PLIEGO DE PRESCRIPCIONES TÉCNICAS RELATIVAS AL CONTRATO PARA LA PRESTACIÓN DE UN SERVICIO DE UNA PLATAFORMA DE FACT-CHECKING PARA LA COMUNIDAD ESPAÑOLA

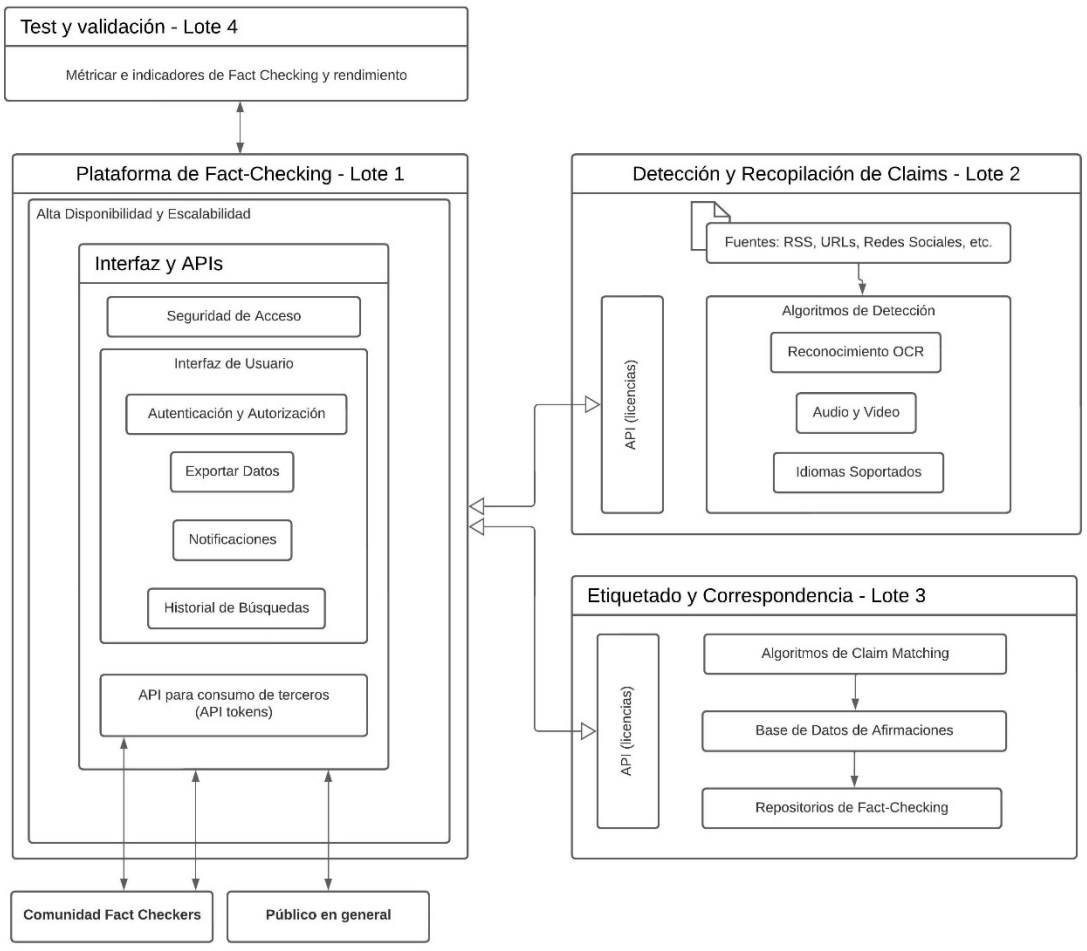
Exp. A/F202403/S

Índice

1 OBJETO DEL CONTRATO

El objeto del contrato es disponer de una plataforma operativa de *fact-checking* y todas las actividades necesarias y recursos humanos, sistemas de alojamiento y computación para la construcción y el mantenimiento productivo para Fundació Barcelona Mobile World Capital Foundation (en adelante, "**MWCapital**"), según se describe en detalle en el informe de necesidad.

