Consorci
Administració Oberta
de Catalunya

Consorci
Administració Oberta
de Catalunya

Pliego de prescripciones técnicas para la contratación de los servicios de desarrollos correctivos, evolutivos y nuevas funcionalidades del servicio de Gobierno Abierto (sede, transparencia y datos abiertos)

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

Fecha: 21 de junio de 2022

Consorci
Administració Oberta
de Catalunya

ÍNDICE

1. Prescripciones técnicas particulares

1.1 Alcance y objeto del contrato

El objeto de esta contratación es la prestación de los servicios de desarrollos correctivos, evolutivos y nuevas funcionalidades del servicio de Gobierno Abierto (sede, t ransparencia y datos abiertos), incluyendo todas las tareas necesarias de análisis, diseño, desarrollo y control de calidad.

Se incluye dentro del alcance todas las tareas necesarias de análisis, diseño técnico, desarrollo y control de calidad (incluyendo los test unitarios, test de integración, así como las pruebas de carga y estrés en los diferentes entornos).

Ofrecer soporte técnico especializado en lo que respecta a la detección, diagnóstico y resolución de las incidencias técnicas derivadas del uso del servicio de Gobierno Abierto.

El objeto de este pliego de prescripciones técnicas es pues definir el conjunto de requerimientos necesarios para ofrecer los servicios anteriores, de acuerdo a la metodología de trabajo descrita en el anexo 2.

1.2 Objetivos

Los objetivos del proyecto son:

- Realización de tareas de desarrollo de un nuevo conjunto de funcionalidades y módulos para el servicio de Gobierno Abierto.

- Realización del mantenimiento correctivo de los servicios de Gobierno Abierto.

- Ofrecer soporte técnico especializado en cuanto a la detección, diagnóstico y resolución de las incidencias técnicas derivadas del uso de los servicios de Gobierno Abierto.

1.3 Situación actual del proyecto

1.3.1 Antecedentes

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno , establecen un régimen jurídico específico para la transparencia en la actividad pública de las Administraciones Públicas.

Desde el pasado 1 de enero de 2016 está en vigor la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en todo lo referente al ámbito de la publicidad activa de las administraciones locales, constituyendo un hito muy relevante dentro

del proceso de regeneración y profundización de la democracia impulsado por todas las administraciones públicas catalanas.

Al amparo del Convenio Marco para colaborar en materia de transparencia, acceso a la información pública y buen gobierno, firmado el pasado 2 de junio de 2015 por la Generalitat, las Diputaciones, el Consorcio Administración Abierta de Cataluña, la Asociación Catalana de Municipios y la Federación de Municipios de Cataluña; el Consorci AOC tiene el encargo de ofrecer a las administraciones locales catalanas una serie de recursos para el cumplimiento de esta ley.

Entre estas tareas, destaca la de ofrecer una solución común de Espacio de la Transparencia para los entes locales que les permita cumplir con las obligaciones de la citada Ley, así como en la detección, configuración y puesta a disposición de los distintos conjuntos de datos en formato abierto e interoperable que la Ley obliga a publicar y que ya han sido, en algún momento, facilitados por los entes locales en alguna entidad supramunicipal.

En este sentido, se ha desarrollado una solución informática en un entorno web que permite la generación y subsiguiente gestión de un Espacio de la Transparencia que permite a los entes locales que así lo deseen de disponer de un Espacio propio de Transparencia y que contiene la información que obliga a publicar la normativa vigente en formato abierto e interoperable, es decir, en formato de datos abiertos. La información de esta solución está integrada dentro de la sede electrónica de cada ente local, dado que éste es el ámbito donde cada entidad pública gestiona sus servicios electrónicos de información y tramitación con garantías de seguridad y veracidad. Por este motivo, el Espacio de la Transparencia está concebido como un apartado de la sede electrónica.

La solución se estructura básicamente en 2 partes:

- una solución de gestión de portales y de contenidos para la entrada de información en la sede electrónica y en el Espacio de Transparencia.
- una plataforma de gestión de datos abiertos para la visualización y descarga e integración de información, que permite también a los entes publicar sus propios conjuntos de datos.

1.3.2 Situación actual

El servicio de Seu-e y Transparencia va dirigido a todas las administraciones públicas locales catalanas. La prestación de este servicio no comporta ningún coste para las administraciones públicas.

Dentro de los servicios de Gobierno Abierto la solución de Sede electrónica es utilizada actualmente por casi 1000 entes locales (entre ayuntamientos, consejos comarcales o entes locales dependientes). La sede electrónica permite cumplir con todos los requerimientos legales fijados por las leyes 39/15 y 40/15 de procedimiento administrativo común y régimen jurídico del sector público, y se encuentra perfectamente integrada con el ecosistema de los servicios de gobierno abierto y por tanto con los requerimientos de la Ley 19/14 de Transparencia. En este sentido cabe destacar que todos los entes que disponen de la solución de Sede electrónica necesariamente también cuentan con el Portal de Transparencia y datos abiertos, haciéndose así la mejor interrelación entre ambas aplicaciones (tanto a nivel tanto de contenidos internos que se enlazan, como nivel de gestión y edición de los portales que se convierte en común).

Si nos fijamos específicamente con el número de entes usuarios del Portal de Transparencia y datos abiertos cabe destacar que la cifra actual de usuarios es de más de 1.200 entes locales dados de alta. Y concretamente en el caso de los ayuntamientos catalanes, es importante destacar que el portal AOC de transparencia es el estándar de facto al ser la solución disponible en el 95% de los mismos. Paralelamente son ya 35 los entes locales que disponen del portal de datos abiertos con la posibilidad de autogestión de conjuntos de datos propios a publicar.

Se puede encontrar más documentación sobre el servicio así como el listado detallado de los usuarios de sede y transparencia en la web del Consorci AOC. Concretamente en:

- *Datos generales del servicio:*

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

- *Portal de soporte del servicio de gobierno abierto* (guías, manuales sobre cómo mejorar la visualización del portal a gestionar datos abiertos propios, FAQ's, modelo de solicitud...):

  https://www.aoc.cat/portal-suport /transparencia/idservei/transparencia/

- *Ejemplos del servicio de Seu-e, Transparencia y Datos Abiertas:*

  Sede electrónica: https://www.seu-e.cat/web/santjustdesvern

  Portal de Transparencia y datos abiertos: https://www.seu-e.cat/web/castellardelvalles

  Detalle entorno datos abiertos: https://seu-e.cat/ca/web/castellardelvalles/dades-obertes

El espacio de trabajo: la página principal de la Sede 2.0

La página principal de la Sede electrónica 2.0 está compuesta por los siguientes elementos:

- una cabecera compuesta por :
  - un buscador
  - un grupo de destacados
- un cuerpo central compuesto por tres grupos de elementos:
  - trámites
  - servicios
  - ítems de transparencia
- grupos de destacados: junto al buscador y debajo del cuerpo central
- un pie de página compuesto por:
  - indicadores
  - datos abiertos
  - atención a la ciudadanía

Puede ver la estructura de forma más visual en el siguiente enlace: https://www.seu-e.cat/web/santjustdesvern

El espacio de trabajo: espacio de gobierno abierto y transparencia

El espacio de trabajo *del espacio de gobierno abierto y transparencia*está compuesto por los siguientes elementos:

- La cabecera, idéntica a la cabecera de la*Sede electrónica 2.0.*
- Los ítems de transparencia agrupados por temáticas.
- El apartado*Ayúdanos a mejorar,* donde están todas aquellas iniciativas de participación ciudadana.
- Un pie de página compuesto por:
  - Indicadores.
  - Datos abiertos.
  - Participación ciudadana.

En paralelo existe la posibilidad de que los entes locales se personalicen y publiquen tanto en el hombre del portal como en la familia de información institucional y organizativa, un módulo específico de organización política que permite explicar de forma ágil, clara y descriptiva los ítems siguientes:

- Cartipás: organización política
- Cargos electos
- Grupos políticos/municipales
- Órganos de gobierno y funciones
- Altos cargos y cargos eventuales: perfil, datos de contacto, retribuciones y actividades y bienes

Por último también pueden incorporar en visualización un sencillo componente que permite mostrar tanto a la hombre como en el apartado de "Gestión económica" un resumen de indicadores económicos del ente, que muestra la evolución y comparativas con comarca, provincia y Cataluña. Este componente se genera de forma automática a partir de datos publicados en el portal de datos abiertos.

Puede ver la estructura de forma más visual en el siguiente enlace: https://www.seu-e.cat/web/castellardelvalles/govern-obert-i-transparencia

1.3.3 Los ítems de transparencia: clasificación

El Consorci AOC, a con la colaboración con la Red de Gobiernos Transparentes de Cataluña[1], ha elaborado una lista de unos 140 ítems de transparencia que contiene el espacio de transparencia y buen gobierno, para dar respuesta a los preceptos de la Ley 19/2014 y el Decreto 8/ 21 sobre la transparencia y el derecho de acceso a la información pública.

Más allá de ir dado cumplimiento principalmente a estas dos normas que contempla el ordenamiento catalán en transparencia, la estructura del portal pretende que la información esté estructurada de forma que sea fácil e intuitiva de localizar por parte del ciudadano y con un vocabulario comprensible .

1 La Red de Gobiernos Transparentes de Cataluña (XGT) es un marco de colaboración estable creado en 2015 para facilitar el cumplimiento de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno, a los más de 2.200 entes que componen la Administración local de Cataluña.

La creación de la Red proviene de un mandato parlamentario (Moción 179/X, de febrero de 2015, del Parlamento de Cataluña) que insta a la Generalitat a crear un espacio de colaboración con el mundo local para desplegar y aplicar la Ley en este ámbito competencial, facilitando las formas de cooperación necesarias entre las diferentes instituciones obligadas por ley.

La creación de la Red se materializó en la firma de un convenio marco de colaboración en cuatro grandes ámbitos, y fue impulsado por los siguientes entes: la Generalitat, mediante el Departamento de Políticas Digitales y Administración Pública; la Escuela de Administración Pública de Cataluña; el Consorcio de Administración Abierta de Cataluña; las cuatro diputaciones; la Asociación Catalana de Municipios y Comarcas, y la Federación de Municipios de Cataluña. En fecha 10 de noviembre de 2016, por acuerdo del plenario, se adhirió el Área Metropolitana de Barcelona.

