PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA PRESTACIÓN DE LOS SERVICIOS DE MANTENIMIENTO Y OPERACIÓN DE LA PLATAFORMA DE GESTIÓN DE IDENTIDADES DE LA UNIVERSITAT OBERTA DE CATALUNYA

Expediente HSE00002/2020

ÍNDICE

1. Objeto del Contrato

La UOC dispone de un sistema de Gestión de Identidad y de Gestión de Accesos (en adelante GdI) basado en software OpenIAM y Shibboleth. Con este sistema se gestionan las más de 700.000 identidades y 450.000 usuarios, recopilando información de los diferentes repositorios, añadiendo las cuentas y permisos necesarios y proporcionando un acceso único gracias al proveedor de identidad Shibboleth. La Gestión de la Identidad y la Gestión de Accesos se han convertido en sistemas críticos para la infraestructura tecnológica de la UOC, y por tanto se hace necesario garantizar por un lado la vigilancia proactiva de la salud del sistema, un mantenimiento correctivo que dé una respuesta ágil a las posibles incidencias, y por otro lado la adecuación a las necesidades de integración con sistemas terceros que no comporten cambios importantes al sistema.

El objeto de este pliego es la contratación de los mencionados trabajos, de acuerdo con las prescripciones que se articulan más adelante dentro del presente pliego.

2. Objetivos del Contrato

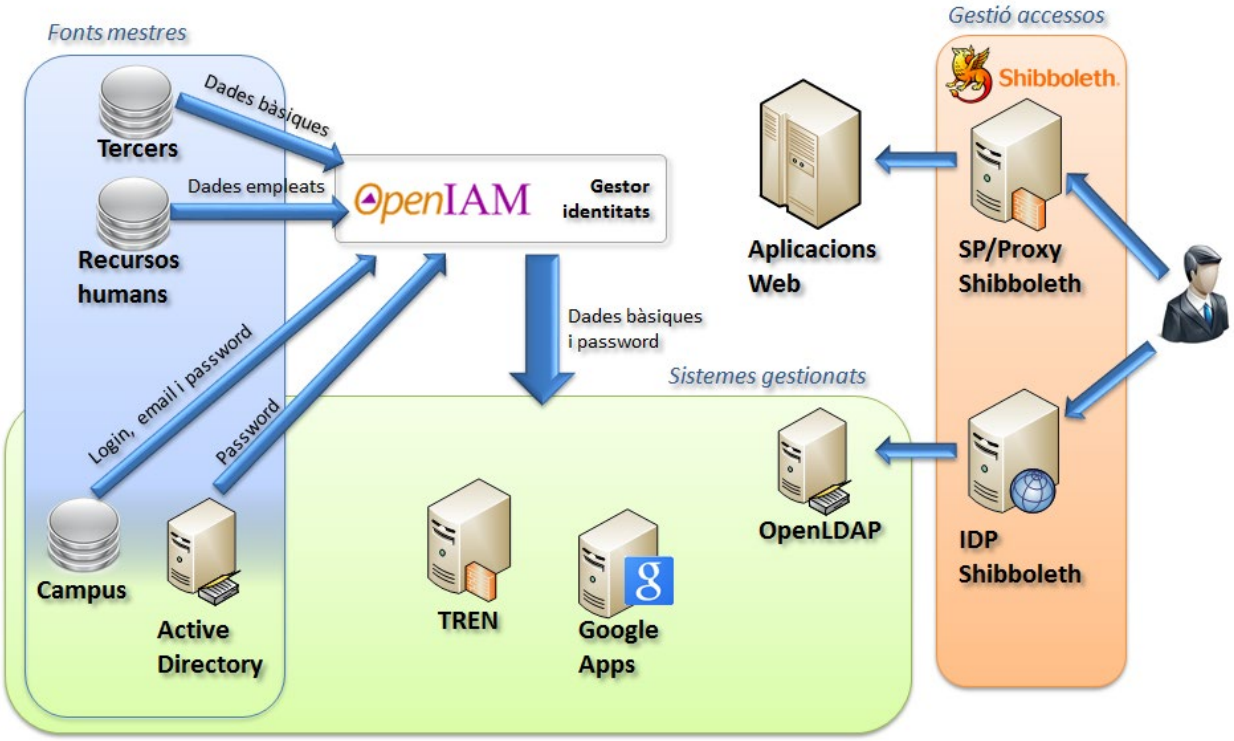
El objeto del presente contrato es el servicio de mantenimiento y evolución de la solución de Gestión de la Identidad que permita a la UOC mantener en buen estado este sistema y evolucionarlo de acuerdo con las nuevas necesidades que aparezcan, de acuerdo con los siguientes objetivos:

- Asegurar el funcionamiento ordinario de la GdI (Gestión de la Identidad), dando soporte de tercer nivel y garantizando el mantenimiento de aplicaciones del tipo correctivo, preventivo, y pequeño evolutivo.
- Vigilancia del correcto funcionamiento de la GdI y seguimiento de su uso.
- Detección rápida de riesgos y vulnerabilidades.
- Apoyo a la administración.
- Atención y resolución de las incidencias relacionadas con la GdI.
- Dar respuesta a peticiones de evolutivo de la Gestión de la Identidad relacionados con el su mantenimiento y que no supongan cambios importantes al sistema ni desarrollos de importancia.
- Renovación de la suscripción de soporte del distribuidor del producto OpenIAM sin limitación de usuarios, transacciones, CPUs, instancias o cualquier otro límite, asumiendo el adjudicatario la responsabilidad de la comunicación con el fabricante y las gestiones por la adquisición o renovación de esta suscripción en nombre de la UOC.

3. Descripción de la Gestión de la Identidad

3.1. Visión global del sistema.

El sistema de Gestión de la Identidad implantado en la UOC se encarga de reconciliar datos de los diferentes repositorios agregando datos y credenciales del usuario, reconciliándolas con los sistemas gestionados, asignando permisos automáticamente en base a un perfilado del usuario y generando las cuentas según este perfilado. A continuación se puede ver una visión global del sistema:



Donde los repositorios son:

- Terceros: sistema de información que recopila todas las identidades de personas que tienen o han tenido relación con la UOC. Contiene datos personales y un perfilado básico

que determina si un usuario es empleado, profesor, alumno, antiguo alumno u otros.

- Sistema de RRHH (Endalia): aplicación en modalidad SaaS (Software as a Service) que contiene los datos de los empleados de la UOC, con información de sede de trabajo, contacto, área a la que pertenece, responsable y estado.
- Campus: aplicación de Campus Virtual y portal corporativo. Es la fuente de datos de las credenciales UOC, es decir, también constituye un repositorio de credenciales.
- Active Directory. Repositorio de cuentas corporativas por los empleados y colaboradores UOC.
- TREN: sistema de permisos de acceso a las aplicaciones corporativas. Contiene información de roles, perfiles y accesos concretos a aplicaciones.
- Google Apps: la UOC dispone de un dominio de Google Apps que permite crear cuentas asociadas a los usuarios UOC. OpenIAM también gestiona estas cuentas y puede crear, desactivar o eliminar automáticamente las credenciales asociadas.
- OpenLDAP. OpenIAM gestiona automáticamente un directorio LDAP con las credenciales, datos básicos y otros que se utiliza para integrar sistemas internos (como por ejemplo JIRA) y por la Gestión de Accesos (Shibboleth).

La UOC ha contratado a finales de 2019 un proyecto en un año con el objetivo de renovar la infraestructura de autenticación y autorización, por lo tanto durante la prestación del servicio objeto de este pliego, la infraestructura se verá modificada en los siguientes aspectos principales:

- El proveedor de identidad (Shibboleth) estará desplegado en la nube de AWS.
- El sistema de gestión de sesiones sufrirá modificaciones y se llevará a la nube.
- El directorio de personas (LDAP) se llevará a Amazon Directory Service.
- El aplicativo de recordatorio y cambio de contraseña se renueva completamente.

3.2. Repositorios y sistemas gestionados

Actualmente la Gestión de la Identidad gestiona los siguientes repositorios y sistemas gestionados:

Repositorio	Descripción	Volumen (aprox)	Integración	Periodicidad
TERCEROS	Datos de personas, tipologías. Fuente autoritativa.	700.000	BD (Orcle)	Sincroniza cambios cada 30 minutos

Campus	Login usuario, tipo de usuario.	450.000	BD (Orcle)	Sincroniza cambios cada 30 minutos. Actualiza datos básicos del usuario.
Active Directory	Cuentas corporativas, grupos	2.500	Conector OpenIAM	Crea usuarios. Actualiza datos. Sincroniza todo el repositorio cada 30 minutos
TREN	Roles, accesos a aplicaciones	50.000	BD (Orcle)	Crea permisos. Sincroniza cambios cada 60 minutos.
Endalia (aplicación de gestión de personas en modo SaaS)	Datos empleados.	2.500	API REST	Sincroniza cambios cada 60 minutos.
Google Apps	Cuentas de Google	100.000	API GruGapps (propietaria)	Crea, deshabilita o elimina usuarios.
OpenLDAP	Credenciales.	450.000	Connector OpenIAM.	Mantiene una réplica de las credenciales de los usuarios. Calcula permisos en base a grupos.

3.3. Reconciliaciones

La mayor parte de los sistemas gestionados se reconcilian cada determinado periodo de tiempo con Tareas Programadas de OpenIAM. Estas tareas programadas se resumen en:

- Tareas de sincronización de Active Directorio (AD):

    - **Active Directory - Empresas Externas**: creación de unidades organizativas (OUs) de las empresas externas.
    - **Active Directory - Reconciliar grupos**: lee los grupos nuevos creados en el repositorio.
    - **Active Directory - Reconciliar usuarios**: reconcilia los usuarios nuevos en AD.
    - **Active Directory - Recursos Humanos**: completa el AD con la información recibida de la aplicación de gestión de Personas (Endalia).
- **CAMPUS - Reconciliación Aplicación/Tipo/Subtipo:** lee los cambios de asignación de usuarios a tipos / subtipos.
- **Envío auditoría syslog**: envía al SYSLOG los logs antiguos y los borra de la base de datos (BD).
- **Extractor Perfiles**: genera excels con la información de perfilado para detectar nuevos perfiles de usuario y ayudar a la asignación automática de permisos.
- **Gestión de Permisos - Informes de Conformidad**: generación de los informes de conformidad y seguridad.
- **OpenLDAP - Carga Usuarios Kivuto**: agrega permisos en el LDAP a los usuarios que se pueden descargar el software de Kivuto (añade entitlements a los usuarios matriculados en un aula).
- **Reconciliaciones Consecutivas**: reconciliación de usuarios de TERCEROS, Campus y AD. Solo cambios.
- Endalia:
    - **RRHH - Reconciliación Roles**: reconcilia roles con la aplicación de Personas.
    - **RRHH - Reconciliación Sedes**
    - **RRHH - Reconciliación Unidades Funcionales**
    - **RRHH - Reconciliación Usuarios**
- **TERCEROS - Reconciliación Entornos y Tipologías**
- **TERCEROS - Reconciliación de personas a no activar**
- **TREN - Reconciliación Recursos**
- **TREN - Reconciliación Roles**

3.4. Interceptación de cambios de contraseña.

Uno de los objetivos de la Gestión de la Identidad es la de gestionar las contraseñas y

mantenerlas sincronizadas en todos los sistemas gestionados. Por lo tanto, cuando un usuario se cambia la contraseña en el portal Campus, OpenIAM detecta el cambio y actualiza la contraseña al resto de repositorios si los tiene (por ejemplo, a Active Directory o al LDAP). Para hacerlo, OpenIAM captura los cambios de contraseña con un conector (DLL) instalado en los Domain Controllers de Active Directory, y con un llamamiento en un Web Service en la página de cambio de contraseña de Campus.

