

**PLIEGO DE PRESCRIPCIONES TÉCNICAS
PARTICULARES PARA LA CONTRATACIÓN DE UN
SERVICIO EN LA NUBE DE GESTIÓN DE
IDENTIDADES Y ACCESO DE CLIENTES (CIAM),
SINGLE SIGN ON (SSO) Y GESTIÓN DE
CONSENTIMIENTOS
MEDIANTE PROCEDIMIENTO ABIERTO**



EXPEDIENTE: 2024.104

24/09/2024(Versión 0)

1.	INTRODUCCIÓN Y ANTECEDENTES.....	4
1.1	INTRODUCCIÓN	4
1.2	ANTECEDENTES.....	5
2.	OBJETO	7
3.	ALCANCE	9
3.1.	REQUISITOS FUNCIONALES DEL SERVICIO	9
3.1.1.	GESTIÓN DE IDENTIDAD DE USUARIO, FLUJOS DE REGISTRO Y LOGIN	9
3.1.2.	REQUISITOS FUNCIONALES DE LA PLATAFORMA DE ADMINISTRACIÓN	12
3.1.3.	REQUISITOS FUNCIONALES DE LA GESTIÓN DE CONSENTIMIENTOS	13
3.1.4.	REQUISITOS FUNCIONALES DE INTEGRACIÓN	14
3.1.5.	DESCRIPCIÓN DE LOS PROCESOS DE AUTENTICACIÓN DE USUARIOS EN DISPOSITIVOS SMART TV /HBBTV.....	15
3.2.	REQUISITOS NO FUNCIONALES DEL SERVICIO	16
4.	FASES DE EJECUCIÓN.....	19
4.1.	FASE I: DESPLIEGUE, ADAPTACIÓN E IMPLANTACIÓN A LAS NECESIDADES DE LA EC DEL SERVICIO DE CIAM, SSO Y GESTIÓN DE CONSENTIMIENTOS EN MODO SERVICIO EN LA NUBE.....	21
4.1.1.	MIGRACIÓN DEL SERVICIO	21
4.1.2.	CONFIGURACIÓN DENTRO DEL SISTEMA CIAM DE LAS PLATAFORMAS EXISTENTES	22
4.1.3.	ACOMPañAMIENTO A LOS EQUIPOS DE DESARROLLO EN LA INTEGRACIÓN DEL SERVICIO EN LAS PLATAFORMAS EXISTENTES	23
4.1.4.	INTEGRACIÓN CON EL SISTEMA DE PARTICIPACIÓN DE USUARIOS	23
4.1.5.	FORMACIÓN	24
4.2.	FASE II: SERVICIO DE CIAM, SSO Y GESTIÓN DE CONSENTIMIENTOS EN MODO SERVICIO EN LA NUBE.....	25
4.2.1.	SOPORTE TÉCNICO, CORRECTIVO Y EVOLUTIVO	25
4.2.1.1	.SOPORTE TÉCNICO CARÁCTER PREVENTIVO	25
4.2.1.2.	SOPORTE TÉCNICO CARÁCTER CORRECTIVO	25
4.2.1.3	SOPORTE EVOLUTIVO	27
4.2.2.	LICENCIAMIENTO DEL SISTEMA DE CIAM/SSO Y GESTIÓN DE CONSENTIMIENTOS	27
4.2.3.	SERVICIOS ADICIONALES OPCIONALES	27
4.2.3.1.	CONFIGURACIÓN DENTRO DEL SISTEMA CIAM DE PLATAFORMAS ADICIONALES A LAS CONFIGURADAS EN LA FASE I	27

4.2.3.2.ACOMPAÑAMIENTO TÉCNICO A EQUIPOS DE DESARROLLO PARA LA INTEGRACIÓN DEL SERVICIO EN PLATAFORMAS ADICIONALES A LAS CONFIGURADES EN LA FASE I	28
5. PRECIO Y FACTURACIÓN	28
6. RECURSOS PROFESIONALES PARA LA PUESTA EN MARCHA DEL SERVICIO	28
6.1. CONDICIONES	28
6.2. CONDICIONES	30
7. SEGUIMIENTO DEL SERVICIO	31
8. PLAN DE SALIDA	31
9. PRUEBAS DE VALIDACIÓN TÉCNICA DE LA SOLUCIÓN TECNOLÓGICA OFERTADA ..	32
10. PENALIZACIONES	32
11. REQUERIMIENTOS EN MATERIA DE SEGURIDAD	32
12. DOCUMENTACIÓN A PRESENTAR POR LAS CANDIDATAS.....	33
12.1. SOBRE B.- DOCUMENTACIÓN RELATIVA A LA OFERTA EVALUABLE AUTOMÁTICAMENTE A TRAVÉS DE FÓRMULAS.	33

1. INTRODUCCIÓN Y ANTECEDENTES

1.1 Introducción

Euskal Irrati Telebista – Radio Televisión Vasca (en lo sucesivo, EITB) es un ente público de derecho privado dependiente del Gobierno Vasco creado en 1982 por el Parlamento Vasco para atender la exigencia social que demandaba a los poderes públicos un grupo de comunicación audiovisual propio, de carácter público, al amparo del artículo 19 del Estatuto de Autonomía.

El objetivo de EITB, desde su creación, es velar por la defensa de la libertad de expresión, el derecho a comunicar y recibir libremente información y cumplir con este cometido conforme a las exigencias de una sociedad democrática, impulsando la normalización del uso del euskera.

EITB también opera a través de la sociedad EITB MEDIA, S.A.U (en lo sucesivo, EITB MEDIA, Entidad Contratante o EC, indistintamente) de la que ostenta el 100 por cien de participación y que aglutina todos sus medios de televisión, radio e internet.

El conjunto de entidades, comprendiendo al Ente y la citada sociedad Anónima, es lo que viene a identificarse con la denominación de “Grupo EITB”.

Actualmente, el Grupo EITB afronta un momento crucial en el que ha de tomar decisiones estratégicas que marcarán su actividad en los próximos años, tanto en lo referente a la futura “apuesta” tecnológica, como en lo referente a la definición y lanzamiento de diversos proyectos corporativos de transformación y adaptación al mercado audiovisual.

En línea con lo expuesto, el Grupo EITB aprobó en el año 2021 su Estrategia con el horizonte puesto en el año 2030. Uno de los pilares de esa estrategia es, sin duda, la digitalización.

A este respecto, la Estrategia EITB 2030 determina que:

“[...] los continuos avances tecnológicos, los cambios sociales y los nuevos hábitos de consumo influyen en la misión, objetivos y actividades de EITB como grupo audiovisual público con medios de comunicación al servicio de la sociedad vasca. Estos factores, unidos a la digitalización, permiten nuevos modos de generación y difusión de contenidos, mientras conviven en el mismo universo empresas tradicionales y nuevos modelos de negocio, globales y locales. Las nuevas posibilidades de distribución y de acceso a los contenidos digitales de todo tipo, tanto informativos como de entretenimiento, son determinantes en el panorama actual. En este entorno, EITB debe adaptar su actividad, sus objetivos y acciones para responder a esta transformación.”

La visión y estrategia de EITB queda en línea con lo indicado resumida en el siguiente enunciado recogido en la Estrategia EITB 2030:

“[...] debemos ser la garantía de contenidos audiovisuales vascos y en euskera ante los nuevos consumos y soportes digitales, con nuestros medios de comunicación como referente para la sociedad vasca en información y servicio público, conectando con la juventud, siendo una ventana vasca al mundo y garantizando la sostenibilidad del “proyecto EITB”.

Dentro de este contexto, EITB ha estimado necesario concertar mediante la presente contratación un servicio en la nube que ofrezca una plataforma para la gestión de identidades (CIAM), un sistema de registro único (SingleSign-On), así como un sistema para la gestión de consentimientos de los usuarios que hagan uso de las distintas plataformas digitales de la EC (WEBS, OTTS, HbbTV, APPS NATIVAS ANDROID/IOS, ANDROID TV, APP TV, TVS CONECTADAS...).

1.2 Antecedentes

EITB MEDIA, S.A.U. cuenta en la actualidad con los siguientes tipos de plataformas audiovisuales:

- Plataformas OTT: incluye la publicación de contenido audiovisual en distintas ventanas de publicación:
 - Web
 - Aplicaciones nativas IOS/ANDROID
 - Aplicaciones para Smart TV
 - HBBTV

A modo informativo, actualmente se dispone en producción de 2 plataformas OTT (PRIMERAN, MAKUSI) y una tercera en fase de desarrollo.

Las *stores* de aplicaciones para Smart TV en los que la EC publica sus plataformas OTT son:

- Google Play Store (Android TV)
 - Samsung App Store (Tizen)
 - LG Content Store (WebOS)
 - Apple App Store (Apple TV)
 - Amazon Appstore (Amazon Fire TV y Fire TV Stick)
 - Hisense VIDAA Store (Hisense Smart TVs)
- Plataforma CMS/DXP: incluye la publicación de contenido audiovisual en distintas ventanas de publicación:
 - Web (desktop/mobile)
 - Apps nativas IOS/ANDROID (móviles y tablets)

A modo informativo, actualmente la plataforma CMS/DXP aloja en producción 1 portal web (MAKUSI.EUS) y hasta 10 portales más en fase de desarrollo e implementación, algunos de ellos dispondrán de su propia app nativa IOS/ANDROID.