Actualmente, la Red funciona a través de varios grupos de trabajo que tratan materias muy diversas: temas de transparencia, de publicidad activa, de buen gobierno, o de formación dirigida a los entes locales. La Red facilita el conocimiento y el intercambio de recursos jurídicos, tecnológicos y de formación.

En este sentido, estos ítems, se han clasificado a nivel temático, en los siguientes apartados y subapartados:

- Información institucional y organizativa:
    - Información institucional
    - Organización política y retribuciones
    - Empleados públicos
- Gestión económica:
    - Presupuesto
    - Gestión económica
    - Patrimonio
- Acción de gobierno y normativa:
    - Acción de gobierno y partidos políticos
    - Normativa, planes y programas
    - Urbanismo
    - Gestión documental y archivo
- Contratos, convenios y subvenciones:
    - Relación de contratos
    - Información de la contratación pública
    - Convenios y subvenciones
    - Concesionarias
- Catálogo de servicios y trámites:
    - Trámites
    - Servicios
    - Estado de los servicios
- Participación ciudadana

En el siguiente enlace s incluye una relación de los diferentes ítems de transparencia y su estructura: https://www.aoc.cat/knowledge-base/items-de-transparencia-i-govern-obert-disponibles-al-portal/idservei/transparencia/

Y puede ver un ejemplo de la implantación de esta estructura en el siguiente enlace:

https://www.seu-e.cat/web/castellardelvalles/govern-obe rt-i-transparencia

1.3.4 Los ítems de transparencia: fuentes de información

Estos ítems de transparencia provendrán de dos fuentes de información diferentes:

- *Fuente interna*: datos introducidos por el propio Ens.
    - Estos datos pueden proceder de ítems manuales sin estructura (que crea el propio ente), ítems manuales con estructura (los llena el ente sobre la propuesta de tabla / contenido definido en el ítem), o pueden ser ítems manuales completamente libres mediante la creación de nuevos ítems propios.
    - Estos ítems disponen de la posibilidad de complementarse con recursos (vistas, tablas, gráficas) de la información del portal de datos abiertos que se ofrece. Esta

fuente complementaria se encuentra sólo activa en aquellos entes (actualmente 35) que disponen de portal de datos abiertos con autogestión.

- *Fuente externa*: datos que el Consorci AOC ha recopilado de:
    - Las bases de datos de organismos supramunicipales a los que (por diferentes obligaciones) los entes locales deben enviar la información. Por ejemplo: del Departamento de Políticas Digitales y Administración Pública, de los diarios oficiales, Sindicatura de Cuentas, etc.
    - Las bases de datos de servicios prestados por el Consorci AOC. Por ejemplo, e-Tablero, Perfil del Contratante, etc.

De esta forma facilitaremos el trabajo administrativo de los entes locales, garantizando que la numerosa información pública que éstos envían a organismos supramunicipales o que se genera con el uso de los productos y servicios del Consorci AOC se publicará automáticamente en el servicio de transparencia, con el objetivo de evitar duplicar tareas administrativas de envío o publicación de información.

En relación con cada uno de los ítems, desde el Consorci AOC, se ha realizado un modelado de datos de cada uno de los ítems. Esto es, la identificación de cada uno de los campos de información que debe tener cada uno de los ítems de transparencia.

1.3.5 La personalización de la sede-e y los espacios de transparencia

En relación con la personalización de la solución de sede-e y espacio de transparencia, pueden editarse los siguientes elementos:

- Sede-e:
    - Destacados compartidos con espacio de transparencia
    - Cuerpo central
    - Destacados propios
- Espacio de transparencia:
    - Destacados compartidos con sede-e
    - Ítems de transparencia
        - Visualización o no de los ítems
        - Visualización o no de los datos automáticos
        - Visualización o no de los datos manuales
        - Incorporación de datos manuales
        - Eliminación de datos manuales
        - Elaboración de borradores
        - Descartar borradores
        - Incorporación de ' ítems propios
        - Interacción de los ítems con recursos (tablas, mapas, gráficas...) desarrollados a partir de datos abiertos propios

1.3.6 Marco legislativo aplicable

Las sedes electrónicas y espacios de transparencia generados con esta herramienta deben cumplir con los requisitos legales establecidos por el marco que las regula. De forma general, los requisitos legales establecidos por las leyes:

- Ley 59/2003, de 19 de diciembre de firma electrónica.
- Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas catalanas
- Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Transpone la Directiva 2003/98/CE, de 17 de noviembre de 2003.
- Ley 18/2015, de 9 de julio, de modificación de la Ley 37/2007, de 16 de noviembre, sobre la reutilización de la información del sector público
- Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas
- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público
- Ley 56/2007, de impulso de la sociedad de la Información

Y de forma específica, en el ámbito de transparencia en la siguiente normativa:

Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y buen gobierno.

- Ley 19/2014, de 29 de diciembre, de Transparencia, acceso a la información pública y buen gobierno.
- Decreto 8/21 sobre la transparencia y el derecho de acceso a la información pública

Por otra parte, el servicio también da cobertura a los requerimientos de los siguientes indicadores:

- los indicadores de Transparencia Internacional
- los indicadores Infoparticipa de la Universidad Autónoma de Barcelona

Para más información se puede consultar:

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

https://www.aoc.cat/portal-suport/transparencia/idservei/transparencia/

1.4 Descripción del servicio

Este proyecto se centrará en las siguientes actividades:

Desarrollo de nuevos módulos, servicios, funcionalidades o mejoras según el siguiente procedimiento (micro-proyecto):

- El Consorci AOC proporcionará la información funcional y técnica suficiente para que el adjudicatario pueda realizar el análisis de la solución a implementar. Esta valoración se realizará en tiempo no superior a 10 días laborales. La propuesta deberá detallar:
    - Tiempo previsto de ejecución
    - Esfuerzo por perfil
- El adjudicatario realizará el análisis detallado y el diseño técnico de la solución y el Consorci AOC deberá validarlos.
- Una vez aprobada la propuesta por parte del Consorci AOC y fijado el calendario de ejecución, la empresa adjudicataria asumirá el desarrollo completo de la solución y la codificación del mismo de acuerdo a la metodología que se describe en el presente documento. Las desviaciones sobre el mismo, no imputables a cambios en la definición, podrán ser imputadas a la empresa adjudicataria, en función de la gravedad y el impacto a criterio del Consorci AOC.
- Gestión y control del código fuente. Esta gestión se llevará a cabo con el sistema centralizado de código fuente que dispone el Consorci AOC (basado en el sistema de control de versiones GIT).
- El adjudicatario será el responsable de la definición del plan de pruebas, de integración y de rendimiento, en su caso, y de su ejecución en los entornos de integración y preproducción. El adjudicatario por tanto será el responsable del control de calidad y de validar el buen funcionamiento de los evolutivos tanto a nivel funcional como técnico.
- El adjudicatario deberá preparar los paquetes de despliegue para los entornos de preproducción y producción, de acuerdo al procedimiento de despliegue definido por el Consorci AOC.
- El adjudicatario deberá elaborar la documentación técnica y los manuales de usuarios correspondientes, así como mantener actualizada la documentación existente
- . El adjudicatario deberá prestar la formación a los usuarios que determine el Consorci AOC cuando éste lo considere necesario.

Los evolutivos a implementar podrán responder a distintas necesidades:

- Evolutivos funcionales: tienen que ver con las funcionalidades que se desean incorporar o modificar del servicio, basados en las necesidades detectadas por la AOC y también con la colaboración de la de gobiernos Transparentes.
- Evolutivos de carácter legal y/o normativo: tienen que ver con el cumplimiento de la normativa vigente.
- Evolutivos de cariz técnico: tienen que ver con necesidades de carácter tecnológico (mejoras en la arquitectura base, actualización del software base y/o de librerías, mejoras de rendimiento en determinadas funcionalidades, mejoras en el nivel de seguridad del servicio... etc .Para

cada uno de estos micro-proyectos el adjudicatario deberá proporcionar los siguientes entregables:

- Diseño funcional
- Diseño técnico
- Planes de pruebas unitarias y de integración
- Manual de explotación
- Documentación para el CAU
- Código fuente en el sistema centralizado del CAOC
- Despliegue en entorno de desarrollo
- Procedimiento de despliegue en PRE y PRO

Mantenimiento correctivo

- , incluyendo tanto incidencias a nivel funcional, como de rendimiento.

- serviciotareas de mantenimiento correctivo que el Consorci AOC determine que es necesario implementar con carácter o gente, se priorizarán por delante de de mantenimiento evolutivo que se estén realizando en el momento de la incidencia. Estas tareas, se someterán al control del Acuerdo Nivel de Servicio derivado de la categoría de la incidencia que ha originado el correctivo, y las penalizaciones asociadas se tratarán siguiendo estos criterios.

- Los informes de seguimiento tendrán que reflejar estos correctivos realizados, y los Niveles de Servicio conseguidos para cada uno de ellos. Se contemplará finalizado el correctivo cuando las pruebas en el entorno de preproducción determinen la validez del mismo. El equipo responsable de realizar el correctivo, deberá realizar la documentación necesaria para la subida en el entorno de preproducción y su correspondiente validación conjuntamente con el equipo de Tecnología del Consorci AOC.

Apoyo de tercer nivel

El servicio de apoyo avanzado consiste en realizar todas aquellas tareas necesarias para dar respuesta a todas aquellas consultas que plantee el Consorci AOC en relación con el servicio de Gobierno Abierto.

Los tipos de consultas pueden ser varios:

- Consultas relacionadas con cualquier funcionalidad del servicio.
- Consultas relacionadas con el diseño de cualquiera de los módulos de la aplicación.
- Consultas relacionadas con la forma en que se utiliza de cualquiera de las funcionalidades de la aplicación.
- Consultas relacionadas con respuestas que el Consorci AOC considere inesperadas del servicio.
- Consultas relacionadas con los mensajes de error obtenidos del servicio.
- Consultas relacionadas con la configuración vigente del servicio.
- Consultas relacionadas con los estándares y normativas en las que se basa el servicio.

