o capacidades, y está decididamente comprometido a asegurar que sus servicios sean fáciles de utilizar y comprensibles para todo el mundo.

2. Objeto de la licitación

El presente pliego se divide en 4 bloques de tareas notoriamente diferenciadas que se contratarán mediante 4 lotes independientes.

Este documento recoge los requerimientos técnicos para la valoración de los 4 lotes. El formato de las ofertas presentadas se tendrá que ajustar a la descripción realizada en este pliego.

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

- **Lote 1: Centro de excelencia en Cloud (CCoE)**. La principal función y responsabilidad del CCoE serán garantizar que este proceso de transformación digital se lleva a cabo de acuerdo en el marco metodológico que determinan los principales hyperscalers de cloud público.
- **Lote 2: Construcción de servicios comunes y evolución de los actuales servicios del AOC hacia tecnologías basadas en nube pública**. La principal función y responsabilidad de este lote es la construcción de nuevos módulos, transformación y evolución de los servicios del AOC hacia la nube pública.
- **Lote 3: Servicios de desarrollo de aplicaciones Frontend y Accesibilidad**. Las principales funciones y responsabilidades de este lote son desarrollar el Frontend y llevar a cabo las acciones necesarias para garantizar que los nuevos módulos, las transformaciones y las evoluciones de los servicios del AOC se desarrollen dando conformidad en el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.
- **Lote 4: Implementación de procedimientos para la mejora de la calidad de las aplicaciones del Consorci AOC**. Los objetivos y responsabilidades de estos lotes son los siguientes principalmente; la implementación de test unitarios, funcionales y sobre todo de UI automatizados para la validación de los despliegues de nuevas versiones de los aplicativos. Implementación de análisis de código para detección de vulnerabilidades y calidad del código para poder aplicar mejoras en el desarrollo y reducir la exposición de las aplicaciones.

El alcance de cada uno de los lotes, así como el calendario asociado a las diferentes actuaciones de estos, se describe a continuación. Este alcance se ha definido partiendo del supuesto de que los diferentes contratos estarán operativos el 1 de julio de 2024 y que llegarán hasta el 30 de junio de 2026. Aunque se pudiera retrasar la fecha de inicio de algunos de estos lotes, la fecha de finalización se mantendrá fija en el 30 de junio de 2026. Por este motivo es importante destacar que el alcance de cada uno de los lotes se mantendrá en todo momento y que en caso de que el inicio del servicio se demore más allá del 1 de julio de 2024 en alguno de los lotes, el adjudicatario correspondiente tendrá que incrementar la dedicación de los recursos asignados con el fin de poder garantizar que se alcanza el alcance definido.

Para dar cumplimiento a la Orden HFP/1030/2021, de 29 de septiembre, por la cual se

configura el sistema de gestión del Plan de recuperación, transformación y resiliencia, en los apartados 8 Condiciones de ejecución y 9 Modelo de relación se determinan los mecanismos de control, así como las pruebas y análisis que el Consorci AOC llevará a cabo para garantizar la consecución de este alcance y del correspondiente calendario.

3. Objetivos, hitos y calendario Lote 1: Centro de excelencia en el Cloud (CCoE)

3.1 Situación actual Lote 1

El Consorci AOC dispone de un plan de transformación estratégico para el periodo 2022-2026 adaptado a sus necesidades y objetivos específicos. Este plan se centra en la adopción e implementación de nuevas tecnologías, en la renovación profunda de los activos digitales del Consorci AOC, y al implementar una cultura de gestión del cambio, acompañada de una reorganización interna muy significativa. Todo eso con la finalidad de poder ofrecer nuevos modelos de negocio, dar respuesta a nuevos requerimientos y necesidades de la organización, o maximizar la eficiencia de los modelos de negocio tradicionales.

El plan estratégico define un marco de referencia basado en diferentes ejes y ámbitos (destacamos los principales):

- **Apoderar la ciberseguridad** como pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de los servicios de administración electrónica que el Consorci AOC ofrece a las administraciones públicas catalanas.
- **Alineación de los servicios TIC con las necesidades de la organización** e incorporación de mecanismos que impulsen la innovación, así como dotación de instrumentos y prácticas de Gobernanza que permitan garantizar la consecución de las necesidades de la organización.
- **Flexibilizar la asignación de recursos TIC** para poder ofrecer una respuesta más ágil y rápida a las nuevas demandas de la organización.
- **Modernización y renovación de los activos digitales** del Consorci AOC que permitan gestionar el incesante incremento de infraestructura tecnológica que requiere el Consorci AOC para poder seguir ofreciendo sus servicios con todas las garantías de disponibilidad y nivel de servicio que se requiere.
- **Gestión del cambio** para preparar al personal del Consorci AOC para las nuevas formas de trabajar que requiere el plan estratégico, y fomento de metodologías que faciliten un mejor control del rendimiento de los servicios.

- **Automatización de procesos** y tareas repetitivas que permitan mejorar la eficiencia operacional, y priorización de estándares que impulsen la homogeneización de los servicios.

Para poder llevar a cabo estos objetivos, el Consorci AOC definió como principal línea de actuación, y eje central sobre lo que pivota el plan estratégico, la implantación de un nuevo modelo de gestión TIC basado en la adopción y evolución en el cloud público. Esta decisión se fundamentó en la demostrada capacidad del cloud público a la hora de incorporar y ofrecer las mejoras tecnológicas presentes y futuras que van apareciendo al mercado TIC, así como para la optimización de recursos que permite alcanzar, o por el amplio catálogo de soluciones flexibles y ágiles que proporciona. La adopción del cloud público, pero tiene que venir acompañada de la correspondiente simplificación de la arquitectura de Centros de Proceso de Datos (CPD), que actualmente tiene disponible el Consorci AOC para diversificar riesgos y disponer de mecanismos de contingencia en caso de incidencia en alguna de las plataformas o servicios críticos.

Fruto de la implantación de este nuevo modelo TIC, el Consorci AOC definió una hoja de ruta clara a la hora de transformar sus servicios y migrarles al cloud público, y estableció la priorización de los servicios y los principales hitos a alcanzar.

Este plan estratégico se inició el año 2022 y actualmente se encuentra en un punto de madurez bastante avanzado con un amplio conjunto de servicios esenciales que ya están desplegados y operativos en el cloud público.

Durante el periodo de vigencia de esta licitación (junio 2024-juny 2026), el plan de transformación estratégico del Consorci AOC alcanzará su momento culminante y el CCoE tiene que jugar un rol fundamental para alcanzar los objetivos e hitos del plan.

3.2 Descripción y alcance Lote 1

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

- **Asesoramiento en la adaptación del plan de transformación estratégico**. El plan de transformación estratégico se tiene que ir adaptando y ajustando a medida que el Consorci AOC recibe nuevos encargos que tiene que alcanzar. Estas nuevas peticiones y objetivos de negocio se tienen que analizar en detalle y se tiene que determinar el impacto y el encaje que pueden tener sobre el plan de transformación estratégico.

  El CCoE tiene que asesorar en los equipos directivo y técnico del Consorci AOC, en caso de que sea necesario adaptar el plan de transformación estratégico, determinando los cambios y ajustes que hay que aplicar sobre la línea base del plan, estableciendo los nuevos marcos de gobernanza y de organización, definiendo los resultados esperados y los principales indicadores de evaluación y seguimiento, identificando las principales barreras de adopción, etc.

  El CCoE se tiene que convertir por lo tanto en un actor en clave ofreciendo un nivel de soporte especializado que tiene que acompañar en todo momento al Consorci AOC a lo largo de todo el proceso de implantación del nuevo modelo TIC. El

objetivo por lo tanto del CCoE tiene que ser proporcionar el nivel de acompañamiento que permita garantizar el éxito del proceso de transformación que se promueve y detallar la situación final deseada en un marcado contexto de cloud público después de racionalizar, reorganizar, y reestructurar los diferentes CPDs que el Consorci AOC dispone en la actualidad.

Calendario: 3 meses desde la formalización del contrato.

- **Impulsar la transformación digital que requiere el nuevo modelo TIC**. Colaborar con el Consorci AOC a 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 CCoE por lo tanto se tendrá que convertir en el principal vector de impulso en la promoción y dinamización del nuevo modelo en TIC, fomentando su aceptación por parte de toda la organización.

  Calendario: 18 meses desde la formalización del contrato.

- **Ajustar y definir las nuevas métricas e indicadores que permitan la evaluación continua del grado de avance de la adopción del nuevo modelo TIC**. El proceso de adopción del nuevo modelo TIC es un proceso continuo y de largo plazo (2022-2026). Fruto de los nuevos encargos y cambios de requerimientos pedidos por el negocio, hay un alto riesgo de que la implantación del nuevo modelo se pueda desviar e incluso llegar a descontrolarse. Es por este motivo que resulta indispensable disponer de métricas e indicadores actualizados que permitan medir y conocer 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 tienen que 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 diferentes equipos de trabajo internos. El objetivo del CCOE tiene que ser en todo momento reconducir estos tipos de situaciones alineando los intereses de todos los equipos de trabajo con la estrategia del plan de transformación. Estas métricas e indicadores se tendrán que reflejar en un cuadro de mandos y en un conjunto de informes de control que permitan conocer en todo momento el estado de situación para facilitar la toma de decisiones.

  Calendario: 4 meses desde la formalización del contrato.

- **Mantenimiento y actualización del plan de seguridad en el cloud**. Actualmente el Consorci AOC dispone de un plan de seguridad común para todos los servicios y

plataformas desplegadas en el cloud público. Este plan adopta el principio de la seguridad por diseño y establece las normas, procedimientos, políticas y requerimientos de seguridad, que tienen que garantizar el cumplimiento de la normativa, vigente.

El plan de seguridad está implementado a nivel de la Landing Zone y aplica de forma transversal sobre todos los servicios y recursos de cloud público del Consorci AOC.

A lo largo de la prestación del contrato, y para todos los nuevos servicios que se vayan migrando en el cloud público, el CCoE tendrá que definir cómo se tiene que realizar el encaje del nuevo servicio dentro del plan de seguridad global. El objetivo tiene que ser garantizar que sobre los nuevos servicios migrados al cloud público se aplican todas estas políticas y requerimientos de seguridad para asegurar la confidencialidad, integridad y disponibilidad de los nuevos servicios.

Además, cuando sea necesario, el CCoE tendrá que adaptar y ajustar el plan de seguridad para cubrir las nuevas tecnologías y necesidades que se vayan introduciendo. Será por lo tanto responsabilidad del CCoE, y para cada uno de los entornos de trabajo (integración, preproducción y producción), establecer la nueva arquitectura de seguridad, definir el esquema de líneas de defensa (soluciones Anti-DDoS, IDS/IPS, WAF, etc.) y el perímetro de seguridad propuestos, determinar la gestión de identidades y la seguridad de accesos (creando las diferentes cuentas de cloud público y delimitando la seguridad de accesos siguiendo el principio de mínimo acceso necesario), definir las políticas de acceso condicional en el momento de acceder al portal de gestión del cloud público (acceso a través de VPN, restricciones de IP autorizadas, autenticación con multi factor, etc.), delimitar la fragmentación de redes y subredes, los requerimientos de auditoría y la centralización de logs, especificar las reglas de Firewall y las políticas de cifrado, etc.

Es importante destacar que el CCoE tendrá que seguir en todo momento las directrices que determine la Unidad de Seguridad del Consorci AOC y tendrá que adaptarse a los procedimientos y herramientas (SIEM, SOAR, etc.) que la unidad de Seguridad establezca en cada momento.

Calendario: 18 meses desde la formalización del contrato.

- **<u>Definir el plan de backup para cada nuevo servicio migrado al cloud público</u>**. El Consorci AOC tiene definido y aplicado un plan de backup integral y automatizable que cubre todos los tipos de datos, infraestructura y recursos IT desplegados al cloud público. Este plan de backup presta especial atención a la hora de garantizar la coordinación de los diferentes orígenes de datos que forman parte de un mismo servicio de administración electrónica del Consorci AOC. El plan de backup determina las políticas de cifrado, así como los requerimientos que exige la normativa vigente en el ámbito de los backups (especialmente el ENS

nivel alto y RGPD).

De acuerdo con este plan de backup global, y sotas las directrices que determine la Unidad de Seguridad del Consorci AOC, para cada nuevo servicio a migrar al cloud público, el CCoE tendrá que establecer las diferentes políticas de retención que hay que aplicar, así como las medidas a llevar a cabo para poder cumplir con los RPO (Recovery Point Objective) y RTO (Recovery Time Objective) que el Consorci AOC determine para cada uno de los servicios. El CCoE también tendrá que determinar el plan de continuidad de negocio y/o de contingencia para cada uno de los servicios que el Consorci AOC requiera. El CCoE tendrá que diseñar, así como ejecutar y auditar de forma periódica (como mínimo 1 vez al año) un plan de restauración que permita validar el plan de continuidad de negocio, y/o el plan de contingencia, con el objetivo de confirmar que se cumplen los Acuerdos de Nivel de Servicio (ANS), los RTOs y los RPOs definidos en el plan de backup.

Finalmente, 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.

Calendario: 20 meses desde la formalización del contrato.

- Para cada nuevo servicio a migrar al cloud, **determinar el encaje del marco de gobernanza global y la nueva solución cloud propuesta**. Actualmente el Consorci AOC dispone de un modelo global de gobernanza que tiene como objetivo minimizar los riesgos de gestión y financieros del nuevo modelo TIC. Este modelo de gobernanza determina las políticas, procedimientos, roles y herramientas transversales a toda la organización que permiten reducir los esfuerzos de adopción que requiere el nuevo modelo TIC. Además, este modelo de gobernanza permite amortiguar la complejidad creciente por el uso de las nuevas y varias tecnologías que se van implantando a medida que se va desplegando el nuevo modelo TIC.

  El objetivo de este marco de gobernanza es evitar abusos de autogestión por parte de los diferentes equipos de trabajo que puedan provocar un entorno caótico difícil de reconducir, pero evitando a la hora un modelo excesivamente rígido que pueda dificultar la productividad y estropear la agilidad intrínseca en torno a cloud público.