3.5. Gestión de Accesos - Shibboleth.

Otro componente de la Gestión de la Identidad es una Gestión de Accesos basada en el estándar SAML 2.0 (http://suml.xml.org/saml-specifications) que proporciona aserciones de autenticación, se federa con "hubs" institucionales y en definitiva permite a los proveedores de servicios integrarse con un proveedor de identidad centralizado (IdP). Los metadatos de este IdP se pueden consultar en https://id- provider.uoc.edu/idp/shibboleth.

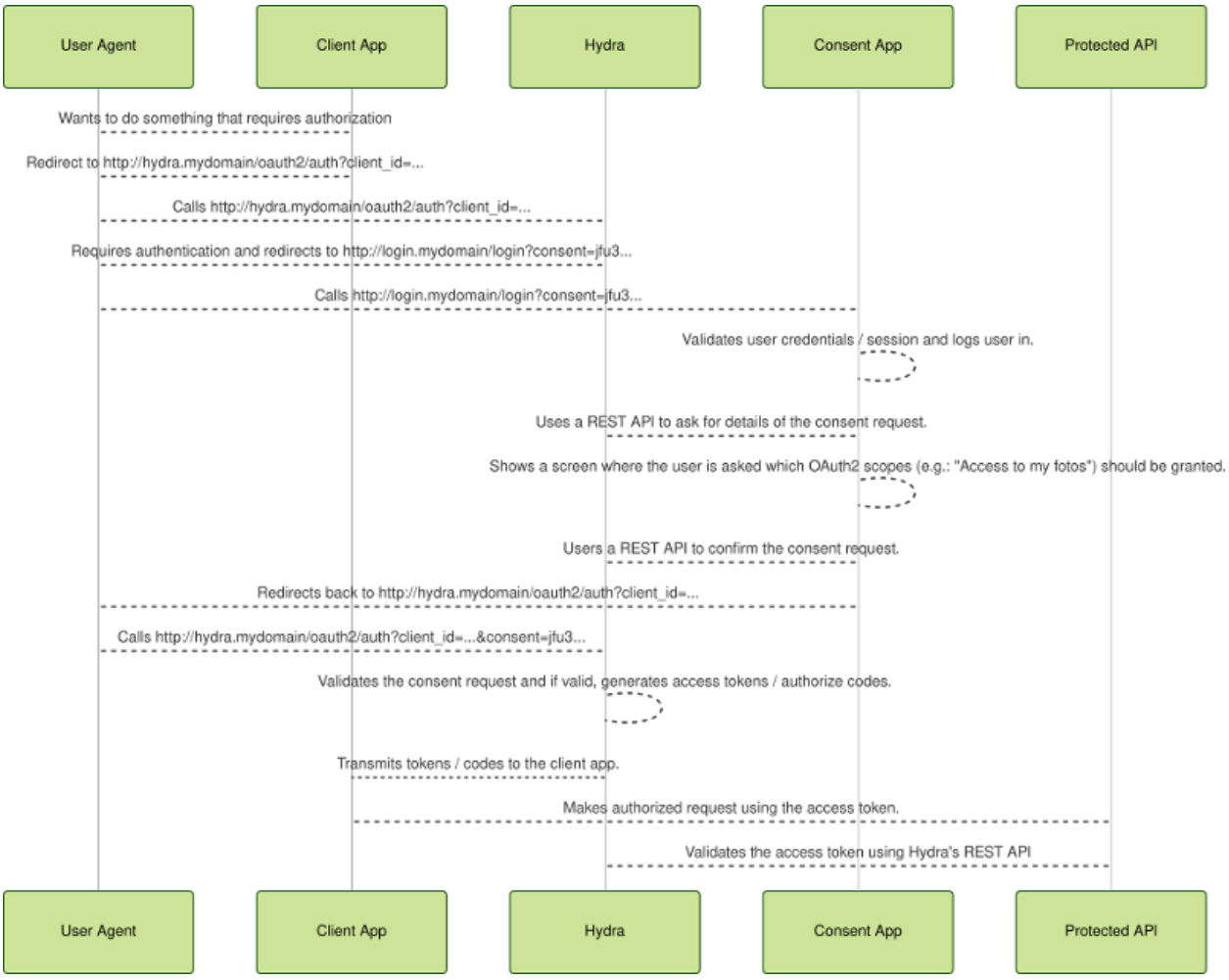
Actualmente, el IdP de la UOC se integra con la OpenLDAP que genera automáticamente OpenIAM con los datos de credenciales, datos básicos y perfilado, aunque como se describe a este pliego, Shibboleth se desplegará a la nube y se conectará a un repositorio en AWS (Amazon Directory Service). Aunque hay muchas integraciones (muchos proveedores de servicio), las más importantes son:

- La propia página de inicio del LMS (Learning Management System) de UOC (www.uoc.edu), con unas 70.000 autenticaciones diarias.
- Google Suite, unas 10.000 autenticaciones diarias
- Federación con Microsoft Azure. Proporciona a los 35.000 alumnos acceso al paquete Office 365 de Microsoft.
- Federación con el SIR2 de RedIris (https://www.rediris.es/sir2/). Accesos a múltiples recursos de biblioteca, descarga de software de Microsoft (MS Imagine), conexión a EduGain o descuentos en la tienda Apple.
- Federación con la FiD del CSUC (https://www.csuc.cat/ca/recerca/federacio-d-identidades-unificado).
- Orcle Cloud Financials.

Se prevé que el número de integraciones crezca en los próximos años, y por tanto el adjudicatario tiene que prever que desde el servicio de mantenimiento objeto de este pliego se de soporte a las integraciones futuras, así como solución a los posibles problemas con las existentes.

3.6. OAuth2 y aplicación de consentimiento (BridgeKeeper).

Entre los componentes de autenticación y autorización se encuentran el proveedor de OAuth2 (Hydra) y la aplicación BridgeKeeper, una aplicación de consentimiento desarrollada en Django, el mantenimiento de la cual tendrá que ser asumido por el servicio objeto de este pliego. Técnicamente, BridgeKeeper es un SP (Service Provider) que enlaza los tokens OAuth2 de tipos "authorization code grant" con el IdP SAML. La información del usuario autenticado se envía a la aplicación en forma de metadatos (OpenId). Este flujo de autenticación se puede ver en el siguiente diagrama (BridgeKeeper aparece como Consent App):



3.7. Código y documentación.

Se dispone de todo el código de las adaptaciones desarrolladas para la UOC, así como documentación de los procesos y de su funcionamiento interno. También se dispone de documentación del producto OpenIAM. Este código y esta documentación se pondrá a disposición del adjudicatario, que se responsabilizará de mantenerla actualizada.

4. Alcance del servicio.

4.1. Visión global del servicio

Los servicios objeto de este pliego se dividen en:

- Suscripción de apoyo del producto OpenIAM.
- Gestión del servicio.
- Servicio operacional, incidental y evolutivo.
    - **Operación**: Mantenimiento y vigilancia de la Gestión de la Identidad.
        - Generación de indicadores clave.
        - Mantenimiento preventivo.
        - Revisión del perfilado.
        - Apoyo a la administración.
        - Incorporación de nuevas aplicaciones y grupos al BridgeKeeper.
        - Atención a consultas.
        - Monitorització del buen funcionamiento del servicio.
    - Atención a incidencias :
        - Atención de incidencias y diagnosis.
        - Corrección de datos.
        - Gestión de incidencias con el fabricante.
        - Solución a problemas urgentes (prioridad alta) de código, aplicación de parches en caso necesario.
    - Mantenimiento **evolutivo** menor. Evolutivos o cambios en el comportamiento del componentes, que pueden incluir:
        - Integraciones de nuevos proveedores de servicio al IdP.

- Integración de nuevos conectores.
- Mejora procesos.
- Generación de nuevos informes (BIRT).
- Apoyo a evolutivos de aplicaciones satélite.
- Corrección de problemas no urgentes detectados en el servicio incidental.

4.2. Suscripción de apoyo del producto.

Para disponer de apoyo 24x7 del fabricante del software base (OpenIAM), el adjudicatario gestionará la suscripción en nombre de la UOC al servicio estándar de apoyo nivel Platinum de OpenIAM ofrecido por el propio fabricante. Esta suscripción formará parte de los servicios ofertados. Las condiciones de servicio de esta suscripción están en el enlace https://www.openiam.com/products/subscriptions

4.3. Gestión del servicio.

El adjudicatario asignará un técnico que asumirá las tareas de gestión del servicio, es decir, que lleve la operativa diaria de la Gestión de la Identidad y Gestión de Accesos. El perfil tiene que ser de una persona proactiva, con habilidades de comunicación y negociación, capacidad para gestionar el servicio, con castellano, catalán e inglés fluido. A pesar de que el servicio se prestará en las instalaciones del adjudicatario, se prevé que la persona que haga este papel tenga que trasladarse con frecuencia a las instalaciones de la UOC. El adjudicatario tendrá que presentar el CV de la persona propuesta y que tendrá que cumplir los requerimientos de solvencia técnica pedidos al PCP.

Las tareas a ejecutar al ámbito de gestión del servicio son:

- **Seguimiento y reporting** a la UOC de la bolsa de tareas pendientes, detección de desvíos y feedback a la UOC.
- **Recepción de consultas**, peticiones de nuevas **integraciones** (Proveedores de Servicio u otros), **estudio previo y recogida de necesidades**. De manera general esto comporta la asistencia a reuniones de toma de requerimientos o recepción de peticiones informales por parte de Negocio.
- **Seguimiento de las integraciones** con terceros, resolución de dudas y pruebas de aceptación. Por ejemplo, esto aplica a seguir el estado de integraciones de nuevos SP's con los proveedores de servicios.
- **Seguimiento de incidencias** de proveedores de servicio, como por ejemplo materiales o portales asociados. Esto aplica también en el caso de Federaciones de Identidad como

RedIris o UNIFICT.

- **Análisis y vigilancia de las incidencias repetidas** para detectar posibles mejoras o defectos ocultos.
- **Reuniones con los servicios de atención** (Servicio Atención al Estudiante y Servicio Atención al Usuario) para hacer el seguimiento del uso de la consola, incidencias repetidas y detección de casos anómalos. De estas reuniones se pueden derivar acciones de mejora o nuevos incidentales.
- **Gestionar periodos especiales** (inicio semestre, evaluación, final semestre…), asegurar el funcionamiento correcto de los sistemas clave y gestionar operativos especiales de vigilancia.
- **Seguimiento de proyectos** (o evolutivos de más alcance) **que afecten a la Gestión de la Identidad,** detección de cambios necesarios en los procesos de operación o pequeño evolutivo, detección de la necesidad de cambios a procesos de backup o vigilancia.

4.4. Servicio operacional, incidental y evolutivo.

4.4.1. Recepción de peticiones y seguimiento.

El adjudicatario pondrá a disposición un servicio de registro, recepción y formalización de las peticiones, con el objetivo de tipificar las peticiones independientemente del servicio que las atienda finalmente. En esta fase se podrá pedir más información cuando sea necesario, y se llevará un registro del total consumido, cumplimiento de ANS y número de incidencias. A pesar de que el adjudicatario puede proponer canales adicionales de comunicación y registro, el método de registro y seguimiento será la herramienta JIRA de Atlassian de la UOC. La atención de incidencias de prioridad inmediata se hará mediante teléfono móvil, a pesar de que el incidente se tendrá que registrar a posteriori en JIRA.