Control de calidad

El adjudicatario será el responsable del control de calidad del servicio en todos aquellos desarrollos de nuevos evolutivos y correctivos que realice. En particular deberá llevar a cabo las siguientes tareas:

- Definición de los indicadores y métricas de calidad que deben cumplir los evolutivos/correctivos e identificar las medidas que se utilizarán para evaluar la calidad.
- Creación de un modelo de gestión de la calidad que asegure y garantice los acuerdos de nivel de servicio (ANS) definidos.
- Control de calidad de los evolutivos. Validación del correcto funcionamiento de éstos tanto a nivel funcional como técnico. Ejecución de pruebas unitarias y de integración. Ejecución de pruebas funcionales y de regresión. Ejecución de pruebas de rendimiento, en su caso.
  Apoyo a los equipos de desarrollo mediante la definición de los estándares y directrices que deben cumplir todos los evolutivos para ser certificados.
- Revisión y auditoría del cumplimiento de estos estándares/directrices para asegurar que se siguen los procedimientos establecidos.
- Revisión y seguimiento de la calidad de la documentación generada por los equipos de desarrollo.
- Comunicación y formación a los usuarios que determine el Consorci AOC.
- Apoyo a los usuarios durante la fase de implantación y aceptación de los evolutivos de acuerdo con la metodología descrita en el anexo 2.

Todas estas actividades estarán directamente dirigidas y coordinadas por el Consorci AOC. Será responsabilidad del adjudicatario velar y preocuparse de recaudar todos y cada uno de los requerimientos que afecten a la solicitud de los evolutivos y correctivos.

1.5 Requerimientos técnicos

1.5.1 Infraestructura necesaria para llevar a cabo el proyecto

El adjudicatario aportará las infraestructuras informáticas, licencias de desarrollo y cualquier otro componente o medio técnico necesario para la realización de los trabajos.

Para los tests unitarios el adjudicatario deberá disponer de un entorno de integración en sus instalaciones para realizar el control de calidad de los evolutivos desarrollados. En el anexo 1 se incluye una descripción de la infraestructura tecnológica del servicio.

Se utilizarán las mismas herramientas de desarrollo que han servido para crear el software (indicadas detalladamente en el anexo 1), pero si se considera beneficioso para el proyecto se podría migrar a versiones más recientes de estas herramientas o incorporar nuevas.

Entre otras, las siguientes:

- Sistema de desarrollo de software: gestor de contenidos Liferay 6.2 (basante con tecnología J2EE) para la gestión de los diferentes catálogos de trámites integrados dentro del proyecto de sede electrónica y transparencia ya existente y que da servicio a más de 1200 organismos generales de la parte web visible con toda la ciudadanía de Cataluña como potencial usuario.
- Servidor Web: apache 2.4 y tomcados 8 balanceados.
- Sistema de base de datos: Oracle 12, SQLServer 2008.
- Servidor de datos abiertos: CKAN
- El adjudicatario mantendrá en todo momento la actualización del código fuente en el sistema de Control de Versiones del Consorci AOC (GIT).

- La ejecución de las tareas encomendadas se tendrán que poder llevar a cabo en las instalaciones del adjudicatario, pero es posible que en alguna ocasión sea necesario el desplazamiento de alguno de los miembros, del adjudicatario a las instalaciones ciones del Consorci AOC.

Para cada ámbito de los anteriormente descritos será necesario disponer de la descripción detallada del conjunto de actuaciones que se prevean, el detalle de la tecnología y herramientas que se utilizarán en cada caso, así como el grado de compatibilidad de cada propuesta con el servicio actual .

1.5.2 Propiedad intelectual

El adjudicatario acepta expresamente que la propiedad 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 el adjudicatario pueda conservar, ni obtener copia de los mismos o facilitarlo a terceros.

La empresa adjudicataria no podrá 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, directa o extractada, original o reproducida, sin autorización expresa del Consorcio AOC, que la daría, en su caso, previa petición formal del adjudicatario con expresión del fin.

1.6 Equipo de proyecto

Para garantizar la máxima eficiencia, control y coordinación del servicio objeto de este contrato, la empresa adjudicataria tendrá que disponer de un equipo con un amplio conocimiento y experiencia tecnológica y funcional para ejecutar de forma eficiente las tareas las descritas en este pliego técnico.

En el sobre A deberá acreditarse la solvencia técnica de la empresa y del equipo.

La ejecución del proyecto en relación a las horas y el importe podrá no ser proporcional a la duración del contrato, sino que deberá adaptarse a las necesidades y requerimientos del servicio, pudiendo fluctuar en función de la carga de las tareas encomendadas, habiendo meses en los que se pueda requerir un mayor o menor dimensionado del equipo de trabajo.

El adjudicatario debe garantizar que para la resolución de incidencias y para dar respuesta a las peticiones urgentes de operación siempre habrá un mínimo de una persona disponible (este requerimiento incluye explícitamente períodos vacacionales, días semi festivos, puentes, etc. .).

El Consorci AOC realizará, en su caso, entrevistas a las personas del equipo de proyecto propuesto y, si es necesario, pedirá alternativas a las personas presentadas.

El Consorci AOC se reserva el derecho a solicitar 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.

1.6.1 Prestación temporal del servicio

El número mínimo y máximo de horas de los servicios a prestar está concretado en el pliego administrativo, apartado de Criterios de Valoración (H2), sección “Mediante cifras o porcentajes obtenidos a través de fórmulas”.

En caso de baja de cualquiera de los miembros del equipo, el adjudicatario deberá sustituirle en menos de 15 días laborables de acuerdo con los responsables del Consorci AOC. Cualquier cambio en uno de los miembros del equipo a instancia del adjudicatario deberá ser pactado con el Consorci AOC. En estos casos, se fijará un tiempo de 2 semanas de formación/adaptación del nuevo miembro que correrán a cargo del adjudicatario.

1.7 Condiciones de ejecución

1.7.1 Obligaciones básicas

El adjudicatario deberá cumplir las siguientes obligaciones básicas:

- El adjudicatario deberá gestionar cualquier alteración del servicio en las condiciones expresadas en este pliego.
- El adjudicatario tendrá que realizar reuniones periódicas con el Consorci AOC para exponer el cumplimiento del servicio y tratar los posibles problemas o mejoras del servicio.
- El adjudicatario deberá realizar la formación de los técnicos designados, en todos aquellos aspectos que el Consorci AOC crea oportunos y que sean de directa aplicación a los servicios requeridos.
- Toda la documentación generada por el equipo será en catalán y en el formato propuesto por Consorci AOC.
- Presentación de informes mensuales de presentación del servicio de acuerdo con los indicadores que el Consorci AOC considere apropiados:
    - Informe resumen de las actuaciones ya resueltas (micro-proyectos) 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.
- Actualización del software y bases de datos para incorporar los evolutivos.
- Elaboración de la documentación técnica.
- Elaboración de manuales y otra documentación destinada a la formación de los usuarios.
- Informe de fin del contrato con el resumen de horas y tareas realizadas.

1.7.2 Horario

El horario a cubrir será de 40 horas semanales, con horario de 08:30 ha 18 h de lunes a viernes durante todo el año. El calendario de festivos será el que aplique el Consorci AOC. Cualquier cambio deberá pactarse con el Consorci AOC.

Los días que sea necesario realizar despliegues a producción la empresa adjudicataria se pondrá a disposición del Consorci AOC en el horario que éste determine en función de las necesidades del servicio.

1.7.3 Herramientas de gestión y control

El adjudicatario será responsable de:

- La ejecución formal de los procesos de gestión tanto por el desarrollo de evolutivos como del mantenimiento correctivo definidos y aprobados por el Consorci AOC.

- Proponer las herramientas adicionales a las herramientas corporativas del Consorci AOC que deben permitir el seguimiento y el control global del contrato.

- El Consorci AOC se reserva el derecho a validar, y en su caso definir, las herramientas que deban utilizarse para la gestión y control del servicio.

1.7.4 Garantía

Las tareas objeto del contrato tendrán una garantía de 6 meses. Durante este período, el adjudicatario se compromete a resolver satisfactoriamente todas aquellas incidencias o defectos detectados en cualquiera de las actividades llevadas a cabo por sus equipos de trabajo que le sean imputables con él por acción u omisión.

1.7.5 Plan de transición y devolución del servicio

El adjudicatario tendrá que asumir el plan de transición para hacerse cargo del servicio. Al término del servicio el adjudicatario tendrá que planificar y ejecutar el plan de devolución del servicio en caso de cambio de proveedor. El plan de transición tendrá que tener una duración de 1 mes con una dedicación mínima de 160h. Tanto la duración (1 mes) como la dedicación (160h) serán adicionales a la prestación principal del servicio de 12 meses.

El adjudicatario deberá devolver el código fuente y todas las actualizaciones realizadas.

El Consorci AOC proporcionará al adjudicatario todas las contraseñas necesarias para la explotación del servicio y las modificará a la finalización del servicio. El adjudicatario no podrá modificar las palabras de paso sin el consentimiento explícito del Consorci AOC.

1.8 Seguridad

1.8.1 Clasificación de la información y el servicio

Para determinar las medidas de seguridad aplicables para proteger los datos y el servicio, se ha clasificado la información y el servicio en función del valor que ésta tiene para la organización.

La clasificación del sistema se ha realizado siguiendo las guías de Agencia Catalana de Ciberseguridad y del Esquema Nacional de Seguridad.

Según la guía GUIT049-C de la Agencia Catalana de Ciberseguridad, la clasificación de la información se puede medir en 5 niveles (Muy crítico, Crítico, Sensible, Interno y Público) y la clasificación del servicio en 4 niveles (Esencial, Estratégico, Importante y Básico).

Denominación del subsistema	**Servicio (Disponibilidad)**	**Información (Seguridad)**	**RTO/RPO**
Servicio de Gobierno Abierto	Básico	Interno	5 días/1 día

La clasificación del sistema según el Esquema Nacional de Seguridad se ha realizado siguiendo la guía CCN-STIC 803. Según esta metodología la clasificación del sistema se puede medir en 3 niveles (Alto, Medio y Bajo).

La clasificación del servicio según esta metodología es:

Denominación del subsistema	**Tipo**	**C**	**Y**	**D**	**En**	**T**	**DP**
Servicio de Gobierno Abierto	Información y servicio	B	B	B B	B	B	B
La valoración del sistema es baja (C=B, I=B, D=B, A=B, T=B, DP=B)							

1.8.2 Medidas de seguridad que deben incorporar los Servicios

Durante el tiempo de ejecución del contrato, el adjudicatario deberá implementar las medidas de seguridad de nivel BAJO del Esquema Nacional de Seguridad descritas en el Anexo 3, “Medidas de seguridad de nivel Baix” que afectan directamente a los Servicios como solución y plataforma tecnológica.