A continuación, se presenta una arquitectura funcional simplificada de la plataforma:



La plataforma deberá proporcionar los siguientes grupos de funcionalidades:

- **Detección y recopilación de *Claims* (*Claim Detection*):** La plataforma será capaz de identificar y recoger *claims* procedentes de una amplia gama de fuentes abiertas y accesibles. Esto incluye RSS, URLs, redes sociales accesibles, aplicaciones de mensajería privada, archivos de bases de datos (en diversos formatos: CSV, JSON, etc.) y otros tipos de medios como texto en imágenes (reconocimiento OCR), audio y vídeo (speech-to-text). Deberá funcionar en las siguientes lenguas: inglés, castellano, catalán, euskera y gallego.

- **Etiquetado de *Claims* y Correspondencia con *Fact-Checks* Existentes (*Claim* Matching):** La plataforma proporcionará funcionalidades para etiquetar *claims* (categorizar/calificar/clasificar cada *claim*) con el objetivo de compararlas con *fact-checks* existentes, ya sean de repositorios privados o abiertos, y hallar las correspondencias.

- **Interfaz de usuario y APIs:** La plataforma proporcionará un conjunto de herramientas de *fact-checking* abierto y accesible. Los usuarios finales podrán interactuar con la plataforma a través de una interfaz de usuario intuitiva y fácil de usar. Además, la plataforma ofrecerá APIs robustas para facilitar la integración con las herramientas existentes de los usuarios i/o con repositorios abiertos de *fact-checking* existentes o que aparezcan en el futuro.

- **Testing y validación**: La plataforma dispondrá de un sistema de evaluación del óptimo rendimiento funcional de la misma con especial enfoque en el *Claim Detection* y el *Claim Matching*

2 LOTE 1: OFICINA TÉCNICA Y SERVICIOS NECESARIOS PARA EL DESARROLLO, IMPLANTACIÓN, MANTENIMIENTO, SOPORTE Y GESTIÓN DE LA PLATAFORMA DE *FACT-CHECKING*

2.1 OBJETO

El objeto de este lote es el desarrollo, la gestión del desarrollo y la coordinación y seguimiento de todos los lotes del contrato, la puesta en marcha, gestión en producción y mantenimiento de una plataforma de *fact-checking*, en los términos y condiciones definidos en este pliego y todas las tareas y actividades asociadas y los recursos adecuados para llevarlas a cabo, ya sean recursos humanos o sistemas de alojamiento y computación.

El objetivo es disponer de una interfaz de usuario y las APIs que proporcionarán un conjunto de herramientas de *fact-checking* abierto y accesible. Los usuarios finales podrán interactuar con la plataforma a través de una interfaz de usuario intuitiva y fácil de usar. Además, la plataforma ofrecerá una API robusta que permita la integración con herramientas existentes de los usuarios i/o con repositorios abiertos de *fact-checking* existentes o previstos en el futuro.

2.2 ALCANCE

El contrato alcanza todas las tareas, actividades y licencias para la consecución del objeto del contrato, así como la descripción los requerimientos funcionales en forma de épica y la definición de las historias de usuario que se derivan de cada épica, la colaboración con el *Product Owner* para definir y refinar las historias adecuadamente con el suficiente nivel de detalle per alcanzar la definición de preparado (*Definition of Ready*), así como la redacción de los criterios de aceptación de cada historia de usuario. También forma parte del alcance la generación de todos los entregables previstos en la metodología y el modelo de calidad.

2.2.1 Etapas

Para dar cumplimiento al objeto del contrato, la ejecución se divide en dos etapas diferenciadas y consecutivas en el tiempo:

1) Etapa de la construcción e implantación de la plataforma: (8 meses)

    a) Fase de Elaboración: la elaboración de los requisitos, el diseño funcional, la arquitectura del sistema y su aceptación por parte de MWCapital. Semanas 1 a 6.

    b) Fase de Construcción e Implementación: refinamiento de los diseños funcionales y desarrollo de toda la arquitectura software de la plataforma: la interfaz de usuario y su *backend*, las APIs e integraciones para el consumo de los servicios de las licencias de *claim matching* y *claim detection*. Semanas 7 a 30.

    c) Fase de puesta en marcha: estabilización en producción y gestión del cambio (comunicación, formación, soporte). Semanas 31 a 35.

2) Etapa de gestión, mantenimiento, soporte y disponibilidad ininterrumpida y alojamiento de la plataforma: Mes 9 al mes 32 (24 meses).