  El CCoE tendrá que establecer en todo momento las bases que tienen que permitir el crecimiento constante y la mejora continua del nivel de madurez cloud (según el modelo CMM) del Consorci AOC, creando y adaptando las políticas, procedimientos y herramientas de gobernanza existentes a medida que vaya aumentando el nivel de madurez del Consorci AOC. Además, el CCoE tendrá que definir al modelo de competencias organizativas de cada nuevo servicio que se migre al cloud público y tendrá que establecer el encaje de estos nuevos servicios con el modelo global adaptando, si procede, el modelo global de gobernanza.

Calendario: 20 meses desde la formalización del contrato.

- **Diseñar la arquitectura de cada nuevo servicio, plataforma o iniciativa** que haya que migrar al cloud público estableciendo el modelo de cloud idóneo y el patrón de migración (Re-host, Re-platform, Re-architect o Re-build), la propuesta detallada 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 de el/los proveedor/es 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.

  El CCoE deberá tener en cuenta los requerimientos necesarios que tiene que cumplir cualquier solución de cloud público para poder ser utilizada. Para definir la nueva arquitectura tendrá que priorizar el catálogo de servicios cloud estándar definido por el Consorci AOC, las diferentes plantillas base de recursos y el conjunto de servicios comunes definidos.

  Para cada nuevo servicio a migrar al cloud público el CCoE tendrá que proporcionar el documento de arquitectura que incluirá:

  - Diseño de la nueva arquitectura cloud del servicio.
  - Diseño del nuevo entorno de ejecución incluyendo la solución de contenedores, plataformas PaaS y/o servicios SaaS. Este nuevo entorno de ejecución tendrá que estar alineado con la estrategia cloud y el marco de referencia de arquitectura global.
  - Definición del modelo de gobernanza del nuevo servicio y encaje con el modelo global.
  - Definición de la gestión de cuentas y accesos.
  - Diseño de la solución de almacenamiento.
  - Diseño de los requerimientos de seguridad del nuevo servicio (especialmente de la solución de cifrado y protección de los datos), encaje con el modelo global de seguridad e integración con las herramientas corporativas SIEM y/o SOAR del Consorci AOC.
  - Diseño de la solución para el plan de continuidad de negocio y/o del plan contingencia.
  - Diseño de la solución de monitorización.
  - Definición de los requerimientos de auditoría.
  - Definición de la nomenclatura de objetos.

  Calendario: 20 meses desde la formalización del contrato.

Diseñar, implementar y ejecutar el plan de migración de datos de cada nuevo servicio o carga de trabajo que haga falta migrar al cloud público. El CCoE tendrá que diseñar el plan de migración de datos detallando la estrategia de migración más adecuada, los recursos necesarios, los posibles riesgos y la planificación. El plan de migración tendrá que incluir la preparación de los datos (los datos tendrán que ser limpiados y normalizadas para asegurar la calidad de los datos, se tendrán que convertir y formatear los datos, se tendrán que eliminar duplicidades y/o datos incoherentes, etc.), el rediseño de las estructuras de datos para adaptarlas al nuevo sistema en el cloud, las reglas de transformación de datos, las herramientas de migración a utilizar teniendo en cuenta las volumetrías de datos y la infraestructura de red y/o los dispositivos de almacenamiento físico disponibles, la monitorización del proceso de migración para identificar y resolver cualquier problema que se pueda producir (interrupciones de red, errores de transferencia de datos, problemas de rendimiento, etc.), las pruebas postmigración que se tendrán que ejecutar para asegurar que los datos se han migrado correctamente y verificar la integridad de los datos, etc.

Una vez el Consorci AOC apruebe el plan de migración de datos, el CCoE tendrá que ejecutar y auditar el proceso de migración, y las pruebas postmigración.

Calendario: 20 meses desde la formalización del contrato.

- **Fijar y automatizar las políticas de control y supervisión**: selección, configuración y puesta en marcha de las herramientas necesarias que permiten 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 respetan los modelos de gobernanza, que se minimizan 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 mandos y los informes de control que periódicamente se tendrán que presentar al Consorci AOC.

  Calendario: 6 meses desde la formalización del contrato.

- **Diseñar e implementar el sistema de observabilidad/monitorización**: Colaborar con el Consorci AOC en el diseño e implementación del sistema corporativo de observabilidad y monitorización. Este sistema de observabilidad tiene que poder garantizar, la detección, recepción y tratamiento de los acontecimientos informativos que se configuren con el fin de garantizar la observabilidad global de la infraestructura y servicios asociados. El sistema de observabilidad tendrá que

disponer de la capacidad de recepción de sucesos ante 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 de lo mismo.

La plataforma de monitorización podrá ser centralizada o distribuida, pero en cualquiera de los casos tendrá que proporcionar una visión global del estado del funcionamiento de las plataformas y en particular de todos sus elementos, en cuanto a la capacidad existente, rendimiento, el consumo de servicios de cloud público y privado, detección de malfuncionamientos o errores y proyección de impacto en las diferentes capas de servicio.

El Consorci AOC proporcionará al proveedor las instancias y licencias requeridas por el sistema de observabilidad.

Calendario: 8 meses desde la formalización del contrato.

Establecer el modelo de cálculo de costes idóneo para cada nuevo servicio y plataforma desplegado en el cloud público en modalidad de pago por uso. Establecer e implementar al modelo más idóneo para estimar los costes económicos de cada nuevo servicio a migrar al cloud público. Este modelo tiene que incluir todas las vertientes: infraestructura, servicios, operación, mantenimiento, monitorización, seguridad, etc. con el objetivo de poder determinar los costes de los diferentes servicios y plataformas que haya que desplegar 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 la migración al cloud del servicio en cuestión y también a medida que vaya aumentando el grado de madurez cloud del Consorci AOC.

El CCoE tendrá que proponer las herramientas de gestión, informes, etc. que permitan hacer el seguimiento exhaustivo del avance del gasto de cloud público y mantener el control en todo momento del grado de ejecución del presupuesto global de infraestructura de cloud público del Consorci AOC. Este seguimiento exhaustivo tendrá que hacerse a 2 niveles: tanto a nivel global respecto del presupuesto total asignado en la partida de infraestructura de cloud público, como también a nivel detallado de cada uno de los servicios que el Consorci AOC despliegue en el cloud público para los diferentes entornos de ejecución (integración, preproducción y producción). El CCoE tendrá que facilitar periódicamente (p. ej. una vez al mes) al equipo del Consorci AOC estos informes.

Calendario: 3 meses desde la formalización del contrato.

Finalmente, el CCoE tendrá que definir e implementar las alertas automáticas, basadas en los presupuestos asignados a cada servicio, que permitan detectar de

forma inmediata cualquier tipo de desviación respecto de la estimación inicial.

- **Para cada nuevo servicio que se tenga que migrar al cloud público, 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 tienen que permitir la automatización de los procesos y el aprovisionamiento de las plataformas necesarias para la integración continúa (CI) y el despliegue continuo (CD) a lo largo del ciclo de vida completo de los servicios del Consorci AOC que se migren en el cloud público. Este nuevo marco de referencia DevOps propuesto tendrá que estar adaptado a las necesidades del contexto del nuevo modelo TIC y tendrá que estar preparado para funcionar en un entorno de cloud público.

  Calendario: 20 meses desde la formalización del contrato.

  Mantenimiento y actualización de la documentación relativa a la ejecución del nuevo modelo TIC. El CCoE tendrá que mantener un espacio web donde se recoja y se organice de forma exhaustiva toda la documentación relativa a este lote 1: 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. Toda esta documentación es una documentación “viva” que se tiene que mantener a lo largo de la duración de la ejecución del contrato dentro del alcance de este lote, aunque se deja la opción al licitador de ampliar este catálogo:

  - Análisis de situación actual.
  - Plano estratégico cloud.
  - Requerimientos cloud y servicios comunes.
  - Propuesta de arquitectura de CPDs y aplicaciones.
  - Marc 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.
  - 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 darán apoyo a estos aspectos documentales.

Calendario: 20 meses desde la formalización del contrato.

Dentro del alcance del lote 1 se tendrán que incluir también 100 horas de dedicación del servicio AWS Profesional Services, también conocido como AWS ProServe, para complementar el CCoE con las habilidades y experiencia especializada del equipo global de expertos de AWS en aquellos ámbitos y tareas que el Consorci AOC determine. AWS ProServe tendrá que proporcionar asesoramiento especializado según el marco de referencia Well Architect Framework y a las mejores prácticas y recomendaciones de AWS. Es importante destacar que estas 100 horas se tendrán que poder consumir de forma intermitente a lo largo de la duración del contrato de acuerdo con las necesidades del Consorci AOC.

3.3 Equipo de trabajo Lote 1

Para garantizar la máxima eficiencia, control y coordinación del servicio objeto de este lote, la empresa adjudicataria tendrá que disponer en el momento iniciar el contrato de un equipo con las características que se detallan al PCAP de esta licitación. El Consorci AOC considera necesaria de los siguientes perfiles y roles:

- **Responsable CCoE / Experto cloud**. Las principales funciones de este perfil serán:
    - Seguimiento detallado del plan derivado del contrato e interlocución directa con el Consorci AOC en caso de incidencias críticas a lo largo de la ejecución del servicio.
    - Dirección del servicio y coordinación de los recursos asignados al servicio, tanto materiales como personales.
    - Establecer las planificaciones de las diferentes tareas encomendadas al CCoE, velando por que cada una de estas tareas se realizan de forma diligente y dentro de la planificación acordada. Informar al Consorci AOC de las desviaciones tan pronto como se detecten.
    - Generar la documentación asociada al servicio y realizar los informes de seguimiento.
    - Supervisión del trabajo del resto de personas del equipo con el objetivo de maximizar la calidad de los entregables.
    - Definir e implementar la estrategia de migración de los diferentes servicios a migrar al cloud, especificando la configuración y el despliegue de acuerdo con las necesidades del negocio.
    - Diseñar, crear y optimizar la arquitectura cloud de los servicios a migrar al cloud público.

- Proporcionar formación y soporte, tanto al resto de miembros del CCoE como del equipo técnico del Consorci AOC, en las tareas de transformación de los servicios de negocio y la adaptación de estos servicios al ámbito del cloud.
- Determinar e implementar el plan de continuidad de negocio y la estrategia de recuperación de desastres de los servicios a migrar al cloud.

- **Cloud Engineers**. Las principales tareas que tendrán que asumir estos perfiles serán:
  - Mantenerse al día de las últimas actualizaciones y características de los proveedores de cloud público.
  - Diseñar los nuevos sistemas en el cloud creando y adaptando la nueva arquitectura de los servicios a migrar.
  - Trabajar juntamente con los diferentes equipos de desarrollo del Consorci AOC para facilitar la adaptación y el despliegue al cloud de los nuevos servicios a migrar.
  - Configurar e implementar las nuevas infraestructuras, recursos y servicios cloud que requieran los nuevos servicios a migrar.
  - Definir e implementar el plan de migración de los datos de los servicios a migrar al cloud.
  - Analizar y optimizar los costes asociados con el uso de los servicios cloud.
  - Identificar las tareas y procesos que se puedan automatizar y proponer la mejor manera de hacerlo.
  - Definir los mecanismos necesarios para mantener todos los sistemas cloud actualizados y operativos de la forma más eficiente.
  - Auditar los sistemas cloud en explotación para confirmar que se ciñen al diseño y definición iniciales del CCoE.
  - Identificar y resolver los problemas técnicos relacionados con el cloud.

- **Cloud Security Engineer**. Las principales responsabilidades de este perfil serán:
    - Mantenerse al día de las últimas amenazas de seguridad y también de las últimas actualizaciones y novedades que presentan los proveedores de cloud público en el ámbito de la seguridad.
    - Definir, implementar y mantener las políticas, procedimientos y controles de seguridad (reglas de firewalls, sistemas de detección de intrusiones, políticas de cifrado, gestión de identidades y permisos, etc.) tanto globales como de los diferentes servicios a migrar al cloud que tienen que garantizar la integridad de los datos y la seguridad de las aplicaciones.
    - Diseñar y mantener infraestructuras cloud seguras con el objetivo de garantizar la seguridad e integridad de los datos y de los servicios a migrar.
    - Diseñar, ejecutar y auditar de forma periódica el plan de backup de cada nuevo servicio a migrar.
    - Asegurar que los servicios a migrar al cloud cumplen con la normativa y regulación vigentes (especialmente ENS nivel alto y GDPR).
    - Realizar de forma regular auditorías de seguridad y evaluaciones de riesgos para identificar amenazas a la seguridad y corregir vulnerabilidades.
    - Colaborar con el Consorci AOC en la respuesta a incidentes de seguridad, investigando las causas y proponiendo soluciones.
    - Proporcionar formación y concienciación sobre seguridad tanto al resto de miembros del CCoE, como del personal del Consorci AOC.

El Consorci AOC se reserva el derecho a pedir el cambio de cualquiera de los miembros del equipo mínimo con una antelación de 20 días naturales a la fecha de sustitución.

Además de estos perfiles, se considera necesaria la figura de un responsable del contrato a quien concentrará y recibirá las comunicaciones a alto nivel del Consorci AOC sobre la dirección, estrategia y evolución del servicio. Este responsable del contrato será por lo tanto el interlocutor y el punto de contacto a quienes el Consorci AOC transmitirá la visión de negocio y los requerimientos transversales que son objeto del contrato. El responsable del contrato también será el encargado de gestionar los recursos tanto materiales como personales asignados al contrato.

En caso de baja de cualquiera de los miembros del equipo a instancias del adjudicatario, el adjudicatario tendrá que sustituirlo en menos de 15 días laborales y tendrá que asumir un tiempo de 2 semanas de formación y adaptación del nuevo miembro que tendrán que ir a cargo del adjudicatario. El Consorci AOC tendrá que

validar el cambio y podrá acordar el calendario con el fin de minimizar el impacto en el servicio.

4. Objetivos, hitos y calendario Lote 2: Construcción de servicios comunes y evolución de los servicios actuales del AOC hacia tecnologías basadas en nube pública

4.1 Objeto

El objeto de esta contratación es la prestación de servicios para abordar nuevos desarrollos de servicios y mantenimiento evolutivo, soporte a las aplicaciones y control de calidad sobre algunos de los sistemas de información basados en tecnología Java del Consorcio Administración Abierta de Cataluña.