1.8.3 Medidas de seguridad que debe cumplir el adjudicatario

Durante el tiempo de ejecución del contrato, el adjudicatario deberá implementar las medidas de seguridad en sus procesos internos de nivel bajo del Esquema Nacional de Seguridad. Concretamente son las descritas en el Anexo 4. Requisitos de seguridad (ENS) por los proveedores de servicios.

El Consorci AOC auditará en un plazo no superior a 6 meses, que el adjudicatario cumple con los requerimientos. La auditoría se realizará mediante la entrega de evidencias indicadas en el anexo.

El adjudicatario estará exento de la auditoría si aporta una certificación vigente del Esquema Nacional de Seguridad de nivel bajo expedido por una empresa certificadora independiente y homologada.

En caso de auditoría externa de la plataforma de Gobierno Abierto, el adjudicatario deberá participar en la auditoría en las tareas que le correspondan, entregando las evidencias que el auditor reclame y realizando las adecuaciones necesarias que les correspondan.

1.8.4 Apoyo en la declaración de Conformidad con el Esquema Nacional de Seguridad

El adjudicatario deberá apoyar al Consorci AOC en la Declaración de Conformidad con el Esquema Nacional de Seguridad aportando las evidencias que sean necesarias para justificar que se cumplen todos los controles de seguridad descritos en los puntos 1.8.2 y 1.8.3.

1.8.5 Control de acceso al sistema

El adjudicatario deberá adaptarse en todo momento a los mecanismos de control de acceso a los sistemas de información que imponga la AOC para acceder a sus sistemas.

1.8.6 Control de personal

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

En caso de baja de un usuario, de forma inmediata el adjudicatario deberá tramitar la revocación de sus derechos de acceso a los sistemas.

1.8.7 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 de la AOC en sus sistemas o en soportes portátiles como USBs, DVDs, portátiles, tabletas, etc. En caso de tener que hacerlo habrá que pedir la autorización de la AOC y que el soporte esté cifrado.

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

Estos archivos temporales deben ser borrados una vez haya dejado de ser necesarios para la finalidad que motivó su creación.

Al finalizar la relación entre la AOC y el adjudicatario, éste deberá entregar toda la información propiedad de la AOC (procedimientos, código fuente, etc.) y realizar un borrado seguro de los soportes donde ésta esté almacenada.

1.8.8 Protección de los soportes

El adjudicatario no puede descargar información de la AOC en sus sistemas.

1.8.9 Requerimientos de protección de datos

Por cada ámbito objeto de análisis que comporte el tratamiento de datos de carácter personal será necesario realizar un informe de las medidas a adoptar para implantar las medidas de privacidad desde el diseño y por defecto para dar cumplimiento a los requerimientos establecidos en el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales ya la libre circulación de estos datos ya la Ley orgánica 3/2018 , de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, el informe deberá contener el análisis de qué principios del Reglamento permite dar cumplimiento a cada una de las medidas aportadas, justificándolo también en base a la normativa específica que regula el ámbito de actuación de las administraciones usuarias del servicio y la adecuación de cada medida propuesta por su propósito de cumplir los principios de protección de datos y reducir el riesgo por los derechos y libertades.

Habrá que tener en cuenta como mínimo las Guías publicadas tanto por el Comité Europeo de protección de Datos como por la Agencia Española de Protección de Datos y las que pueda publicar la Autoridad Catalana de Protección de Datos.

1.9 Acuerdos de Nivel de Servicio

Cuando se ponga en marcha un nuevo evolutivo puede suceder que se generen incidencias de carácter funcional y tecnológico que impidan el funcionamiento operativo de la aplicación por parte de los usuarios. Para solucionar estas incidencias se establece el siguiente procedimiento de trabajo y Acuerdo de Nivel de Servicio (ANS):

Definiciones:

Nivel	Descripción
Bloqueante	Una incidencia se catalogará con criticidad bloqueando si impide la utilización total del servicio a todos los usuarios del mismo.
Alta	Una incidencia se catalogará con alta criticidad si impide la utilización de una parte concreta del servicio, a todos o algunos usuarios, y la afectación por el negocio es elevada.
Media	Una incidencia se catalogará con criticidad media si impide la utilización de una funcionalidad concreta de alguno de los servicios a todos o algunos usuarios externos a la plataforma y la afectación por el negocio es relativamente baja.
Baja	Una incidencia se catalogará con criticidad baja si no impide la utilización ni parcial ni total de alguno de los servicios a ninguno 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 es 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 tiene en cuenta los posibles incrementos de tiempo provocados por la intervención inevitable de terceros en el proceso de resolución (por ejemplo, soporte de Oracle, intervención de otros organismos, etc.). ..).

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

Criticidad Incidencia	Tiempo de respuesta (horas)	Tiempo de resolución (horas)	Horario	% de resolución dentro del tiempo comprometido
0 Bloqueando	0, 5	2	horario garantizado	95 %
1 Alta	1	16	horario garantizado	95 %
2 Media	1	40	horario garantizado	95 %
3 Baja	1	64	horario garantizado	95 %

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

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

1.10 Modelo de relación

El adjudicatario tendrá que explicar en su propuesta cuál es el modelo de relación que propone para garantizar el éxito del proyecto.

Sin embargo, como mínimo, será necesario que se establezca los siguientes niveles de interlocución:

Reuniones de estrategia y dirección con las siguientes características:

- Interlocutores: responsable del servicio por parte del adjudicatario. Jefe de servicio del servicio por parte del Consorci AOC.
- Periodicidad: 1 mes
- Objetivo: realizar el seguimiento del contrato, analizando diversos aspectos: productividad, control de horas, temas de facturación, seguimiento de metas (a alto nivel), etc.
- Entregables: actas de las reuniones, informes ejecutivos, informes con control de horas (hechas y pendientes) 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 jefe de servicio y el jefe de proyecto, o alguno de los técnicos asignados al proyecto.

- Objetivo: seguimiento del cumplimiento del ANS, rendimiento de la plataforma e incidencias más destacables.
- Entregables:

    - 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,...

La comunicación, gestión de las tareas, incidencias y propuestas de mejora se realizará mediante la herramienta JIRA y/o Teams del Consoci AOC.

1.11 Mejoras adicionales

Aparte de las prestaciones recogidas en este documento se valorarán todas aquellas prestaciones superiores o complementarias a las exigidas que las empresas licitadoras proporcionen en sus ofertas y que se consideren de valor añadido para facilitar la gestión del servicio.

Los ámbitos de estas mejoras adicionales están concretados en el pliego administrativo, apartado de Criterios de Valoración (H2), sección “Sujetos a juicio valor”.

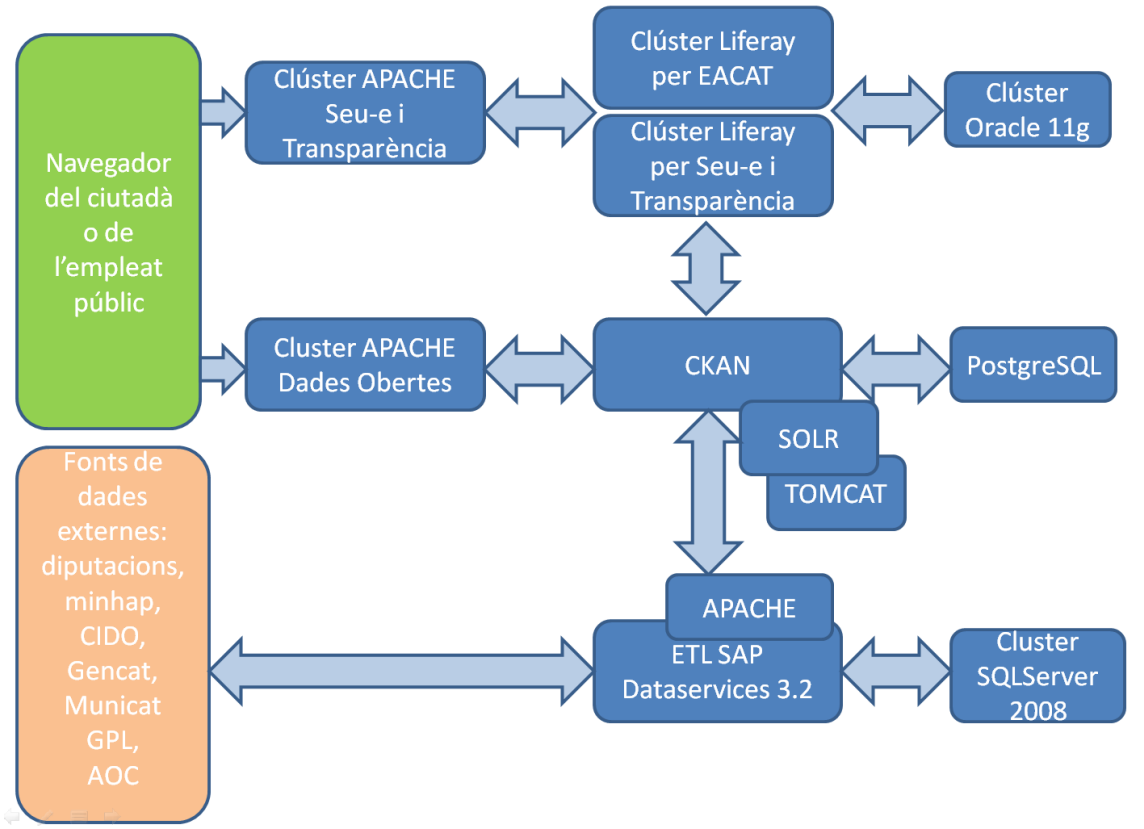
Barcelona, a 21 de junio de 2022

Manel Rella

Jefe de Proyectos

Subdirección de estrategia e innovación

ANEXO 1. Arquitectura del servicio de Gobierno Abierto



Servidor de aplicaciones

- Liferay 6.2
- Liferay 4.0
- CKAN
- ETL SAP Dataservices 3.2

Servidores de base de datos

- Oracle 12 (English)
- Microsoft SQL Server 2008 R2 Service Pack 1 (English)
- PostgreSQL
- Solr

BI

- Últimas versiones públicas de Tableau y Power BI

Anexo 2: Metodología de trabajo

Cada una de las versiones a desarrollar por el servicio de Gobierno Abierto debe tratarse como un proyecto propio que debería desarrollarse velando por el cumplimiento de esta guía metodológica.