Como tarea adicional de seguimiento, se incluyen las reuniones periódicas de seguimiento, que se harán por los tres servicios en conjunto y se describen más adelante y la generación de informes de cumplimiento de los ANS.

4.4.2. Servicio de operación.

La Gestión de la Identidad tiene como objetivo simplificar, gestionar y optimizar los procesos relacionados con la vida de los usuarios UOC, su perfilado y la información necesaria para las tareas de autenticación y autorización. Para conseguir estos objetivos, se pide un servicio de mantenimiento y vigilancia proactivo de la Gestión de la Identidad que vele para que se sigan las líneas marcadas.

En este servicio se incluyen las siguientes tareas:

4.4.2.1. Generación de indicadores clave.

Generación de informes que permitan valorar el estado de salud de la Gestión de la Identidad y hacer un seguimiento de su evolución. Estos indicadores como mínimo serán:

- volumen global de usuarios e identidades gestionados,
- número de cambios de contraseña en un periodo determinado,
- usuarios activos por tipos,
- colaboradores sin responsable asignado,
- empleados sin datos organizativos,
- permisos técnicos no incluidos en los roles de negocio,
- afiliaciones asignadas a los usuarios y su coherencia con los datos maestros,
- detección de situaciones anómalas (inconsistencia de datos).

En esta tarea también se analizará la evolución de los indicadores para medir el avance en los objetivos globales.

4.4.2.2. Preventivo.

En esta tarea el adjudicatario hará una vigilancia técnica de la plataforma a partir de los indicadores de la tarea anterior, más otras de tipo técnico (carga de los servidores, trazas de errores, alertas de Nagios, caídas de los sistemas…). Con esta información se identificarán riesgos o vulnerabilidades y se propondrán acciones preventivas, nuevas pruebas funcionales o, en caso necesario, se generarán nuevas acciones correctivas. Este servicio tendrá que tener la disponibilidad como la principal prioridad, identificando riesgos y diseñando los planes necesarios para conseguir minimizarlos.

El adjudicatario tendrá que tener en cuenta que parte de la infraestructura puede residir a la nube (en particular, a AWS), y por tanto los mecanismos de vigilancia, el personal asignado a estas tareas y las posibles actualizaciones del software base se tendrán que adaptar a este entorno de ejecución.

4.4.2.3. Revisión del Perfilado.

Uno de los objetivos de la Gestión de la Identidad es la detección de perfiles y roles de negocio que nos permitan poner orden a la asignación de permisos (TREN, AD, Google Apps). Para conseguir este objetivo, OpenIAM ejecuta periódicamente una tarea de detección de nuevos perfiles en base a los permisos y datos organizativos de los usuarios. Por lo tanto, el adjudicatario hará la revisión periódica de los permisos asignados a los usuarios, propondrá nuevos modelos de permisos y se pondrá en contacto con los responsables del área y de seguridad para automatizar la asignación (y posterior desasignación) de permisos y realizará limpiezas

controladas de permisos obsoletos.

4.4.2.4. Mantenimiento de permisos al BridgeKeeper.

Tal y como se ha visto en la descripción de la plataforma, entre los componentes de autenticación y autorización se encuentran Hydra (componente que provee el OAuth2) y la aplicación BridgeKeeper (aplicación de consentimientos). El adjudicatario asumirá el mantenimiento y vigilancia tanto de Hydra como de BridgeKeeper, así como el mantenimiento de permisos dentro del servicio de Operación. Típicamente, las peticiones de mantenimiento de permisos serán: Alta, Baja o Modificación de aplicaciones, acceso a un "scope" a una lista de usuarios, o bien mantenimiento del literales traducidos por la parte de consentimiento.

4.4.2.5. Atención a consultas.

Por último, en este servicio de mantenimiento y vigilancia el adjudicatario dará respuesta a consultas y dudas técnicas sobre el funcionamiento de la Gestión de la Identidad. Estas dudas pueden surgir debido a las necesidades de evolución de la herramienta, integración de nuevos sistemas terceros o sobre cambios en el modelo de los permisos, y tienen que garantizar un buen funcionamiento de la plataforma.

4.4.3. Servicio incidental.

El adjudicatario tendrá que garantizar la continuidad del soporte a incidencias sobre todos los elementos tecnológicos de la Gestión de la Identidad a partir de esta fecha, teniendo en cuenta que el adjudicatario tiene que dar servicio sin interrupción y garantizar un correcto traspaso del conocimiento.

Este servicio tiene como objetivo principal garantizar la máxima disponibilidad de la Gestión de la Identidad, localizar y eliminar los posibles defectos del software o en los datos que genera. Se entiende por defecto cualquier característica del sistema que tiene la potencialidad de producir una quiebra, es decir, un comportamiento del sistema diferente al que está establecido en las especificaciones.

El servicio de atención de incidencias tendrá que cumplir con los siguientes procedimientos:

- dar en un tiempo mínimo una respuesta con la previsión de solución y pidiendo los datos que necesite para solucionar el incidente,
- proponer acciones paliativas que permitan minimizar el impacto,
- en caso de que la incidencia no sea urgente, derivar al servicio de evolutivo al desarrollo de la corrección; si la incidencia es urgente, esta solución se hará directamente en el propio servicio,
- solución al incidente en caso de que se pueda resolver con acciones simples y procedimentadas,

- aplicar parches (patches) en el software (tanto OpenIAM como el resto de software que forma parte de la solución),
- escalado en caso necesario al servicio de apoyo del fabricante.

4.4.3.1. Canales de recepción de incidencias.

Se tiene que tener en cuenta que la UOC dispone de una serie de servicios y canales que pueden recibir o bien originar peticiones relacionadas con la Gestión de la Identidad. Los actores que pueden generar peticiones al incidental son por lo tanto:

- **Servicio de vigilancia y operaciones**. Se trata del primer nivel de atención y monitorització de sistemas. En caso de que se detecte un problema crítico en el servicio o que se reciba una llamada al servicio de operaciones UOC de 7x24, lo gestionará y si no lo puede resolver, la escala. Cuando estén relacionadas con la Gestión de la Identidad, en el caso de incidencias de gravedad Alta o Inmediata este servicio lo escalará al servicio incidental. El canal de comunicación tendrá que ser telefónico.
- **Servicio de Atención al Usuario (SAU)**. Primer nivel de atención de peticiones e incidencias por el personal de gestión. En este caso, este servicio escalará al servicio incidental cuando estén relacionadas con la Gestión de la Identidad. Estas peticiones o incidencias serán de gravedad media o baja. El canal de comunicación tendrá que ser intermediando JIRA.
- **Servicio de Atención al Estudiante**. En caso de que se detecten problemas graves o repetidos con los sistemas de autenticación o gestión de las contraseñas, se escalarán peticiones con JIRA al servicio de atención incidental de la Gestión de la Identidad.
- El propio **servicio de Operación de la Gestión de la Identidad** puede detectar incidencias o posibles mejoras que, una vez aprobadas por la UOC, se introducirían en el circuito o bien de evolutivos o bien de incidental, con el canal de JIRA.

El canal de comunicación de las incidencias será vía JIRA excepto en el caso de que sean de gravedad Alta o Inmediata, que serán vía telefónica. En caso necesario el servicio de incidental puede escalar la petición al servicio de atención del fabricante (OpenIAM).

4.4.3.2. Información sobre el estado de la incidencia.

En el servicio de incidental el adjudicatario se responsabiliza de dar feedback en todo momento tanto del diagnóstico como sobre el estado de la incidencia al emisor de la misma. El total de incidencias, estado y ANS se reportará en los comités correspondientes tal como se explica en el punto 5.

4.4.3.3. Garantizar la disponibilidad de la Gestión de la Identidad.

El servicio tiene que atender peticiones con la máxima celeridad posible a las incidencias que

provoquen una disrupción importante o bien una parada del servicio. Este servicio tiene que atender peticiones según los ANS que se detallan más adelante, valorar y analizar el problema y dar respuesta tan pronto como sea posible.

4.4.3.4. Corrección de los defectos de software o de datos.

Cuando sea necesario modificar software o datos en la Gestión de la Identidad UOC, el adjudicatario se encargará de

- aplicar las correcciones necesarias al código desarrollado, en caso de que la incidencia sea de prioridad Inmediata o Alta; en caso de que la incidencia tenga prioridad Media o Baja se derivará al servicio de evolutivo, a pesar de que el seguimiento se hará desde este servicio,
- probar la solución aplicada
- hacer las pasos necesarios para distribuir la solución según los circuitos que se especifican en el apartado 7. Anexo A – Flujo de trabajo del JIRA
- y documentar la solución aplicada.

En caso de que se trate de un problema de datos o que el incidente haya provocado una corrupción de las mismas, se ejecutarán todos los pasos necesarios para restablecer la consistencia de los datos, incluyendo si fuera necesario la recuperación de copias de seguridad.

En caso de que el incidente no se pueda resolver a los dos primeros niveles, que necesite de un evolutivo o preventivo con un tiempo de respuesta mayor del que se especifica al ANS o que lo requiera, se escalará al fabricante OpenIAM.

4.4.3.5. Modificaciones de los componentes base.

Si la incidencia solo se puede resolver modificando cualquiera de los componentes base de la solución, en este servicio el adjudicatario gestionará

- la actualización de las versiones del software base,
- solución de incidentes del producto,
- seguimiento de desarrollos (evolutivos) que solucionen problemas del producto,
- Soporte in situ por el diagnóstico o, en caso necesario, solución de problemas con el producto o su configuración. Si fuera necesario para garantizar la disponibilidad, este soporte se podrá prestar fuera de horario de oficina.

4.4.4. Mantenimiento evolutivo.

Servicio destinado a dar respuesta a peticiones de evolutivo de la Gestión de la Identidad que no supongan cambios importantes al sistema ni desarrollos de importancia, y relacionados con el

mantenimiento del servicio. El adjudicatario tendrá que justificar las horas dedicadas a cada uno de los trabajos. En este servicio se incluirán los siguientes tipos de actuaciones:

- **Integración de nuevos proveedores de servicio (Service Provider) a la Gestión de Accesos (Shibboleth)**. Puede suponer la configuración de nuevos issuers, apoyo a incidencias con la integración o añadir nuevos atributos en las respuestas SAML.
- **Mejora de procesos**. Mejoras o ajustes sobre los procesos de sincronización o reconciliación, ejecución de las reglas de negocio, tareas programadas o simplificación de la estructura de permisos.
- **Integración de conectores**. Incorporación de conectores a la solución de Gestión de la Identidad por la gestión de nuevos sistemas externos (por ejemplo, repositorios LDAP, bases de datos …), siempre que esta integración no suponga desarrollo.
- **Creación de nuevos informes**. Construcción de nuevos informes bajo demanda. OpenIAM se basa en BIRT para el diseño de reports.
- **Apoyo a la administración**. En esta tarea se apoyará a la configuración de estructuras de la Gestión de la Identidad, y los posibles cambios en la estructura y modelo de permisos de OpenLDAP, que puedan surgir debido a nuevas necesidades en la evolución del proyecto. Son ejemplos la creación de empresas externas, reglas de pertinencia a roles, nuevos atributos…
- **Corrección defectos**. Los defectos de software de prioridad media o baja que se detecten en el servicio incidental se corregirán en este servicio, de este modo los desarrollos y la gestión del código se simplifican.