4.2 Objetivos

Los objetivos del proyecto son diversos:

- Realización de tareas de desarrollo en tecnología Java de una serie de funcionalidades adicionales a los servicios existentes del Consorci AOC, así como la creación de nuevos servicios y la renovación cumplida de servicios existentes para desplegarlos en la nube (AWS).
- Ofrecer soporte técnico especializado con respecto a la detección, diagnóstico y resolución de las incidencias técnicas derivadas del uso de los productos del Consorci AOC.

4.3 Descripción del servicio

Por la diferente naturaleza de los servicios a prestar, el lote contempla dos vertientes diferenciadas:

- Prestación de servicios tecnológicos recurrentes de mantenimiento evolutivo y adaptativo, soporte a las aplicaciones y control de calidad de algunos de los sistemas de información basados en tecnología Java del Consorci AOC.
- Construcción y desarrollo de nuevos servicios de administración electrónica en la nube (Representa, entre otros, así como los nuevos componentes de arquitectura y servicios comunes que tienen que conformar la nueva Plataforma de Colaboración Interadministrativa).

Este lote consta de una serie de proyectos de mantenimiento a desarrollar en paralelo sobre diferentes servicios del Consorci AOC, basados en tecnología Java y valorados globalmente en un total de 54.656 horas que habrá que realizar en su totalidad en el periodo de duración del contrato.

La empresa adjudicataria, en función de la duración del contrato, y del volumen de horas previsto para realizar los proyectos, tendrá que dimensionar adecuadamente el equipo de trabajo para dar respuesta a los requerimientos valorados, en tiempo y forma. Es decir, la disponibilidad de las horas ejecutadas puede, puntualmente, no ser proporcional a la duración del contrato, sino que se tendrá que adaptar a las

necesidades y requerimientos del servicio, pudiendo fluctuar en función de la carga de las tareas encomendadas, habiendo meses en que se pueda requerir un mayor o menor dimensionado del equipo de trabajo.

Las tareas que se contemplan en este lote son muy relativas al ciclo de vida cumplido de las aplicaciones, sistemas de información y soluciones, que van desde los estudios, preliminares y la gestión, hasta la implantación y el soporte posterior, y que pueden variar en función de las tipologías de aplicaciones, herramientas y entornos tecnológicos, así como de los requerimientos específicos de cada proyecto y/o servicio:

- Gestión (gestión del proyecto y/o servicio, gestión y de la calidad y la seguridad).
- Análisis de viabilidad, definición tecnológica, conceptualización y análisis funcional.
- Construcción y pruebas (análisis y diseño, prototipaje, desarrollo, parametrización y/o configuración, documentación, pruebas unitarias, técnicas y de integración).
- Implantación y gestión del cambio (migración de datos y pruebas de aceptación).
- Mantenimiento evolutivo y adaptativo (que puede incluir actividades de gestión, construcción, pruebas e implantación).
- Realización de pruebas de concepto.

4.4 Prestación de servicios tecnológicos de mantenimiento evolutivo, soporte a las aplicaciones y control de calidad

Con respecto al mantenimiento evolutivo y adaptativo, se contemplan las modificaciones en el software que sean necesarias para dotar a los servicios de nuevas funcionalidades, adaptaciones a cambios en las normativas vigentes o con el fin de evitar la obsolescencia tecnológica, así como implementar los ajustes necesarios para evolucionar los actuales servicios del AOC hacia tecnologías basadas en nube pública.

4.4.1 Evolutivos sobre la herramienta de firma centralizada

Mantenimiento de la herramienta de firma centralizada basada en Java WebStart y que adicionalmente dispone de una aplicación nativa que permite la ejecución de una herramienta de firma electrónica basada en certificados digitales de usuario final dentro de las aplicaciones que funcionan con un navegador web.

https://signador.aoc.cat/signador/init

4.4.2 Evolutivos sobre la aplicación VALId e idCAT Móvil

La Generalitat de Catalunya en Acuerdo de Gobierno encargó al Consorci AOC la creación de servicios alternativos al uso de los certificados electrónicos.

Para dar respuesta a este encargo, el Consorci AOC desarrolló en el 2015 un servicio denominado IdCAT Móvil y una herramienta que agrupa diferentes servicios de identificación denominada VALId.

Tanto los servicios VALId como el idCAT Móvil se encuentran ya operativos y dando servicio en entornos productivos, pero periódicamente hay que realizar una serie de mejoras enfocadas evolucionar el servicio, a mejorar el rendimiento y a la seguridad.

Concretamente hay que seguir con las tareas de mantenimiento del servicio actual, entre otros:

- Realizar evolutivos funcionales para incorporar nuevos mecanismos.
- Adicionalmente hay que realizar tareas de mantenimiento sobre el proceso de autorregistro online de los ciudadanos para el uso del idCAT Móvil (https://idcatmobil.cat).

https://www.aoc.cat/serveis-aoc/valid/

https://suport-altresserveis.aoc.cat/hc/ca/sections/4405993188765-V%C3%80Lid

4.4.3 Evolutivos sobre el IDP de EACAT 3.0

El IDP (Identity Provider) de los servicios del AOC orientados al trabajador público está basado en el estándar OAuth2 (protocolo alineado con el utilizado en el servicio VALId) y habrá que adaptar las aplicaciones que se basan en el IDP actual (principalmente el portal y aplicaciones EACAT) para que hagan uso de la nueva versión, así como aplicar un nuevo diseño.

4.4.4 Integraciones y adaptaciones diversas de servicios del CAOC derivadas de requerimientos de la Administración General del Estado

- Sistema de Interconexión de Registros con el Estado (SIR): La Administración General del Estado (AGE), con el objetivo de fomentar el concepto de Ventanilla Única dispone de un sistema que permite el traslado de la documentación que un ciudadano presenta a una Administración Pública hacia otra Administración Pública, de forma totalmente electrónica y con el correspondiente registro de entrada.

  Este 2024 también está previsto renovar el servicio con el fin de adaptarlo a la nube, a la arquitectura EACAT 3.0 y al estándar SICRES 4 aunque mientras la nueva versión no esté terminada será necesario seguir manteniendo el servicio actual.

Alcance: EACAT, PCI.

https://administracionelectronica.gob.es/ctt/sir

- Mantenimiento de los servicios de integración del CAOC con el Punto de Acceso General de Intercambio de Expedientes: realizar las integraciones que se requieran para mantener al día las funcionalidades de este hub de carpetas ciudadanas.

  Alcance: PCI.

  https://administracionelectronica.gob.es/ctt/ccd

- Adaptación de los servicios de interoperabilidad del CAOC con el fin de contemplar los procedimientos administrativos grabados al Sistema de Información Administrativa (SEA) del Estado. Se prevé que los servicios afectados sean los servicios proporcionados y consumidos por el MINHAP desde su Plataforma de Intermediación.

  Alcance: PCI.

4.4.5 Evolutivos del servicio e-Valisa

Actualmente el Consorci AOC ofrece a los usuarios de la Generalitat de Catalunya un servicio de Valija electrónica que permite ahorrar costes eliminando el gasto en mensajería que inherente al traslado de papel entre las diferentes dependencias de la Generalitat.

Con el fin de seguir potenciando el servicio y dar respuesta a nuevos requerimientos planteados se prevé que durante la duración del contrato haga falta realizar diferentes evolutivos, así como finalizar el desarrollo de la nueva versión adaptada a la nube y a la arquitectura EACAT 3.0.

Alcance: EACAT.

https://www.aoc.cat/serveis-aoc/e-valisa/

4.4.6 Evolutivos del servicio de Copia Auténtica

El servicio de Copia Auténtica tiene como objetivo la generación de copias auténticas que tengan la misma validez y eficacia que los documentos originales convirtiendo los documentos en papel en documentos electrónicos y que los documentos electrónicos sean también válidos en papel.

Así, se dispone de una aplicación web de generación de copias auténticas que se ha adoptado como solución corporativa y transversal por los diferentes servicios de administración electrónica que ofrece el Consorci AOC. Como tal, se invocada desde las diferentes aplicaciones del Consorci AOC (ERAS, e-NOTUM, EACAT, entre otros).

Asimismo, permite dar cumplimiento a los requisitos de la ley 39/2015 y, en concreto, al artículo 27 que regula la validez y eficacia de las copias realizadas por las administraciones públicas. También tiene en cuenta las especificaciones técnicas que se establecen en la NTI de digitalización de documentos y la NTI de procedimiento de copiado auténtico y conversión de documentos entre documentos electrónicos.

Con el fin de seguir potenciando el servicio y dar respuesta a nuevos requerimientos planteados se prevé que durante la duración del contrato haya que seguir realizando diferentes evolutivos sobre la herramienta.

https://www.aoc.cat/serveis-aoc/copia/

4.4.7 Evolutivos del servicio Vía Oberta

Bajo la denominación Vía Abierta, el Consorci AOC engloba los servicios que ha desarrollado para facilitar la transmisión telemática de datos y documentos electrónicos procedentes de las administraciones y, en general de las instituciones públicas y entidades, posibilitando la sustitución de la aportación de certificados y otros documentos en soporte papel, en los procedimientos administrativos por parte de los interesados.

De manera continuada, hay que ir incorporando al catálogo de consultas disponibles nuevos servicios de interoperabilidad a medida que los diferentes emisores de datos los publican (principalmente organismos de la Administración General del Estado, Departamentos de la Generalitat de Catalunya y Colegios Profesionales).

Asimismo, dentro de los proyectos Vía Abierta, se contempla dar apoyo a la unidad de Soporte Técnico del AOC que se encarga del mantenimiento correctivo de los webservices conectores del Padrón Municipal de Habitantes de los Ayuntamientos que han puesto en línea su padrón

(http://dadesobertes.seu-e.cat/csv/ens_amb_padro_en_linia.csv).

Alcance: PCI, EACAT.

https://www.aoc.cat/serveis-aoc/vía-abierta/

https://suport-viaoberta.aoc.cat/hc/ca/sections/4415410061201-Integraci%C3%B3

4.4.8 Evolutivos del servicio e-NOTUM / e-NOTUM Lite

Servicio que permite realizar notificaciones de actos administrativos (resoluciones, decretos, notificaciones para contratación, notificaciones de sanciones de tráfico, convocatorias de órganos colegiados, etc.) y comunicaciones por medios electrónicos, con todas las garantías jurídicas que establece la normativa vigente.

Con el fin de seguir potenciando el servicio incorporando nuevas funcionalidades y dar respuesta a los requerimientos de disponibilidad que se requieren en un servicio de estas características se prevé que durante la duración del contrato haya que seguir realizando diferentes evolutivos sobre la herramienta.

Alcance: PCI, EACAT, frontal ciudadano.

https://www.aoc.cat/serveis-aoc/e-notum/

https://github.com/ConsorciAOC/eNotum

https://github.com/ConsorciAOC/eNotumLite

4.4.9 Evolutivos del servicio e-TAULER

Servicio del Consorci AOC que permite la publicación y la gestión de edictos

electrónicos online. Es una herramienta de publicación certificada con automatismos asociados a la gestión de la publicación de los edictos (control de periodos de exposición, generación de diligencias, etc.). El e-TAULER permite gestionar las evidencias electrónicas del proceso de publicación con el fin de garantizar los tiempos de exposición y la integridad de la información. No sólo es una herramienta de envío y recepción electrónica de edictos internos, también permite gestionar externos, provenientes de otras administraciones a través EACAT. El e-TAULER se integra en la sede electrónica de las entidades en modalidad marca blanca. Aunque este 2024 está previsto arrancar la renovación del servicio con el fin de adaptarlo en la nube, mientras no esté terminada la nueva versión será necesario seguir manteniendo y evolucionando el servicio actual.

Alcance: PCI, EACAT, frontal ciudadano.

https://www.aoc.cat/serveis-aoc/e-tauler/

https://github.com/ConsorciAOC/e-TAULER

4.4.10 Evolutivos en el backoffice del servicio E-TRAM

E-TRAMO es el módulo de gestión municipal de solicitudes y trámites por Internet del Consorci AOC.

Aunque el portal del ciudadano de este proyecto queda fuera del alcance de este contrato, el backoffice de E-TRAMO se apoya sobre la PCI. Así, se prevé que, durante la duración del contrato, haya que realizar algún tipo de mantenimiento evolutivo y correctivo sobre estos servicios de backoffice del servicio.

Alcance: PCI.

https://www.aoc.cat/serveis-aoc/e-tram/

4.4.11 Evolutivos del servicio Representa

Servicio del Consorci AOC que permite la gestión de representaciones y apoderamientos online. Aunque este 2024 está previsto arrancar la renovación del servicio con el fin de adaptarlo en la nube, mientras no esté terminada la nueva versión será necesario seguir manteniendo y evolucionando el servicio actual.

Alcance: PCI, EACAT, frontal ciudadano.

https://www.aoc.cat/serveis-aoc/representa/

https://suport-representa-ciutadania.aoc.cat/hc/ca

https://suport-representa.aoc.cat/hc/ca

https://github.com/ConsorciAOC/representa_documentacio

4.4.12 Hub de Carpetas Ciudadanas

El Hub de Carpetas Ciudadanas del AOC es el servicio tecnológico y la infraestructura que facilita que mi Espacio (fuera del alcance de este contrato) ofrezca una visión interadministrativa a la ciudadanía desde un solo lugar, con una gestión fácil y rápida.

Esencialmente, hace de elemento de intermediación recopilando y cohesionando información de servicios propios del AOC, información de otras entidades públicas y de terceros. Por ejemplo, trámites, notificaciones, comunicaciones, expedientes, consultas que hacen las administraciones a tus datos, datos abiertos, etcétera.

Operativamente, se basa en consultas bajo un modelo de datos estandarizado que permite la intermediación de la información. Concretamente, define una APIO que los entes integrados implementan para ser consultados y permite disponer esta información agrupada.

Alcance: PCI.

https://github.com/ConsorciAOC/hubcarpetes_documentacio

4.4.13 Motor de Transacciones de Interoperabilidad (MTI / componente de arquitectura)

Migración del MTI en la nube. El MTI se encarga de la orquestación y trazabilidad de la ejecución de las peticiones (individuales vs lotes y síncronas vs asíncronas) de los diferentes servicios y controla la intermediación entre requirentes y los emisores finales de los datos de cada uno de los servicios de interoperabilidad y aplicaciones del AOC. Para más detalles de este componente y su encaje en la arquitectura PCI ved el anexo *PCI 3.0 - Arquitectura PCI (resumen)* de este documento.