A continuación se detallan las fases por las que debe pasar cada una de estas versiones desde su definición hasta su puesta en marcha.

Introducción de los evolutivos en el JIRA

El jefe de servicio traduce los objetivos estratégicos que marca el comité estratégico en las peticiones de mejora y evolutivos que deben permitir alcanzar estos objetivos. A continuación los introduce como Tarea y/o subtarea en el proyecto del JIRA que representa el propio servicio. En el momento de entrar cada asunto indica su prioridad ordenándolo según el número de versión que considera que sería el más adecuado para su implementación.

Fase de definición

La fase de definición de la versión consiste en seleccionar cuáles son los requerimientos funcionales que deben entrar a formar parte de la próxima versión a desarrollar. El jefe de proyecto estudia todos aquellos requerimientos que se pueden incluir en una ventana tipo que el Consorcio aplica a sus servicios (unos 3 meses entre la puesta en marcha de cada versión). El jefe de proyecto consensúa con el jefe de servicio el alcance de la versión y se confecciona la lista definitiva trasladando esta lista de peticiones a un proyecto específico del JIRA que representa a la versión a desarrollar.

El jefe del servicio informará al comité estratégico de las líneas maestras de actuación que englobará la versión mediante la elaboración de un breve documento de conceptualización de la versión. El responsable de servicio define el plan de comunicación que deberá realizarse antes de que la versión llegue a los usuarios finales.

El jefe de proyecto introduce toda esta información en el proyecto del JIRA que representa la versión e informa al comité de seguimiento en la próxima reunión. Finalmente, el jefe de servicio comunica la planificación al comité estratégico y/oa los promotores implicados.

Una vez cerrada la planificación de la versión no se aceptará modificación alguna en la lista de requerimientos a desarrollar hasta la próxima fase de definición de la nueva versión.

Análisis

El adjudicatario partirá de la recopilación de evolutivos a satisfacer que se han seleccionado en el JIRA para la nueva versión y deberá realizar las reuniones de toma de requerimientos (intentando que sean las mínimas reuniones posibles) para poder realizar la recaudación detallada de todos los requisitos solicitados. Será responsabilidad del adjudicatario velar y preocuparse de recaudar todos y cada uno de los requerimientos que afecten a la solicitud del evolutivo.

El adjudicatario elaborará un preanálisis de la solución que propone incluyendo una estimación del impacto que supone el evolutivo. En caso de que existan diferentes alternativas, el adjudicatario deberá explicarlas indicando las ventajas e inconvenientes de cada una.

El Consorci AOC decidirá si finalmente se lleva a cabo ese evolutivo y en caso afirmativo el adjudicatario realizará el análisis detallado de la solución incluyendo la propuesta de las interfaces de usuario, el plan de pruebas unitarias, de integración y rendimiento.

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 conjuntamente con el adjudicatario la planificación detallada de la versión asignando las tareas entre los distintos técnicos desarrollo.

Desarrollo

Las tareas que comportará esta fase son:

- Generación del código
- Ejecución de pruebas unitarias
- Ejecución de pruebas de integración
- Ejecución de pruebas de rendimiento, en su caso
- Elaboración de la documentación funcional y técnica.

El adjudicatario tendrá que hacer un uso frecuente del repositorio de código (GIT) del servicio para sincronizar los distintos 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 desarrolladores) sería hacerlo una vez al día (p. ej. a primera hora de la mañana) de forma que se detecte cuanto antes los conflictos entre los distintos desarrollos.

Antes de subir nada al repositorio, cada desarrollador deberá garantizar en el tamaño que sea posible que el código subido es íntegro. Si no es posible subir los cambios de forma diaria, sí que debe garantizarse que cada equipo de desarrollo subirá los cambios al menos con una frecuencia semanal.

En el repositorio de código se debe incluir todo tipo de cambio: código del servidor web, código de base de datos, cambios en la estructura de la base datos, scripts que de inicialización de datos, etc. Y también deberá incluirse la propia documentación.

Todos los scripts de base de datos deberán compactarse en un único archivo para facilitar su despliegue entre los diferentes entornos.

La codificación y las pruebas unitarias deben realizarse en el entorno de desarrollo de cada uno de los técnicos.

Fase de implantación y aceptación

En base a las entregas de la fase anterior se procederá a realizar la implantación del evolutivo sobre los distintos 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 el entorno de pre-producción y posteriormente al de producción.

En caso de que en este proceso los resultados obtenidos no sean los esperados (es decir, los que se obtuvieron en el entorno de desarrollo del adjudicatario) el adjudicatario deberá dar el apoyo necesario, si es necesario presencial, para solucionarlo lo.

Una vez realizada la ejecución del plan de pruebas con el 100% de las pruebas funcionando en el entorno de pre-producción y producción se dará el proyecto por cerrado. A partir de ese instante entrará en vigor el período de garantía del evolutivo.

A partir de ese momento ya debe entrar en vigor la etapa de apoyo, es responsabilidad del adjudicatario realizar las tareas necesarias de traspaso, formación y documentación del proyecto, de operación, y procedimental para que los nuevos desarrollos ya puedan ser objeto del servicio de soporte 24x7.

Implantación y aceptación

Una vez terminada la etapa de codificación y superadas las pruebas, el equipo de desarrollo deberá preparar el plan de implantación. El plan de implantación incorpora todas las acciones dirigidas a que la versión llegue a los usuarios finales. Hay que tener en cuenta que ninguno de los técnicos de desarrollo tiene 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. La petición de despliegue se enlazará con las diferentes peticiones de evolutivos/correctivos 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 debe haber llegado a más tardar el día de antes, para que se pueda preparar junto con el resto de despliegues de otros servicios del Consorci AOC.

El despliegue lo ejecuta el área de Explotación del Consorci AOC. Antes, el área de Explotación realiza un backup completo del entorno por si es necesario ejecutar el proceso de rollback.

Una vez desarrollado a preproducción, es el adjudicatario quien deberá ejecutar el plan de pruebas para realizar la validación final. El jefe 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 a producción (los despliegues en el entorno de producción se realizan los miércoles por la tarde). En caso contrario, el equipo de desarrollo realizará las correcciones necesarias dando todo el soporte necesario para solucionarlo en la mayor brevedad posible.

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

En la fase de implantación también se incluye el plan de comunicación definido por el responsable de servicio. El plan de comunicación incluye las diferentes acciones y formatos de comunicación asociados a la versión que el responsable de servicio deberá llevar a cabo, así como la formación y acompañamiento a los usuarios finales.

Pilotaje

Antes de la puesta en marcha definitiva a todos los usuarios finales, puede convertirse en necesario asegurar que la versión responde a las expectativas a través de la puesta en marcha controlada del servicio. La prueba piloto no sólo incluye el software sino todos los entregables asociados al plan de comunicación y formación.

Es importante destacar que la prueba piloto tiene todas las variantes posibles de ejecución de la solución. Además, la prueba piloto debe tener la duración necesaria para que se puedan validar todos los procesos reales que se han desarrollado en la nueva versión.

Evaluación

Una vez definidos los requerimientos que formarán parte de la versión, el jefe de proyecto define las métricas e 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 jefe 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 mando del servicio.

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

Por último, 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) para poder aprender y mejorar de cara a la nueva versión.

JIRA

El 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 adelanto de ésta, así como la evolución estratégica que seguirá el servicio en un futuro medio. Es por 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 jefe de proyecto por reflejar en el JIRA los distintos puntos de vista. Esta diferente visión se plasma en el JIRA a partir de los siguientes proyectos:

- **Servicio:** evolución estratégica del servicio a medio/largo plazo. En este proyecto del JIRA los requerimientos se agrupan y ordenan en ideas conceptuales cercanas a las líneas de actuación que marca el comité estratégico. Este proyecto permite obtener una idea global de lo que se pretende conseguir con el servicio a medio o largo plazo. El jefe de servicio es el principal responsable del mantenimiento en el JIRA de este proyecto y debe 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 distintos requerimientos funcionales y técnicos que debe 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/os que está/n 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 debe 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 se tercia, cualquiera de estos 2 proyectos principales se pueden complementar con otros proyectos que permitan agrupar líneas de actuación que se llevarán a cabo a largo plazo o bien que se llevarán a cabo en paralelo, pero en fechas diferentes. El objetivo de estos proyectos complementarios debe ser el de facilitar la lectura del estado presente y futuro del servicio a los distintos actores.

Anexo 3. Medidas de seguridad de nivel BAJO

Naturaleza	Grupo	Medida	Nivel	Descripción Nivel
Medidas de Organización	Normativa, procedimientos y estándares de protección de datos	Normativa	Básico	1. La Normativa de protección de datos debe plasmar de forma clara y precisa, al menos, el siguiente: a) Organización de protección de datos: - Designación del Delegado de Protección de Datos (DPD) de los tratamientos automatizados y no automatizados. - Designación del Comité o Comités para la gestión y coordinación de la protección de datos, detallando su ámbito de responsabilidad, sus miembros y su relación con otros elementos de la organización. - Designación del Responsable de ciberseguridad y cumplimiento de protección de datos. - Definición de los roles y funciones definiendo para cada uno los deberes y responsabilidades. b) Definición de la categorización de cada puesto de trabajo en materia de protección de datos que defina las funciones, deberes y obligaciones del personal; y los criterios y reglas de uso encaminados a la correcta utilización de las herramientas de trabajo y servicios. Debe incluir la responsabilidad de los usos indebidos y las medidas disciplinarias asociadas. c) Modelo de relación con la autoridad de control. d) Registro de Actividades de Tratamiento que deberá contener al menos los siguientes campos: - Nombre y datos de contacto del DPD, del Responsable del Tratamiento y, en su caso, del corresponsable y del representante del responsable. - Actividades y finalidades de los tratamientos. - Descripción de las categorías de datos y de los interesados. - Categorías de los destinatarios a los que se le han comunicado o comunicarán los datos, incluidos los destinatarios en terceros países u organizaciones internacionales. - Transferencias internacionales de datos. - Cuando sea posible, los plazos previstos para la supresión de las distintas categorías de datos. - Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad. e) Si se actúa como encargado del tratamiento, deberá llevar un registro de las categorías de actividades de tratamiento que lleva a cabo por cuenta

				de un responsable que deberá contener la siguiente información: - Nombre y datos de contacto del encargado y de cada responsable por cuenta de lo que actúe y, en su caso, del representante del responsable o del encargado y del DPD. - Categorías de tratamientos efectuados por cuenta de cada responsable. - Transferencias internacionales de datos. - Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad. f) Identificación de las actividades de tratamiento y sistemas de información asociados. g) Definición de los niveles de riesgo de las actividades de tratamiento y los criterios para la clasificación. h) Metodología de Evaluación de Impacto relativa a la Protección de Datos (AIPD). i) Identificación de las medidas de ciberseguridad asociadas a los distintos niveles de riesgo. 2. La normativa referida en este apartado deberá mantenerse en todo momento actualizada y será revisada siempre que se produzcan cambios relevantes. 3. Cualquier incumplimiento o excepción de la normativa deberá ser correctamente documentado.
		Procedimientos	Básico	1. Se dispondrá, como mínimo, de los siguientes documentos que detallen de forma clara y precisa cómo llevar a cabo los tratamientos automatizados: a) Control de acceso lógico (gestión de usuarios). Debe incluir el control de acceso a los datos que tienen limitado el tratamiento. b) Identificación y autenticación. c) Gestión de soportes. d) Copias de seguridad y restauración de datos. e) Control de acceso físico. f) Tratamiento de archivos temporales. g) Eliminación segura de información en la reutilización o destrucción de soportes y sistemas. h) Devolución de activos. i) Registro de accesos. j) Gestión de excepciones. k) Trabajo fuera de los locales del responsable de las actividades de tratamiento o encargados de los tratamientos. l) Notificación, registro y gestión de incidencias.