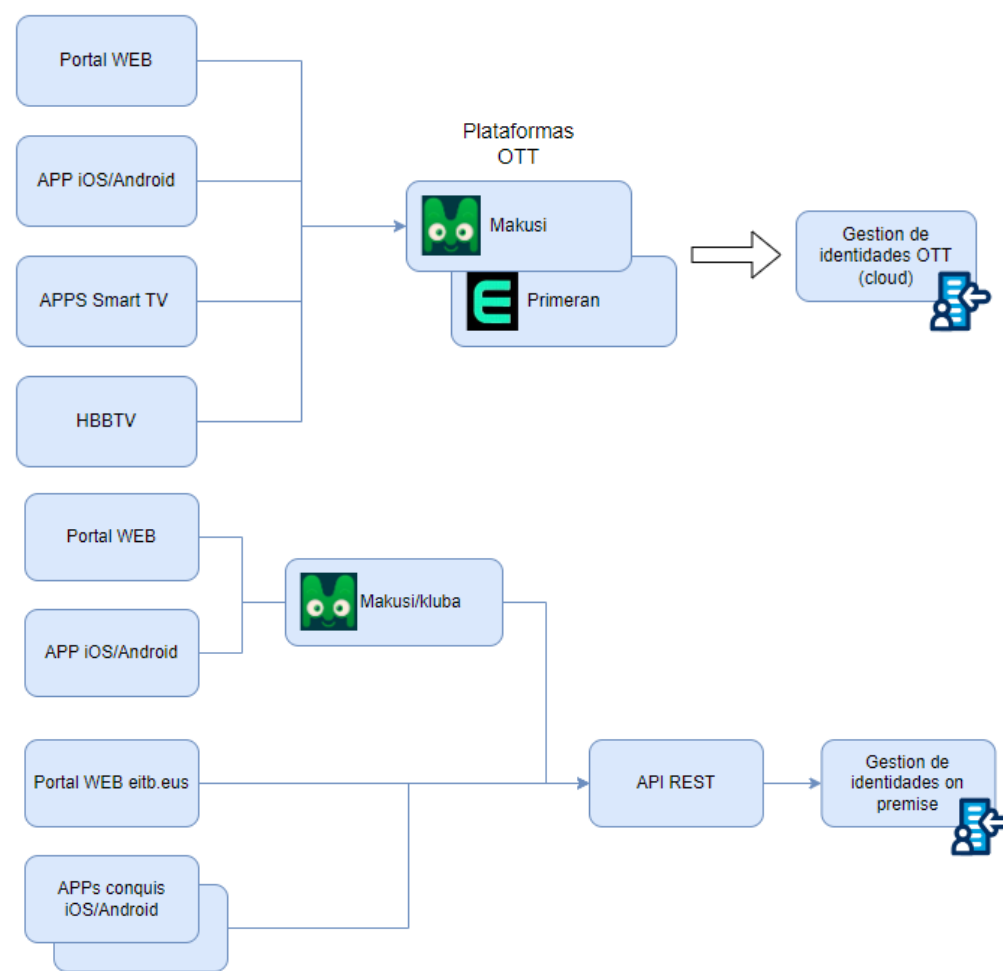
- Plataforma EITB.EUS: incluye la publicación de contenido audiovisual en distintas ventanas de publicación:
 - Web (desktop/mobile)
 - Apps nativas IOS/ANDROID (móviles y *tablets*) de ciertas secciones o contenidos destacados de EITB.EUS.

A modo informativo, se dispone de una web (*eitb.eus*) y varias aplicaciones nativas para noticias y algunos programas como (Baserria y el Conquis).

La gestión de identidades de los usuarios que interactúan con las distintas plataformas de la EC está dividida en dos. Por un lado, las plataformas OTT disponen de un sistema propio de gestión de identidades común a todas ellas, y por otro lado, el resto de plataformas se conectan a otro sistema de gestión de identidades desarrollado por la propia EC y alojado en las instalaciones de la misma.

Este último sistema de gestión de identidades se diseñó para ofrecer a los usuarios un entorno más ágil y con menos limitaciones para la participación en distintas iniciativas que dispone la EC. En dicho sistema, se utiliza una API REST desde la que se generan tokens JWT que identifican al usuario, disponiendo de una información básica cifrada de dicho usuario en el payload del token. Todas las peticiones a las plataformas están tokenizadas y son completamente privadas.

A través de esta plataforma no sólo se dispone de un sistema de gestión de identidades y consentimientos, sino que también se proporciona una gestión de participaciones en diferentes iniciativas, tales como concursos o subidas de contenidos. Estas participaciones están siempre referenciadas a diferentes comunidades de usuarios, y a su vez pueden estar vinculadas a un proyecto concreto dentro de una comunidad para categorizar dicha información.



Con la puesta en marcha de las plataformas OTT y del CMS/DXP, se constató la necesidad de aportar a los usuarios de las distintas plataformas digitales de la EC la funcionalidad de Single Sign On (SSO), además de mecanismos de seguridad como la autenticación de doble factor (MFA) o biometría. Otra necesidad es la de incorporar mecanismos de login/registro para las televisiones conectadas, tales como códigos QR, MagicLink o similares.

Teniendo en cuenta, por tanto:

- 1 La necesidad de gestionar la identidad de todos sus usuarios conectados a las diferentes plataformas de forma unificada y centralizada, proporcionando al usuario una estrategia unificada de gestionar su identidad y consentimientos en todas ellas.

- 2 Las perspectivas de alto crecimiento en cuanto a usuarios conectados a las distintas plataformas actuales y futuras.
- 3 La necesidad de desplegar nuevas plataformas digitales en los próximos años.
- 4 La necesidad de enriquecer la experiencia de los usuarios ofreciéndoles un login único para todas las ventanas de publicación de las distintas plataformas.
- 5 Conseguir un sistema de gestión de identidad y SSO robusto, seguro, estable, sencillo y rápido de integrar que permita garantizar la seguridad de los datos almacenados en el mismo, cumpliendo con las leyes sobre seguridad y protección de datos que se indican en el Esquema nacional de seguridad (ENS).

En virtud de lo expuesto se ha estimado necesario la contratación de un servicio en la nube de gestión de identidad (CIAM), Single Sign-On (SSO) y de gestión de consentimientos para ofrecérselo a los usuarios que se conectan a las distintas plataformas digitales de la EC desde sus distintas ventanas de publicación de contenidos.

2. OBJETO

De conformidad con lo indicado el presente pliego tiene por objeto definir y fijar las condiciones técnicas que regirán la contratación de **un sistema en modo servicio en la nube de gestión de identidades de usuarios (en lo sucesivo, CIAM), de Single Sign-On (SSO) y de gestión de consentimientos** para los usuarios que se conecten a las diferentes plataformas digitales de la EC.

De acuerdo con lo expuesto, la presente contratación comprenderá la realización de los siguientes trabajos/servicios:

- ✓ Despliegue, implantación y adaptación a las necesidades de la EC del servicio de CIAM, SSO y gestión de consentimientos en modo servicio en la nube.

Dentro del despliegue e implantación quedara incluido:

- Análisis de las necesidades del servicio que requiere la EC. Entrega de documento funcional.
- Configuración global del sistema de CIAM, SSO y gestión de consentimientos.
- Diseño e implementación de los flujos para el registro/login de los usuarios en las distintas plataformas digitales y ventanas de publicación multidispositivo que se soliciten, así como posibles desarrollos ad hoc requeridos según necesidades del servicio, previo acuerdo con la EC.
- Migración del sistema actual de gestión de identidades de la EC o, en el caso que tras el análisis se haya acordado con la EC hacer una migración "en caliente" de los usuarios, la puesta en marcha de la misma.
- Configuración específica en el sistema CIAM y SSO de cada plataforma digital a integrar existentes en producción o en fase de puesta en marcha en el momento de la adjudicación de la presente licitación. A modo informativo, en el punto 4 (Alcance) de este documento se especifican las plataformas y ventanas de publicación a integrar incluidas en el despliegue.
- La entrega de las APIs/SDKs necesarias para hacer uso de los servicios de forma automatizada adaptándolas en caso necesario según lo requiera la EC.

- Integraciones necesarias para alimentar los diferentes sistemas analíticos de la EC (Adobe Analytics, Comscore, datos en bruto...) con los datos del sistema de CIAM.
- Servicios profesionales para acompañamiento técnico en las integraciones del servicio de CIAM/SSO/gestión de consentimientos a los equipos de desarrollo de las plataformas existentes en producción o en fase de puesta en marcha en el momento de la adjudicación de la presente licitación.
- Servicios profesionales para la integración del sistema de participación de usuarios de la EC compuesta por la base de datos y API REST de desarrollo propio.
- Preparación, realización e impartición de una formación (técnica y operativa) relativa a los servicios ofrecidos por la plataforma y cuantas aplicaciones/herramientas hayan sido puestas a disposición de la EC para el correcto resultado y uso de los mismos. Incluye la entrega de un plan de formación.
- ✓ Soporte técnico, correctivo y evolutivo para nuevas configuraciones o modificaciones en la configuración global o de plataformas de la EC ya configuradas en el servicio.
- ✓ Licenciamiento del sistema de CIAM, SSO y gestión de consentimientos para el volumen usuarios que la EC requiere, basándose en la media anual de usuarios activos en el sistema. La EC prevé un volumen máximo de 700.000 usuarios activos de media anual (teniendo en cuenta los picos de usuarios activos).

Así mismo, la adjudicataria deberá, a solicitud de la EC, prestar servicios de:

- ✓ Configuración en el servicio de CIAM/SSO en la nube de plataformas digitales de la EC adicionales a las configuradas en la fase de despliegue y puesta en marcha del servicio.
- ✓ Acompañamiento técnico en las integraciones del servicio de CIAM/SSO/gestión de consentimientos a los equipos de desarrollo de plataformas digitales de la EC adicionales a las configuradas en la fase de despliegue y puesta en marcha del servicio.

Para garantizar la continuidad del servicio y la mejor experiencia posible en el uso del sistema, sus servicios y las herramientas complementarias puestas a disposición de la EC (así como su soporte y mantenimiento correspondiente), deberán estar comprendidas y garantizadas en la presente licitación, de acuerdo con los niveles de servicio exigidos para el cumplimiento de la disponibilidad y rendimiento detallados más adelante.

La prestación de los servicios se deberá efectuar en todo caso con arreglo a los requerimientos y condiciones que se estipulan en este Pliego, así como en el correspondiente Pliego de Cláusulas Administrativas Particulares (en adelante, PCAP), relativas a esta contratación, de los que se derivan los derechos y obligaciones de las partes contratantes.

3. ALCANCE

El sistema en modo servicio en la nube de CIAM, SSO y de gestión de consentimientos para los usuarios que se conecten a las diferentes plataformas digitales de la EC, debe ser una solución única procedente de un único fabricante. No se considerarán soluciones válidas aquellas que dependan de la integración de múltiples productos de distintos fabricantes, asegurando así una mayor cohesión, uniformidad en el soporte, actualizaciones centralizadas y una experiencia de usuario optimizada.

Los trabajos correspondientes a la producción, explotación y mantenimiento del sistema de CIAM/SSO/Gestión de consentimientos a modo servicio en la nube deberán dar cumplimiento de los requisitos descritos a continuación.