Los evolutivos se ejecutarán bajo demanda de la UOC. El adjudicatario recibirá las peticiones de evolutivo de la UOC y tendrá que hacer una propuesta en horas por perfil. Una vez aprobadas por la UOC se gestionarán con un ciclo de vida equivalente a cualquier desarrollo de software, es decir, con un análisis de la solución, desarrollo, pruebas y despliegue. Todos los evolutivos tendrán que tener una garantía de seis meses a partir de su puesta en marcha. El adjudicatario se compromete a valorar los evolutivos en un máximo de una semana natural a partir de su recepción, dando una primera solución técnica, una valoración de esfuerzo y una planificación.

El licitador tendrá que respetar el plan de traspaso de mantenimiento de nuevos evolutivos, en concreto:

- Definición de la duración del plan de traspaso a mantenimiento
- Método previsto para hacer la transferencia de conocimiento y la transferencia tecnológica
- Requerimientos mínimos para pasar a mantenimiento un nuevo sistema/aplicación
- También se tiene que proponer el plan de entrega de:
  - Conocimiento: determinar el número de sesiones de traspaso y tipologías de estas

(workshops, formación, etc.)

- Documentación: determinar la documentación técnica que se entregará y los plazos de entrega
- Servicio: determinar las condiciones del plan de traspaso a mantenimiento, incluyendo el plan de comunicación de cambio al usuario

4.5. Volumetría y dimensionado del servicio.

A continuación se dan métricas y previsiones de la volumetría de número, tipo y complejidad de las peticiones para permitir hacer un dimensionado correcto del servicio. Aun así, el adjudicatario tiene que prever mecanismos para dar respuesta a las posibles variaciones en el servicio siempre que no comporten una modificación del contrato, de acuerdo con los supuestos previstos en el Pliego de Cláusulas Particulares.

4.5.1. Dimensionado de la gestión del servicio.

Para ejecutar las tareas relacionadas con la gestión del servicio (ver apartado “4.3. Gestión del servicio”), se prevé una dedicación de 20 **horas semanales**. Los desplazamientos seguirán los criterios definidos en el apartado “5.7.4. Desplazamientos”.

4.5.2. Evolutivos.

A continuación se da una previsión por tipo de evolutivo, siempre teniendo en cuenta que se trata de una previsión orientativa y por tanto se tiene que prever un margen suficiente de error. La previsión es anual.

Concepto	**Número**	**Número de horas medio**
Incorporación de nuevos Service Providers a la Gestión de Accesos basada en Shibboleth, apoyo a la integración, modificación de los atributos u otros que modifiquen los atributos SAML o que requieran el cálculo de un nuevo atributo.	15	12
Modificación en los procesos de reconciliación, reorganización de las tareas programadas, reprogramación de las funciones internas de las tareas.	2	24
Modificación del comportamiento de los conectores o del cálculo de los atributos necesarios, cambios asociados en la configuración de OpenIAM, provisión de nuevos valores.	2	24

Incorporación de nuevos sistemas gestionados, creación de las reglas de negocio necesarias, integración con las APIs del sistema gestionado y configuración de los entornos.	2	240
Nuevas provisiones con sistemas terceros, creación de los nuevos atributos y nuevas reglas asociadas, integración con las APIs o librerías necesarias y creación de nuevos parámetros de configuración.	2	240
Creación de nuevas reglas de negocio, creación de las dependencias con los sistemas gestionados afectados, integración con sistemas ajenos.	1	260
Creación de nuevos informes BIRT (https://www.eclipse.org/birt/)	5	16
Soporte en la administración. Modificación en la configuración de los sistemas base (Shibboleth, OpenIAM, OpenLDAP, …). Cambios en la configuración y el apoyo asociado a Operaciones Tecnológicas de la UOC.	10	16
Integración con sistemas externos	1	32
Otros evolutivos	5	32
Corrección de defectos de media o baja prioridad, pruebas y distribución de la solución en todos los entornos.	3	16

4.5.3. Incidencias.

A continuación se da una previsión por tipo de actuación, a pesar de que la lista no limita el tipo de peticiones que el servicio tiene que atender. La previsión es anual.

Actuación	**Número**	**Tiempo medio de la actuación**
Actuaciones sobre sistemas. Parada e inicio de sistemas, revisión de logs, modificación de configuraciones y otras actuaciones que comporten la modificación de los sistemas base.	10	2
Corrección de datos y reaprovisionamiento de usuarios. Creación de	5	4

scripts para corregir situaciones anómalas a los datos de la Gestión de la Identidad, modificación del código responsable de la incidencia, reaprovisionamiento de los usuarios en sistemas gestionados.		
Correcciones a incidencias urgentes en el código, pruebas y distribución de la solución en todos los entornos.	5	16
Errores en la conexión con sistemas gestionados. Anomalías en la conexión con los sistemas gestionados (Active Directory, Google Apps, etc…) que provoquen incidencias en estos sistemas externos.	20	4
Errores en la provisión o reconciliación de usuarios. Errores al código que se encarga de la provisión o reconciliación de los usuarios.	10	2
Atención a casos anómalos de usuarios finales, diagnosis y solución de caso o escalado	50	1
Otros (peticiones descartadas, no reproducibles…)	5	2

Se estima que el 5% de las peticiones tendrán prioridades Inmediata o Alta.

4.5.4. Variaciones en el servicio.

El adjudicatario tiene que prever que el dimensionado del servicio puede variar en función de las necesidades:

- En el caso de los evolutivos, si la valoración agregada de las peticiones de mantenimiento evolutivo ya realizadas y las pendientes de realizar con valoración aprobada superara el presupuesto destinado al servicio de evolutivo, la ejecución de estas peticiones pendientes se tendrá que supeditar a las posibles modificaciones de contrato establecidas al Pliego de Cláusulas Particulares.
- En el caso de las incidencias y correctivos, se tiene que tener en cuenta que el número es por naturaleza más imprevisible y por tanto necesita de una mayor flexibilidad en el servicio, por lo tanto se asumirá que el número de peticiones puede superar hasta un 20% el previsto al apartado anterior sin que comporte una ampliación del contrato. Las modificaciones de contrato por variaciones superiores a un 20% se recogen al Pliego de Cláusulas Particulares.

El seguimiento del consumo de horas y las desviaciones leves sobre la previsión se discutirán en la comisión de seguimiento, y las posibles desviaciones graves que puedan provocar una modificación de contrato a la comisión de gestión.

5. Condiciones del servicio

5.1. Modelo de relación

El modelo de relación define las funciones y responsabilidades de la empresa adjudicataria y la UOC en un marco de actuación común, para asegurar el cumplimiento de las obligaciones de cada una de las partes. Es un marco de relación que permite acordar el contenido y nivel de la prestación de los servicios, así como el seguimiento de la prestación real en los aspectos estratégicos, contractuales, tácticos y operativos.

5.1.1. Perfiles asignados al servicio y responsabilidades

A continuación se detalla una estructura mínima de responsables que actuarán como interlocución con la UOC:

- **Responsable del servicio**: el licitador propondrá un responsable del servicio. Es la figura de referencia responsable de la prestación del conjunto de servicios (gestión del servicio, incidental, operación, y evolutivos). Esta figura se mantendrá durante toda la vida del contrato en la gestión comercial, durante la ejecución del servicio y hasta la devolución de este. También será responsable de las gestiones necesarias en el supuesto de que se produzcan cambios en el alcance o volúmenes de los servicios que puedan impliquen una modificación contractual. Sus funciones son:
  - Garantizar la atención a los responsables del Servicio de la UOC en todos los ámbitos del servicio, atendiendo a las necesidades de negocio de la UOC
  - Mantener la visibilidad global de la prestación del servicio, en todas sus dimensiones
  - Garantizar la calidad del servicio en todos sus ámbitos
- **Gestor del servicio**: el licitador propondrá un gestor del servicio, que será el principal interlocutor con la UOC y quien asumirá la Gestión del Servicio. Las principales responsabilidades son:
  - Gestión y seguimiento diario del servicio
  - Resolución de conflictos
  - Elaboración de los informes de servicio y justificación del cumplimiento de los ANS
  - Seguimiento y control de los recursos asignados a los servicios
  - Control de consumos, estimación de esfuerzos y su seguimiento
  - Analizar desviaciones del servicio (alcance, consumos)
- **Jefe de proyecto**:

- Su función es el control de los evolutivos, que funcionarán como pequeños proyectos.
- Gestión de los recursos necesarios, asignación de nuevos recursos en caso necesario.
- Gestión del calendario e hitos del evolutivo.
- Gestión de riesgos y seguimiento de los mismos.
- Creación de los informes de seguimiento y asistencia a las reuniones de seguimiento técnico.

- **Arquitecto**:
  - Su función es aportar conocimiento, soluciones y diagnosis a los servicios de operación, incidental y evolutivo.
  - Responsable del diseño conceptual de la solución y la arquitectura de componentes tecnológicos necesarios para cubrir las necesidades del servicio.
  - Definir las diferentes alternativas posibles para dar cobertura a los objetivos que se pretenden conseguir, determinando la mejor solución posible de todas las disponibles, siempre con la visión de diseñar un sistema el más parametritzable y flexible posible
  - Aportar conocimiento de las herramientas para resolver incidencias que comprometan la disponibilidad de la Gestión de la Identidad
- **Técnico**
  - Responsable de la ejecución de las tareas y primera atención a consultas o incidencias.
  - Creación y vigilancia de procesos de reconciliación entre repositorios.
  - Aportar conocimiento de las herramientas para resolver incidencias que comprometan la disponibilidad de la Gestión de la Identidad

Órganos de Gestión (Comités)

A continuación se detallan los mecanismos mínimos que servirán como herramientas de control por parte de la UOC y que tienen como objetivo garantizar el correcto funcionamiento.

La estructura básica de control y seguimiento es la siguiente:

- **Comité de Dirección**: asumirá las funciones de supervisión de la ejecución del contrato así como la toma de decisiones que afecten al objetivo y alcance del contrato. Las principales funciones del Comité de Dirección son:
  - Asegurar la adecuación del equipo según las necesidades de cada fase del servicio
  - Seguimiento ejecutivo y de los riesgos del servicio. Cambios de planificación
  - Gestión de conflictos, validaciones de peticiones de cambios
  - Seguimiento contractual del servicio (inicio, aprobación de trabajos, finalización, cambios

de alcance)

El Comité de Dirección se reunirá al inicio del servicio, con periodicidad trimestral, y siempre que la situación lo pida para resolver conflictos, cambios a los términos del contrato o en general situaciones extraordinarias. Por parte del adjudicatario se compondrá como mínimo por el Responsable del Servicio y el Gestor del Servicio, y de los representantes que la UOC determine.

- **Comité de Seguimiento**: las principales funciones del Comité de Seguimiento son:
  - Seguimiento de la evolución del servicio
  - Aprobación de re-planificaciones y cambios o proponer al Comité de Dirección los cambios estratégicos, económicos, de alcance y de gestión que considere oportunos por la buena marcha del servicio y si se tercia, las modificaciones contractuales que correspondan
  - Seguimiento de la operación diaria del servicio, y verificar la correcta gestión de peticiones y cambios
  - Desarrollar y mantener los procedimientos operativos necesarios para el correcto funcionamiento del servicio
  - Análisis de peticiones y situaciones de cambio en los servicios
  - Gestión de riesgos
  - Resolución de conflictos

El Comité de Seguimiento se reunirá, como mínimo el Gestor de Servicio y los representantes que la UOC determine, con una periodicidad bisemanal aunque se podrá convocar con carácter extraordinario siempre que se considere necesario.

5.2. Fases del servicio.

Los servicios descritos en este pliego contemplan las fases siguientes:

- Transición del servicio
- Ejecución del servicio
- Devolución del servicio

A continuación detallamos las fases del servicio.