Alcance: PCI.

https://github.com/ConsorciAOC/PCI

4.4.14 Evolutivos de otros servicios del CAOC

Algunos de los servicios sobre los cuales se prevé que habrá que realizar tareas de mantenimiento son los siguientes:

- **PSCP (Plataforma de contratación)**: El Consorci AOC ofrece una APIO pasarela ninguno los servicios de la PSCP 2.0 del Departamento de Economía y Hacienda de reciente creación. Dado que el Departamento incorpora periódicamente nuevas funcionalidades al servicio, se prevé que durante la duración del contrato haya que realizar diferentes evolutivos sobre la pasarela.

  Alcance: PCI.

  https://www.aoc.cat/serveis-aoc/e-contractacio-perfil-de-contractant/

  https://suport-pscp.aoc.cat/hc/ca

  https://github.com/ConsorciAOC/PSCP/wiki/Document-d'integraci%C3%B3

- **Registro unificado / MUX**: El servicio de Registro Unificado (MUX) permite la integración de los servicios del Consorci AOC con el registro general de entradas y

salidas propio del ente. Con esta integración, las anotaciones de registro de entrada o salida que generan los servicios AOC se realizan directamente en el registro general del ente, en lugar de realizarse en el registro electrónico auxiliar de EACAT como se había hecho hasta ahora.

Alcance: PCI, EACAT.

https://www.aoc.cat/serveis-aoc/registro-unificado-mux/

https://suport-registreuniificat.aoc.cat/hc/ca

4.5 Construcción de servicios comunes y evolución de los actuales servicios del AOC hacia la nube

En paralelo a las tareas de mantenimiento evolutivo de las aplicaciones recogidas en el apartado anterior hará falta abordar construcción de nuevos servicios comunes y renovar completamente algunos de los servicios del AOC con el fin de facilitar la transición hacia la nube.

Hay que tener en cuenta que la definición final de cada nuevo desarrollo, así como la arquitectura será definida conjuntamente entre el adjudicatario y el Consorci AOC.

Por otra parte, será el Consorci AOC quien proporcionará la infraestructura y recursos necesarios para abordar los desarrollos a AWS.

Así, se prevé que, durante la duración del contrato, haya que llevar a cabo las iniciativas que se enumeran a continuación.

4.5.1 Evolución del servicio Representa hacia la nube

Representa es el servicio de Registro Electrónico de Apoderamientos que el AOC pone a disposición de los ciudadanos y de las administraciones públicas catalanas.

El servicio permite a los entes inscribir representaciones y a la ciudadanía gestionarlas en un entorno tanto presencial como on-line.

Por otra parte, el servicio está integrado con Copia y el Registro del Consejo General del Notariado (mediante Vía Abierta) y permite a la vez la integración con otros servicios de tramitación administrativa (cómo puede ser Canal Empresa de la Generalitat o, próximamente, Apodera).

Representa consta, por lo tanto, de tres entornos:

- Portal del empleado (vía el portal EACAT) para la gestión del registro de representaciones que hace el empleado público.
- Portal del ciudadano para la gestión de representaciones que hace directamente la ciudadanía.
- Integración: exposición de modalidades de consulta, inscripción y validación de representaciones a través de la PCI del AOC.

Portal del empleado

En EACAT los nos disponen de un portal donde pueden inscribir representaciones, consultar las inscritas, validar/denegar la documentación adjunta de las representaciones, realizar toda la operativa permitida desde el portal de ciudadano con el fin de aceptarla o renunciarla, y, por último, gestionar todo un catálogo de trámites que se pueden asociar a estas representaciones.

Portal del ciudadano

Una vez el ciudadano se identifica mediante VALId este puede entrar en el portal público donde puede solicitar la inscripción de un apoderamiento o de una representación (es decir, donde podrá pedir ser representante de alguien o que alguien sea su representante). Este portal, a la vez, le permitirá gestionar sus representaciones, pudiendo aceptar las que estén pendientes o, simplemente, consultar el estado de las que tiene.

El aplicativo, al igual que en el caso del portal del empleado, le permite consultar el histórico de acciones, así como descargar toda la documentación anexada durante el proceso.

Integración (PCI)

Una parte importante del Representa afecta a las integraciones y servicios expuestos con el fin de hacer altas, consultas, cambios de estado, inscripciones o validaciones. Existen varias modalidades que exponemos y que entidades como Canal Empresa, GABJUR, o varios Ayuntamientos utilizan con el fin de consolidar sus representaciones, y que se pueden consultar después con en nuestros portales.

Toda esta parte se realiza utilizando los servicios de la Plataforma de Tramitación Interadministrativa de AOC (PCI).

Tecnologías

El servicio Representa está formado básicamente por dos componentes: el Core y los Portales.

La parte correspondiente al Core, hecha con Java (jdk 1.8) y Spring, permite operar sobre las representaciones mediante llamamientos WebService SOAP. Se comunica internamente con los portales (se expone un WSDL) y las integraciones de terceros expone un subconjunto de funcionalidades disponibles a través de la PCI (Weblogic 12).

Tenemos una base de datos (Oráculo 12) con toda la información de las representaciones, usuarios, notificaciones y catálogo de trámites, y una parte de gestión en disco, donde se guarda la documentación anexada y las evidencias y firmas de las representaciones.

El core también está integrado con servicios del AOC como el servicio de Notarios de Vía Abierta, o el de firma centralizada (vía MSC). Y se ocupa del envío de notificaciones vía correo electrónico (y próximamente, también SMS), con plantillas

hechas con Mustache.

Respecto de los Portales, tenemos un frontend donde se utiliza Angular 8 y Bootstrap, y que se integra con un backend Java (también con Spring) al que se accede mediante peticiones RISTRE seguras.

Hoja de ruta y alcance del proyecto

La intención es, aparte de diferentes integraciones y evolutivos planificados, actualizar el Representa con un nuevo diseño de los portales, y aprovechar este cambio para migrar el servicio hacia la nube (AWS).

4.5.2 Servicio común de integración de sellos electrónicos

El Consorci AOC, como prestadorc de servicios de confianza con acuerdo en lo que establece el Reglamento (UE) 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza, en adelante ReIDAS, presta entre otros los servicios de emisión y custodia de certificados calificados de sello electrónico que las administraciones públicas catalanas utilizan en el ámbito de la actuación administrativa automatizada.

Tal como les define el artículo 3 de ReIDAS, un sello electrónico son los datos electrónicos anexados a otros datos, o vinculados de manera lógica con ellas, con el fin de garantizar su integridad y origen, sin necesidad que este sea una persona física. En el ámbito de las administraciones públicas, con acuerdo en lo que establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público en su artículo 42, se establece como mecanismo para la actuación administrativa automatizada el sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público basado en un certificado cualificado.

Con el objetivo de facilitar su gestión y uso, el Consorci AOC ofrece a las Administraciones Públicas Catalanas un servicio de custodia y uso de este tipo de certificados. El servicio actualmente se presta utilizando una solución de mercado, como aplicación de firma remota gestionada por el propio Consorcio, a la que las aplicaciones de las administraciones públicas catalanas se integran para hacer uso de sus sellos electrónicos. Teniéndolo en cuenta, y siendo conscientes de la limitación en la duración de los contratos en el sector público, se requiere del desarrollo de un módulo de integración que permita independizar a las aplicaciones usuarias del proveedor que esté ofreciendo el servicio en cada momento.

A grandes rasgos, las funcionalidades que tendrá que cubrir este módulo de integración serán:

- Gestionar altas, bajas y permisos de las aplicaciones usuarias, que se tendrán que identificar con Certificados de Dispositivo Aplicación, (CDA).
- Las aplicaciones usuarias, si disponen del permiso para hacerlo, tendrán que poder seleccionar un certificado de sello electrónico cedido para producir firmas con los certificados custodiados en los siguientes formatos: Firma PAdES de documentos pdf, firmas XAdES-BES en formato enveloped y enveloping, firmas XAdES-T en formato enveloped y enveloping con sello de tiempo emitido por el

Consorci AOC y firma CMS

4.5.3 Servicio común de gestión de terceros

Servicio común para gestionar de manera centralizada los datos de los entes contraparte con los que los servicios del AOC interactúan.

Se prevé que los datos de estos nos procedan de:

- Registros públicos:
  - Municat: https://analisi.transparenciacatalunya.cat/Sector-P-blic/Dades-generals-dels-ens-locals-de-Catalunya/6nei-4b44
  - Registro ente sector público de la Generalitat: https://analisi.transparenciacatalunya.cat/Sector-P-blic/Registre-del-sector-p-blic-de-la-Generalitat-de-Ca/gr39-ik6u
  - Organismos dependientes de los entes: https://analisi.transparenciacatalunya.cat/Sector-P-blic/Organismes-dependents-o-adscrits/hjnn-7hfb
- Alta manual si no existe ningún registro. La información de cada ente, y aparte de los datos cargados automáticamente a partir de las fuentes principales, se tiene que poder completar con:
  - Dirección a efectos de registro
  - Tipo de registro de entrada y salida (S@rcat, etc.)
  - Código INE10 registro de entrada y salida
  - Unidad mayor/Unidad menor (sólo ente S@rcat)
  - DIR3 asociado
  - Tipología de ente macro en función de categorías de Municat / registro ente sector público
  - Logos asociados que los servicios del AOC aplicarán en la personalización del ente
  - Colores asociados que los servicios del AOC aplicarán en la personalización del ente
- Para cada ente también habrá que contemplar:
  - Gestión y asociación de organismos dependientes:
  - https://analisi.transparenciacatalunya.cat/Sector-P-blic/Organismes-dependents-o-adscrits/hjnn-7hfb

- A qué Departamento pertenece (ámbito Generalitat de Catalunya): https://analisi.transparenciacatalunya.cat/Sector-P-blic/Registre-del-sector-p-blic-de-la-Generalitat-de-Ca/gr39-ik6u
- Las Oficinas de registro DIR3 que tiene asociadas.
- Cuando uno nos aparezca en un registro público en un estado no activo hay que indicarlo de alguna manera con el fin de hacer actuaciones a posteriori para gestionar las bajas de los servicios.
- Gestión de duplicados.
- Toda esta información y su gestión tiene que ser accesible vía API.

4.6 Perfil profesional del equipo de trabajo

4.6.1 Experiencia profesional

- Responsables de OT (3) e Ingenieros de Software (8): Las personas con estos perfiles tendrán que satisfacer los siguientes requisitos.
    - Titulación: Formación Profesional, Ingeniería Técnica en Informática o titulación superior.
    - Experiencia mínima: 4-5 años (demostrables) en funciones de desarrollo, testeo, mantenimiento correctivo y evolutivo de aplicaciones Java.
    - Requisitos:
        - Conocimiento y experiencia Java EE, Spring, React, Angular, Hibernate.
        - Experiencia en integración de servicios (Webservices, SOAP, WSDL, RISTRE, etc.).
        - Conocimiento de metodologías ágiles para la planificación, desarrollo y mantenimiento de sistemas de información.
        - Experiencia en las tecnologías indicadas en el anexo PCI 3.0 - Arquitectura PCI (resumen) (Weblogic 12c, Tomcat 8 o superior y programación Java EE, webservices, base de datos Oracle 12) y conocimientos en herramientas para la gestión y construcción de proyectos (ECHAZÓN para el control de versiones, Gradle, Jenkins o similares).
        - Experiencia profesional como miembro de un equipo responsable de servicios de mantenimiento evolutivo, correctivo y soporte de aplicaciones, y en especial de aplicaciones en entornos productivos y críticas.
        - Para los responsables de OT: experiencia demostrable en gestión de equipos.

- Desarrolladores Java: Las personas con este perfil (5) tendrán que satisfacer los siguientes requisitos.
    - Titulación: Formación Profesional, Ingeniería Técnica en Informática o titulación superior.
    - Experiencia mínima: 2-3 años (demostrables) en funciones de desarrollo, testeo, mantenimiento correctivo y evolutivo de aplicaciones Java.
    - Requisitos:
        - Conocimiento y experiencia Java EE, Spring, React, Angular, Hibernate.
        - Experiencia en integración de servicios (Webservices, SOAP, WSDL, RISTRE, etc.).
        - Conocimiento de metodologías ágiles para la planificación, desarrollo y mantenimiento de sistemas de información.
        - Experiencia en las tecnologías indicadas en el anexo PCI 3.0 - Arquitectura PCI (resumen) (Weblogic 12c, Tomcat 8 o superior y programación Java EE, webservices, base de datos Oracle 12) y conocimientos en herramientas para la gestión y construcción de proyectos (ECHAZÓN para el control de versiones, Gradle, Jenkins o similares).

4.6.2 Funciones

- Desarrollo tanto en el lado cliente (EACAT, frontales del ciudadano) como el servidor (servicios de backoffice, módulos comunes y componentes de interoperabilidad).
- Realizar y ejecutar los planes de pruebas.
- Adicionalmente, los perfiles de Responsables de OT tendrán que actuar de interlocutor entre el equipo de trabajo y los responsables técnicos de cada servicio dentro del alcance de este pliego. Asimismo, tendrá que dirigir, coordinar, supervisar y representar a lo equipo técnico de trabajo y velar por el nivel de calidad de los trabajos.

4.7 Metodología

Las tareas que realizar contempladas en esta partida se engloban dentro del mantenimiento evolutivo y correctivo de gran parte de las aplicaciones que forman parte del catálogo de servicios del Consorci AOC durante la fase continúa de su ciclo de vida.

Así pues, los servicios existentes objeto de este contrato tienen un alto grado de madurez y se meten dentro del conjunto de servicios que el Consorci AOC ofrece.

Asimismo, hace falta tener en cuenta que los servicios de los que son objeto este contrato presentan una cierta complejidad en su gestión por los siguientes motivos:

- La dirección estratégica de cada uno de los servicios está liderada por un jefe de Servicio -que el rol de promotor- con unos objetivos y unos plazos, pero que ocasionalmente puede presentar una interdependencia con otros servicios.
- Alta dependencia con terceros (p.ej. organismos externos en el AOC que pueden impactar tanto en el alcance funcional como con los plazos de ejecución previstos inicialmente).
- Alto solapamiento y concurrencia de tareas de diferentes servicios.