3.1. Requisitos funcionales del servicio

El sistema en modo servicio en la nube de gestión de identidades de usuarios (CIAM), de Single Sign-On (SSO) y de gestión de consentimientos para los usuarios deberá conectarse a las diferentes plataformas digitales que la EC disponga durante la duración de la presente contratación, para las funciones de registro y *login* en sus distintas ventanas de publicación:

- Web
- Aplicaciones nativas IOS/ANDROID
- Aplicaciones para Smart TV
- HBBTV

3.1.1. Gestión de identidad de usuario, Flujos de registro y login

De cara a facilitar el uso de todo el ecosistema de plataformas de la EC, la solución propuesta deberá disponer de las siguientes funcionalidades en lo que se refiere a la gestión del registro y *login* de usuario:

- Capacidad de **orquestrar flujos personalizables** para la EC asociados a los procesos de registro y *login* de usuarios, recuperación de contraseña..., diferenciables por cada plataforma / ventana de publicación. El orquestador de flujos deberá disponer al menos de las siguientes características:
 - Interfaz de usuario amigable para la creación de flujos, incluyendo **funcionalidades de Drag-and-Drop** sobre un lienzo, y uso de plantillas prediseñadas. La interfaz debe **permitir crear flujos sin necesidad de introducir código/scripts**, sólo siendo necesario en caso de flujos complejos y siendo dichos desarrollos responsabilidad del licitador.
 - Disponer de entorno de preproducción y desarrollo para testear los flujos contruidos.
 - Disponer de herramientas de depuración visual de los flujos contruidos.
 - Disponer de capacidad de importar, exportar y compartir flujos.
 - Orquestación disponible para cualquier modelo de implementación.
- Capacidad de **construir formularios personalizables** que componen los flujos asociados a los procesos de registro y *login* de usuarios, tales como:
 - Formulario de registro de usuarios (incluyendo registro a través de redes sociales).
 - Formulario de *login* de usuario (incluyendo *login* a través de redes sociales).
 - Formularios de recuperación de contraseña.

- Formulario de consulta y edición de datos de usuario (área privada de usuario).

La interfaz de usuario para la construcción de formularios deberá ser amigable para el usuario, incluyendo **funcionalidades de Drag-and-Drop** sobre un lienzo, y uso de plantillas prediseñadas. La interfaz debe permitir crear formularios **sin necesidad de introducir código/scripts**, sólo siendo necesario en caso de formularios complejos y siendo dichos desarrollos responsabilidad del licitador.

Look and feel de los formularios: todos los elementos con los que interactúe el usuario (formularios, área de cliente, correos electrónicos, etc.) deberán tener un estilo y funcionamiento completamente configurable y adaptable a las diferentes aplicaciones en las que estarán incluidos y pudiendo definir la lógica de validación de cada uno de los campos. Los diseños deberán ser responsive, teniendo siempre presente el enfoque *mobile-first*.

El idioma en que los formularios y sus elementos se muestran al usuario será configurable por cada una de las plataformas que se integren con el sistema CIAM, permitiendo incluso disponer de **formularios en multi-idioma**.

Los formularios dispondrán de reglas de validación de campos, tales como contenido de los campos de registro válidos, formatos de fechas, etc., con sus correspondientes avisos para el usuario final en el idioma en el que se esté realizando el proceso.

- La herramienta deberá ofrecer las siguientes funcionalidades que permitan el perfilado de los usuarios:
 - Capacidad de definir atributos (custom data) o campos asociados al perfil de usuario, añadiendo/modificando a demanda de la EC. Como mínimo se podrán definir 30 atributos.
 - Lo definido en el punto anterior deberá tenerse en cuenta en el diseño de los formularios y la validación de los datos introducidos en ellos (campos obligatorios/opcionales, formatos...) con sus correspondientes avisos para el usuario final en el idioma en el que se esté realizando el proceso.
- La herramienta deberá disponer de, al menos, los siguientes mecanismos de registro e inicio de sesión:
 - Capacidad de crear un **registro ligero** que permita a los usuarios inscribirse a *newsletters* u otros servicios que no requieran crear una cuenta, usando simplemente el correo electrónico. Posibilidad de definir *singleopt-in* (sin confirmación de correo) o *doubleopt-in* (con confirmación de correo).
 - Capacidad de diseñar **registros progresivos** que permitan el perfilado progresivo de usuarios, mediante los cuales es posible el registro con los datos mínimos y necesarios, y con la posibilidad de completar el perfil posteriormente cuando sea necesario. A tal efecto la herramienta permitirá definir flujos condicionales y configurables para soportar esta funcionalidad.
 - Registro "tradicional" con cuenta de usuario con correo electrónico a modo de ID de usuario, nombre de usuario y contraseña.
 - **Social login o registro/login** mediante las redes sociales más conocidas, vinculando los datos que tenga el usuario en una cuenta operativa en una red social.

- Ofrecerá acceso a datos de origen (siempre basados en permisos) tales como foto de perfil, intereses... que quedarán almacenados en la plataforma.
 - Deberá mantener sincronizado el perfil ante cambios en esa red social como puede ser la edición de un dato o incluso la eliminación de la cuenta.
 - Se aplicará una normalización de los datos cuando el usuario utilice distintas plataformas de red social. Siempre que el correo electrónico vinculado a la red social sea el mismo, se considerará un usuario único dentro del sistema CIAM.
- **Registro/login *password-less***, es decir, sin una contraseña reutilizable, usando en su lugar una verificación OTP (one-time password) mediante el cual el usuario recibe un código de un solo uso por SMS o correo electrónico.
 - **Inicio de sesión federado a través de los protocolos estándares SAML, OpenID entre otros.**
 - **Login para Smart TV y HbbTV:** Debido a la naturaleza de estos dispositivos y de cara a mejorar la experiencia de usuario, además de la posibilidad de introducir las credenciales con el mando a distancia, se requieren los siguientes mecanismos de autenticación según se detalla en el punto 3.1.5 de este Pliego de Prescripciones Técnicas:
 - Autenticación con código alfanumérico en pantalla
 - Autenticación mediante Dispositivo Móvil (Push Notifications).
 - Autenticación mediante Código QR (URL única)
 - Autenticación mediante Biométricos (si es compatible).
- Actualización del perfil: se debe permitir al usuario la edición de sus datos personales mediante formularios completamente personalizables

Sea cual sea el mecanismo de registro/login, deberá poder contar con medidas de protección y seguridad, incluyendo como mínimo:

- **Autenticación multifactor (MFA)**, es decir, mecanismos de protección adicionales a la contraseña, que debe funcionar con distintos proveedores de OTP (one-time password) como correo electrónico, SMS, entre otros.
- Validación de cuenta y recuperación de contraseña al menos por correo electrónico, preguntas/respuestas o con token de restablecimiento generado a través de llamadas al API.
- Recordatorio de usuario (remember me).
- Integración de **mecanismos que verifiquen que el usuario detrás del registro/login es humano y no un bot**, tales como CAPTCHA (con distintos formatos como caracteres, imágenes...).
- Políticas de actualización de contraseñas que permitan establecer plazos de renovación.
- Reglas configurables de complejidad para las contraseñas.
- Posibilidad de forzar el cierre de sesión en todos los dispositivos.

- Posibilidad de conocer todos los dispositivos en los que está iniciada la sesión de la cuenta del propio usuario, incluyendo la fecha de última actividad.
- Re autenticación: Volver a identificarse cuando se acceda a sitios clave.
- **Autenticación basada en riesgos (RBA).** El sistema ha de tener mecanismos para evaluar el nivel de riesgo asociado con un intento de inicio de sesión o una transacción (ubicación, número de intentos fallidos de login...) y aplicar medidas de seguridad adicionales cuando el riesgo es alto, tales como el envío de un e-mail de aviso al usuario.

Cualquier mecanismo de login o medida de seguridad asociada deberá poder activarse/desactivarse para cada una de las plataformas a integrar en el servicio de CIAM/SSO.

3.1.2. Requisitos funcionales de la plataforma de administración

La plataforma de gestión y administración de usuarios deberá dar cumplimiento a los siguientes requisitos funcionales

- Gestión y administración de usuarios:
 - Capacidades de configuración de reglas de vinculación y comportamiento entre cuentas/perfiles con diferentes roles ("padres" - "hijos")
 - Posibilidad de bloqueo o cancelación de cuentas
 - Mecanismos que permitan automatizar reglas para la gestión del tiempo de expiración de las cuentas de los usuarios y las notificaciones a los usuarios de caducidad o baja de sus cuentas.
 - Configuración del periodo de validez de las sesiones de usuario, una vez logueado en un dispositivo.
 - Configurar si se quiere auto-loguear tras verificar la cuenta.
- Configuración flexible de las políticas de generación y reutilización de contraseñas:
 - Determinar las características de la contraseña (longitud, complejidad).
 - Posibilidad de definir un tiempo de vida de las contraseñas, tras el cual forzar al usuario a un cambio de contraseña.
 - En relación con el punto anterior, poder configurar si se permite reutilizar contraseñas.
- Visión completa de métricas y data, tanto en tiempo real como histórico, tanto de la base de datos de usuarios como de su actividad en los distintos soportes, siendo posible su consulta en la plataforma de administración mediante dashboards y/o generación de informes:
 - Número de usuarios por estado (activos, logueados, última conexión...) e información por periodos temporales configurables.
 - Datos relevantes de actividad de usuario (nuevos registros, bajas, modificaciones, actividad sospechosa...)
 - Posibilidad de seguir la interacción del usuario en las diferentes plataformas y dispositivos utilizados.
 - Capacidad de exportar los datos granulares de usuarios y su actividad a sistemas externos:
 - De forma automática y programada a un repositorio externo mediante protocolos de transferencia de archivos habituales.
 - Haciéndolos accesibles vía **API REST segura**.

- Disponer de sistemas de alerta y monitorización del sistema CIAM/SSO que permitan a la EC verificar en tiempo real la salud del mismo. Los sistemas de alertas deberán incluir al menos:
 - Envío de correos electrónicos a administradores y cuentas adicionales configurables.
 - Envío de mensajes /traps a sistemas de monitorización propios de la EC.
 - Servicios de datos para su acceso desde herramientas o sistemas externos a la plataforma de autenticación con sus correspondientes mecanismos para garantizar un acceso seguro.
- Posibilidad de configurar niveles de riesgo de autenticación (RBA) por cada una de las plataformas a integrar en el sistema CIAM.
- Disponer de herramientas de recuperación de datos, incluyendo operaciones de administración y monitorización. El licitador tiene que explicar en la documentación técnica los métodos de recuperación de datos, tipos de datos a los que puede acceder y el método de acceso individual y acceso masivo.
- Disponer de herramientas de borrado e inserción de datos, incluyendo operaciones de administración y monitorización. El licitador tiene que entregar la documentación que describa el método de eliminación de datos, tipos de datos que se pueden eliminar y los métodos de eliminación individual y eliminación masiva.
- Disponer de un grado elevado de customización de los correos electrónicos y otros elementos con los que interactúan los usuarios, con mensajes y estilos diferenciados.