5.2.1. Transición del servicio

A la transición del servicio, usamos la terminología siguiente:

- **Adjudicatario saliente**: Se el proveedor que en la actualidad se hace cargo del servicio o servicios objeto de este pliego.

- **Adjudicatario entrante**: Es el adjudicatario futuro y por tanto será el responsable de la provisión del servicio o servicios objeto de la licitación.
- **Fase de captura de conocimiento**: Es la fase previa a la fase de transición, durante la cual, y antes de que se inicie la ejecución del contrato, el adjudicatario entrante realiza con el apoyo del adjudicatario saliendo la captura del conocimiento y la transferencia tecnológica necesaria que le permitirá lograr la provisión definitiva del servicio al final de la fase de transición. Esta fase no será facturable.
- **Fase recepción servicio**: Es el periodo de tiempo, dentro de la fase de transición, en la que el adjudicatario entrante empieza a asumir el servicio con el apoyo y acompañamiento del adjudicatario saliente y que finaliza en el momento que el adjudicatario entrante se hace cargo completamente del servicio asumiendo los niveles de servicio requeridos.

5.2.1.1. Modelo de transición

El modelo de transición, que incluye la fase de captura de conocimiento y la fase de recepción del servicio, tendrá una duración total máxima de 2 meses a partir de la fecha de formalización del contrato. Finalizará en el momento en que el adjudicatario entrante asume completamente la ejecución del servicio tanto en cuanto a los nuevos desarrollos como las tareas de apoyo y mantenimiento. Se relacionan a continuación las condiciones aplicables al modelo de transición.

Los roles y las responsabilidades de cada parte en cada una de las fases son:

Fase	Responsabilidad del adjudicatario saliente	Responsabilidad del adjudicatario entrante
Durante la adjudicación del contrato y la firma del nuevo contrato	– Facturación de los servicios recurrentes – Tiene la responsabilidad de la prestación del servicio y el cumplimiento de los ANS actuales	
Fase de transición: Captura de conocimiento.	– Facturación de los servicios recurrentes – Tiene la responsabilidad de la prestación del servicio y el cumplimiento de los ANS actuales – Facilita la atención, la colaboración y la información necesaria para realizar una correcta transferencia de conocimiento y tecnológica que permitirá al nuevo adjudicatario hacerse cargo del servicio.	– Tiene que proponer la temporalidad de la fase de captura del conocimiento y de recepción del servicio. – También tiene que proponer los procesos seguidos para garantizar esta transferencia. – No facturará los servicios recurrentes. El coste de esta fase tiene que estar incluido en la oferta presentada. – A la finalización de esta fase, tendrá que entregar un documento donde

		se detalle los procesos básicos del servicio, el plan de actuación de la siguiente fase y las carencias detectadas con el plan de recepción.
Fase de transición: Recepción del servicio por el adjudicatario entrante	− Facturación de los servicios recurrentes − Sigue teniendo la responsabilidad de la prestación del servicio y el cumplimiento de los ANS. − Apoyará al adjudicatario entrante para que este asuma el servicio sin interrupción.	− Tendrá que seguir las etapas y la temporalidad de la fase de transición. − No facturará los servicios recurrentes. El coste de esta fase tiene que estar incluido en la oferta presentada. − Tendrá que entregar un informe sobre la ejecución de la transición, con el detalle del cambios efectuados por la resolución de los problemas detectados a la fase anterior.
Finalizada la fase de transición. (Fase de ejecución)		− Facturación de todos los servicios (recurrentes más suscripción producto) − Tiene la responsabilidad del cumplimiento de los ANS establecidos

El adjudicatario entrante, el adjudicatario saliente y la UOC acordarán la finalización de esta fase mediante la firma de un documento de aceptación. Previamente la UOC realizará una comprobación formal de la capacitación del adjudicatario entrante para asumir el servicio. El adjudicatario entrante empezará a facturar el servicio a partir de la firma de este documento.

5.2.2. Ejecución del servicio

5.2.2.1. Mecanismos de control y reporting

Para la ejecución y gestión del servicio, el adjudicatario tendrá que hacer uso de las herramientas de registro y calidad según se especifica en el apartado 5.5. Herramientas de registro y calidad.

Los informes de seguimiento de los servicios se elaborarán con la periodicidad establecida y con mecanismos que permitan la navegación por los mismos y faciliten la comparación y cruce entre

los diferentes elementos de servicio medidos. El responsable del servicio por parte del adjudicatario presentará el informe, exponiendo los hechos relevantes del periodo, el seguimiento de los indicadores de servicio y el análisis del periodo incluyendo el plan de acciones de mejora.

5.2.2.2. Acuerdos de Nivel de Servicio (ANS)

Los ANS servirán para definir el compromiso de servicio acordado entre la UOC y el adjudicatario del contrato y se tendrán que aplicar los mecanismos de gestión necesarios para controlar su grado de cumplimiento. Estos MÁS BIEN se aplicarán a las peticiones de correctivo, y son efectivos en horario de 7x24.

Cada ANS está determinado por los siguientes parámetros:

- Indicadores de medida
- Valores aceptables por los indicadores
- Objetivo de cumplimiento del ANS
- Frecuencia de las medidas

Las peticiones llevarán asociada una prioridad: Inmediata, Alta, Mediana y Baja. La prioridad Inmediata es un caso especial en casos de máxima criticidad.

Los indicadores son los siguientes:

- Indicadores de actividad: mesuran volúmenes y son indicativos, sin estar sometidos a ningún ANS
- Indicadores de Compromiso: sometidos a acuerdos de nivel de servicio y miden el grado de cumplimiento del servicio en términos de eficiencia y efectividad del servicio:
  - Tiempo de evaluación y compromiso de peticiones
  - Tiempo máximo en circuito de las peticiones
  - Tiempo de resolución de peticiones

A excepción de las actividades de evolutivos, peticiones y acciones de mejora que estén ligadas a tareas de desarrollo, los valores y objetivos de cumplimiento mínimos de los indicadores de compromiso son:

	Tiempo evaluación y compromiso		**Tiempo máximo en circuito**		**Tiempo resolución**	
Prioridad	**Condiciones**	**Objetivo**	**Condiciones**	**Objetivo**	**Condiciones**	**Objetivo**

Inmediata	<= 2h	95%	<= 8h	98%	<= 4h	95%
Alta	<= 6h	90%	<= 70h	98%	<= 12h	90%
Media	<= 16h	88%	<= 90h	95%	<= 36h	88%
Baja	<= 24h	85%	<= 90h	95%	<= 60h	85%

5.2.2.3. Circuito evolutivos.

Las peticiones de evolutivo incluirán una descripción de los requerimientos del nuevo desarrollo por parte de la UOC y se harán con la herramienta JIRA que opcionalmente se acompañará con documentación de apoyo.

En un plazo no superior en una semana, el adjudicatario tendrá que valorar el evolutivo y proponer una solución técnica, que incluya:

- Relación de los sistemas afectados.
- Participación otras organizaciones.
- Estimación de los trabajos necesarios para llevarlo a cabo.

Se considerará cada uno de estos evolutivos como un proyecto de llaves en mano, incluyendo por lo tanto el compromiso en la valoración y la garantía correspondiente.

El seguimiento de los evolutivos en curso se hará a las reuniones de seguimiento periódicas. En estas reuniones el licitador tendrá que presentar, como mínimo, la siguiente información:

- Visión global de los evolutivos identificando los evolutivos que necesitan una atención especial puesto que se encuentran en riesgo o bien hay una desviación respeto la planificación inicial
- Valoración de los aspectos más relevantes de cada evolutivo:
  - Planificación (en fechas o atrasado)
  - Riesgos (altos, moderados, leves, externos o sin riesgos)
  - Valoración global del evolutivo: valoración media del evolutivo en base a la planificación y los riesgos (evolutivo en riesgo, a seguir o en curso normal)
- Identificación de los principales riesgos que afectan a nivel global el servicio y las acciones de mitigación correspondientes

El licitador definirá y propondrá en la UOC los mecanismos de control y recursos que permitan realizar el seguimiento de las diferentes tareas y el estado de los evolutivos en curso.

En cuanto a los desarrollos de evolutivos el licitador tendrá que contemplar una fase de garantía.

5.2.2.4. Sistema de penalizaciones

Las penalizaciones a aplicar en caso de incumplimiento de los niveles de servicio acordados se recogen al Pliego de Cláusulas Particulares.

5.2.3. Devolución del servicio

En caso de cese o finalización del contrato, el proveedor estará obligado a devolver el control de los servicios objeto del contrato, teniendo que realizar en paralelo los trabajos de devolución con los de prestación del servicio, sin coste adicional por la UOC. En caso de que se tenga que ejecutar la devolución, esta se llevará a cabo durante los dos últimos meses del contrato, durante los que el adjudicatario continuará siendo el responsable del servicio.

5.2.3.1. Modelo de devolución

El modelo de devolución tendrá que cumplir, como mínimo, los siguientes requerimientos:

- La fase de devolución tiene una duración temporal de 2 meses para completar la correcta transferencia de conocimientos y la transferencia tecnológica por el tipo de servicio.
- Se aplicarán las mismas condiciones del punto *5.2.1.1 Transición del servicio.* de este pliego, aplicando al adjudicatario de este contrato las condiciones de adjudicatario saliente.
- Durante la fase de devolución el adjudicatario saliente se compromete a dedicar como mínimo el soporte de un Técnico a dedicación completa para facilitar al adjudicatario entrando la fase de ejecución de la transición.
- En caso de que la devolución del servicio no sea satisfactoria a la finalización del segundo mes, es decir, que no se cumplan los requerimientos de este pliego, podrá ser requerido el soporte del adjudicatario saliente durante los siguientes dos meses.

5.3. Perfil del rol de gestor del servicio.

La persona que asuma el rol de gestión del servicio tendrá que cumplir los requerimientos y solvencia que se detallan al PCP. Por otro lado, la UOC validará periódicamente el correcto cumplimiento del servicio en las funciones que lo correspondan, y se reserva el derecho de exigir el cambio al adjudicatario en el supuesto de que la persona no se haya integrado satisfactoriamente en el equipo de trabajo o haya problemas de coordinación técnica con el resto de equipos técnicos de la UOC.

5.4. Metodología

La UOC tiene establecida una serie de metodologías, estándares y normativas y el adjudicatario tendrá que garantizar su cumplimiento. En los siguientes anexos se detallan los requerimientos

mínimos metodológicos más destacables en el momento de redacción del presente pliego:

- Anejo A: Flujo de trabajo del JIRA
- Anejo B: Estándares metodológicos y de calidad
- Anejo C: Desarrollo seguro del software
- Anejo D: Requerimientos de Arquitectura
- Anejo E: Ciclo de CI/CD.

5.5. Herramientas de registro y calidad

Se usará la herramienta JIRA de Atlassian para el registro y tratamiento de las peticiones e incidencias reportadas por el usuario de los servicios objete de este contrato.

La comunicación con otros departamentos y en concreto con Arquitectura y Sistemas (AiS) está procedimentada con la misma herramienta JIRA.

El entorno a desarrollo UOC se compone de un conjunto de herramientas que se tendrán que utilizar a cualquier tarea de desarrollo y mantenimiento, siguiendo unos procedimientos previamente marcados por el paso de las aplicaciones entre entornos, pruebas y aceptación. Se puede ver el ciclo de CI/CD en el anejo correspondiente.