Aunque gran parte de los servicios están en producción desde hace años, podemos considerar cada una de las versiones a desarrollar como un proyecto propio que se tendrá que desarrollar siguiendo el cumplimiento de esta guía metodológica.

A continuación, se detallan las fases por las que tiene que pasar cada una de estas versiones de un determinado servicio desde su definición hasta su puesta en marcha.

4.7.1 Introducción de las tareas a JIRA

La Cabeza de Servicio traduce los objetivos estratégicos que marca el comité estratégico en las peticiones de mejora y evolutivos que tienen que permitir alcanzar estos objetivos. A continuación, los introduce como *tarea de Servicios* en la herramienta JIRA. En el momento de entrar cada tarea (en forma de ticket) indica su prioridad.

4.7.2 Fase de definición

La fase de definición de la versión consiste al seleccionar cuáles son los requerimientos funcionales que tienen que entrar a formar parte de la próxima versión a desarrollar.

El jefe de Proyecto (Área de Tecnología) estudia todos aquellos requerimientos que se pueden incluir dentro de una ventana tipo que el Consorci aplica a sus servicios (para servicios grandes, versiones cada 3 meses aproximadamente entre la puesta en marcha de cada versión, aunque en servicios más pequeños esta ventana se reduce).

El jefe de Proyecto consensua con la jefe de Servicio el alcance de la versión y se confecciona la lista definitiva de tareas trasladando esta lista de peticiones en tareas de Proyectos JIRA que representa la versión a desarrollar.

En caso de que ocurra, es la de Servicio quien define el plan de comunicación que se tendrá que llevar a cabo antes de que la versión llegue a los usuarios finales y dentro de este plan seleccionará los usuarios y organismos que tendrán que participar en la prueba piloto, si se estima oportuno.

El jefe de Proyecto introduce toda esta información en los tickets JIRA que conforman la versión. Una vez cerrada el alcance de la versión, no se aceptará ninguna modificación en la lista de funcionalidades a desarrollar hasta la próxima fase de definición de la nueva versión.

4.7.3 Análisis

El adjudicatario partirá de la recopilación de funcionalidades a satisfacer que se han seleccionado en el JIRA para la nueva versión y tendrá que realizar las reuniones de toma de requerimientos para poder hacer la recaudación detallada de todos los requisitos tanto funcionales como tecnológicos pedidos. Será responsabilidad del adjudicatario velar y preocuparse de recaudar todos y cada uno de los requerimientos que afecten al alcance de una determinada versión.

El adjudicatario elaborará un análisis previo de la solución que propone incluyendo una estimación del impacto que supone el evolutivo. En caso de que haya diferentes alternativas, el adjudicatario las tendrá que explicar indicando las ventajas e inconvenientes de cada una.

4.7.4 Planificación

El jefe de Proyecto añadirá al JIRA las tareas técnicas que considera necesarias para poder desarrollar la versión (documentación técnica, plan de pruebas, etc.) y prepara juntamente con el adjudicatario la planificación detallada de la versión asignando las tareas entre los diferentes técnicos de desarrollo.

4.7.5 Desarrollo de tareas planificadas

Las tareas que comportará esta fase son:

- Generación del código.
- Ejecución de pruebas unitarias.
- Ejecución de pruebas de integración.
- Ejecución de pruebas de rendimiento, si procede.
- Elaboración de la documentación funcional y técnica.

El adjudicatario tendrá que hacer un uso frecuente de la herramienta de control de versiones de código (GitHub) del servicio para sincronizar los diferentes desarrollos. La frecuencia ideal de sincronización (tanto para subir al repositorio los cambios realizados como para descargar todos los cambios que han introducido el resto de los desarrolladores) sería hacerlo una vez al día (p. ej. a primera hora de la mañana) de forma que se detecte cuanto antes mejor los conflictos entre los diferentes desarrollos.

Antes de subir nada al repositorio cada desarrollador tendrá que garantizar en la medida de lo posible que el código subido es íntegro. Si no es posible subir los cambios de forma diaria, sí que se tiene que garantizar que cada equipo de desarrollo subirá los cambios como mínimo con una frecuencia semanal.

Los diferentes técnicos tienen un control total sobre el entorno de desarrollo y pueden desplegar tantas veces como lo necesiten.

4.7.6 Implantación y aceptación

En base a las entregas de la fase anterior se procederá a realizar la implantación del evolutivo sobre los diferentes entornos. En primer término, en el entorno de desarrollo. El adjudicatario procederá a realizar la ejecución del plan de pruebas. En caso de que se supere satisfactoriamente procederá a promocionar el cambio en torno a preproducción y posteriormente en el de producción.

Caso que en este proceso los resultados obtenidos no sean los esperados (es decir, los que se obtuvieron en el entorno de desarrollo) el adjudicatario tendrá que dar el soporte necesario, si hace falta presencial, para solucionarlo.

Una vez se haya realizado la ejecución del plan de pruebas con el 100% de las pruebas funcionando en el entorno de preproducción y producción se dará el proyecto por cerrado. A partir de este instante entrará en vigor el periodo de garantía del evolutivo.

A partir de este momento ya tiene que entrar en vigor la etapa de soporte, es responsabilidad del adjudicatario realizar las tareas necesarias bisiestas, formación y documentación del proyecto, de operación, y procedimental a fin de que los nuevos desarrollos ya puedan ser objeto del servicio de soporte 24x7.

Una vez acabada la etapa de codificación y superadas las pruebas de integración en torno a preproducción, el equipo de desarrollo tendrá que preparar el plan de implantación con la colaboración del equipo de Soporte de la AOC (también dependiendo del Área de Tecnología). El plan de implantación incorpora todas las acciones dirigidas a que la versión llegue a los usuarios finales.

Hace falta tener en cuenta que ninguno de los técnicos de desarrollo, sin embargo, tiene -por defecto- acceso a los entornos de preproducción y producción.

Para llevar a cabo el plan de implantación cada equipo de desarrollo prepara el paquete de despliegue y realiza una petición al proyecto Despliegues del JIRA. En la petición de despliegue se indicará la versión del JIRA a la que corresponde el despliegue.

Los despliegues en torno a PRE se realizan los jueves por la tarde y la petición de despliegue tiene que haber llegado como muy tarde el día de antes, a fin de que se pueda preparar junto con el resto de los despliegues de otros servicios del Consorci AOC. Adicionalmente y con el objetivo de agilizar y garantizado la corrección de los despliegues, se está implantando un sistema de integración continúa y despliegue automático.

Una vez desplegado en preproducción, es el adjudicatario quien tendrá que ejecutar el plan de pruebas para realizar la validación final. El de proyecto del Consorci AOC decidirá si la versión supera satisfactoriamente el plan de pruebas. En caso afirmativo, el equipo de desarrollo preparará y solicitará a través del JIRA la petición de despliegue en producción (los despliegues en torno a producción se realizan los miércoles por la tarde). En caso contrario, el equipo de desarrollo realizará las correcciones necesarias dando todo el apoyo necesario para corregir las incidencias detectadas en la mayor brevedad posible.

Una vez la versión se haya desplegado en producción entrará en vigor el periodo de garantía del evolutivo.

4.7.7 Evaluación

Una vez definidos los requerimientos que formarán parte de la versión, la Cabeza de Proyecto define las métricas y los indicadores que permitirán evaluar el cumplimiento de los objetivos marcados para la versión.

Después de un cierto tiempo de la puesta en marcha de la versión, el j de Servicio realizará el seguimiento de los indicadores a través de encuestas, auditorías y cualquier otra herramienta de gestión de la calidad que considere adecuada, estableciendo el cuadro de mandos del servicio.

Este cuadro de mandos se pondrá a disposición del comité estratégico con el objetivo de mantenerlo informado de la marcha del servicio.

Finalmente, el comité de seguimiento realizará una sesión de retrospectiva analizando conjuntamente qué cosas han ido bien durante la versión y qué cosas han ido mal (desde el punto de vista de todos los actores) con el fin de poder aprender y mejorar de cara a la nueva versión.

4.7.8 JIRA

La herramienta corporativa JIRA se convierte en la piedra angular de la versión en tanto permite reflejar en detalle el estado actual de la versión, el grado de consecución de esta, así como la evolución estratégica que seguirá el servicio en un futuro medio. Es por lo tanto una herramienta fundamental para mantener coordinados a todos los actores.

La información del JIRA se hace visible a todos los actores que participan en el servicio, pero dado que cada uno de los actores priorizará un tipo de información diferente, se requiere de un esfuerzo por parte del jefe de Servicio y del j de Proyecto por reflejar en el JIRA los diferentes puntos de vista. Esta diferente visión se plasma en el JIRA a partir de los siguientes proyectos:

- Servicio: evolución estratégica de un servicio en medio/largo plazo. En este proyecto del JIRA los requerimientos se agrupan y se ordenan en ideas conceptuales próximas a las líneas de actuación que marca al comité estratégico. Este proyecto permite obtener una idea global de lo que se pretende conseguir con el servicio en medio o largo plazo.

  Para los requerimientos más prioritarios, que inicialmente son los candidatos que seleccionar para la próxima versión, el responsable del servicio realizará el análisis funcional detallado.

  El jefe de Servicio es el principal responsable del mantenimiento en el JIRA de este proyecto y tiene que reflejar todos los cambios y documentos con la máxima periodicidad posible.

Proyecto: vista detallada del futuro inmediato del servicio. En este proyecto del JIRA se descomponen las peticiones de evolutivos en los diferentes requerimientos funcionales

y técnicos que tiene que cumplir la nueva versión. Los asuntos que componen este proyecto se encuentran bien definidos y detallados, disponen de una estimación de su coste, el/los recurso/s que está/asignado/s, así como su grado de adelanto. Este proyecto permite obtener una idea detallada del estado actual del servicio y su objetivo es mantener informado con el mayor nivel de detalle posible a los diferentes actores que participan en el desarrollo diario del servicio.

> El jefe de Proyecto es el principal responsable del mantenimiento en el JIRA de este proyecto y tiene que reflejar todos los cambios con la máxima periodicidad posible. En este proyecto se incluirán todos los documentos técnicos (diseño técnico, documentos de integración, etc.)

Si procede, cualquiera de estos 2 proyectos principales se puede complementar con otros proyectos que permitan agrupar líneas de actuación que se llevarán a cabo a largo plazo o bien lo cual se llevarán a cabo en paralelo, pero en fechas diferentes. El objetivo de estos proyectos complementarios tiene que ser simplemente el de facilitar la lectura del estado presente y futuro del servicio a los diferentes actores.

4.8 Requerimientos técnicos y personales

El licitador tendrá que disponer en el momento iniciar el contrato, de los recursos que se han indicado a la descripción del lote del contrato.

El proveedor tiene que garantizar que para la resolución de incidencias y para dar respuesta a las peticiones básicas de operación siempre habrá un mínimo de dos personas formadas en cada uno de los entornos y que, como mínimo, siempre hay una disponible.

En caso de baja (temporal de más 4 días de duración o definitiva) de cualquiera de los miembros del equipo, el adjudicatario tendrá que sustituirlo en menos de 5 días laborables de acuerdo con los responsables del Consorci AOC. Cualquier cambio en uno de los miembros del equipo a instancias del adjudicatario tendrá que ser validado por el Consorci AOC. Habrá que acordar el calendario de cambio con el Consorci AOC con el fin de minimizar el impacto en los desarrollos en curso. fuera de estos compromisos los periodos de vacaciones y permisos de todos los miembros del equipo.

Cuando se cambie un miembro del equipo de trabajo a instancias del adjudicatario, se fijará un tiempo de 2 semanas de formación /adaptación del nuevo miembro que serán a cargo del adjudicatario.

El Consorci AOC se reserva el derecho a pedir el cambio de cualquiera de los miembros del equipo sin necesidad de justificación con una antelación de 20 días naturales a la fecha de sustitución.

Además de los perfiles descritos para cada lote, habrá que aportar un gestor del servicio de alto nivel que se encargará de las siguientes funciones:

- Interlocución a alto nivel.
- Diseño y seguimiento del plan derivado del contrato.
- Velar porqué cada fase del proyecto se realice de forma diligente y dentro de las fechas acordadas.
- Informar de las desviaciones de las fechas de finalización de cada fase tan pronto como se detecten.
- Gestionar los recursos asignados, tanto materiales como personales.

5. Objetivos, hitos y calendario Lote 3: Servicios de desarrollo de aplicaciones Frontend y Accesibilidad.

5.1 Objetivo

El objetivo de este lote es dar conformidad al Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público, a los servicios que presta el Consorci AOC.

Dado que se ha detectado la importancia que tiene el desarrollo Frontend en el cumplimiento de este objetivo, se ha decidido ligarlo con el resto de las tareas referentes a la accesibilidad que se tienen que realizar con el fin de conseguirlo, y es por este motivo que se ha incluido conjuntamente en un mismo lote.

Uno de los objetivos será poder detectar el más bien posible cualquier incumplimiento de la accesibilidad en cada una de las fases del desarrollo, ya que eso a la larga ahorrará tiempo en la resolución de los errores.

5.2 Descripción y alcance Lote 3

Las tareas que forman parte del alcance del lote 3 las dividiremos en dos tipos de servicios:

5.2.1 Servicios de desarrollo de aplicaciones Frontend:

En primer lugar, aclaramos que entendemos por Frontend la parte de código de una aplicación que se ejecuta dentro del navegador del usuario.

Respecto del lote 3, a la hora de participar en el desarrollo de los nuevos módulos, las transformaciones y las evoluciones de los servicios del AOC, seguiremos como norma general las siguientes fases:

1. Diseño: dado un diseño que se nos facilitará, se realizará uno primero análisis de la accesibilidad, para detectar posibles problemas al diseño. Una vez corregidos estos problemas se pasará a la siguiente fase.
2. Desarrollo Frontend: dado el diseño accesible se realizará la maquetación accesible. Eso dará como resultado un conjunto de archivos HTML, CSS

(SASS, etc.), imágenes, javascript, etc. Estas maquetas se facilitarán a los desarrolladores del Lote 2.