				m) Notificación de vulneraciones de seguridad. 2. Los documentos referidos en este apartado se mantendrán en todo momento actualizados y serán revisados siempre que se produzcan cambios relevantes.
		Procedimientos de autorización	Básico	1. Se establecerá un proceso formal de autorizaciones que cubra, como mínimo, los siguientes aspectos: a) Uso de dispositivos móviles (ordenadores portátiles, dispositivos móviles inteligentes, tabletas, agendas electrónicas , etc.). b) Uso de soportes (dispositivos ópticos (CD's, DVD's), discos duros externos, cintas y discos de copias de seguridad, unidades USB o pendrives, tarjetas de memoria (SD, microSD, etc.)). c) Salida de dispositivos móviles y soportes. d) Tratamiento fuera de los locales del Responsable del Tratamiento o Encargado del Tratamiento. e) Acceso remoto. f) Ejecución de los procedimientos de recuperación de datos. g) Entrada en producción y mantenimiento de equipos y aplicaciones. 2. Los documentos referidos en este apartado se mantendrán en todo momento actualizados y serán revisados siempre que se produzcan cambios relevantes.
	Conocimiento de la normativa, procedimientos y estándares de protección de datos	Deberes y obligaciones del personal	Básico	1. Se informará al personal de: a) Las funciones, deberes y obligaciones tanto durante el período que desempeña el puesto de trabajo como en caso de finalización de la asignación o traslado a otro puesto de trabajo. b) Los requisitos a cumplir respecto a los datos a los que ha tenido acceso, en particular, en términos de confidencialidad, tanto durante el período en el que ha sido adscrito como posteriormente a su finalización. c) Las medidas disciplinarias en caso de incumplimiento.
		Formación y concienciación	Básico	1. En coordinación con el DPD, deben llevarse a cabo las acciones necesarias para formar y concienciar regularmente al personal sobre su papel y responsabilidad en materia de protección de datos para que la seguridad de los tratamientos automatizados y no automatizados alcance los niveles exigidos. En particular, en lo que se refiere a: a) La normativa, procedimientos y estándares de seguridad relativa al buen uso de los sistemas y tratamientos en papel. b) La detección y reacción a incidentes de seguridad, actividades o comportamientos sospechosos.

				c) El procedimiento de notificación de incidentes y vulneraciones de seguridad. d) La gestión de la información en cualquier formato en el que se encuentre. Se cubrirán al menos las siguientes actividades: puestos de trabajo aseados, almacenamiento, transferencia, copias, distribución, destrucción y uso de ficheros temporales.
Medidas de Gestión	Protección de datos en el diseño y por defecto	Arquitectura de seguridad	Básico	1. Diseñar y configurar los sistemas y redes aplicando la regla de mínima funcionalidad y la seguridad por defecto. 2. El diseño de arquitectura de seguridad contemplará las instalaciones, sistemas, esquema de líneas de defensa y sistemas de identificación y autenticación. 3. Se configurarán de forma segura los equipos, previamente a su entrada en producción de forma que se apliquen medidas técnicas y organizativas que garanticen, por defecto: a) la limitación del tratamiento de datos por parte de los usuarios de los diferentes sistemas de información de acuerdo con las funciones que el usuario debe desarrollar. b) la retirada de cuentas y contraseñas por defecto. c) que no se proporcionen funciones innecesarias, ni de operación, ni de administración, ni de auditoría, de modo que se reduzca su perímetro al mínimo imprescindible. d) que no se proporcionen funciones que no sean de interés, ni sean necesarias e, incluso, las que sean inadecuadas al fin que se persigue. 4. Se debe mantener documentación tanto del diseño de arquitectura como de la configuración de los equipos. 5. De forma previa a la entrada en producción se realizará un análisis de vulnerabilidades. 6. Se solicitará autorización relativa a la entrada en producción y mantenimiento de equipos y aplicaciones.

		Desarrollo seguro	Básico	1. El desarrollo de aplicaciones debe realizarse sobre un sistema diferente y separado del de producción y no debe haber herramientas o datos de desarrollo en el entorno de producción. 2. Se aplicará una metodología de desarrollo reconocida que: a) Tome en consideración los aspectos de seguridad en todo el ciclo de vida. b) Utilice algoritmos, software y bibliotecas reconocidas. c) Contemple la generación y el tratamiento de pistas de auditoría que permita registrar las actividades de los usuarios tal y como se especifica en la medida Id 20 "Registro y protección de actividad de los usuarios". 3. De forma previa a la entrada en producción se realizará: a) Comprobación del correcto funcionamiento de la aplicación. b) Análisis de vulnerabilidades.
		Pruebas	Básico	1. Las pruebas deben realizarse en un entorno aislado del de producción. 2. Las pruebas anteriores a la entrada en producción o modificación no se realizarán con datos reales, salvo que se asegure que el entorno en el que se realicen las pruebas tenga implementadas las medidas de ciberseguridad establecidas por el nivel de seguridad del tratamiento de los datos.
	Gestión de accesos de los usuarios	Requisitos de acceso y segregación de funciones	Básico	1. Los requisitos de acceso deben atenerse a lo que se indica a continuación: a) Todo sistema de información debe disponer de mecanismos de autenticación para validar la identidad de los usuarios que acceden a ella. b) Los recursos del sistema deben protegerse con algún mecanismo que impida su utilización, salvo las entidades, usuarios o personas que disfruten de derechos de acceso suficientes. c) Los derechos de acceso de cada recurso deben establecerse según las decisiones de la persona responsable del recurso, y deben atenerse a la normativa de seguridad del sistema. d) Particularmente, se controlará el acceso a los componentes del sistema ya sus ficheros o registros de configuración.

		Identificación y autenticación	Básico	1. Antes de proporcionar las credenciales de autenticación a los usuarios, éstos deben haberse identificado y registrado de forma fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se prevén diversas posibilidades de registro de los usuarios: - Mediante la presentación física del usuario y la verificación de su identidad de acuerdo con la legalidad vigente, frente a un funcionario habilitado para ello. - De forma telemática, mediante DNI electrónico o un certificado electrónico calificado. - De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los que prevea la normativa aplicable. 2. Los mecanismos de autenticación empleados en cada sistema deben adecuarse al nivel del sistema y responder a los mecanismos autorizados en el Reglamento Europeo 910/2014 (eIDAS) y reglamentos de ejecución del mismo, así como el Protocolo de Identificación y Firma Electrónica, aprobado por la Orden GRI/233/2015, de 20 de julio, y la Política de Identificación y Firma Electrónica del Marco Normativo de Seguridad de la Información de la Generalidad de Cataluña. Los mecanismos pueden utilizar los siguientes factores de autenticación: - “Factores de conocimiento”: contraseñas o claves concertadas. Tienen que disponer de reglas básicas de calidad (extensión, tipos de caracteres, etc.). - “Factores de posesión”: componentes lógicos (como certificados de software) o dispositivos físicos (tokens, teléfonos móviles, dispositivos). - "Factores inherentes o propios del usuario": elementos biométricos. 3. En el ámbito básico se requerirá al menos un factor de autenticación. Los factores anteriores se pueden utilizar de forma aislada o combinarse para generar mecanismos de autenticación fuerte (ver niveles superiores). 4. La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación: a) Los identificadores de usuario deben cumplir con el MCPD y el Marco Normativo de la Seguridad de la Información de la Generalidad de Cataluña. b) Pueden utilizarse como identificador único los sistemas de identificación que prevea la normativa aplicable. c) Cuando el usuario tenga diferentes roles frente al sistema (p.ej. como

				ciudadano, como trabajador interno del organismo y como administrador de los sistemas), recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad. d) Cada entidad (usuario o proceso) que accede al sistema debe disponer de un identificador único de modo que: - Se puede saber quién recibe y qué derechos de acceso recibe. - Se puede saber quién ha hecho algo y qué ha hecho. 5. Las credenciales se gestionarán de la siguiente forma: a) Se activarán una vez estén bajo el control efectivo del usuario. b) Deben estar bajo el control exclusivo del usuario. c) El usuario debe reconocer que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida. d) Deben ser inhabilitados en los siguientes casos: cuando el usuario deja la organización por cualquier causa; cuando el usuario cesa en la función para la que se requería la cuenta de usuario; o cuando la persona que le autorizó da orden en sentido contrario. En definitiva, cuando termina la relación con el sistema. e) Se retendrán durante el período necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a los mismos. A este período se le denomina período de retención. f) Se revisarán periódicamente los identificadores y verificarán si es necesario que accedan a los sistemas de información. g) En caso de que sean contraseñas, deben configurarse según el estándar de contraseñas del Marco Normativo de Seguridad de la Información de la Generalidad de Cataluña. Concretamente, en lo referente a la complejidad, longitud, caducidad, limitación del número de intentos fallidos, reutilización y almacenamiento. En caso de utilizar OTPs éstos no tendrán una duración superior a 24 horas.