3.1.3. Requisitos funcionales de la gestión de consentimientos

La solución deberá garantizar la posibilidad de manejar los consentimientos que debe aceptar el usuario para poder hacer uso de las plataformas digitales de la EC. Estos deben poder ser diferenciados por cada plataforma a integrar en el sistema de gestión de consentimientos.

El sistema de gestión de consentimientos deberá cumplir los siguientes requisitos:

- El sistema debe permitir a los usuarios gestionar sus consentimientos de manera individualizada para el uso de sus datos personales, registrando además la aceptación o rechazo de cada consentimiento por parte del usuario, incluyendo la fecha y hora de cada acción.
- El usuario debe además ser capaz de revocar su consentimiento en cualquier momento a través de una interfaz amigable y accesible.
- El sistema debe proporcionar a los usuarios una vista detallada de los consentimientos otorgados, incluyendo la finalidad del uso de sus datos y los terceros con los que se comparte la información.
- Se garantizará el almacenamiento seguro y la consolidación de un número ilimitado de consentimiento y preferencias personalizadas en el registro del usuario en un repositorio único de todos los canales.
- Registro y auditoría de consentimientos.

El sistema debe mantener un registro histórico de todos los consentimientos otorgados, modificados y revocados por cada usuario. Debe permitir a administradores autorizados generar reportes de auditoría detallados que incluyan todos los cambios en los consentimientos.

- El sistema debe ofrecer API seguras para que aplicaciones externas puedan consultar y actualizar el estado de los consentimientos de los usuarios en tiempo real.
- El sistema debe permitir la recopilación escalable de datos de consentimiento y preferencias antes, durante y después del registro.
- Debe existir sincronización entre el consentimiento y las preferencias de usuario en el entorno.
- Se deben poder configurar flujos de trabajo para permitir a los usuarios aprobar o rechazar fácilmente todos los procesos relacionados con el consentimiento, incluidos los términos deservicio, las políticas de privacidad, el consentimiento de cookies (ePrivacy), las comunicaciones de marketing, encada etapa del recorrido del usuario.
- Configuración de la declaración de consentimiento.

Mediante una interfaz intuitiva en la herramienta de administración se tiene que poder definir fácilmente no solo el tipo de declaración, sino el hecho de que la política deba renovarse por su versión o por fecha, la fecha en la que entrará en efecto, y la fecha antes de la cual solicitar una renovación. Las declaraciones también deben poder configurarse como obligatorias u opcionales, según sea la EC lo disponga.

- Versionar los consentimientos para añadir modificaciones legales en los mismos, de forma que se mantenga la información de qué versión de un consentimiento concreto tiene aceptada un usuario determinado, y si no tiene aceptada la última versión disponible se le muestre en la siguiente interacción la posibilidad de aceptar dicha versión.
- **Los textos de los consentimientos deben ser multi-idioma**, permitiéndole al usuario visualizar el texto en el idioma que desee de entre los disponibles.
- Flujos automáticos de consentimientos.

El sistema debe permitir automatizar para obligar al usuario a volver a otorgar el consentimiento ante cambios mayores en los términos del mismo.

3.1.4. Requisitos funcionales de integración

La integración de la plataforma en las aplicaciones conectadas, así como otros procesos externos de diversos propósitos (analítica, migración de usuarios, base de datos de participación, etc.) es un elemento clave, siendo necesarias como mínimo las siguientes funcionalidades:

- API que permita la consulta, inserción, modificación y eliminación de datos de usuario.
- Integración con Adobe analytics.
- API que permita las mismas operaciones que se pueden realizar desde la plataforma de administración.

- Integración con aplicaciones móviles nativas mediante SDKs específicos para iOS, Android y TVs conectadas.
- Scripts para WEB, pudiendo insertar directamente en el código HTML.
- Integración a través de protocolos de autenticación como OpenID y SAML entre otros.
- Integraciones masivas de datos, dentro del contexto de una migración (tanto volcado como extracción de la plataforma CIAM) sin impacto en la experiencia de usuario.
- Permitir login desde aplicaciones backend. Se admite tanto API REST como librerías para lenguajes de programación más conocidos, tales como .NET, JAVA, PHP, python.

3.1.5. Descripción de los procesos de autenticación de usuarios en dispositivos Smart TV /HbbTV

Los mecanismos de autenticación desde Smart TVs presentan desafíos y oportunidades únicos debido a la naturaleza del dispositivo y su uso. La experiencia del usuario debe ser simple y accesible, y al mismo tiempo, mantener altos niveles de seguridad. A continuación, se describen mecanismos de autenticación de usuarios requeridos para Smart-TV y HbbTV:

- Autenticación con código alfanumérico en pantalla

El proceso a seguir sería el siguiente:

- Generación del Código: El usuario abre la aplicación en la Smart TV y selecciona la opción de iniciar sesión. La aplicación muestra un código alfanumérico único en la pantalla de la TV, junto con una URL específica.
- Ingreso del Código en un Dispositivo Secundario: El usuario abre un navegador web en su dispositivo móvil o computadora y navega a la URL proporcionada. En la página web, el usuario introduce el código alfanumérico mostrado en la TV.
- Autenticación en el Dispositivo Secundario: Después de ingresar el código, el usuario inicia sesión en el dispositivo secundario con sus credenciales. Una vez autenticado, la sesión se activa en la Smart TV.

- Autenticación mediante Dispositivo Móvil (*Push Notifications*).

El proceso a seguir sería el siguiente:

- El usuario selecciona iniciarsesión en la aplicación de la Smart TV.
- La aplicación envía una notificación push a un dispositivo móvil previamente registrado.
- El usuario aprueba la solicitud de inicio de sesión en el dispositivo móvil.
- La sesión se activa en la Smart TV.

- Autenticación mediante Código QR (URL única)

El proceso a seguir sería el siguiente:

- Inicio de sesión en la aplicación: El usuario abre la aplicación en la Smart TV donde se desea iniciar sesión.

- Generación del código QR: La aplicación en la Smart TV muestra un código QR único en la pantalla.
- Escaneo del código QR: El usuario utiliza un dispositivo móvil (como un smartphone o tablet) con cámara para escanear el código QR que aparece en la pantalla de la Smart TV.
- Redirección al sitio web de autenticación: Al escanear el código QR, el dispositivo móvil redirige al usuario a un sitio web específico.
- Inicio de sesión en el sitio web: En el sitio web al que se redirige, el usuario inicia sesión con sus credenciales.
- Confirmación y vinculación: Una vez que el usuario ha iniciado sesión correctamente en el sitio web, se confirma la autenticación y la cuenta se vincula con la aplicación en la Smart TV.
- Acceso a la aplicación: Después de completar el proceso, la aplicación en la Smart TV reconoce la autenticación y permite al usuario acceder a todas las funcionalidades y contenidos asociados con su cuenta.

Nota: Junto con el código QR deberá aparecer en pantalla la URL única (la misma que está codificada en el código QR) para garantizar la compatibilidad con dispositivos que no tengan la capacidad de leer códigos QR

- Autenticación mediante Biométricos (si es compatible).
 - La Smart TV o un dispositivo emparejado (como un teléfono móvil) solicita la autenticación biométrica (huella digital, reconocimiento facial).
 - El usuario completa la autenticación biométrica en el dispositivo.
 - La sesión se activa en la Smart TV

3.2. Requisitos NO FUNCIONALES del servicio

Con el fin de garantizar el cumplimiento de los estándares de calidad necesarios y el óptimo funcionamiento del sistema, la adjudicataria deberá dar cumplimiento en la ejecución a los siguientes requerimientos:

- **Confidencialidad, seguridad y protección de datos**

El servicio objeto de esta licitación debe proporcionar la confidencialidad y la seguridad de los datos almacenados, de los servidores y procesos de negocio. En particular, la solución y servicio propuestos deberán cumplir al menos los siguientes requerimientos en esta materia:

- El servicio de CIAM y SSO deberá ser prestado a modo servicio en la nube garantizando la separación de datos con respecto a otras plataformas, así como su control de acceso. Deberá ser gestionado por la adjudicataria con un servicio de soporte y mantenimiento 24x7.
- Deberá garantizar la seguridad de acuerdo con lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en lo sucesivo, ENS), de las comunicaciones con los servicios API, las aplicaciones de usuario/a final, las aplicaciones de gestión y monitorización, y el acceso los datos de los usuarios, mediante protocolos seguros: HTTPS, certificados SSL o TLS, y Tokens.

- El servicio deberá disponer de protección contra ataques DDos, y configuración de *Whitelist* y *Blacklist* que garanticen un tráfico seguro entre la EC y la plataforma.
- Los centros de datos que se utilizarán para la prestación del servicio estarán ubicados en la Unión Europea.
- El servicio deberá contar con políticas y prácticas de almacenamiento de *backups*, procedimientos y entornos de seguridad física y lógica relevantes, así como detalles técnicos, factor de replicación, procesos de recuperación antes desastres, etc.
- El servicio gestionado, es decir, los procesos operativos en los que se soporta dicho servicio y el personal involucrado deberán estar cualificados y ser acorde para mantener el nivel de seguridad exigido.
- La plataforma deberá cumplir la normativa vigente en materia de privacidad y protección de datos (GDPR), disponiendo entre otras, de herramientas de gestión, exportación y eliminación de datos personales de los usuarios a través de una interfaz de usuario. La empresa adjudicataria deberá tratar los datos de carácter personal dentro del Espacio Económico Europeo y no se podrán tratar fuera de este espacio ni directamente ni a través de cualquiera de los subcontratistas autorizados.
- La solución tiene que registrar los datos de cada intento de acceso a la plataforma, incluyendo información relativa a la identificación unívoca del usuario, fecha y hora, información a la que se ha accedido y tipo de acceso. Estos registros tendrán que custodiarse durante un mínimo de doce meses.
- La solución debe garantizar el procesamiento inmediato de las bajas de los usuarios mediante las herramientas de administración de las aplicaciones, inhabilitando el acceso a dichas aplicaciones con el código de usuario dado de baja. La baja de un usuario implica su bloqueo al menos temporal, antes de proceder a su eliminación definitiva.
- Gestión e Incidentes de Seguridad: Se debe garantizar la fluidez en las comunicaciones y el cumplimiento de los plazos establecidos en la gestión y registro de los incidentes de seguridad, integrándose con los procedimientos que se citan la "Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad", aprobada por Resolución, de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, donde se establece que las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información y el artículo 33 "Notificación de una violación de la seguridad de los datos personales a la autoridad de control" del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

La adjudicataria deberá por tanto responsabilizarse en el caso de ataque o consecuencias derivadas del uso de las aplicaciones cliente en los dispositivos de los/as usuarios/as finales.