2.3 CARACTERÍSTICAS TÉCNICAS Y FUNCIONALES

Los requisitos técnicos de las distintas funcionalidades de la plataforma son las siguientes:

2.3.1 Requisitos generales

1) La plataforma debe proporcionar una interfaz de usuario intuitiva y fácil de usar, permitiendo a los usuarios interactuar de manera eficiente con la funcionalidad ofrecida.

2) Soporte multiplataforma e interoperabilidad: La plataforma debe ser compatible con múltiples sistemas operativos y navegadores. El sistema debe ser multiusuario. El acceso debe realizarse por medio de navegador web, en las versiones publicadas en el periodo de ejecución del contrato de cualquiera de los navegadores estándares actuales: Mozilla Firefox, Google Chrome, Internet Explorer/Edge y Safari).

3) Seguridad y protección de los datos: La plataforma deberá cumplir con las medidas de seguridad pertinentes para proteger los datos de los usuarios y la información confidencial. Esto incluye la implementación de protocolos de cifrado para asegurar los datos tanto en tránsito como en reposo. Adicionalmente, deberá estar en conformidad con las regulaciones de protección de datos existentes como el Reglamento General de Protección de Datos (RGPD).

4) Seguridad de acceso a la plataforma:

   a) Interfaz de usuario: La plataforma deberá proporcionar mecanismos robustos de autenticación y autorización de usuarios para proteger el acceso no autorizado. Esta protección puede incluir el uso de proveedores de gestión de identidad y acceso de terceros (IAM) como Google, Facebook entre otros. Asimismo, cabe la posibilidad, y por tanto debe incluirse en los requerimientos, de que sea preciso disponer de 2FA (*two factor authentication*) de acuerdo a la legislación europea.

   b) API: Deberá proteger las APIs para evitar accesos no autorizados y garantizar la identidad de la plataforma a las aplicaciones que se conectan a ella. La protección de las API puede incluir técnicas como la autenticación basada en tokens, limitación de tasa por usuario (*rate-limiting*), y la validación y saneamiento de los datos de entrada.

5) Alta disponibilidad: La plataforma debe ser diseñada para ser tolerante a fallos y capaz de manejar de forma eficiente picos de demanda de manera automática para manejar incrementos en los datos procesados y en la cantidad de interacciones con los usuarios, proporcionando así una alta disponibilidad de servicio. Deberá tener en cuenta la gestión adecuada de la carga y ser capaz de añadir y gestionar más recursos sin interrumpir las operaciones en curso, por ejemplo, durante un evento de *fact-checking* en tiempo real de un debate electoral.

6) Mantenibilidad y actualización: El sistema debe ser fácil de mantener y actualizar, debe permitir la incorporación de nuevas características o mejoras con la mínima interrupción de servicio.

2.3.2 Requisitos específicos

1) La plataforma debe ser capaz de integrarse e interactuar con otros sistemas o aplicaciones existentes de los usuarios, incluyendo la capacidad de importar y exportar datos en formatos estándar comúnmente aceptados (csv, excel, json) para, por ejemplo, permitir a los usuarios realizar un análisis más detallado en otras herramientas si así lo desean. La plataforma debe proporcionar una API a consumir por parte de estos sistemas y servicios de terceros, y para permitir a los usuarios la posibilidad de utilizar sus propios algoritmos desde otras plataformas. Se prevé hasta un máximo de 12 organizaciones externas consumirán la API. Debe ser parametrizable en el sistema una política de número de máximos de usuarios de API y el rendimiento de acuerdo con un número máximo de peticiones por método o volumen de registros involucrados en los métodos consumidos.

2) La plataforma debe proporcionar un mecanismo de notificación para alertar a los usuarios sobre los resultados de la detección y *claim matching*. El mecanismo debe ser por notificación dentro de la misma plataforma al usuario estando autenticado, con la opción (a elección de cada usuario) de poder recibir estas mismas notificaciones por correo electrónico.

3) La plataforma debe proporcionar un historial de búsquedas al usuario, ya sea de búsqueda de *claim detection* como búsquedas de *claim matching.*

2.3.3 Colaboración y participación de la comunidad de fact-checkers

El desarrollo de la plataforma y los algoritmos debe ser un proceso inclusivo y colaborativo que involucre activamente a la comunidad de *fact-checkers* del estado español. Para lograr esto, el Servicio debe incluir los siguientes puntos:

Marco de gestión del desarrollo Scrum: Este marco se implementará para permitir un ciclo de retroalimentación continuo y mejoras iterativas. Cada *sprint* ira seguido de una revisión y una oportunidad para hacer ajustes basados en la retroalimentación de la comunidad de *fact-checkers*.