3. Colaboración entre equipos: los equipos del Lote 2 y 3 tendrán que trabajar de manera colaborativa, con el fin de integrar correctamente toda la normativa de accesibilidad en los servicios, en esta parte será muy importante vigilar la interacción de las aplicaciones para asegurar que se haga de forma accesible.
4. Auditoría de accesibilidad: una vez acabado el desarrollo por parte de los equipos del Lote 2 y 3, se realizará una última revisión de la accesibilidad para poder realizar la declaración de accesibilidad que cada servicio debe tener publicada y accesible desde todas las páginas del servicio y realizar al informe IRA (Informe de Revisión de Accesibilidad) que el Consorci AOC tiene la obligación de tener para cada servicio.

   Este punto pertenece a los "Servicios de accesibilidad" pero lo describimos aquí para que quede claro que formará parte de todo el proceso que asegurará la accesibilidad de los servicios y/o webs.

5.2.2 Servicios de accesibilidad

Con el fin de mantener y mejorar la accesibilidad de nuestros servicios y aplicaciones se tendrán que realizar tareas como:

- Revisiones de accesibilidad: se realizarán revisiones continuadas de la accesibilidad web para garantizar el cumplimiento, mediante:
  - monitorización automatizada (para las normas que se pueden automatizar) del cumplimiento de la normativa para facilitar el seguimiento de las incidencias y las correcciones
  - revisión manual, por aquellas partes que sólo se pueden revisar de esta forma
  - elaboración y revisión de las declaraciones de accesibilidad
  - auditorías de accesibilidad: las auditorías las hará un equipo en que colaborarán como mínimo un consultor de accesibilidad visual y un consultor de accesibilidad no visual. A partir de esta auditoría se elaborará el informe IRA (Informe de Revisión de Accesibilidad)
- Formación: se tendrán que hacer formaciones por los desarrolladores y por los generadores de contenidos para que aprendan a crear y mantener el código y los contenidos accesibles.
- Documentos accesibles: velar y hacer el necesario para que todos los documentos publicados en los servicios y webs del Consorci AOC sean accesibles, así como PDF, POWERPOINTS, EXCEL, VIDEOS, etc.

5.3 Equipo de trabajo Lote 3

La empresa adjudicataria dimensionará y propondrá un equipo de trabajo adecuado para la ejecución de los servicios, teniendo en cuenta que este tendrá que ser el necesario para asegurar las funciones que son objeto del contrato. El equipo tendrá que permitir mantener a un modelo de relación fluido con la persona designada por el Consorci AOC para liderar el proyecto, siempre de acuerdo con las diversas tipologías y casuísticas de trabajo que se tendrán que tratar y resolver.

Hay que hacer énfasis en que este no es un contrato por horas, sino un contrato de servicios y la dotación de recursos tiene que ser suficiente para alcanzar todas las tareas que le serán exigidas a la empresa adjudicataria.

Se considera que el equipo de trabajo tendrá que disponer de los siguientes perfiles que se detallan a continuación. Hay que recalcar que las funciones que se describen son una descripción mínima de tareas, pero la empresa adjudicataria tiene que poder garantizar y dar respuesta al conjunto de necesidades descritas en el contrato.

Responsable OT

La persona con este perfil tendrá que satisfacer los siguientes requisitos:

- Titulación: Grado o titulación universitaria equivalente, en cualquier ámbito
- Experiencia mínima demostrable de 3 años en funciones de cabeza de proyecto liderando equipos de como mínimo 3 integrantes con metodologías de trabajo ágiles.
- Experiencia mínima de 3 años en equipos de trabajo en accesibilidad web

Las principales funciones de este perfil serán:

- Seguimiento detallado del plan derivado del contrato e interlocución directa con el Consorci AOC.
- Dirección del servicio y coordinación de los recursos asignados al servicio, tanto materiales como personales.
- Establecer las planificaciones de las diferentes tareas encomendadas, velando por que cada una de estas tareas se realizan de forma diligente y dentro de la planificación acordada. Informar al Consorci AOC de las desviaciones tan pronto como se detecten.
- Generar la documentación asociada al servicio y realizar los informes de seguimiento.
- Supervisión del trabajo del resto de personas del equipo con el objetivo de maximizar la calidad de los entregables.

Consultor de Accesibilidad

La persona con este perfil tendrá que satisfacer los siguientes requisitos:

- Titulación: Grado o titulación universitaria equivalente, en cualquier ámbito.
- Se valorará tener un Posgrado o Máster en Tecnologías Accesibles o similar.
- Experiencia mínima de 3 años en equipos de trabajo en accesibilidad web.
- Experiencia mínima de 2 años elaboración de PDF's accesibles.
- Experiencia mínima de 2 años subtitulación y audio descripción de vídeos.

Las principales funciones de este perfil serán:

- Revisión continuada de la accesibilidad web para garantizar el cumplimiento de la normativa con el nivel AA de las WCAG 2.1.
- Revisión de la parte visual en lo referente a la accesibilidad.
- Elaboración y revisión de las declaraciones de accesibilidad.
- Elaboración de informes IRA (Informe de Revisión de Accesibilidad).
- Formaciones de accesibilidad.
- Revisión y corrección de documentos para hacerlos accesibles (PDF, POWERPOINTS, EXCEL, VIDEOS, etc.)

Consultor de Accesibilidad no visual

La persona con este perfil tendrá que satisfacer los siguientes requisitos:

- Titulación: Grado o titulación universitaria equivalente, en cualquier ámbito.
- Se valorará tener un Posgrado o Máster en Tecnologías Accesibles o similar
- Experiencia mínima de 3 años en equipos de trabajo en accesibilidad web
- Experiencia mínima de 3 años en el uso de lectores de pantalla

Las principales funciones de este perfil serán:

- Revisión continuada de la accesibilidad web para garantizar el cumplimiento de la normativa con el nivel AA de las WCAG 2.1.
- Revisión de la parte no visual en lo referente a la accesibilidad.
- Elaboración de informes IRA (Informe de Revisión de Accesibilidad) en la parte de no visual.
- Formaciones de accesibilidad

Desarrollador frontend accesible

Las personas con estos perfiles tendrán que satisfacer los siguientes requisitos:

- Titulación: Ciclo Formativo de Grado Medio o Superior, o Grado o titulación universitaria.
- Experiencia mínima de 2 años en equipos de trabajo en accesibilidad web.
- Experiencia mínima de 2 años en desarrollo Frontend accesible.
- Conocimiento avanzado de HTML y HTML semántico.
- Conocimiento avanzado de CSS y paradigmas como OOCSS y SMACSS.
- Conocimiento de JavaScript y sus características que afectan a la accesibilidad.
- Conocimiento avanzado de las WCAG 2.2 y de cómo testear sus criterios.
- Conocimiento de WAI-ARIA y de patrones de componentes accesibles.
- Se valorará positivamente la familiaridad con lectores de pantalla y como utilizarlos para testear problemas de accesibilidad.
- Se valorará positivamente el conocimiento de los framework React y Angular.
- Se valorará positivamente el conocimiento y la experiencia Design Systems, Atomic Design y Figma

Las principales funciones de estos perfiles serán:

- Desarrollo Frontend de los servicios y/o webs que marque el equipo del Lote 2.
- Una vez hecho este desarrollo, tendrá que colaborar con el equipo del Lote 2 con el fin de integrar en el desarrollo final el código accesible generado y solucionar posibles barreras de accesibilidad que se puedan generar en la integración.
- Elaboración de código para hacer correos HTML accesibles.
- Creación de una librería de componentes accesibles para poder reutilizarlos en proyectos futuros.

6. Objetivos, hitos y calendario Lote 4: Implementación de procedimientos para la mejora de la calidad de las aplicaciones del Consorci AOC

6.1 Situación actual Lote 4

El Consorci AOC dispone de un plan de transformación estratégico para el periodo 2022-2026 adaptado a sus necesidades y objetivos específicos, que entre otras medidas intenta poner el foco en la calidad que suponga una mejora de la seguridad, experiencia de usuario, tiempo de entrega, disponibilidad y rendimiento de las aplicaciones y servicios que ofrece el Consorci AOC.

De forma resumida los principales objetivos que persigue este lote son:

· **Identificación y prevención de errores**: Mediante la automatización de los test, revisiones de código y otras técnicas se pretende identificar y prevenir los errores antes de la salida a producción con la mejora que eso supone en dos aspectos: reducción de costes (por el aumento de la eficiencia del proceso) y la percepción del servicio por parte del usuario final.

· **Automatizar el flujo de despliegues**: Mediante la automatización de los flujo de despliegue desde su construcción, hasta las diferentes etapas de revisión de código y test previo, hasta el despliegue, posterior validación funcional, contemplando la posibilidad de marcha atrás, así como el etiquetado y guardado de los artefactos de las aplicaciones versionados se pretende mejorar el procedimiento donante más garantías sobre el correcto despliegue, agilizando la marcha atrás en caso necesario y dando flexibilidad al proceso para que se pueda realizar de forma continua al no depender directamente como hasta ahora de que una persona realice de forma manual el proceso de construcción, despliegue y posterior validación.

· **Monitorear el rendimiento**: Mediante la definición de un procedimiento que determina métricas e indicadores de rendimiento que nos permiten evaluar mediante la ejecución de pruebas, la capacidad de las diferentes versiones de las aplicaciones para poder compararlas y validar las mejoras o detectar errores que puedan reducir el rendimiento.

· **Revisión de la seguridad**: Revisar de forma estática y dinámica el código, sus dependencias y las aplicaciones en funcionamiento; para detectar posibles vulnerabilidades de estas, y de esta forma revisarlas, clasificarlas y corregirlas en función de la gravedad y afectación a la que nos expongan.

· **Métricas**: Definición de métricas y cuadros de control relacionados con la calidad de las aplicaciones y de los despliegues para detectar posibles riesgos, mejoras y funcionamiento general del flujo de despliegues de las aplicaciones.

· **Acompañamiento implementación y técnicas de test automatizado**: Acompañamiento a los proyectos para la adopción de las diferentes metodologías de test, herramientas etc. y si en la implementación de las primeras pasas para la adopción de un modelo de shit left testing.

Para poder llevar a cabo estos objetivos, desde el Consorci AOC se creó desde 2022 un área de Gobernanza y Calidad. Esta área es la encargada de revisar, definir y validar diferentes herramientas y metodologías para la implementación de los mecanismos necesarios para conseguir estos objetivos.

Actualmente ya se dispone de la implementación de diferentes procedimientos, métodos y componentes. Los principales componentes implementados hoy en día son el siguientes: un pipeline de orquestación del despliegue continúo encargado de las diferentes etapas del flujo, uso de herramientas externas como sonarqube o LoadRunner para la monitorización del rendimiento y finalmente herramientas como ELK / Grafana para la recopilación de métricas y la definición de paneles de indicadores.

Lo que se pretende es pues, dar impulso y seguimiento a las medidas iniciadas para acelerar la implantación y si ocurre implementar nuevos mecanismos o procedimientos que puedan ayudar a la mejora de la calidad y que no se hayan tenido en cuenta hasta ahora.

6.2 Descripción y alcance Lote 4

Las tareas que forman parte del alcance del lote 4 son las siguientes:

· **Definición de metodologías, frameworks y herramientas para la ejecución de los test funcionales UI (en adelante test) y por el análisis de calidad y seguridad de código (en adelante análisis de código)**. El plan de mejora de la calidad pasa por mejorar la eficiencia y la calidad del código y de los despliegues, garantizando que se pueden realizar despliegues de forma continuada gracias a la validación automatizada de los mismos, y que en caso de error estas se detectan antes dentro del flujo de desarrollo mejorando de esta forma la eficiencia del proceso. De la misma manera, la revisión de código para la detección de vulnerabilidades y de error de forma precoz mitiga la exposición de posibles vulnerabilidades y/o errores debido a problemas del código.

· **Instalación, configuración y gestión de las diferentes herramientas y plugins necesarios para la ejecución de los test y los análisis de código**. Una parte importante del plan de calidad se la selección de las herramientas y/o frameworks necesarios para llevar a cabo las tareas indicadas. La selección dependerá de los conocimientos del equipo, de las necesidades y de los objetivos perseguidos entre otros. En caso de que se requiera de una herramienta, aplicación o servicio no existente dentro del flujo, la instalación y/o configuración, así como la gestión de actualizaciones y disponibilidad si procede entrará dentro del alcance de este lote.

· **Definición de test basados en metodología BDD** Con el fin de poder implicar miembros de equipos funcionales, será importante definir metodología BDD (herramientas y procedimientos) para poder escribir requerimientos de los test funcionales con lenguaje natural como podría ser con Gherkin, y poder enlazarlos con la implementación de la automatización de las pruebas p.ej. con Cucumber.

· **Implementación de las diferentes etapas para la ejecución de los test y de los análisis de código**. Actualmente al Consorci AOC ya se dispone de Jenkins y de CodePipeline como orquestadores de los flujos de CI/CD para el despliegue y análisis de las aplicaciones. En caso de que se añada una fase de test o de análisis de código, será necesaria la implementación de los llamamientos o ejecuciones dentro de estos flujos.

· **Impulsar la adopción e implementación de test por parte del equipo de proyectos**. Para intentar fomentar y potenciar la cultura de la calidad y la importancia de la ejecución de test, será importante acompañar en los casos necesarios a los desarrolladores en la implementación de las primeras fases de los test, ya sea sugiriendo estrategias, haciendo formaciones o incluso generando algunos test que sirvan de ejemplo.

· **Definición del formato de los reportes con el resultado de las ejecuciones de los test**. Será importante definir el formato de reporte con el resultado de los test sobre todo en los casos de errores con el fin de proporcionar la información necesaria para facilitar al máximo la resolución por parte del equipo de proyectos. Será pues importante que, en caso de error, aparezca toda la información disponible como pueden ser capturas de pantalla, navegador, etc.

· **Asesoramiento y seguimiento de la implantación de test en los diferentes proyectos**. Con el fin de impulsar la adopción y la implementación de test funcionales, será una parte clave, asesorar y hacer seguimiento de los diferentes proyectos con respecto a la implementación de estos test, teniendo en consideración la importancia de que sean fiables, mantenibles y resilientes con respecto al equilibrio entre la cobertura y el tiempo de ejecución.