Las candidatas deberán asimismo indicar en este apartado sus propuestas los mecanismos de auditoría de seguridad sobre la plataforma y el contenido del mismo, que tiene previsto mantener durante la ejecución del presente contrato. Los sistemas de seguridad deberán en todo caso presentar una cadencia de auditoría al menos semestral.

La EC se reserva, en todo caso, la facultad de realizar pruebas o solicitar las certificaciones que correspondan en materia de seguridad a fin de comprobar los términos de seguridad indicados.

- **Escalabilidad de aplicaciones a conectar.**

Se debe garantizar la escalabilidad a futuro para dar cabida a nuevas aplicaciones que requieran de integración de la solución de gestión única de identidad. Esa previsión de crecimiento deberá así mismo tener en cuenta la necesidad de adaptarse a una amplia gama de entornos como puede ser dispositivos móviles, tablets y desktop.

- **Escalabilidad de usuarios.**

El sistema tiene que ser capaz de crecer en cuanto a volumen de usuarios, partiendo de una situación inicial de una media anual de unos 200.000 usuarios activos, pasando por incrementos de franjas de usuarios según demanda y llegando en un posible escenario final a ser capaz de soportar una media anual de hasta 700.000 usuarios únicos activos. A los efectos de esta licitación, un usuario registrado, es un usuario que se registra en cualquier plataforma digital de la EC, o bien que se registra mediante el login delegado en redes sociales. Para tal fin, un usuario registrado tiene como mínimo que indicar su email. Se define como usuario único registrado, al conjunto de usuarios registrados que comparten un mismo email.

- **Rendimiento**

Se debe asegurar un rendimiento óptimo en todas las webs/dispositivos, asegurando que la inserción de la solución de identidad unificada en el ecosistema de la EC no penaliza la experiencia de los usuarios.

El tiempo máximo de respuesta satisfactoria para una petición no puede exceder los 500 milisegundos, independientemente de la concurrencia o picos de usuarios conectados.

- **Calidad de servicio**

Con objeto de agilizar y mantener una buena experiencia de usuario/a, se requiere que la integridad y disponibilidad del servicio esté garantizada al 99,95 % (SLA) del tiempo, así como el uso de las aplicaciones asociadas al mismo.

- **Repositorios de usuarios por entorno**

Deben existir al menos un entorno de producción, otro de preproducción y otro de desarrollo.

- **Multi-Idioma**

El usuario, dentro de su actividad en las plataformas digitales de la EC se encontrará con distintos puntos de contacto, entre otros: formulario de login, registro, área privada de usuario, avisos al usuario final, avisos/formulario para la gestión de los consentimientos, avisos por e-mail.

El servicio de CIAM/SSO deberá poder configurarse para mostrar todos los elementos con los que interactúa el usuario en distintos idiomas, entre los cuales deben estar al menos el castellano, euskera, inglés y francés. Los criterios para mostrar un idioma u otro los definirá la EC según distintos criterios (definido según plataforma, host, URL u otros)

- **Documento de análisis de las necesidades del servicio**

Durante la fase de despliegue y adaptación del servicio (Fase I) se deberá entregar un documento donde el licitador tras una fase de análisis de las necesidades de la EC, proponga soluciones y estrategias a seguir para la implantación y adaptación de su solución CIAM, SSO y gestión de consentimientos.

- **Test y QA**

Durante la fase de despliegue e implantación del servicio se deben realizar pruebas integrales que validen el correcto funcionamiento de la solución en todas las plataformas / ventanas de publicación identificados.

- **Plan de migración de usuarios al nuevo sistema CIAM**

El licitador deberá entregar, dentro la fase de despliegue (Fase I), un plan de migración de usuarios al nuevo sistema CIAM.

- **Plan de formación**

Tras el análisis de las necesidades del servicio, la adjudicataria deberá entregar dentro la fase de despliegue (Fase I) un plan de formación técnica y operativa relativo al servicio y cuantas aplicaciones/herramientas hayan sido puestas a disposición de la EC para el uso y monitorización del mismo.

- **Plan de salida**

Tras el análisis de las necesidades del servicio, la adjudicataria deberá entregar dentro la fase de despliegue (Fase I) un plan para la salida ordenada del servicio una vez concluido el periodo contratado en el caso de no ser adjudicataria de la continuidad del mismo. Dicho plan deberá actualizarse en función de las evoluciones que se implementen y que puedan tener afectación en el planteamiento inicial.

- **Plan de asesoría técnica para integraciones del sistema CIAM/SSO**

Tras el análisis de las necesidades del servicio, la adjudicataria deberá entregar dentro la fase de despliegue (Fase I) un documento donde se defina el acompañamiento técnico en las integraciones del servicio de CIAM/SSO/gestión de consentimientos en las plataformas existentes en producción o en fase de puesta en marcha en el momento de la adjudicación de la presente licitación (Documentación, sesiones online, chat de consulta online, email...)

- **Plan de Gestión, Evaluación y Respuesta ante ataque y pérdidas de información**

Tras el análisis de las necesidades del servicio, la adjudicataria deberá entregar dentro la fase de despliegue (Fase I) un documento donde se defina la propuesta de un Plan de Gestión, Evaluación y Respuesta ante ataque y pérdidas de información en el sistema de CIAM objeto de esta licitación.

4. FASES DE EJECUCIÓN

Los servicios objeto de la presente contratación deberán ser ejecutados en atención a las siguientes fases:

1. Fase I: IMPLANTACIÓN.

La adjudicataria durante esta fase deberá completar las siguientes tareas:

- Análisis de las necesidades del servicio incluyendo la entrega de un documento funcional donde se incluye la propuesta de la configuración del sistema y la implementación de los flujos ad-hoc para la EC.
- Configuración global del sistema CIAM, SSO y gestión de consentimientos para la EC.
- Definición e implementación de formularios y flujos de registro y login dentro del sistema CIAM/SSO.
- Migración del sistema actual de identidades de la EC al nuevo sistema CIAM. Dependiendo de la estrategia a seguir, esta tarea incluirá el volcado de usuarios al sistema o el desarrollo necesario para una migración "en caliente" de los usuarios.
- Entrega de APIs/SDK necesarias para fases posteriores.
- Integración con sistemas analíticos de la EC: implica el desarrollo de las distintas exportaciones de datos a realizar a los sistemas que EITB tiene actualmente para la explotación de datos.
- Configuración específica en el sistema CIAM/SSO de cada plataforma a integrar.
- Acompañamiento técnico en las integraciones de las plataformas existentes: Soporte a cada uno de los equipos de desarrollo que tengan que realizar la integración el sistema CIAM/SSO en su plataforma. Integración del sistema de participación de usuarios de la EC según se detalla en el punto 4.1.3 del presente PPTP.
- Formación técnica para la EC según se detalla en el punto 4.1.5 del presente PPTP.

2. Fase II: SERVICIO.

La adjudicataria durante esta fase deberá completar las siguientes tareas:

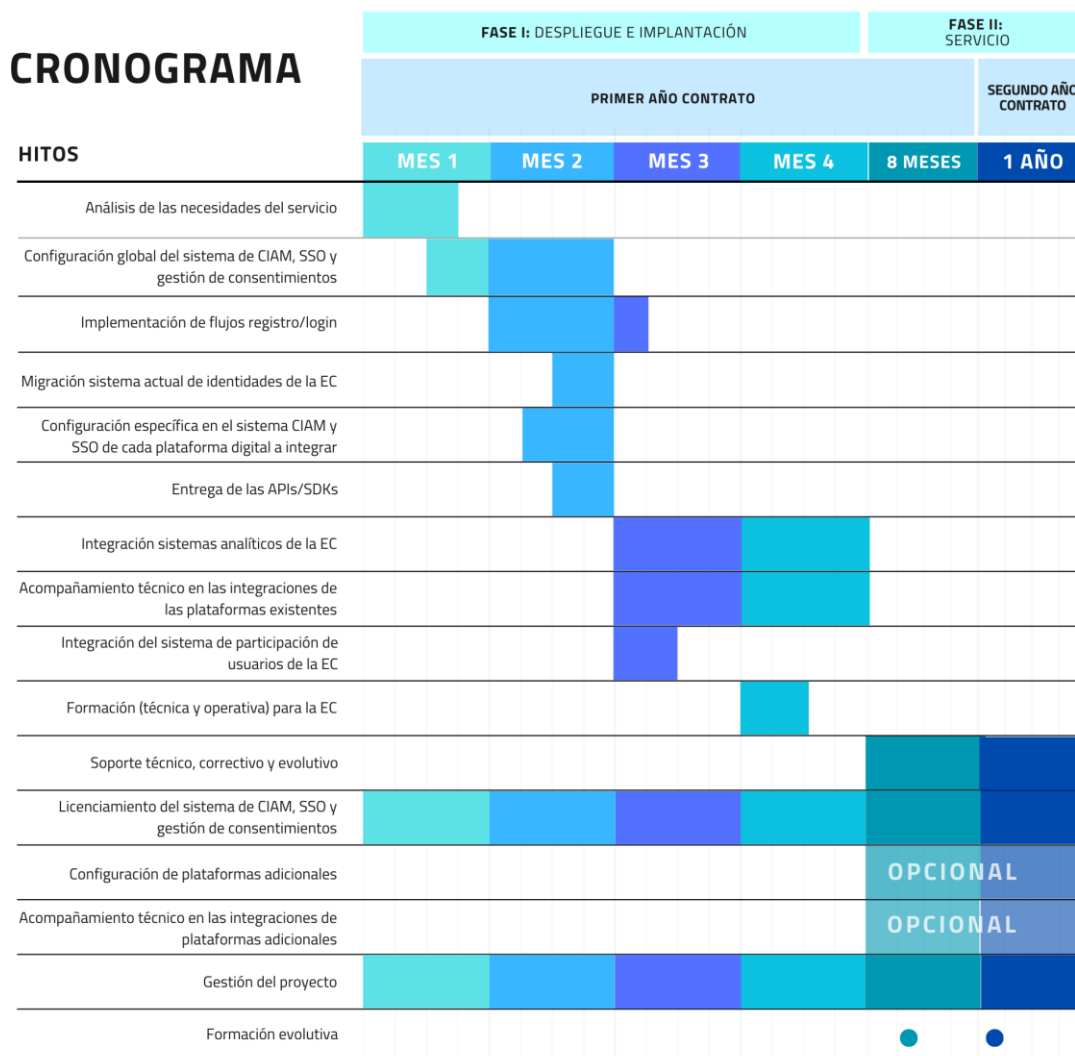
- Soporte técnico, correctivo y evolutivo para nuevas configuraciones o modificaciones en la configuración global o de plataformas de la EC ya configuradas en el servicio según se detalla en el punto 4.2.1 del presente PPTP.
- Licenciamiento del sistema de CIAM, SSO y gestión de consentimientos para el volumen usuarios que la EC requiere, basándose en la media anual de usuarios activos en el sistema. La EC prevé un volumen máximo de 700.000 usuarios activos de media anual (teniendo en cuenta los picos de usuarios activos).