		Gestión de derechos de acceso de los usuarios	Básico	1. La asignación y uso de los privilegios de acceso debe estar restringida y controlada. La asignación de derechos de acceso privilegiados debe estar recogida en un proceso formal de autorización, de acuerdo con la normativa de control de acceso aplicable. Sólo el personal autorizado podrá conceder, alterar o anular la autorización de acceso a los recursos, de conformidad con los criterios establecidos por su propietario. 2. Los derechos de acceso de cada usuario se limitarán atendiendo a los siguientes principios: a) Mínimo privilegio. Los privilegios de cada usuario deben reducirse al mínimo estrictamente necesario para cumplir sus obligaciones. b) Necesidad de conocer. Los privilegios deben limitarse de forma que los usuarios sólo accedan al conocimiento de aquella información requerida para cumplir sus obligaciones. 3. La asignación de derechos debe tener en cuenta lo siguiente: a) Deberían identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso (p.ej. sistema operativo, sistema de gestión de BBDD, aplicaciones) junto con los usuarios a los que deben asignarse. b) Se autorizará la asignación de privilegios y se registrarán todos los privilegios asignados. Los derechos de acceso no deben hacerse efectivos hasta que se complete el proceso de autorización. c) Deben definirse los requisitos para el vencimiento de los derechos de acceso privilegiados. d) Los derechos de acceso deben asignarse a un identificador de usuario. e) Deben revisarse periódicamente los permisos asignados a los usuarios y verificar que se corresponden a sus funciones. f) En caso de que sea recomendable por criterios de eficiencia y no genere riesgos de seguridad, la asignación de permisos de usuario se podrá realizar en base a la definición y parametrización de roles, de acuerdo con lo establecido en el Marco Normativo de Seguridad de la Información de la Generalidad de Cataluña. g) Se deben establecer y mantener procedimientos para evitar el uso no autorizado del identificador de usuario, en especial en lo que se refiere a aquellas credenciales con permisos de administrador.

		Acceso local y remoto	Básico	Se considera acceso local el realizado desde puestos de trabajo dentro de las propias instalaciones de la organización y desde los recursos propios ubicados en dichas instalaciones. Se considera acceso remoto el realizado desde fuera de las propias instalaciones de la organización, a través de redes o recursos de terceros que no estén puestos a disposición específicamente como recursos locales o propios de la Generalidad de Cataluña. 1. Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implica proteger tanto el acceso en sí mismo como el canal de acceso remoto. La concepción de acceso remoto deberá aplicarse a las formas establecidas de Teletrabajo en el Marco Normativo de Seguridad de la Información de la Generalidad de Cataluña. 2. Los accesos tendrán que cumplir con las siguientes medidas según el nivel de los tratamientos: a) Se deben prevenir ataques que puedan revelar información del sistema sin llegar a acceder a ellos. La información revelada a la que intenta acceder debe ser la mínima imprescindible (los diálogos de acceso sólo deben proporcionar la información indispensable). b) El sistema informará al usuario de sus obligaciones, si fueran específicas, inmediatamente después de obtener el acceso. Esta información en relación con las obligaciones generales aplicables a los sistemas de la Generalidad se mostrará la primera vez que el usuario acceda al sistema. c) Pasado cierto tiempo de inactividad en la sesión del usuario, ya sea con el sistema o con una aplicación en particular, se cancelarán las sesiones abiertas desde dicho puesto de trabajo. 3. Se aplicarán a las conexiones en remoto las medidas de seguridad establecidas para el acceso local, siempre y cuando resulten adecuadas. En caso contrario, se definirán medidas equivalentes para alcanzar un nivel de seguridad equiparable.

	Gestión de Servicios Externos	Contratación y acuerdos de nivel de servicio	Básico	1. Se suscribirán, si son de aplicación los escenarios descritos, los siguientes contratos u otros actos jurídicos con los siguientes actores: a) Encargados del Tratamiento. Éstos deben establecer de forma clara y concisa, como mínimo: - Objeto. - Duración. - Naturaleza y finalidad del tratamiento (características del servicio prestado). - Tipo de datos personales. - Categoría de los interesados. - Obligaciones, responsabilidades y derechos del Responsable. - Obligaciones, responsabilidades y derechos del Encargado según el clausulado del artículo 28.3 RGPD. - Medidas técnicas y organizativas que ofrezcan unas garantías suficientes de acuerdo al nivel de riesgo de los datos. - Niveles de servicio (tiempo de respuesta en caso de violaciones de seguridad, resolución de incumplimientos, etc.). - Consecuencias del incumplimiento. - Devolución o destrucción de los datos en la finalización del encargo. b) Prestadores de servicios sin acceso a datos. Éstos deben establecer de forma clara y concisa, como mínimo: - Naturaleza y finalidad del servicio. - Prohibición de acceder a datos personales. - Obligación de deber de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación de servicio. - Consecuencias del incumplimiento. 2. Los Encargados del Tratamiento deben suscribir contratos u otros actos jurídicos con los subencargados que utilicen para llevar a cabo determinadas actividades de tratamiento. Éstos tendrán que establecer, como mínimo, las mismas obligaciones de protección que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado. Las subcontrataciones deben estar autorizadas por el Responsable del Tratamiento. 3. El Responsable del tratamiento debe identificar las actividades de los tratamientos y sistemas de información tratados por cuenta de terceros con referencia expresa al encargado, al contrato o documento que regule las condiciones y la vigencia del encargo. 4. Si se actúa como Encargado del Tratamiento se deben identificar y registrar las actividades de tratamiento y sistemas de información que trata por cuenta de terceros, en su caso, con referencia expresa al Responsable del tratamiento, al contrato o documento que

				regule las condiciones y la vigencia del encargo. 5. En caso de disponer de encargados de tratamiento, el Responsable deberá establecer un sistema de garantías para acreditar la calidad y adecuación profesional del encargado de tratamiento. Éste deberá introducirse en los modelos de acreditación de la solvencia técnica en los procedimientos de contratación y se podrá basar en la acreditación profesional mediante certificados y modelos de cumplimiento voluntarios (como por ejemplo códigos de conducta) reconocidos a nivel nacional y/o internacional.
Medidas de Protección	Protección de las instalaciones e infraestructuras	Acondicionamiento de los locales	Básico	1. Los locales donde se ubiquen los sistemas de información y sus componentes deben disponer de elementos adecuados para el funcionamiento eficaz del equipamiento instalado allí. Y, especialmente: a) Condiciones de temperatura y humedad. b) Energía eléctrica, y sus tomas correspondientes, necesaria para funcionar, de forma que se garantice el suministro de potencia eléctrica y el correcto funcionamiento de las luces de emergencia. c) Protección contra las amenazas identificadas en el análisis de riesgos. d) Protección del cableado contra incidentes fortuitos o deliberados. 2. Se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general y garantizará el tiempo suficiente para que finalicen ordenadamente los procesos, salvaguardando la información.

		Control de acceso físico	Básico	El equipamiento debe instalarse en áreas específicas para su función (áreas de CPDs o salas técnicas, edificios o ubicaciones donde se encuentre ubicado este equipamiento). Se controlarán los accesos a las áreas indicadas de forma que sólo pueda accederse por las entradas previstas y vigiladas. 1. Deben quedar registradas la entrada y salida de las personas en las áreas separadas y concretamente la identificación de la persona, la fecha y hora de entrada y salida. 2. El registro de accesos debe estar controlado por una persona autorizada.
		Registro de entrada y salida de equipamiento y soportes	Básico	Se debe garantizar que el equipamiento y los soportes están bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un sitio a otro. A tal efecto: 1. Se llevará un registro detallado de cualquier entrada y salida de equipamiento y soportes de los CPDs, salas técnicas, edificios o ubicaciones donde se encuentren estos equipamientos o soportes, incluyendo la identificación de la persona que autoriza el movimiento. El registro debe reflejar: fecha y hora, identificación inequívoca del equipamiento, persona que realiza la entrada o salida, persona que autoriza la entrada o salida y persona que realiza el registro. 2. Se elaborará una lista de servicios autorizados de transporte o mensajería a utilizar. 3. Se debe disponer de un procedimiento informal que compare las salidas con las llegadas para detectar algún incidente.
	Monitorización de la actividad e incidencias	Controles de auditoría de los sistemas de la información	Básico	1. El Responsable de tratamiento deberá tener un modelo de cumplimiento que permita el seguimiento, revisión y autoevaluación de las medidas de seguridad aplicadas a los tratamientos de datos de carácter personal. Este modelo de cumplimiento debe permitir acreditar y disponer de las evidencias pertinentes para acreditar el nivel de cumplimiento en relación con el presente MCPD o con las medidas excepcionales que se hayan determinado en las correspondientes AIPD.

		Registro y protección de la actividad de los usuarios	Básico	1. Se deben registrar las actividades de los usuarios en el sistema, de modo que: a) El registro debe indicar quién realiza la actividad, cuándo la realiza y sobre qué información y las actividades efectuadas con éxito y los intentos fallidos. b) Se incluirá la actividad de los usuarios y, en especial, la de los operadores y administradores cuando puedan acceder a la configuración y actuar en el mantenimiento del sistema. c) La determinación de qué actividades deben registrarse y con qué niveles de detalle deben adoptarse a la vista del análisis de riesgos realizado sobre el sistema y las capacidades del mismo. 2. Se deben activar los registros de actividad en los servidores. 3. El período de conservación de la información se regirá por la normativa de gestión de trazas del Marco Normativo de Seguridad de la Información de la Generalidad de Cataluña (18 meses). 4. En caso de producirse incidentes o un incremento de riesgo en relación con amenazas o bien se produzca un requerimiento de carácter legal, se podrá recuperar, revisar y analizar la información asociada a esta actividad siempre aplicando criterios de necesidad, idoneidad y proporcionalidad .
		Gestión de incidentes y sistema de notificaciones de incidentes	Básico	1. Se establecerá un registro de incidentes en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso , detectado, la persona que hace la notificación, a la que se le comunica, los efectos derivados y las medidas correctoras aplicadas. Además, se tendrán que registrar las restauraciones de copias de seguridad, indicando la persona que realiza el proceso, los datos restaurados y los datos que hayan tenido que grabar manualmente en el proceso de recuperación.
	Protección de activos	Inventario de activos	Básico	1. Deben mantenerse inventarios actualizados de todos los elementos del sistema (información, software, hardware, servicios, terceros, personas, instalaciones, soportes de información), detallando los mismos como mínimo: a) El responsable. b) Tipo de activo (servidor, ordenador, router, etc.). c) Identificador, fabricante y modelo. d) Ubicación. 2. Los inventarios se actualizarán en función de los plazos establecidos en la normativa.