Las herramientas implicadas al proceso de desarrollo son:

- Herramienta de seguimiento de errores, incidencias y gestión operativa de proyectos: JIRA + plugins
- Repositorio de código, donde tiene que residir todo el código desarrollado, Git, Git Lab y Subversion.
- Visualizador de los repositorios de código: Fisheye
- Entorno a integración continua por los desarrollos Java, que se encarga de lanzar las compilaciones e informes de calidad de los desarrollos de forma automático: Maven y Jenkins
- Monitorització de la calidad del código: SonarQube
- Repositorio de artefactos que sirve para almacenar versiones liberadas : Artifactory
- Herramienta de documentación integrada con la de seguimiento: Confluence y Drive
- VPN, que permite a usuarios externos acceso en la red de desarrollo y de pruebas.

5.6. Auditorías

La UOC podrá realizar auditorías para verificar el cumplimiento de los compromisos contractuales y la fiabilidad de la información facilitada.

El adjudicatario proporcionará su total cooperación a la realización de estas auditorías. Esto incluirá la entrega de documentación y el acceso físico en las instalaciones donde se estén realizando los servicios objeto del contrato, al personal de la UOC o a los terceros subcontratados.

No habrá que dar aviso previo para realizar tareas de auditoría donde no se requiera colaboración activa del personal del adjudicatario. En los casos en que la UOC pida una colaboración activa del personal del adjudicatario, se dará aviso con una semana de antelación.

5.7. Otras condiciones

5.7.1. Ubicación del servicio

Los servicios se prestarán en general desde las instalaciones del adjudicatario, a excepción de las actividades que la UOC estime en cada momento que para dar un mejor servicio conviene que se lleven a cabo a las instalaciones de la UOC.

5.7.2. Horario del servicio

Este horario se refiere en el periodo que el adjudicatario tiene la obligación de atender al usuario, ya sea directamente o indirectamente a través de un nivel de atención superior. El horario es de lunes **a viernes de 08:30 a 18:30.**

Más allá de este horario, se pactarán los horarios concretos de las guardias y actuaciones fuera de horario habitual. El adjudicatario tiene que proporcionar un servicio de atención y resolución de incidencias críticas en horario de 7x24 con los Acuerdos de Nivel de Servicio que se detallan en el apartado 5.2.2.2. Acuerdos de Nivel de Servicio (ANS)

5.7.3. Calendario de trabajo

El calendario laboral de la UOC no contempla periodos de cierre por vacaciones y, por lo tanto, el servicio contratado tendrá que estar disponible durante todo el año incluyente vacaciones de verano, Semana Santa y Navidad.

5.7.4. Desplazamientos

Los costes de cualquier desplazamiento a las dependencias de la UOC para la resolución de peticiones, incidencias, asistencias técnicas, reuniones de seguimiento o cualquier otra tarea contemplada dentro del servicio serán a cargo del adjudicatario y con medios de transporte facilitados por él mismo. Todas las oficinas de la UOC se encuentran en el área metropolitana de Barcelona.

5.7.5. Equipación

La UOC pondrá a disposición de los profesionales del adjudicatario que tal y como se indica en el apartado anterior “ubicación del servicio” tengan que desarrollar su actividad a las instalaciones de la UOC una mesa y les garantizará el acceso a la red.

Todo el resto de equipaciones y en especial aquellos que el adjudicatario disponga a sus dependencias por la ejecución del servicio, será a cargo del adjudicatario. Esto también aplica a las posibles cuentas a proveedores de cloud que el adjudicatario pueda necesitar para prestar el servicio.

Los equipos conectados en la red de la UOC tendrán que ser configurados de acuerdo con los estándares y políticas de la UOC.

5.7.6. Comunicaciones

Los costes de las comunicaciones (voz y datos) e intercomunicaciones entre los centros de trabajo del adjudicatario y de la UOC, ocasionados por la prestación del servicio, serán a cargo del adjudicatario.

6. Anejo A: Flujo de trabajo del JIRA

Actualmente la metodología de trabajo de los equipos de desarrollo utiliza la herramienta JIRA de Atlassian para poder hacer la gestión de los proyectos, el seguimiento de las incidencias, tareas, funcionalidades nuevas, mejoras y el flujo de trabajo por el despliegue a producción. Además todo esto complementado con la herramienta de documentación Confluence de Atlassian.

La herramienta JIRA se utiliza en la UOC como mecanismo de relación, seguimiento de tareas así como herramienta para hacer las peticiones necesarias de los recursos necesarios (tanto tecnológicos como de gestión). En concreto, las tareas principales son:

- **Gestión de proyectos**. Con esta herramienta se vehicula la ficha de información básica del proyecto, petición de herramientas asociadas (espacios a los repositorios, por ejemplo), y por otro lado se acompaña con un espacio al Confluence que recoge tareas pendientes, documentación y otros artefactos documentales del proyecto, a pesar de que los documentos como tal residen en Google Drive.
- **Instalación y actualización de los proyectos**. Tanto la puesta en producción inicial del proyecto como las actualizaciones sucesivas se vehiculan con JIRA (como se puede ver en el apartado del ciclo de CI/CD). Por otro lado, JIRA es la herramienta de relación con el departamento de Operaciones o la Oficina del Cloud en caso de necesitar cualquier acción sobre la infraestructura.
- **Peticiones e incidencias**. Las peticiones asociadas a modificaciones funcionales o de código de la aplicación irán acompañadas con un JIRA que detalla los requerimientos, prioridad y fecha de necesidad de la tarea. El circuito que estas peticiones seguirán dependerá del tipo de petición.

El adjudicatario recibirá documentación en detalle sobre los circuitos por cada uno de los tipos de peticiones, los accesos necesarios para hacer esta tarea y, en caso necesario, formación sobre su uso.

7. Anejo B: Estándares metodológicos y de calidad

Independientemente de la metodología seguida por la organización que desarrolle el software, la UOC considera que el proceso tiene que producir y mantener una documentación mínima por la correcta consecución de un proyecto o cualquier modificación del código objete de este servicio. Estos entregables no tienen que ser considerados como un trámite burocrático, sino que tienen que ser de valor para el cliente final o el equipo de desarrollo.

Los entregables a nivel metodológico que se consideran mínimos por la UOC son:

- Documentación:
  - recogida de las características de la aplicación, las necesidades, restricciones e integración con otros sistemas,
  - recogida de los requerimientos del sistema, recogidos de una manera formal
  - descripción funcional del sistema, preferentemente con los casos de os principales,
  - detalle de la integración con otros sistemas,
  - diseño técnico (interfaz de usuario, lógica, detalle de los casos de uso, etc),
  - detalle de las pruebas realizadas al sistema con su resultado (pruebas unitarias, funcionales y de estrés si es necesario),
  - manual de uso de la aplicación
  - manual de instalación de la aplicación,
  - manual de operación y administración cuando sea necesario.
- En la documentación se recogerán diferentes diagramas que describan:
  - la funcionalidad del sistema,
  - los objetos o clases a construir al marco de la aplicación (diagramas de bases de datos, clases, packages, librerías...),
  - la estructura del proyecto con sus componentes (bases de datos, librerías, ejecutables, organización del código...),
  - los elementos necesarios por su ejecución (red, máquinas implicadas, y otros requerimientos físicos y de arquitectura),
  - el comportamiento dinámico del sistema
  - la interacción (mensajes, llamamientos) entre los diferentes componentes del sistema

- Respecto al código librado:
  - seguirá los estándares de calidad definidos por la UOC
  - contendrá las pruebas unitarias del código
  - seguirá las normativas de seguridad fijadas por la UOC
  - utilizará las herramientas y APIOS estándares por el interconexionado con los sistemas de la UOC (autenticación, internacionalización, etc)

El contenido de toda esta información puede relacionarse con los documentos fijados por la metodología que siga el proyecto. En todo caso, se completarán con todos los que se consideren necesarios en cada caso.

Artefactos principales	**Qué contiene**	**Formato**
Ficha del evolutivo	- Información básica – Alcance y descripción del proyecto - implicados (actores) - Fechas - Indicadores y Riesgos - Presupuesto	- JIRA
Ficha de Aplicación	- Información básica – Alcance y descripción de la aplicación - Implicados (actores) - Fechas - Información por la operación de la aplicación - Nivel de servicio	- JIRA
Documentación	- Kick-off - Cierre - Actas de reuniones - Gestión del cambio - Informas de seguimiento - Glosario: Termas y vocabulario	- Confluence - Google Drive
Requerimientos	- Descripción textual - Calidad - Infraestructura - Reqs. No funcionales	- JIRA - Confluence
Pruebas Funcionales	- Pla de pruebas de la aplicación - Definición de los procesos principales	- TestRail
Arquitectura de software	- Modelo datos - Comportamiento dinámico - Despliegue	- JIRA - Confluence

	- Manual instalación	
Código	- Manual de uso - Manual de operación - Pruebas unitarias - Pla de pruebas ejecutado - Artefactos	- SVN / Git - Jenkins - Sellenium - Artifactory

8. Anejo C: Desarrollo seguro del software.

8.1. Introducción

Este anexo establece el compromiso de acuerdo entre la UOC y el adjudicatario para maximizar la seguridad del software de la aplicación (de ahora en adelante la aplicación) de acuerdo con los siguientes términos.

8.2. Filosofía

Este anexo está destinado a clarificar los derechos y obligaciones relacionadas con la seguridad de las relaciones comerciales de las partes involucradas en el desarrollo de la aplicación. Al más alto nivel, estas partes acuerdan que:

Las decisiones de seguridad estarán basadas en el riesgo: Las decisiones de seguridad se tomarán conjuntamente entre UOC y el adjudicatario basándose en una alta comprensión del riesgo que puede tener la aplicación.

Las actividades dedicadas a la seguridad estarán balanceadas: Los esfuerzos dedicados a la seguridad de la aplicación estarán fuertemente distribuidos durante todo el ciclo de vida de su desarrollo.

Se integrarán las actividades dedicadas a la seguridad: Todas las actividades y la documentación generada aquí hará falta que se integre en el ciclo de vida de desarrollo del software de la aplicación y no podrán en ningún caso estar separadas del resto del proyecto. Nada en este anexo implica un desarrollo especial de software.

Podrán aparecer vulnerabilidades: Este anexo asume que todo software puede tener errores y que algunos de estos pueden crear incidentes de seguridad. Tanto UOC como el adjudicatario se esforzarán al identificar las vulnerabilidades con la mayor celeridad posible durante el ciclo de vida de la aplicación.

La seguridad de la información será completamente revelada: Toda información relacionada con la seguridad de la información de la aplicación, será compartida entre UOC y el adjudicatario de forma inmediata y completa. El proveedor especificará por escrito qué aspectos de la seguridad relacionada con el desarrollo piensa no cumplir.

Solo se requiere aquella documentación que sea útil en aspectos de seguridad: La documentación de seguridad no tiene que ser extensa en exceso en orden a clarificar, describir el diseño de la seguridad, el riesgo, el análisis y los incidentes

8.3. Actividades del ciclo de vida de la aplicación

Comprensión del riesgo: UOC y el adjudicatario acuerdan trabajar de manera conjunta para comprender y documentar los riesgos que pueden afectar a la aplicación. Este esfuerzo se enfocará a identificar posibles vulnerabilidades que afecten a los activos y las funcionalidades de la aplicación. Habrá que considerar cada uno de los puntos, funcionalidades y casos de uso definidos en la parte de los requerimientos de la aplicación.