Así mismo, la EC durante la vigencia de la presente contratación podrá con cargo al precio ofertado en el apartado correspondiente de su propuesta económica solicitar los siguientes trabajos:

- Servicios de configuración en el servicio de CIAM/SSO en la nube de plataformas digitales de la EC adicionales a las configuradas en la fase de despliegue y puesta en marcha del servicio.
- Servicios profesionales para acompañamiento técnico en las integraciones del servicio de CIAM/SSO/gestión de consentimientos a los equipos de

desarrollo de plataformas digitales de la EC adicionales a las configuradas en la fase de despliegue y puesta en marcha del servicio.

A modo de resumen, las fases y tareas descritas se recogen en el siguiente cronograma:



4.1. Fase I: Despliegue, adaptación e implantación a las necesidades de la EC del servicio de CIAM, SSO y gestión de consentimientos en modo servicio en la nube.

El despliegue, implantación y puesta en marcha efectiva de la plataforma en modo servicio en la nube se deberá realizar en un periodo máximo de DIECISEIS (16) semanas naturales a contar desde el día siguiente a la formalización del contrato por ambas partes.

4.1.1. Migración del servicio

Tras el análisis de las necesidades del servicio y durante la Fase I (Despliegue e Implantación) la adjudicataria presentará una propuesta para la realización del Plan de Migración de los datos de identidades de usuarios que actualmente residen en sistemas de gestión de identidad de la EC, en el que justificará:

- La metodología propuesta

- El cronograma de tareas propuesto para su ejecución
- Las garantías sobre continuidad del servicio durante el periodo de migración
- La calidad y cantidad de los recursos comprometidos

El plan deberá contemplar las siguientes alternativas para ejecutar la migración de los usuarios, con argumentación justificada acerca de la solución más idónea:

1. Migración completa, consistente en el “volcado” de los datos de identidades de usuario residentes en los sistemas de la EC.
2. Migración “en caliente”, en el cual mediante el flujo de login de usuarios, el sistema deberá comprobar si esa identidad existe en los actuales sistemas de gestión de identidad de la EC; en caso afirmativo, deberá registrar al usuario en el nuevo sistema de forma transparente.

La elección de la alternativa más idónea del plan de migración deberá ser consensuada y aprobada por la EC antes de su ejecución.

La migración de los servicios contratados es responsabilidad exclusiva del adjudicatario asumiendo los costes (infraestructura / tráfico, etc.) que ésta implique, incluyendo los derivados del movimiento de la información y contenidos almacenados en los servicios actualmente contratados. En función del plan propuesto y con el objetivo de facilitar dicha migración, la EC valorará la viabilidad de facilitar perfiles especiales de acceso al actual sistema de gestión de identidades de la EC.

4.1.2. Configuración dentro del sistema CIAM de las plataformas existentes

Tras la información recogida en la tarea de Análisis de las necesidades del servicio, la adjudicataria deberá configurar cada una de las plataformas en producción o en fase de puesta en marcha actualmente, pudiendo requerir distintos tipos de configuración y flujos para cada una de ellas, según disponga la EC.

A modo de ejemplo, se expone el caso del club infantil que dispone la EC (MAKUSI), donde el registro tiene la particularidad de asociar usuarios registrados (padres/tutores de los niños) a perfiles infantiles (niños).

En la siguiente tabla se lista la relación de plataformas junto con las distintas ventanas de publicación que requerirán de integración dentro del sistema CIAM/SSO en una primera fase de despliegue, adaptación e implantación.

Tipo plataforma	Ventana de publicación	Número de elementos
OTT	Portal WEB	3
	Aplicación nativa Android	3
	Aplicación nativa iOS	3
	Aplicaciones Smart TV	6
	HbbTV	3
CMS/DXP	Portal WEB	4
EITB.EUS	Portal WEB	1
	API participación usuarios	1
	Aplicación nativa Android	2
	Aplicación nativa iOS	2

Los tipos de aplicaciones Smart TV de las plataformas OTT se publican en los siguientes stores:

Store de aplicaciones de Smart TV	Número de aplicaciones
Hisense VIDAA Store (Hisense Smart TVs)	1
Google Play Store (Android TV)	2
Samsung App Store (Tizen)	2
LG Content Store (WebOS)	2
Apple App Store (Apple TV)	1
Amazon Appstore (Amazon Fire TV y Fire TV Stick)	1

4.1.3. Acompañamiento a los equipos de desarrollo en la integración del servicio en las plataformas existentes

Si bien dentro del alcance del contrato, no se incluye los desarrollos para integrar el servicio licitado en cada una de las plataformas de consumo digital que tiene la EC, sí que está incluido dentro de las tareas del despliegue e implantación del servicio (FASE I) el servicio de asesoría técnica para los equipos de desarrollo de dichas plataformas (Las plataformas en producción o en fase de puesta en marcha actualmente) , y así poder acompañarles durante el proceso de integración para garantizar que se realiza con solvencia, y lo más rápido posible de forma satisfactoria.

Los servicios profesionales de asesoría técnica requeridos para los equipos dependerán del stack tecnológico y del tipo de integración, ya que la complejidad variará considerablemente. En la tabla que aparece en el punto 4.1.2 del presente PPTP, se definen los distintas ventanas de publicación y su naturaleza tecnológica.

Los Servicios profesionales de asesoría técnica deberán comunicarse con los equipos de desarrollo de plataformas digitales de la EC en castellano.

Cada unidad de "Servicios profesionales de asesoría técnica y acompañamiento a los equipos de desarrollo de plataformas digitales" contratada, al menos deberá incluir:

- Sesión formativa técnica inicial presencial u online para integrar el servicio de CIAM/SSO/Gestión de consentimientos en las ventanas de publicación de la plataforma digital.
- Comunicación vía chat (por ejemplo, Teams) con asesor técnico para resolución de dudas durante el periodo de integración del servicio en la plataforma digital.
- Comunicación por videollamadas con asesor técnico para resolución de dudas y corrección de errores durante el periodo de integración del servicio en la plataforma digital.

Este servicio de asesoría técnica y acompañamiento deberá ser un servicio ágil y estar disponible los días laborales (lunes a viernes) en horario de 09:00 h- 17:00 h.

La duración del servicio de asesoría estará supeditada a la finalización de la integración del servicio CIAM/SSO/Gestión de consentimiento en las ventanas de publicación de la plataforma digital.

4.1.4. Integración con el sistema de participación de usuarios

Tal y como se ha detallado anteriormente en el apartado de antecedentes, actualmente la EC dispone de una API para registrar la participación de los usuarios. Para acceder a dicha API la petición debe haber sido validada previamente por el gestor de identidades, es decir, que solo se podrán registrar las participaciones de usuarios validados. El sistema de gestión de identidades (CIAM) debe proporcionar los mecanismos necesarios para llevar a cabo esta validación.

4.1.5. Formación

El propósito de las formaciones es dotar a la EC con el conocimiento necesario para utilizar la herramienta de manera independiente. Esto deberá permitir encontrar información como un perfil específico de un usuario, el estado de los consentimientos, el momento en que se modificó un consentimiento determinado, la consulta de paneles de control, entre otros datos.

Las candidatas deberán formular como parte de su propuesta un plan de formación (presencial u online) detallando la formación que impartirá.

Dicho plan deberá contemplar, al menos, el siguiente contenido:

- UN (1) curso técnico de configuración, administración de la plataforma, supervisión, configuración de las aplicaciones y herramientas web asociados al servicio de, al menos, VEINTE (20) horas a impartir preferiblemente en sesiones de 2 horas diarias durante dos semanas de forma online o presencial en la sede de Bilbao de la EC, coincidiendo con la puesta en marcha del servicio.
 - Introducción al sistema. Conceptos básicos
 - Visión general de la plataforma, describiendo su arquitectura y componentes principales; navegación entre las distintas secciones del panel de control, descripción de los distintos menús y secciones
 - Gestión de usuarios y consentimientos: creación de usuarios y perfiles, configuración del perfilado de usuarios, gestión de consentimiento y mecanismos para auditoría de consentimientos
 - Formularios y demás elementos de interacción con el usuario: Creación y personalización de los formularios de login y registro
 - Flujos de trabajo: Configuración de los flujos de trabajo
 - Métricas, dashboards e informes. Explicación de las posibilidades del sistema para monitorizar métricas mediante dashboards e informes, así como disponibilizarlas métricas a sistemas externos.
- UN (1) curso técnico sobre utilización de la API y SDKs para desarrolladores de, al menos, CUATRO (4) horas que será impartido de forma online o presencial en la sede de Bilbao de la EC, durante la fase de puesta en marcha del servicio.
- UN (1) curso evolutivo anual de configuración, administración y monitorización de la plataforma, de, al menos, SEIS (6) horas anuales que será impartido de forma online o presencial en la sede de Bilbao de la EC con la finalidad de optimizar el uso del servicio debido a actualizaciones en las funcionalidades. Este curso sólo se ejecutará si así la EC lo requiere o considera necesario.

Los cursos de formación deberán ser realizados apoyándose en la Documentación Técnica y los Manuales de administración y configuración, que el Adjudicatario habrá entregado con la suficiente antelación. Los cursos de formación podrán ser grabados para posteriores formaciones internas de la EC y optimizar los tiempos de formación del adjudicatario.