		Ficheros temporales	Básico	1. Los ficheros temporales que se hubieran creado exclusivamente para la realización de trabajos temporales auxiliares tendrán que cumplir con las medidas establecidas que se apliquen a los ficheros considerados definitivos. 2. Todo archivo temporal así creado será borrado una vez haya dejado de ser necesario para la finalidad que motivó su creación.
		Protección de equipos	Básico	1. El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad y requerirá una nueva autenticación del usuario para reanudar la actividad en curso. 2. Los equipos deben disponer de protección antivirus y antimalware. 3. Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con riesgo manifiesto de pérdida o robo, se protegerán adecuadamente. Sin perjuicio de las medidas generales que les afecten, se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se consideran claves de acceso remoto las que sean capaces de habilitar un acceso a otros equipos de la organización, u otros de análoga naturaleza.
		Mantenimiento de equipamiento	Básico	Se deben aplicar las medidas preventivas y correctivas necesarias para mantener el equipamiento físico y lógico asegurando la confidencialidad, integridad y disponibilidad continua de los equipos y sistemas. De acuerdo con lo anterior, se dispondrá de: 1. Las especificaciones de los fabricantes en lo que respecta a la instalación y mantenimiento de los sistemas. 2. Un seguimiento continuo de los anuncios de defectos, utilizando mecanismos, como por ejemplo, la suscripción de correo de avisos de defectos por parte del fabricante. 3. Un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

		Protección de los soportes de información	Básico	1. Los soportes de información deben identificarse mediante etiquetado o mecanismo equivalente de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación. 2. Las etiquetas o mecanismos equivalentes deberían ser fácilmente identificables. Se informará a los usuarios sobre estos mecanismos de identificación para que, bien mediante simple inspección, bien mediante el recurso a un repositorio, puedan entender el significado. 3. Se podrá excluir, por previsión a la normativa, la obligación de etiquetado en caso de soportes en que no se pudiera cumplir por sus características físicas, estableciendo medidas alternativas para asegurar su identificación y localización. 4. Los soportes de información que deban reutilizarse para otra información o entregar a otra organización serán objeto de un borrado seguro de su contenido.
		Devolución de activos	Básico	El personal interno o externo deberá devolver todos los activos de la organización que se encuentren en su poder al finalizar la relación laboral, el contrato o acuerdo.
	Protección de la información	Protección del puesto de trabajo	Básico	1. Se exigirá que los puestos de trabajo estén aseados, sin más material sobre la mesa que el requerido para la actividad que se realiza en cada momento.
		Limitación del tratamiento de datos personales	Básico	Una vez finalice el tratamiento de datos y cuando el Responsable del tratamiento haya establecido que los datos personales deben conservarse por los motivos establecidos en el RGPD o en la legislación aplicable, que impliquen una limitación de uso de las mismas, se tendrán que adoptar medidas técnicas para proteger los datos de acuerdo con este nuevo estado, como los siguientes: 1. Control de acceso. 2. Ubicación de los datos en un sistema distinto. 3. Cifrado.

		Copias de Seguridad	Básico	1. Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una determinada antigüedad. En particular, se considerará la conveniencia o necesidad, según corresponda, de que las copias de seguridad estén cifradas. 2. Estas copias deben tener el mismo nivel de seguridad que los datos originales. 3. Las copias de seguridad incluirán: a) Información de trabajo de la organización que se refiera a datos personales. b) Aplicaciones en explotación, incluyendo los sistemas operativos mediante las que se traten datos personales. c) Claves utilizadas para preservar la confidencialidad de los datos. 4. Semestralmente se verificará la correcta definición, funcionamiento y aplicación de los procedimientos de realización de las copias y procedimientos de recuperación. 5. La recuperación de copias deberá ser autorizada por el Responsable del tratamiento.
	Protección de la información en tratamientos no automatizados	Control de acceso a la documentación	Básico	1. Se limitarán los accesos de los usuarios únicamente a los recursos necesarios para el desarrollo de sus funciones. A tal efecto, el Responsable del tratamiento debe elaborar una relación actualizada de usuarios y perfiles de usuarios y los accesos autorizados para cada uno de ellos.

		Custodia, almacenamiento y destrucción	Básico	1. Se dispondrá de medidas físicas o lógicas, o ambas, que obstaculicen la apertura de los dispositivos de almacenamiento que contengan datos de carácter personal. Si no fuera posible adoptar esta medida el responsable del tratamiento deberá adoptar medidas que impidan el acceso de personas no autorizadas. 2. Si, por encontrarse en proceso de tramitación o revisión, la documentación no se encuentra archivada en los dispositivos de almacenamiento oportunos, la persona que se encuentre al cargo de la misma deberá custodiar la documentación impidiendo el acceso a cualquier persona no autorizada. 3. Se exigirá que los puestos de trabajo estén aseados, sin más documentación sobre la mesa que la requerida para la actividad que se realiza en cada momento. 4. Se destruirá cualquier documento que contenga datos de carácter personal que sea rechazado. 5. La destrucción se llevará a cabo mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en los mismos o su posterior recuperación para eliminar el riesgo de acceso indebido.
		Copia y reproducción de documentos	Básico	1. Deberán destruirse las copias o reproducciones rechazadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
		Traslado de documentación	Básico	1. Cuando el tratamiento de datos se realice fuera de los locales del responsable o del encargado del tratamiento el responsable del tratamiento deberá autorizarlo previamente. 2. Se llevará un registro detallado de cualquier entrada y salida de documentación. El registro debe reflejar: fecha y hora, identificación de la documentación, el número de documentos, el tipo de información que contienen, persona que realiza la entrada o salida, la forma de envío, la persona que autoriza la entrada o salida y la persona que realiza el registro.

		Criterios de archivo	Básico	1. Se debe garantizar la correcta conservación de los documentos, la localización y consulta de la información de conformidad con los criterios previstos en la legislación vigente sobre archivística. Estos criterios deben posibilitar el ejercicio de los derechos previstos en la normativa de protección de datos. En aquellos casos en los que no exista normativa aplicable, el responsable del tratamiento deberá establecer los criterios y procedimientos de actuación que tendrán que seguirse en materia de archivo.
		Gestión de incidentes y sistema de notificaciones de incidentes - papel	Básico	1. Se debe establecer un registro de incidentes en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o si s procede, detectado, la persona que hace la notificación, a quien se le comunica, los efectos derivados y las medidas correctoras aplicadas.
		Procedimientos - papel	Básico	1. Debe disponerse de los siguientes procedimientos para los tratamientos no automatizados: a) Trabajo fuera de los locales del responsable de las actividades de los tratamientos o encargados de los tratamientos. b) Notificación, registro y gestión de incidencias. c) Control de acceso. d) Criterios de archivo. e) Dispositivos de almacenamiento. f) Custodia. g) Copia o reproducción. h) Traslado. i) Destrucción papel.

ANEXO 4. Requisitos de seguridad (ENS) para los proveedores de servicios

Objeto del Anexo

El presente documento define los controles que debería hacer frente una empresa adjudicataria de servicios informáticos en caso de auditoría del ENS de nivel BAJO.

Requerimientos

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

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

ID 3. Procedimiento de revisión de la Política de Seguridad

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

ID 4. Evidencia de la difusión de la Política de Seguridad

Evidencia de la 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 que son responsables mediante el correo electrónico .

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

Evidencia de que la Normativa de Seguridad - ya sea propia o se utilice el Marco Normativo de la Agencia de Ciberseguridad de Cataluña - está disponible en la Intranet, página web, portal, repositorio , librería o 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 deben incluir como mínimo:

1. Cómo llevar a cabo las tareas habituales.
2. Quien debe realizar cada tarea.
3. Cómo identificar y reportar comportamientos anómalos.

ID 13. Evidencia de la difusión de los procedimientos de seguridad o de la posibilidad de acceso por parte de los usuarios.

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

ID 40. Documento de Identificación del Control de Acceso al sistema

Se dispone de un procedimiento formalizado de gestión de usuarios debidamente aprobado y actualizado que se indique:

- Cómo se realiza la gestión de los usuarios y de sus privilegios así como la persona responsable de la gestión de los usuarios
- Que los identificadores de los usuarios deben ser nominales y no se pueden compartir
- El período de retención de los usuarios.

ID 43. Procedimiento de Autenticación del Sistema

Se dispone de un procedimiento debidamente aprobado y actualizado en el que se describen los mecanismos de autenticación de los usuarios o se especifica dentro del procedimiento formalizado de gestión de usuarios los siguientes puntos:

1. Se detalla los sistemas autenticación de los usuarios con la obligación de tener al menos un factor de autenticación.
2. Se detalla y obtiene la evidencia de que el usuario confirma la recepción del identificador, conoce y acepta las obligaciones.
3. Se explica cómo gestionar las bajas de usuarios y el vínculo con RRHH que permita avisar a los responsables de gestión de usuarios del cambio en las relaciones con éstos.
4. Se indica que se utilicen al menos dos factores de autenticación en los sistemas categorizados como nivel medio y alto.
5. En caso de que se utilicen tokens, que éstos utilizan un algoritmo autorizado por el CCN, por ejemplo AES.

ID 46. Documento de Requerimientos de Aceso al sistema

Se dispone de un procedimiento formalizado de gestión de usuarios debidamente aprobado y actualizado que se indique:

- Cómo se realiza la gestión de los usuarios y de sus privilegios así como la persona responsable de la gestión de los usuarios.
- Que los identificadores de los usuarios deben ser nominales y no se pueden compartir.
- El período de retención de los usuarios.

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

Se dispone de una herramienta corporativa específica para la gestión de usuarios.

ID 54. Procedimiento de Gestión de Derechos de Acceso al Sistema

Se dispone de un procedimiento o se incluye dentro del procedimiento formalizado de usuarios del sistema los siguientes puntos:

- Se asignará el rol adecuado a cada usuario con los mínimos privilegios posibles y revisándose los mismos periódicamente.

- Se incluirá la relación entre los permisos que debe tener cada usuario en función de su rol.- Se especificará cuáles son los responsables de los recursos de los sistemas (físicos y lógicos) y quién tiene la responsabilidad delegada de conceder, alterar o anular el acceso a los mismos.