· **Procedimentación y seguimiento de las vulnerabilidades críticas de los diferentes proyectos**. Con el fin de impulsar y trasladar la importancia de la seguridad y la calidad del código, será necesario hacer seguimiento de las vulnerabilidades presentes al código y de su resolución en función de su gravedad. Por eso también será clave, procedimentar lo análisis de estas, el tiempo máximo de resolución o mitigación en función de la gravedad etc.

· **Formación del equipo interno de QA en caso de adopción de nuevas herramientas y/o metodologías de test y análisis de código**. En caso de instalar nuevas herramientas o metodologías que no sean habituales o conocidas al Consorci AOC, será importante hacer una formación interna para poder analizar previamente la viabilidad de la implantación.

· **Definición de métricas y dashboards para el seguimiento de la implantación de los test y de la resolución de vulnerabilidades y errores detectados durante los análisis**. Para el Consorci AOC será clave disponer en todo momento de una foto de la situación actual de las aplicaciones en estos dos ámbitos, que permita entender en qué estado se encuentra a los responsables de la organización.

6.3 Equipo de trabajo Lote 4

La empresa adjudicataria tendrá que conformar el equipo de trabajo necesario en el momento de iniciar el contrato.

Además de los perfiles con dedicación a tiempo cumplido que se detallarán a continuación, se considera necesaria la figura de un responsable del contrato a quien concentrará y recibirá las comunicaciones a alto nivel del Consorci AOC sobre la dirección, estrategia y evolución del servicio. Este responsable del contrato será por lo tanto el interlocutor y el punto de contacto a quienes el Consorci AOC transmitirá la visión de negocio y los requerimientos transversales que son objeto del contrato.

El responsable del contrato también será el encargado de gestionar los recursos tanto materiales como personales asignados al contrato.

En caso de baja de cualquiera de los miembros del equipo a instancias del adjudicatario, el adjudicatario tendrá que sustituirlo en menos de 15 días laborales y tendrá que asumir un tiempo de 2 semanas de formación y adaptación del nuevo miembro que tendrán que ir a cargo del adjudicatario. El Consorci AOC tendrá que validar el cambio y podrá acordar el calendario con el fin de minimizar el impacto en el servicio.

Todos los miembros del equipo de trabajo tendrán que estar asignados a tiempo cumplido y en exclusividad para el servicio.

El Consorci AOC se reserva el derecho a pedir el cambio de cualquiera de los miembros del equipo informando al adjudicatario con una antelación de 20 días naturales a la fecha de sustitución.

Los perfiles requeridos por el equipo de trabajo son los siguientes:

- **Ingeniero de software experto en testing** funciones principales:
    - Definición de metodologías de testing funcional de UI de las diferentes aplicaciones.
    - Definición de métricas y cuadros de mandos para el seguimiento de la implantación de las metodologías definidas.
    - Selección de herramientas y frameworks preferiblemente opensource para la implementación de los test.
    - Acompañamiento en los equipos de proyectos en la implantación y desarrollo de las metodologías de test en las primeras etapas de la implantación.
    - Participación en la definición de las pruebas funcionales de rendimiento que se quieran realizar sobre los frontales web (estrategias, flujo de validación, datos de test etc.) así como de las métricas para la valoración de nivel de asunción de la carga requerida.
    - Formación en el resto de los compañeros de proyectos y QA en los casos requeridos para el a implantación de nuevas herramientas, metodologías etc.
    - Planificación y seguimiento global del grado de implantación de los test

de validación funcional a los diferentes proyectos.

- **Ingeniero de software experto en testing** experiencia requerida:
    - Experiencia con herramientas de CI/CD preferiblemente con Jenkins o CodePipeline, también es tendrán en consideración de otras herramientas de CI/CD Gitlab, GitHub actions, CI etc.
    - Experiencia mínima demostrable de 1 año en implementación, mantenimiento y mejora de flujos de CI/CD.
    - Experiencia con Echazón como control de versiones, preferiblemente a través de GitHub.
    - Experiencia en el uso de herramientas de construcción preferiblemente Gradle o Maven.
    - Se valorará positivamente el conocimiento y la experiencia en desarrollo de aplicaciones en Java (o lenguajes de JVM como Groovy/Kotlin) y Javascript/Typescript (NodeJs).
    - Experiencia en desarrollo de test unitarios (Junit, Spring Test, Spock etc.) y test funcionales UI (preferiblemente utilizando Selenium, Geb o Cypress).
    - Se valorará positivamente la experiencia en la definición de test de rendimiento, preferiblemente con LoadRunner.
    - Se valorará positivamente la experiencia en herramientas de gestión de test (preferiblemente integradas en JIRA - Xray).
    - Se valorará positivamente la experiencia en definición e implementación de test BDD, con herramientas como Gherkin y Cucumber.
- **Ingeniero de software experto en seguridad** funciones principales:
    - Definición de tipo de análisis del código y de los servicios para el detección y corrección de vulnerabilidades, al código, a las dependencias y a los servicios.
    - Definición de procedimientos y flujos de análisis y realización de correctivos en función de la gravedad y la exposición de las vulnerabilidades.
    - Revisión de las posibilidades de explotación de las vulnerabilidades detectadas.
    - Definición de cuadro seguimiento de las vulnerabilidades y su clasificación por tipo, gravedad, proyecto.
    - Seguimiento de las correcciones de las vulnerabilidades con el equipo responsable de su resolución.
    - Responsable en formación de herramientas o métodos de análisis de código para la detección y mitigación de vulnerabilidades.

- Generación de informes de riesgos en el caso de vulnerabilidades que no por algún motivo no puedan ser resueltas con agilidad.
- Implementación de las fases de análisis y revisión dentro de los pipelines internos de CI/CD, con la instalación de los componentes y plugins necesarios para llevarlas a cabo.

- **Ingeniero de software experto en seguridad** experiencia requerida
  - Experiencia con herramientas de CI/CD preferiblemente con Jenkins o CodePipeline, también es tendrán en consideración de otro CI/CD Gitlab, GitHub actions, CI etc.
  - Experiencia mínima demostrable de 1 año en implementación, mantenimiento y mejora de flujos de CI/CD.
  - Experiencia con Echazón como control de versiones, preferiblemente a través de GitHub.
  - Experiencia en el uso de herramientas de construcción preferiblemente Gradle o Maven.
  - Experiencia en desarrollo de aplicaciones en Java (se valorará positivamente conocimiento en otros lenguajes de la JVM como Groovy/Kotlin) y Javascript/Typescript (NodeJs).
  - Conocimiento y experiencia en mecanismos y herramientas de análisis estático y dinámico de código.
  - Experiencia en técnicas de intrusión y análisis de vulnerabilidades de código.

7. Acuerdos de Nivel de Servicio

En este apartado se describe el marco contextual de aplicación de los Acuerdos de Nivel de Servicio para los 4 lotes que son objeto de esta licitación. Se establecerá el siguiente procedimiento de trabajo y el Acuerdo de Nivel de Servicio (ANS) que se detalla a continuación para todos los entregables que se desplieguen en torno a producción.

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.

Requerimientos de nivel de servicio

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 tendrá que ser como mínimo del 90%.
- El nivel ofrecido por quien resulte adjudicatario del lote constituirá un Acuerdo de Nivel de Servicio (ANS), el cumplimiento del cual 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
Bloqueante	Una incidencia se catalogará con criticidad bloqueante si impide la utilización total del servicio a todos los usuarios de este.
Alta	Una incidencia se catalogará con criticistas alta si impide la utilización de una parte concreta del servicio, en todos o algunos usuarios, y la afectación para 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 en todos o algunos usuarios externos en la plataforma y la afectación para el negocio es relativamente baja.
Baja	Una incidencia se catalogará con criticistas baja si no impide la utilización ni parcial ni total de alguno de los servicios en 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 comunicada, 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 ticket de la incidencia hasta el momento en que la incidencia está solucionada. En el cálculo del tiempo de resolución de una incidencia no se tienen en cuenta los posibles incrementos de tiempos 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 mesa 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 Bloqueante	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 tiempos 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 con anterioridad 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 dentro del 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%

Caso 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 en el mes se le aplicará las siguientes penalizaciones:

Porcentaje de incidencias con criticidad 2 y 3 dentro del 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 de lo mismo pueda comportar la resolución del contrato, se prevé la imposición de penalidades.

Las penalidades que 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 los sistemas del Consorci AOC, se tendrá que informar en un tiempo inferior a las 24h.

En la fase inicial del proyecto se tendrá que definir 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 tendrá que informar periódicamente de los incidentes que hayan afectado los sistemas o plataformas del Consorci AOC.

8. Condiciones de ejecución

El adjudicatario de cualquiera de los 4 lotes tendrá que cumplir las siguientes obligaciones básicas:

- Gestionar cualquier alteración del servicio en las condiciones expresadas en este pliego.
- Realizar reuniones periódicas con el Consorci AOC con el fin de exponer el cumplimiento del servicio y tratar los posibles problemas o mejoras del servicio.
- Establecer un marco metodológico de trabajo basado en la metodología 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.
- Elaboración de los manuales y otra documentación destinada a la formación de los usuarios.
- Elaboración de la documentación técnica.
- Mantener en todo momento la actualización del código fuente y de la documentación en el sistema de control de versiones del Consorci AOC (GitHub) a fin de que pueda estar disponible en todo momento por el personal asignado y también para disponer de la opción de control de versiones.
- Toda la documentación generada por el equipo será en catalán y en el formato corporativo propuesto por Consorci AOC.
- Presentación de informes mensuales con el detalle del estado del servicio de acuerdo con los indicadores que el Consorci AOC considere apropiados. Algunos ejemplos de estos informes serían:
    - 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 finalización del contrato con el resumen de las tareas realizadas.
- El Consorci AOC se reserva el derecho a validar, y si ocurre definir, las herramientas que tengan que utilizar para la gestión y control del servicio.

9. Modelo de relación

El adjudicatario de cualquiera de los 4 lotes tendrá que incluir en su propuesta cuál es el modelo de relación que propone para garantizar el éxito del proyecto: la estructura organizativa del servicio, los canales y herramientas de comunicación a todos los niveles entre el proveedor y el Consorci AOC, los procedimientos de escalado ante incidencias susceptibles de afectar o con afectación a los servicios bajo responsabilidad del proveedor, y qué herramientas de control (adicionales en las herramientas corporativas JIRA y Microsoft Teams del Consorci AOC), propone para llevar a cabo el seguimiento y control global del servicio. Hay que destacar que el Consorci AOC se reservará el derecho a validar, y si ocurre definir, estas herramientas de control.

Hará, Como mínimo, falta que se establezcan los siguientes niveles de interlocución:

Reuniones de dirección con las siguientes características:

- Interlocutores: gerente de cuentas y/o responsable del servicio por parte del adjudicatario. Gestor del servicio por parte del Consorci AOC.
- Periodicidad mínima: 2 meses
- Objetivo: hacer el seguimiento del contrato, analizando varios aspectos: productividad, control de horas, temas de facturación, seguimiento de hitos (a alto nivel), etc.
- Entregables: actos de las reuniones, informes ejecutivos, informes con control de horas (hecho y pendiente) etc.

Reuniones de seguimiento con las siguientes características:

- Interlocutores: las personas asignadas por el adjudicatario para llevar a cabo el servicio. Por parte del Consorci AOC será el de proyecto/servicio o alguno de los técnicos asignados al proyecto.
- Periodicidad mínima: 1 mes
- Objetivo: seguimiento del cumplimiento del ANS, rendimiento de la plataforma e incidencias más destacables.
- Entregables:
    - Informes del estado del servicio
    - Informe resumen de las actuaciones ya resueltas y horas realizadas.
    - Informe de situación de las actuaciones en curso y horas realizadas.
    - Informe resumen de las actuaciones pendientes y horas estimadas.
    - Planificación de las actuaciones a realizar.
    - Escandallo de horas total realizadas en el mes.
    - Informe de las incidencias abiertas, resueltas, tiempo de resolución...

10. Horario de ejecución del servicio

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

- Del lunes al viernes, excepto festivos, de 08:00 a 19:00 horas.
- El 90% de los trabajos se realizarán en el horario indicado. En el 10% de los casos restantes se podrá solicitar previamente la realización de tareas fuera del horario anteriormente establecido. El coste de estos trabajos está incluido dentro del presupuesto de licitación de cada lote.

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

Cualquier cambio en uno de los miembros del equipo a instancias del adjudicatario tendrá que 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.

11. Infraestructura necesaria

Los adjudicatarios de cada uno de los 4 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 irán a cargo de los adjudicatarios. Es importante destacar que esta infraestructura tecnológica no podrá contener en ningún momento datos reales. Para los test y pruebas de los diferentes entregables, los adjudicatarios tendrán que disponer de entornos de integración en sus instalaciones para hacer el control de calidad de los evolutivos desarrollados.

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 en 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 tendrá que ser obligatorio para la aceptación de los trabajos.

12. 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 estos o facilitarlo a terceros.

Las empresas adjudicatarias no podrán hacer ningún 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, directamente o extractada, original o reproducida, sin autorización expresa del Consorci AOC, que la daría, si , previa petición formal del adjudicatario con expresión del fin.

13. Requerimientos de seguridad

Los adjudicatarios de cada uno de los 4 lotes tendrán que cumplir con los siguientes requerimientos de seguridad:

Medidas de seguridad y por defecto

El Consorci AOC, con el apoyo del adjudicatario, implementará durante la fase de desarrollo, las medidas de protección de datos desde el diseño y por defecto, recogidas a la guía del APDCAT: La privacidad desde el diseño y la privacidad miedo defecto. Guía para desarrolladores (gencat.cat)

Los adjudicatarios tendrán que documentar:

- El análisis llevado a cabo de las medidas necesarias.
- La verificación de que las medidas han sido aplicadas.