Tanto el profesorado asignado a los cursos, como el temario de los mismos, deberán ser aprobados por la EC. La formación deberá impartirse en castellano.

Documentación Técnica: El licitador indicará en este apartado de su oferta toda la documentación técnica, documentación sobre APIs y todos los manuales de operación incluidos, que va a entregar a la EC en caso de ser adjudicatario y el idioma de los mismos.

Esta documentación técnica será entregada en formato electrónico.

La organización horaria de los cursos será acordada entre la adjudicataria y la EC en la fase de implantación y puesta en marcha del servicio.

4.2. Fase II: Servicio de CIAM, SSO y gestión de consentimientos en modo servicio en la nube.

4.2.1. Soporte técnico, correctivo y evolutivo

La adjudicataria deberá responder a todas las cuestiones relativas al sistema, incluyendo servicios y aplicaciones.

Este servicio de soporte deberá poder comunicarse en idioma castellano por el medio que establezca la adjudicataria en su propuesta de servicio.

Todos los protocolos de comunicación y respuesta deberán ser coordinados con la EC y debiendo garantizar los siguiente niveles atención:

4.2.1.1. Soporte técnico carácter preventivo

El soporte preventivo tendrá por objeto la supervisión proactiva integral sistema: (tiempos de respuesta, SLA de servicio, parámetros de rendimiento, control de calidad de los resultados de los diferentes servicios, estado general de los flujos, disponibilidad de la API, planificación de actualizaciones para evolución del sistema, aplicaciones cliente, subsanación de *bugs*, notificación proactiva de mejoras en la parametrización del servicio, etc.).

Además, la adjudicataria deberá poner a disposición de la EC las herramientas que considere necesarias para la monitorización en tiempo real del servicio de forma integral para la:

- Monitorización en tiempo real del estado del sistema, rendimiento, consumo de recursos, alarmas sobre eventos que impliquen riesgo.
- Dispondrá de mecanismos para la monitorización en tiempo real de la actividad de la misma por parte de la EC. Además, la empresa adjudicataria proporcionará a la EC el acceso a los ficheros de logs correspondientes a cada servicio y sus aplicaciones.

4.2.1.2. Soporte técnico carácter correctivo

Quedará comprendido dentro de la presente contratación un servicio de asistencia y soporte debiendo dar debido cumplimiento, al menos, a los siguientes parámetros:

- Atención 24x7x365 por teléfono, email y herramienta de *ticketing* que la adjudicataria deberá poder proporcionar. La EC en cualquier caso, podrá establecer su propio sistema de *ticketing*, al cual la adjudicataria tendría acceso.
- Concretar un procedimiento para la comunicación entre la EC y la adjudicataria para la coordinación del servicio que tengan como eje el/la responsable del servicio designado.

- Disposición de personal cualificado para atención de primer contacto con conocimiento de la plataforma en cuestión y sus servicios, con un responsable de referencia como interlocutor/a del servicio.
- Respuesta en función de la criticidad de la incidencia
 - ✓ Niveles de criticidad de las incidencias

Las incidencias que lleguen al servicio de soporte se gestionarán y clasificarán según la criticidad con que deben solucionarse. Este nivel de criticidad se establecerá por la EC en el momento de notificar una incidencia.

Los cuatro (4) niveles de criticidad que deberá atenderse al amparo de esta contratación se definen a tal efecto en la siguiente tabla:

Nivel de criticidad Prioridad	Prioridad	Descripción	Criterio de actuación
1	Muy Alta	Incidencia que provoque un paro en los sistemas de negocio o los dificulte gravemente.	Se atiende al 100% hasta su solución
2	Alta	Varios servicios críticos no están disponibles, o funcionando a capacidad reducida afectando a los sistemas de negocio	Se atiende al 100% hasta su solución
3	Media	Sin impacto inmediato en los sistemas de negocio, con pérdida de funcionalidad parcial no crítica	Se evalúa el impacto y se atiende según criticidad
4	Baja	Problema con limitado o ningún impacto en producción. Sin impacto a ningún otro sistema	Se evalúa el impacto y se atiende según criticidad.

De conformidad con lo indicado en la tabla se establecen los tiempos de respuesta y de atención que se deben cumplir, ya sea para solucionar la incidencia o en su defecto para escalarla al servicio del soporte del fabricante correspondiente.

Nivel	Prioridad	TA (Tiempo Atención)	TR (tiempo respuesta)
1	Muy Alta	Inmediato	1 horas
2	Alta	1 hora	4 horas
3	Media	4 horas	NBD (siguiente día laboral)
4	Baja	NBD (siguiente día laboral)	NBD (siguiente día laboral)

En cualquier caso, el formato de resolución de la incidencia siempre será contrastada con la EC a fin de acordar la mejor aplicación de la solución, pero respetando siempre los niveles de criticidad y las formas de resolución de las incidencias marcadas en este documento.

4.2.1.3. Soporte evolutivo

La adjudicataria dentro el servicio de soporte evolutivo deberá atender las necesidades derivadas de:

- Actualizaciones de software, aplicaciones y parches/correcciones de todos los elementos que componen la solución ofertada.
- Actualización de documentación en caso de actualización de herramientas/aplicaciones actualizadas si así lo requiere la EC.
- Cursos de formación evolutivos (relacionados con el uso de la herramienta de administración) en caso de actualizaciones significativas en los procesos, en las funcionalidades de las aplicaciones, o en los endpoints de las APIs que ofrece el sistema si así lo requiere la EC.
- Recomendaciones de modificación del sistema.
- Innovación: incluir sin coste adicional las mejoras que la plataforma tenga previstas en su roadmap.

El precio ofertado por la Adjudicataria en su propuesta deberá incluir **20 horas mensuales** de soporte evolutivo para nuevas configuraciones o modificaciones en la configuración global o sites ya configurados en el servicio.

4.2.2. Licenciamiento del sistema de CIAM/SSO y gestión de consentimientos

La solución ofertada deberá tener en cuenta que el licenciamiento comienza en la Fase I (Despliegue e implantación del servicio) para disponer de licencias para las tareas a realizar en esta fase. El licitador deberá tener en cuenta que, durante los 4 meses previstos para esta fase, sólo se requerirán/usarán por parte de la EC las licencias necesarias que el licitador requiera para realizar el despliegue e implantación del servicio. Será en la fase II (Servicio) donde se requerirá el uso del paquete inicial completo de hasta 200.000 usuarios activos de media anual (pico de usuarios).

4.2.3. Servicios adicionales opcionales

Dentro de la fase de servicio, la EC podrá solicitar OPCIONALMENTE la integración con el sistema CIAM/SSO de nuevas plataformas que a día de hoy se encuentran en fase de desarrollo o en el roadmap.

4.2.3.1. Configuración dentro del sistema CIAM de plataformas adicionales a las configuradas en la Fase I

En la siguiente tabla, se lista a modo orientativo, la relación de plataformas junto con las distintas ventanas de publicación que se prevé que precisen de integración dentro del sistema CIAM/SSO/gestión de consentimientos:

Tipo plataforma	Ventana de publicación	Número de elementos (estimado)
-----------------	------------------------	--------------------------------

OTT	Portal WEB	1
	Aplicación nativa Android	1
	Aplicación nativa iOS	1
	Aplicaciones Smart TV	6
	HbbTV	1
CMS/DXP	Portal WEB	5
OTRAS	Portal WEB	2

4.2.3.2. Acompañamiento técnico a equipos de desarrollo para la integración del servicio en plataformas adicionales a las configuradas en la Fase I

Si bien no entran dentro del alcance del contrato, los desarrollos que haya que realizar en cada plataforma de la EC en la que sea necesario implantar el servicio licitado sí que se incluye la contratación OPCIONAL de servicios de asesoría técnica para los distintos equipos de desarrollo de dichas plataformas y acompañarles durante el proceso de integración para garantizar que se realiza con solvencia y lo más rápido posible de forma satisfactoria.

El servicio de asesoría requerido para los equipos dependerá del stack tecnológico de la plataforma y ventana de publicación en la que integrar el servicio de CIAM/SSO/gestión de consentimientos.

Teniendo en cuenta esto, se realizará la siguiente clasificación de trabajos de asesoría los cuales dispondrán de distinto coste según se especifica en el **ANEXO PCAP: FÓRMULAS MATEMÁTICAS**

- Integración con **complejidad BAJA**

Entrarían en esta categoría las integraciones en portales WEB

- Integración con **complejidad MEDIA**

Estarían incluidas en esta categoría las integraciones en APPS móviles mediante SDKs o integraciones de APIS.

- Integración con **complejidad ALTA**

Corresponderían a esta categoría las integraciones a realizar en aplicaciones Smart TV.

5. PRECIO Y FACTURACIÓN

La EC abonará los servicios prestados de conformidad con los precios fijados por la adjudicataria en su propuesta de acuerdo con los términos recogidos en el apartado "5.2.-Modalidad de pago del precio" de las Cláusulas Específicas del Pliego de Condiciones Administrativas Particulares (PCAP).

6. RECURSOS PROFESIONALES PARA LA PUESTA EN MARCHA DEL SERVICIO

6.1. Condiciones generales

El personal designado a la prestación del servicio dependerá exclusivamente de la contratista, única que ostentará los derechos y obligaciones inherentes a su condición de empleadora.

A tales efectos, la empresa contratista asumirá las siguientes obligaciones:

1. Corresponderá exclusivamente a la entidad que resulte contratista la selección del personal que, reuniendo los requisitos de titulación y experiencia exigidos en la cláusula siguiente del presente pliego formará parte del equipo de trabajo designado a la ejecución del contrato, sin perjuicio de la verificación por parte de la Entidad Contratante del cumplimiento de aquellos requisitos.
2. La contratista procurará que exista estabilidad en el equipo de trabajo, y que las variaciones en su composición sean puntuales y obedezcan a razones justificadas, en orden a no alterar el buen funcionamiento del servicio (cuando existan razones que justifiquen esta exigencia), informando en todo momento a la Entidad Contratante.
3. La contratista asume la obligación de ejercer de modo real, efectivo y continuo, sobre el personal integrante del equipo de trabajo encargado de la ejecución del contrato, el poder de dirección inherente a toda empresa.

En particular asumirá la negociación y pago de los salarios, la concesión de permisos, licencias y vacaciones, las sustituciones del personal en casos de baja o ausencia, las obligaciones legales en materia de Seguridad Social, incluido el abono de cotizaciones y el pago de prestaciones cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como cuantos derechos y se deriven de la relación contractual entre las partes empleada y empleadora.