Requerimientos: Basándose en el riesgo, UOC y el adjudicatario acuerdan trabajar de manera conjunta para definir unos requerimientos de seguridad como parte de las especificaciones del software a desarrollar. Cada uno de los puntos que se hayan enumerado en la sección de requerimientos hará falta que sean discutidos y evaluados conjuntamente por UOC y el adjudicatario. Estos requerimientos tendrán que ser satisfechos en su totalidad por la aplicación.

Diseño: El adjudicatario acuerda proporcionar una documentación que explique de forma clara el diseño que se implementa para lograr los requerimientos de seguridad. Este diseño explicará de forma clara si el apoyo a los requerimientos de seguridad proviene del software desarrollado a la aplicación, de software de terceras partes o de la plataforma en la que se implementa el desarrollo.

Implementación: El adjudicatario acuerda proporcionar y seguir un conjunto de buenas prácticas de programación. Estas guías indicarán como se tiene que formatear el código, como se tiene que estructurar y comentar. Aun así el código podrá ser revisado por alguna persona responsable de la ejecución del proyecto de la UOC que validará los requerimientos de seguridad y las guías de programación antes de que el código de la aplicación sea considerado preparado por maceta.

Seguridad del análisis y pruebas: El adjudicatario acuerda proporcionar y seguir un plan de pruebas de seguridad el cual definirá la aproximación que se haya hecho a cada uno de los requerimientos de seguridad. El nivel del rigor de esta actividad tiene que estar considerada y detallada en el plan del proyecto. El adjudicatario ejecutará el plan de pruebas de seguridad y proporcionará los resultados en la UOC.

Despliegue seguro: El adjudicatario acuerda proporcionar las guías para configurar la aplicación de manera segura, muy documentadas y de tal manera que cubran todos los requerimientos especificados en el plan de proyecto. El adjudicatario incluirá en esta guía una completa descripción de las dependencias de la plataforma soportada, incluyendo el sistema operativo, la base de datos, el servidor web y el servidor de aplicaciones y como estos tendrán que ser configurados para cumplir con los requerimientos de seguridad. El adjudicatario acuerda que la configuración por defecto de la aplicación que librará en la UOC será segura

8.4. Áreas de seguridad

El adjudicatario acuerda que las siguientes áreas serán consideradas durante la comprensión del riesgo y las actividades de definición de los requerimientos de la aplicación.

Validación y codificación: Todo el conjunto de requerimientos que especifican las reglas por canalizar, validar y codificar cada entrada de la aplicación, tanto desde los usuarios, sistema de ficheros, directorios o sistemas externos. La regla por defecto será que todas las entradas son inválidas a menos que cumplan una determinada especificación que lo permita. Adicionalmente, los requerimientos de la aplicación especificarán la acción a emprender cuando se reciba una entrada no válida. Específicamente, la aplicación no será susceptible a inyección, desbordamiento (overflow), manipulación (tampering) u otros ataques de corrupción de entrada de datos..

Autenticación y gestión de la sesión: Los requerimientos de la aplicación especificarán como las credenciales de autenticación y los identificadores de sesión protegidos en todo su ciclo de vida. Se incluirán los requerimientos referidos en el encabezamiento de este párrafo de todas las funciones relacionadas, incluyendo la pérdida de contraseña, los cambios de contraseña, los recordatorios de contraseña, la desconexión por inactividad y la posibilidad del uso de múltiples conexiones simultáneas (multiple login).

Control de acceso: Los requerimientos de la aplicación incluirán una descripción detallada de todos los roles y perfiles usados (grupos, privilegios, autorizaciones) en la aplicación. Los requerimientos habrán también de indicar todo el conjunto de activos y funcionalidades proporcionadas por la aplicación. Los requerimientos tendrán que explicar completa y exactamente los derechos de acceso a cada uno de los activos y funciones de la aplicación por cada uno de los roles. Se sugiere construir una matriz de control para explicar el formato de estas reglas.

Manipulación y gestión de errores: Los requerimientos de la aplicación hará falta que detallen como se gestionan los errores de la aplicación durante el proceso de funcionamiento de la misma. Se entiende que en algunas funcionalidades se tendrá más cura en el tratamiento de errores, sobre todo las que tengan más incidencia en el usuario final, mientras que otros puede ser que acaben en la finalización del proceso inmediatamente.

Registro (Logging): Dentro de los requerimientos hará falta que se especifiquen qué acontecimientos son relevantes por la seguridad y las conexiones de la aplicación, como por ejemplo los ataques detectados, los intentos fallados de acceso y los intentos de ganar privilegios. Los requerimientos también especificarán qué tipo de información queda grabada para cada uno de los acontecimientos generados, incluyendo la fecha, la descripción del acontecimiento, detalles de la aplicación y de otra información forense de utilidad.

Conexión a sistemas externos: Los requerimientos especificarán como se trata la autenticación

hacia sistemas externos a la aplicación, como por ejemplo las bases de datos, directorios y servicios web. Todas las credenciales necesarias para la comunicación con estos sistemas que se almacenen en ficheros de configuración lo harán de forma protegida.

Encriptación: Los requerimientos de la aplicación especificarán qué datos tienen que ser cifradas, como se han cifrado y como se manipularán los certificados y otras credenciales. Las especificaciones se referirán siempre a un algoritmo estándar de alguna biblioteca abastecimiento probada y utilizada.

Disponibilidad: Los requerimientos tendrán que especificar como se protegerá la aplicación de los ataques de denegación de servicio. Englobando los ataques sobre el bloqueo de autenticación, agotamiento de las conexiones y en general otros ataques de exhauriment de recursos.

8.5. Personal y organización

Arquitecto de seguridad: El adjudicatario asignará responsabilidades en materia de seguridad a un recurso, que pase a ser el arquitecto de seguridad del proyecto. Este certificará la seguridad de cada entrega.

Formación en seguridad: El adjudicatario será responsable de asegurar que todos sus miembros del equipo de desarrollo están capacitados en las técnicas de desarrollo seguro.

8.6. Bibliotecas, frameworks de aplicación y productos

Divulgación: El adjudicatario hará público el software de terceras partes usado en el desarrollo de la aplicación, incluyendo las librerías, frameworks, componentes y otros productos, sean comerciales, libres, en código abierto o en código cerrado.

Evaluación: El adjudicatario realizará los esfuerzos razonables para asegurar que todo el software de terceras partes usado en la aplicación, cumple los términos de este anexo. Si las librerías tienen vulnerabilidades publicadas en el momento de la firma del contrato, el adjudicatario se comprometerá a cambiarlas por la versión que no presente vulnerabilidades o por otro producto que ofrezca mayores garantías de seguridad siempre y cuando sea compatible con el proyecto.

8.7. Revisiones de seguridad

Derecho a la revisión: UOC tiene el derecho a revisar el código por fallos de seguridad. El adjudicatario acuerda proporcionar un apoyo razonable posteriormente a la fecha de entrega y

durante el periodo de garantía.

Cobertura de las revisiones: Las revisiones de seguridad incluirán todos los aspectos relacionados con la distribución de la aplicación, incluyendo el código desarrollado, los componentes, productos y la configuración del sistema.

Ámbito de la revisión: Como mínimo, la revisión alcanzará todos los requerimientos de seguridad y busca de otras vulnerabilidades. El examen puede incluir una combinación de escaneos de vulnerabilidades, macetas de penetración, análisis del código fuente, revisiones por terceras partes y revisión del código.

Problemas de seguridad descubiertos: Serán reportados tanto por UOC como el adjudicatario. Todas estas cuestiones serán rastreadas y solucionadas tal y como se especifica en la sección Gestión de los Problemas de Seguridad de este anexo.

8.8. Gestión de los problemas de seguridad

Identificación: El adjudicatario hará un seguimiento de todos los problemas de seguridad descubiertos durante todo el ciclo de vida de la aplicación, diseño, ejecución, ensayos, despliegue y garantía. El riesgo asociado a cada problema de seguridad será evaluado, documentado e informado en la UOC tan rápido como sea posible después de su descubrimiento.

Protección: El adjudicatario protegerá adecuadamente la información relativa a cuestiones relacionadas con la seguridad y la documentación asociada, para ayudar a que queden expuestas en el mínimo las posibles vulnerabilidades de la aplicación.

8.9. Fiabilidad

Fiabilidad: El adjudicatario ofrecerá un "paquete de certificación" que constará de la documentación de seguridad creada a lo largo del proceso de desarrollo. Este paquete de certificación establecerá y describirá como los requerimientos de seguridad, diseño, implementación y los resultados de las pruebas fueron debidamente agasajados y que todas las cuestiones de seguridad se resolvieron adecuadamente.

Certificación: El adjudicatario certifica que la aplicación cumple con los requerimientos de seguridad, que en el desarrollo se han realizado todas las actividades relacionadas con la seguridad y que todos los problemas de seguridad identificados se han documentado y resuelto. Cualquier excepción a la Certificación de la aplicación estará plenamente documentada en la entrega. Esta Certificación estará incluida dentro del "Paquete de Certificación".

Libre de código malicioso: El adjudicatario garantiza que la aplicación no contiene ningún código que no sea compatible con los requerimientos de la aplicación y debilite la seguridad de la aplicación, incluidos los virus, gusanos, bombas de tiempos, puertas secretas, troyanos,

huevos de Pascua y todas las demés formas conocidas de código malicioso.

8.10. Aceptación de la seguridad y garantía

Aceptación: El software de la aplicación no se considerará aceptado hasta que el "Paquete de Certificación" esté completo y todas las cuestiones de seguridad se hayan resuelto.

Investigación de los problemas de seguridad: Después de la aceptación, si se descubren problemas de seguridad o existe una sospecha razonable, el adjudicatario ayudará en UOC a llevar una investigación para determinar la naturaleza de la cuestión. Los hechos se considerarán una novedad.

Cuestiones de seguridad nuevas: El adjudicatario y UOC acuerdan dentro del ámbito de aplicación, que habrá un esfuerzo necesario para resolver los nuevos problemas de seguridad y negociarán de buena fe un acuerdo para realizar las tareas necesarias para corregirlos.

9. Anejo D: Requerimientos de Arquitectura

9.1. Funciones de arquitectura.

El adjudicatario asignará perfiles de Arquitecto de Soluciones para dar respuesta a las necesidades del servicio o proyecto, en la medida de lo necesario. Las funciones del arquitecto del adjudicatario serán:

- Responsable del diseño conceptual de la solución y la arquitectura de componentes tecnológicos necesarios para cubrir las necesidades descritas al pliego. En particular, el arquitecto entregará a primeros del proyecto el documento de Descripción de Arquitectura, que tendrá que ser aprobado por la UOC.
- Definir las diferentes alternativas posibles para dar cobertura a los objetivos descritos al pliego, determinando la mejor solución posible de todas las disponibles, siempre con la visión de diseñar un sistema el más parametritzable y flexible posible.
- Responsabilizarse que los artefactos que se librarán en la UOC lo serán en los términos acordados (hoja de ruta, patrones de diseño y desarrollo, automatización extremo a extremo)

Por su parte, las funciones del arquitecto UOC serán:

- Aportar los principios, estándares, patrones y diseños de alto nivel.
- Dar el visto bueno al documento de Descripción de Arquitectura, haciendo las enmiendas necesarias para que se sigan los principios estratégicos.
- Encajar la nueva solución o partes de la solución a la Arquitectura Empresarial de la UOC.
- Apoyo y acompañamiento a los perfiles equivalentes del adjudicatario.

9.2. Principios de arquitectura

La UOC tiene como principios estratégicos de arquitectura las siguientes directrices:

- Los nuevos sistemas y aplicaciones se regirán por los principios de cloud **first** (y preferentemente a cloud **público**), **mobile first** (en el sentido de multidispositiu) y serán **data-centric** (el dato como activo más importante de la organización)

En en cuanto a la selección de tecnologías, preferimos:

- Si existe un SaaS, es la opción preferente de uso.