Certificaciones de seguridad

Durante el tiempo de ejecución del contrato, el adjudicatario tendrá que implementar las medidas de seguridad de nivel bajo del Esquema Nacional de Seguridad que le sean de aplicación. Concretamente son las descritas a:

- *Anexo - Requerimiento de seguridad (ENS) para los proveedores de software*

El Consorci AOC auditará que el adjudicatario cumple con los requerimientos del Anexo - Requerimiento de seguridad (ENS) para los proveedores de software. La auditoría se hará mediante la entrega de evidencias indicadas en el anexo al Consorci AOC para que esta determinación el grado de cumplimiento. El adjudicatario estará exento de la auditoría si aporta uno de los siguientes certificados:

Una declaración de conformidad con el Esquema Nacional de Seguridad de nivel Bajo, o un certificado de nivel medio o alto, en el ámbito del objeto del contrato.

Control de acceso al sistema

Los adjudicatarios tendrán que adaptarse en todo momento a los mecanismos de control de acceso a los sistemas de información que imponga al Consorci AOC para acceder a sus sistemas.

Control de personal

El adjudicatario tendrá que informar en todo momento de las altas y bajas del personal interno o subcontratado que en su nombre acceda a los sistemas del Consorci AOC.

En caso de baja de un usuario, de manera inmediata el adjudicatario tendrá que informar al Consorci AOC para revocar sus derechos de acceso a los sistemas.

Protección de la información

El adjudicatario no podrá hacer uso de los datos reales de los sistemas de producción en los sistemas de desarrollo.

El adjudicatario no podrá descargar información del Consorci AOC en sus sistemas o en soportes portátiles como USBs, DVDs, portátiles, tabletas, etc. En el caso de tener que hacerlo habrá que pedir la autorización del Consorci AOC y que el soporte esté cifrado.

Los ficheros temporales que se hubieran creado exclusivamente por la realización de trabajos temporales auxiliares tendrán que cumplir con las medidas establecidas que se apliquen a los ficheros considerados definitivos.

Todo fichero temporal así creado será borrado una vez haya dejado de ser necesario para la finalidad que motivó su creación.

14. Plan de devolución del servicio

El adjudicatario de cada uno de los lotes tendrá que asumir, dentro del periodo de garantía, la planificación y ejecución del plan de devolución del servicio al final de la prestación. El plan de devolución tendrá que cumplir con los siguientes requerimientos mínimos:

- Una duración de un mes con una dedicación mínima de 100h y tanto la duración (1 mes) como la dedicación (100h) serán adicionales a la prestación principal del servicio y tendrán que ir a cargo del adjudicatario.
- El adjudicatario tendrá que devolver el código fuente, scripts, documentación, etc. de todas las actualizaciones realizadas.
- El adjudicatario tendrá que destruir y/o devolver al Consorci AOC (o en aquel tercero que este designio) la información propiedad del Consorci AOC. Este retorno se tendrá que realizar de acuerdo con aquello que se establezca legalmente y según las indicaciones del Consorci AOC. El retorno contemplará, los datos de carácter personal que hayan sido objeto de tratamiento por parte de aquel durante la vigencia de lo mismo y así como todos los productos y

software que sea de propiedad del Consorci AOC junto con los soportes o documentos en que conste algún dato de este. El retorno de los datos al Consorci AOC, o en uno tercero designado, se llevará a cabo en el formato y los soportes que se acordarán en el momento de planificar y detallar el plan de finalización del contrato. El adjudicatario tendrá que disponer de un procedimiento de borrado seguro de soportes reutilizados o que lleguen al final de su vida útil. El proveedor tendrá que informar como hace la eliminación segura de la información y tendrá que proporcionar los certificados correspondientes conforme ha realizado esta eliminación segura.

Sergio Gutiérrez Palomino

Responsable Unidad de Arquitectura del Consorci AOC

Salmonete Noguera Arnau

Responsable de Desarrollo del Consorci AOC

Elena Torres Garcia

Jefa de Servicio de Accesibilidad del Consorci AOC

Albert Ciffone Solé

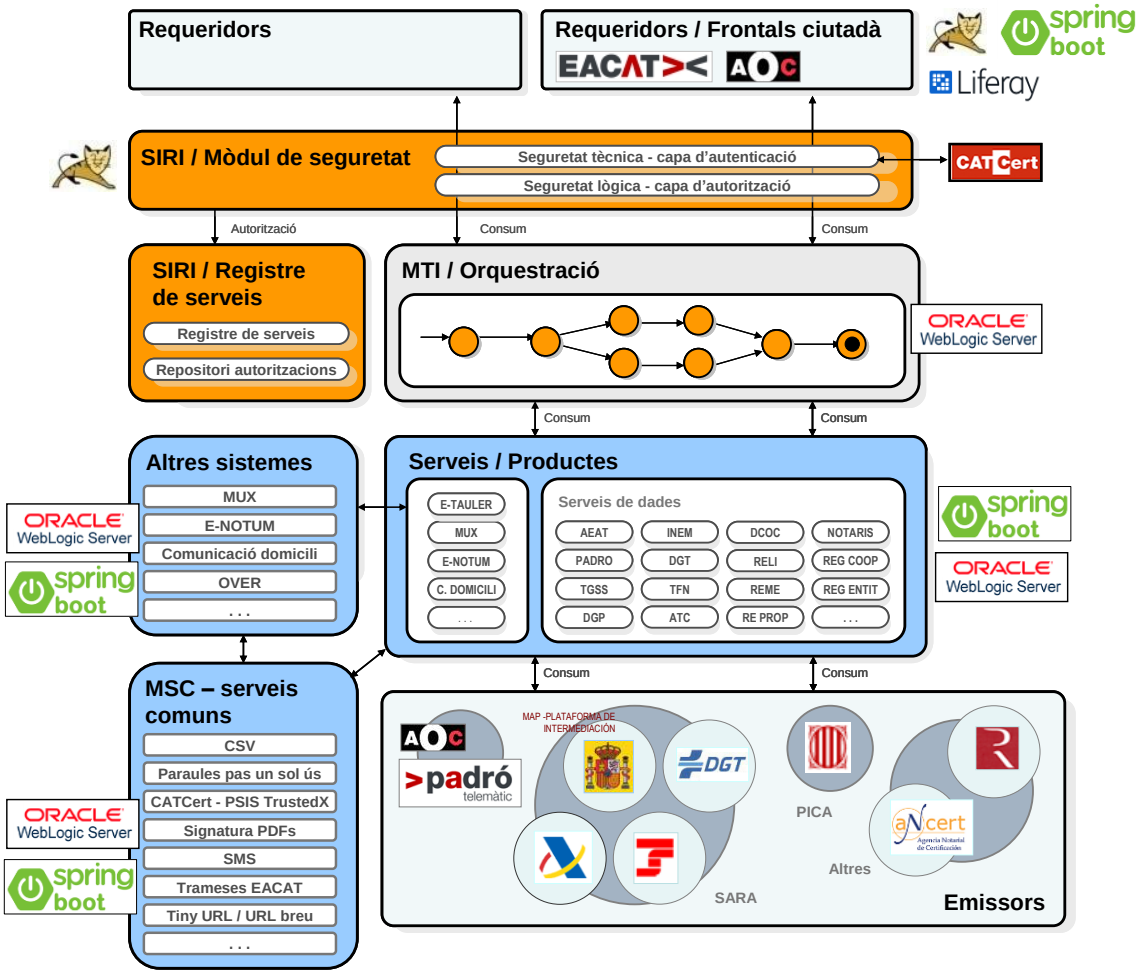
Responsable Unidad de Gobernanza y Calidad del Consorci AOC

Anexo - PCI 3.0 - Arquitectura PCI (resumen)

La Plataforma de Colaboración Administrativa (en adelante PCI) del Consorci AOC es un conjunto de sistemas y componentes orientados a la total disponibilidad de los servicios ofrecidos para las diferentes administraciones con la garantía de la máxima seguridad en el servicio y el acceso a los datos.

Arquitectura lógica

La arquitectura lógica de la PCI sigue un modelo conceptual orientado a servicios. Hay una separación clara entre requirentes, emisores de datos e intermediación de servicios.



La arquitectura lógica de referencia comprende los siguientes componentes:

- **SIRI (Sistema de Información de Recursos de Interoperabilidad)**: componente de seguridad encargado de autenticar y autorizar todos los accesos a PCI de manera centralizada y estandarizada.

  Adicionalmente, el SIRIO contiene el registro de servicios y productos de interoperabilidad ofrecidos por el Consorci AOC y proporciona las herramientas con el fin de gestionar las autorizaciones de acceso a los servicios, así como para supervisar la actividad de la plataforma.

- **MTI (Motor de Transacciones de Interoperabilidad)**: se encarga de la orquestación y trazabilidad de la ejecución de las peticiones (individuales vs lotes y síncronas vs asíncronas) de los diferentes servicios y controla la intermediación entre requirentes y los emisores finales de los datos de cada uno de los servicios de interoperabilidad y aplicaciones ofrecidos.

- **Productos / servicios**: cada uno de los servicios que ofrecen funcionalidades de transmisión telemática de datos y documentos electrónicos entre administraciones (Vía Abierta) así como de otras aplicaciones ofrecidas por el Consorci AOC (e-NOTUM o e-TAULER entre otros).

- **MSC (Módulo de Servicios Comunes)**: publica una serie de componentes y utilidades comunes disponibles por las diferentes plataformas del Consorci AOC (tanto PCI como EACAT o e-TRAM). Por ejemplo: envío de SMS, envío de envíos en EACAT, generador de palabras de paso de un solo uso o funcionalidades de firma digital, entre otros.

Arquitectura de implementación actual

La arquitectura de implementación traduce los componentes lógicos de la PCI a aplicaciones y productos.

Los productos sobre los cuales se apoya la PCI son los siguientes:

- **Weblogic Application Server 12c** (en adelante WL12).

  La implementación de un servicio PCI se puede conseguir con cualquier tecnología, aunque conviene alinearla con el conjunto de tecnologías corporativas. Así, la mayoría del componentes y servicios de negocio ofrecidos por la PCI han sido modelados como aplicaciones Java alineadas con arquitectura de referencia PCI 3.0 (JAX-WS, JAX-B, JPA y base de datos Oracle 12).

  Las aplicaciones se distribuyen en tres clusters con la misma arquitectura lógica según su tipología (servicios de interoperabilidad, servicios de tramitación y otras aplicaciones).

- **Apache Tomcat 8 / Springboot (ciudadano)**: contenedor de aplicaciones web donde se despliegan los frontales de usuario de las aplicaciones que implican relación con el ciudadano, por ejemplo, e-NOTUM o e-TAULER (Springboot, Spring Data JPA, Hibernate, React, Angular –ocasional- y Spring Security).

- **Oracle 12 RAC / PostgreSQL**: base de datos para almacenar datos de negocio.
- **EACAT / Liferay 6**: portal de gestión de contenidos y contenedor de aplicaciones web / portlets donde se despliegan los frontales de trabajador público.
- **Apache Tomcat 8 (EACAT) / Springboot (EACAT30)**: contenedor de aplicaciones web donde se despliegan los frontales de trabajador público que no se despliegan dentro de la plataforma EACAT (por ejemplo, e-NOTUM, e-TAULER, BOE, e-CÒPIA, bandeja de registro o Comunicación de domicilio entre otros). Estas aplicaciones, de reciente factura, se basan con las siguientes tecnologías: Frontend basado en Angular 6, librería Angular-material, TypeScript, XHTML + Material y CSS3. Backend basado en Spring Framework 5 (Spring MVC, Spring Core, Spring Data JPA) y Springboot, Spring Data JPA, Hibernate, React y Spring Security por las nuevas aplicaciones EACAT30 que se despliegan en la nube.

Anexo - Requerimiento de seguridad (ENS) para los proveedores de software

El presente anexo define los controles que tendría que hacer frente una empresa adjudicataria de servicios de desarrollo de software en caso de auditoría del ENS de nivel BAJO.

ID 1. Política de Seguridad

Se dispone de una Política de Seguridad que incluye:

1. Objetivos de la organización
2. Marc 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 tiene que 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 tiene que 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 periodo 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 los usuarios de los cuales son responsables mediante del correo electrónico.

ID 10. Evidencia de la difusión de la Normativa de Seguridad

Evidencia que la Normativa de Seguridad - ya sea propia o se sirva Marco Normativo de la Agència de Ciberseguretat de Catalunya - está disponible en la Intranet, página web, portal, repositorio, librería o a cualquier otro medio accesible para todos los usuarios implicados o bien 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.

Estos tienen que incluir como mínimo:

1. Como llevar a cabo las tareas habituales.
2. Quien tiene que hacer cada tarea.
3. Como 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 están disponibles en la Intranet, página web, portal, repositorio, librería o a 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:

- Como 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 tienen que ser nominales y no se pueden compartir.

- El periodo de retención de los usuarios.

ID 43. Procedimiento de Autenticación del Sistema

Se dispone de un procedimiento debidamente aprobado y actualizado dónde 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 estos.
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 estos 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:

- Como 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 tienen que ser nominales y no se pueden compartir.

- El periodo de retención de los usuarios.

ID 50. Herramienta corporativa específica para la gestión de los usuarios propios

Se dispone de una herramienta corporativa específica para la gestión de los 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 quienes 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 las obligaciones. Esta evidencia puede tomar varias formas:

1. Evidencia de que al crear su identificador se informa al usuario por correo electrónico, y al acceder por primera vez tiene que 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, que los usuarios estén implícitamente aceptándolas para acceder al sistema.

ID 64. Evidencia del último usuario propio dado de baja

Se dispone de la evidencia mostrando la baja de un usuario con la fecha efectiva de la baja.

ID 67. Procedimiento de Acceso en Local

Se dispone de un Procedimiento de Acceso en Local qué 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 (al puesto de trabajo, dentro de las propias instalaciones de la organización, en el servidor, al dominio de red, etc.) no revelen información sobre el sistema al cual se está accediendo.
3. Haga constar que se tiene que informar siempre a los usuarios de sus obligaciones una vez han accedido dentro del sistema.
4. Se tiene que informar al usuario de su último acceso al sistema.
5. Defina unos horarios en que es posible la conexión al sistema y otros en 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 qué se dispone de antivirus a los sistemas de información

Se dispone de la evidencia del uso de mecanismos de prevención ante 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 con 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 tiene que 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 273. Procedimiento de configuración segura del correo.

Se dispone de un procedimiento el cual se detalla cómo se configura el correo con el fin de disponer de un sistema seguro.

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

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