4. Garantizar que el personal designado desarrolle su actividad sin extralimitarse en las funciones desempeñadas respecto de la actividad delimitada en los pliegos como objeto del contrato.
5. La contratista deberá designar al menos una persona coordinadora o responsable del contrato y un responsable por cada área de trabajo definida, perteneciente a su plantilla de personal, que tendrán entre sus obligaciones las siguientes:
 - Actuar como interlocutoras de la entidad contratista frente a la EC, canalizando la comunicación entre la empresa contratista y el personal integrante del equipo de trabajo designado al contrato, de un lado, y la EC, de otro lado, en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.
 - Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir al mismo las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación del servicio contratado.
 - Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tienen encomendadas, así como controlar la asistencia de dicho personal al puesto de trabajo.
 - Organizar el régimen de vacaciones del personal designado a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente la contratista con la Entidad Contratante, a efectos de no alterar el buen funcionamiento del servicio.

- Informar a la EC acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo designado a la ejecución del contrato.
- Garantizar que mientras las personas puestas a disposición del servicio objeto de la presente contratación se encuentren en alguno de los centros de trabajo de la EC, éstas cumplan con las normas de seguridad de la EC y cuenten con los correspondientes distintivos que las identifique como personal de la entidad que resulte adjudicataria del servicio.

Si a consecuencia del incumplimiento por la entidad contratista de las obligaciones asumidas en virtud de esta cláusula, la EC fuera condenada al pago de cantidades con carácter solidario con la empresa contratista, se repercutirá en ésta la suma satisfecha, a cuyos efectos la EC se reserva el ejercicio de cualesquiera acciones, administrativas o judiciales, que sean adecuadas y convenientes hasta la total recuperación de las cantidades pagadas.

6.2. CONDICIONES PARTICULARES

Concretamente, para la correcta prestación de los servicios objeto de la presente contratación, la empresa que resulte adjudicataria deberá contar con, al menos, los siguientes profesionales:

- UNA (1) persona coordinadora.

Con el objeto de coordinar y supervisar los servicios contratados, la adjudicataria deberá nombrar, como se ha señalado anteriormente, un/a responsable del servicio que además de interlocutor será la persona que dirija y coordine los trabajos a realizar.

Se facilitarán los datos de esta persona que será la que se mantenga en contacto con el responsable del contrato de la EC.

El responsable del servicio deberá tener la autonomía y capacidad de gestión y decisión suficiente para garantizar una rápida respuesta ante cualquier incidencia, consulta o necesidad de la EC en relación a todos los aspectos del contrato.

Se reunirá periódicamente (según la periodicidad marcada por el responsable del servicio de la EC) para tratar todos los aspectos del servicio.

El servicio de interlocución se entenderá incluido dentro del precio del contrato.

El profesional propuesto para desarrollar estas funciones deberá contar con, al menos, 3 años de experiencia en la coordinación de equipos que desarrollan aplicaciones similares a la recogida en la presente contratación.

Deberá estar localizable a través de un correo electrónico y un teléfono de contacto para gestionar cualquier aspecto del servicio en horas de oficina.

Esta persona deberá disponer de los siguientes medios:

- Teléfono Móvil
- Correo electrónico
- Equipo mínimo de apoyo

El equipo operativo destinado a la ejecución del servicio por la adjudicataria deberá contar con la experiencia y la formación necesaria para la correcta prestación de los trabajos objeto de la presente contratación.

7. SEGUIMIENTO DEL SERVICIO

Para la seguimiento y coordinación del servicio, la adjudicataria deberá como arte de su propuesta señalar la relación de documentación que propone para en el caso de ser adjudicataria realizar con garantías el seguimiento correcto del servicio.

Al menos dicha documentación deberá contemplar el control de los siguientes elementos:

- Guía/manuales de usuarios de procesos establecidos y herramientas puestas a disposición de la EC (documentación operativa).
- Especificaciones funcionales/técnicas sobre las herramientas de supervisión, configuración y uso de los servicios y las APIs.
- Procesos y responsabilidades.
 - ✓ Uso y gestión de la plataforma
 - ✓ Escalado de la información
 - ✓ Gestión de crisis (descrito en el punto 3.2 del presente PPTP)

Con carácter general y adicionalmente a lo descrito para cada tipo de soporte, como parte del seguimiento del servicio la adjudicataria a petición de la EC deberá:

- Concretar comités/reuniones:
 - “Mensual” para seguimiento de la prestación del servicio en el que se recoja la actividad realizada y el impacto de esta de forma global, incluyendo resultados del seguimiento de los valores de rendimiento y disponibilidad requeridos.
 - Trimestral para analizar la evolución del servicio.
 - Anual para acciones más relevantes llevadas a cabo por el servicio durante ese periodo y los hitos logrados. En esta reunión se hará la evaluación del año anterior y la planificación del siguiente, incorporando acciones preventivas, correctivas, e innovaciones propuestas.

La adjudicataria deberá remitir con anterioridad al comité/reunión los informes asociados al seguimiento a realizar en dicho comité/reunión si la EC así lo requiere.

8. PLAN DE SALIDA

Una vez concluido el contrato la adjudicataria deberá facilitar en cualquier caso y con el mejor esfuerzo la migración de los servicios que viniera prestando hasta esa fecha.

Las acciones precisas para facilitar dicha migración posterior se consideran un servicio profesional incluido en el importe del contrato, y únicamente podrá facturarse y al mismo precio vigente a la fecha de extinción, la prestación temporal del servicio que sea preciso prorrogar durante dicho proceso de migración.

La adjudicataria ejecutará el plan presentado inicialmente junto con las adaptaciones que fueran necesarias a efectos de adaptar aquellos elementos que hubieran aparecido durante la fase de servicio para realizar una salida ordenada del servicio una vez concluido el periodo contractual y en el caso de no ser adjudicataria de la continuidad del mismo.

En dicho plan se compromete a mantener la continuidad del servicio durante la migración al nuevo adjudicatario del mismo si así se diera el caso, con los mismos precios vigentes al final del contrato, así como a facilitar a la contratante la migración todos los datos de identidades de usuario a la plataforma que disponga el nuevo adjudicatario para tal fin.

9. PRUEBAS DE VALIDACIÓN TÉCNICA DE LA SOLUCIÓN TECNOLÓGICA OFERTADA

La EC se reserva el derecho de efectuar pruebas de validación de la idoneidad de los requerimientos técnicos de la plataforma y del servicio ofertado, con carácter previo a la adjudicación del contrato.

A tal fin, una vez clasificadas las proposiciones presentadas, la Mesa de contratación de la EC se pondrá en contacto con la empresa licitadora con el objetivo de realizar una prueba de concepto que certifique el cumplimiento de los requerimientos técnicos de la presente contratación.

La ejecución de dichas pruebas será un requisito previo indispensable para la Adjudicación del contrato.

La empresa licitadora requerida debe estar en disposición de realizar dichas pruebas en un periodo no superior a 15 días hábiles desde la comunicación por parte de la EC.

La EC no asumirá coste alguno, por los servicios que se deriven de la realización de estas pruebas.

Dado el estado del arte de la tecnología, y la rápida evolución del mismo en el ámbito de los servicios que son objeto de la presente contratación, la EC establece expresamente que únicamente serán considerados válidos aquellos requerimientos que están disponibles y funcionales a la fecha de contratación, obviándose aquellos que no se puedan demostrar por encontrarse en fase de desarrollo si se diera el caso.

Si en el transcurso de las pruebas y en un plazo de 15 días naturales a partir de la fecha de inicio de éstas, la empresa licitadora clasificada en primer lugar no pudiera demostrar la prestación efectiva de alguno de los requerimientos establecidos en el presente documento, y como consecuencia pudieran afectar al correcto desarrollo del servicio o a la viabilidad de la migración del mismo, se descartará la oferta presentada por la licitadora y se repetirá el proceso con la empresa que haya obtenido la siguiente mejor puntuación del resto de licitadoras y así sucesivamente.

10. PENALIZACIONES

Serán las establecidas en el Punto **13.- PENALIDADES** del apartado Cláusulas Específicas del Pliego de Cláusulas Administrativas Particulares (PCAP).

11. REQUERIMIENTOS EN MATERIA DE SEGURIDAD

De conformidad con lo previsto en apartado 3 del artículo 2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), (RD 311/2022) y de acuerdo con la política de seguridad de la EC, la adjudicataria deberá certificar, al menos, el nivel medio en el ENS. A tal efecto:

1. Cuando la plataforma pertenezca a una empresa española / cuando el servicio sea prestado por una empresa española será necesario acreditar una de estas dos situaciones:

- a. Que la plataforma adscrita a la ejecución del contrato esté certificada en el Esquema Nacional de Seguridad con Nivel Medio o superior.
 - b. Que la empresa prestadora del servicio esté certificada en el Esquema Nacional de Seguridad en esa tipología de servicio con Nivel Medio o superior.
2. Cuando la plataforma pertenezca a una empresa no española o el servicio sea prestado por una empresa no española será igualmente válido: Que la empresa prestadora del servicio disponga de la norma ISO 27001.
3. En el caso de empresas licitadoras que presten el servicio (objeto del contrato) a través de terceras empresas o bien utilicen plataformas de terceras empresas para la prestación del servicio, será suficiente con que estas terceras empresas sean las que cumplan estos requisitos.

Será, en el caso de ser seleccionada y previa a la adjudicación del contrato, cuando la empresa seleccionada (propuesta con mejor relación calidad/precio) deba acreditar esta situación. En el caso de empresas licitadoras que presten el servicio (objeto del contrato) a través de terceras empresas o bien utilicen plataformas de terceras empresas para la prestación del servicio será necesario la cumplimentación por estas terceras empresas del ANEXO V.1. DISPONIBILIDAD DE LA SOLVENCIA Y MEDIOS DE OTRAS ENTIDADES DURANTE TODA LA VIGENCIA DEL CONTRATO del PCAP.

12. DOCUMENTACIÓN A PRESENTAR POR LAS CANDIDATAS

Las entidades licitadoras deberán presentar la siguiente documentación de acuerdo con lo dispuesto en la cláusula 24 de las cláusulas específicas del PCAP.

12.1. SOBRE B.- DOCUMENTACIÓN relativa a la oferta evaluable automáticamente a través de fórmulas.

Las entidades presentarán sus ofertas ajustándose al modelo de tabla indicado en el **ANEXO** PCAP: FÓRMULAS MATEMÁTICAS.