- Si no existe un SaaS, pero existen productos:
    - Si es un problema común, utilizamos Open Source.
    - Si es un problema poco común, compramos el software.
- Si no existe: construimos, desarrollamos a medida.

Al construir un sistema:

- Se hará sobre servicios administrados (esto es, operación incluida en el servicio) de forma que nos focalizamos en la lógica de negocio, en el código. Esto aplica tanto:
    - a los building blocks de despliegue: PaaS, CaaS, FaaS, SaaS por encima de IaaS/VM.
    - a los servicios existentes en los clouds de referencia: servicios de notificaciones, colas, CDN, storage, …, por encima de soluciones desarrolladas a medida.

Teniendo presente el anterior, un sistema de cierta entidad estará descompuesto en subsistemas que darán respuesta a una necesidad funcional, de negocio, donde la selección anterior podrá aplicar a una parte concreta y podremos mezclar opciones, desarrollando una parte a medida (que será lo core de nuestro negocio) que se integrará con un SaaS o un producto Opensource que resuelve cierta funcionalidad.

En caso de que se trate de nuevas aplicaciones a desarrollar, se aplicarán los siguientes principios generales sobre el diseño de aplicaciones:

1. **Segregación de funciones/responsabilidades:** aplicaciones divididas estructuralmente en bloques disjuntos de funcionalidades, procesos o servicios, siguiendo un patrón de microservicios. Esto tendría que corresponder a una división física en los despliegues: un servicio, una base de datos.
2. **Desacoplamiento** de la presentación (cliente / frontend) y lo backend.
3. **Orientación a servicios**. Posibilidad de consumir las aplicaciones externamente o de integración con terceros. Los backends tienen que exponer sus funcionalidades de negocio vía servicios para facilitar esta integración. Los servicios estarán diseñados para ser fácilmente integrables al APIO Gateway para poder ser securitzats y gobernados de manera centralizada.
4. **Utilizar la memoria cae** siempre que sea posible. Para hacerlo, utilizar la tecnología que mejor se adapte tanto a cliente (html5 cache, localstorage , etc.) como servidor (Redis, Varnish, Memcache, caché personalizada, etc.)
5. **Desacoplamiento de la interfaz de usuario** de aquellos procesos que consuman muchos recursos y que puedan ser ejecutados de manera asíncrona.
6. Cuando sea necesario modificar servicios existentes, considerar siempre la compatibilidad **hacia atrás**.
7. Diseño de la aplicación teniendo en cuenta los **conceptos de elasticidad** (en ninguna

parte para soportar los picos de carga): **alta disponibilidad, alta concurrencia y cero downtime**.

8. Diseño de las aplicaciones pensante en la portabilidad, esto es, que se puedan mover con facilidad de un cloud privado a uno cloud público, por ejemplo.
9. Incorporar aspectos cualitativos al ciclo de vida:
    a. **Pruebas** para verificar la calidad del código, el apoyo de carga o requisitos no funcionales del sistema.
    b. **Documentación** detallada del proyecto (descripción de arquitectura, documento funcional, manual de despliegue, manual de explotación, ...).
    c. **Control de versiones**. El sistema en su conjunto tiene que ser tratado como un producto con sus versiones mayores, menores, etc...
    d. **Despliegue automatizado**, ejecución de pruebas automáticas que verifiquen la instalación e integración continua (ver Ciclo de CI/CD.)
10. En caso de necesitar **datos de otro sistema**, es mejor consumirlas **vía servicios**.
11. Delegar las **decisiones de autenticación utilizando o bien el protocolo SAML o bien OAuth** (si se trata de una SPA, aplicaciones móviles o bien de Apios). Las decisiones de autorización se tendrían que tomar en el ámbito de la aplicación, pero preferiblemente con los datos proporcionados por el sistema de autenticación de la UOC (perfiles, tipos de usuario...).

9.3. Building blocks y hoja de ruta del software

La UOC dispone de un catálogo de tecnologías (o building blocks), que se tendrán que seguir en caso de que aparezca una necesidad. Cualquier elección de una tecnología del catálogo que no se corresponda a la escogida por la UOC se tendrá que justificar y negociar con Arquitectura de la UOC. Por otro lado, la UOC mantiene una hoja de ruta de software con las versiones permitidas por cada una de las tecnologías soportadas, que en general se corresponden a versiones actuales y soportadas por el fabricante. El adjudicatario puede pedir más información tanto de los building blocks como de la hoja de ruta del software.

Ejemplo de extracto de la Hoja de ruta (apartado de lenguajes de programación):

			Obsolet	Suportat	Recomanat UOC
Llenguatges i runtimes	Golang		< 1.11	1.11.x	1.12
	Java		<=7	8	11
	NodeJS		< 8	8.x	10.x
	Python		< 2.7	2.7.x, >3.5	3.7.x

9.4. Entornos

La implantación de una nueva aplicación requiere que esta tiene que quedar configurada en 3 entornos operativos (producción, preproducción, test/integración), independientemente de si se trata de aplicaciones *cloud* privado, *cloud* público o legacy, en base a la siguiente arquitectura:

En torno a Test o Integración

Es el entorno que servirá para probar que los bloques a desplegar según las tecnologías pactadas al Documento de Descripción de Arquitectura y las integraciones con sistemas terceros (UOC o no) funcionan correctamente.

Entorno de Preproducción

Es el entorno que servirá para probar las nuevas versiones de los sistemas desarrollados en uno en torno a ejecución y datos idéntico al de Producción y que tiene que poderse replicar tantas veces como haga falta a partir del entorno de producción, poder detectar errores antes de hacer un cambio de versión en el entorno de Producción y hacerlo cuando se tengan las garantías que se han superado las pruebas necesarias. Este entorno será un clónico de producción donde desplegar todos los elementos que forman el sistema.

En este entorno es donde también se realizarán, normalmente, las formaciones.

Entorno de Producción

Es el entorno productivo de las aplicaciones de la UOC donde se encuentran las aplicaciones que dan servicios en los procesos de negocio de la Universidad.

10. Anejo E: Ciclo de CI/CD.

A continuación se resume el ciclo de integración y entrega continúa (CI/CD) de la UOC, que tiene como objetivo la automatización total del proceso y por tanto libre de errores humanos producidos de forma inevitable por los despliegues manuales. El ciclo tiene que ser end-to-end, es decir, llevar el código fuente de los desenvolupados hasta el en torno a producción sin más acciones manuales que los controles de calidad, seguridad y despliegue. El sistema de CI/CD de la UOC se compone de un conjunto de herramientas entre las que hay Atlassian JIRA, GitLab, Jenkins, Ansible, tal como se verá a continuación.

10.1. Tipo de despliegues.

La naturaleza de las aplicaciones UOC viene diferenciada en los siguientes tipos de despliegues:

- Aplicaciones tradicionales con despliegue manual (MVs)
- Aplicaciones tradicionales con despliegue automatizado en mayor o menor medida (MVs)
- Aplicaciones en contenedores (Openshift)
- Aplicaciones cloud en contenedores (AWS ECS/Fargate)
- Aplicaciones cloud en serverless (AWS Lambda)
- Aplicaciones cloud AWS Beanstalk
- Aplicaciones sobre Azure

10.2. Requisitos de los despliegues.

Para poder ser desplegadas mediante el CI/CD de la UOC, las aplicaciones tendrán que seguir los Building blocks y hoja de ruta del software.

El equipo responsable del CI/CD de la UOC realizará las siguientes tareas:

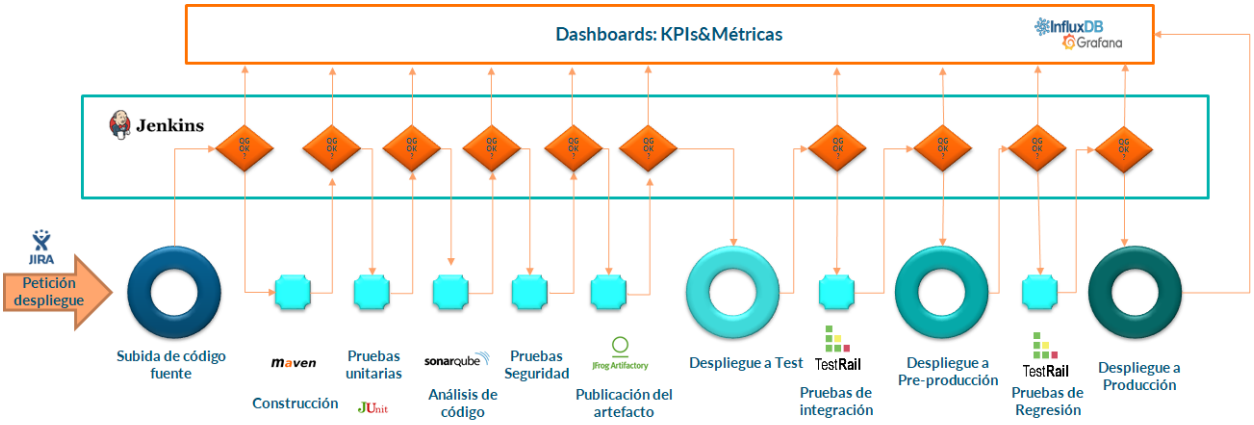
- Creación de todos los repositorios, componentes, etc… necesarios por el despliegue, que tienen que existir antes de la ejecución de los pipelines.
- Configuración de un proyecto JIRA, que gobernará el ciclo de vida de las aplicaciones, ejecutando los jobs de cada componente técnico enviando las órdenes y parámetros necesarios a Jenkins.
- Construir un fichero de configuración por cada componente técnico para ser invocados desde los *pipelines* de despliegue. En este fichero de configuración se incluirán variables de aplicación como la clave del proyecto por JIRA e información del entorno a despliegue.

El Arquitecto de Soluciones del proveedor colaborará en estas tareas resolviendo las posibles

dudas planteadas por el equipo de CI/CD.

10.3. Flujo de integración y despliegue continuo.

Una vez configurados todos los artefactos necesarios, el flujo de despliegue será como se describe a continuación:



A alto nivel, el pipeline de referencia por la integración y entrega continúa es el siguiente:

- El flujo se inicia cuando se abre una petición de despliegue a JIRA, indicando el entorno (TEST, PRE, PRO) y la rama de código.
- Se recupera el código de la rama indicada del repositorio de código GitLab.
- Construcción de los artefactos a partir de la compilación del código, ejecutando las pruebas unitarias. Si el código no compila o las pruebas unitarias fallan, el flujo se detiene.
- Análisis del código con SonarQube, si el umbral del QualityGate es menor que el definido, el flujo se detiene.
- Empaquetado y subida de los artefactos al repositorio JFrog Artifactory.
- Caso de que sea necesario, creación de los contenedores para ECS/Fargate o bien OpenShift.
- Provisión a la plataforma de TEST del entorno a ejecución correspondiente. En este entorno se podrán hacer pruebas de regresión, aceptación o de estrés. Estas pruebas se gestionan con TestRail.
- Una vez la versión se valide y acepte por parte de negocio, se promocionará en el entorno de PRO.
- Una vez finalizada, el pipeline etiquetará el commit del repositorio como desplegado a producción, con la fecha de despliegue y la versión.

En caso de que se detecten anomalías o bien la aplicación no responda correctamente a los “health checks”, se hará un “rollback” automático restaurante de este modo la última versión funcional de la aplicación.