User Journey: El contratista definirá un plan detallado para trabajar con la comunidad de *fact-checkers* para definir el "user journey". Esto implica comprender y documentar cómo los *fact-checkers* utilizarán la plataforma y cómo esta puede ser diseñada para satisfacer sus necesidades y facilitar su trabajo.

Arquitectura API: El contratista diseñará la arquitectura de la API propia y el consumo de las APIs licenciadas, en colaboración con la comunidad de *fact-checkers* para garantizar que la plataforma sea completamente funcional y dentro de los márgenes de rendimiento establecidos por las métricas de los lotes 2 y 3.

Sesiones de Colaboración: El contratista definirá el calendario de las sesiones de colaboración planificadas con la comunidad de *fact-checkers* y los contratistas de los lotes 2, 3 y 4. Estas pueden incluir talleres, reuniones, pruebas de usuario y otros eventos diseñados para recoger retroalimentación y fomentar el compromiso con el desarrollo de la plataforma y los algoritmos.

En todas las etapas del proceso de desarrollo, se debe considerar la retroalimentación de las organizaciones reconocidas por el International Fact-Checking Network (IFCN) o el European Fact-Checking Services Network (EFCSN) como mínimo. La efectividad de este plan de colaboración y participación será un factor importante en la adjudicación del contrato.

Formación y soporte: El contratista debe proporcionar soporte técnico y formación adecuada para los usuarios para garantizar que puedan utilizar la plataforma de manera efectiva.

A tal efecto el contratista preparará y pondrá a disposición de los usuarios, dentro de la misma plataforma:

- Un video tutorial, con videos individuales de máximo 3 minutos, con tantos videos individuales como se requieran para cubrir todas las funcionalidades de la plataforma. Debe cubrir todas las funcionalidades, se presten vía interfaz web o vía API.

- Una guía de acceso rápido y su correspondencia con los video tutoriales indexado por funcionalidades y categorías. Debe cubrir todas las funcionalidades, se presten vía interfaz web o vía API.
- Asimismo, el contratista deberá prestar un servicio de soporte de acuerdo con los Acuerdos de Nivel de Servicio del apartado 2.7 Acuerdos de Nivel de Servicio *ANS*.

2.3.4 Directrices de desarrollo y requisitos técnicos de construcción

Arquitectura

Como normal general toda aplicación debe seguir la metodología 12factor (https://12factor.net), tanto en el modelo de desarrollo como en la arquitectura y ciclo de vida de la aplicación.

En esencia se trata de establecer un contrato claro con el sistema operativo, de forma que las aplicaciones tengan máxima portabilidad, puedan escalar, carezcan de dependencias fuertes con una instancia concreta (ficheros), y mínimos en las diferencias con el entorno de desarrollo

- Se pide una aplicación web Modelo Vista Controlador (MVC) o Modelo Vista Vista Modelo (MVVM) con las siguientes características:
- En lenguaje de aplicación PHP en su última versión estable.
- Motor de BDD relacional: MariaDB o equivalente en su última versión estable.
- Frameworks PHP preferidos: Symfony, Laravel, Phalcon . En ningún caso se considerará un framework que no disponga de una comunidad de desarrollo suficientemente numerosa y con frecuentes actualizaciones. En cualquiera éste debe ser validado y aprobado por MWCapital justo al inicio del contrato.

HTML5

- Diseño *responsive* basado en el framework CSS foundation, Bootstrap o similar.
- Utilización de librerías o frameworks javascript de solvencia contrastada.
- Concatenación, compresión y minificación de CSS y JS en los archivos posibles utilizando el sistema de *assets pipeline*.
- Sass (*Syntactically Awesome Style Sheets*) como lenguajes de estilos.
- Se pretende que las aplicaciones estén listas para ser desplegadas en los servidores clásicos, pero también en la nube, ya sea privada, pública o mixta.

Devops y contenedores

- El entorno y el despliegue a producción se basará en contenedores (Docker, Kubernetes..). Debe tenerse en cuenta en el diseño de la arquitectura de la plataforma.

- Asimismo se pide que el/los contenedor/s del servicio de motor de BDD tengan el tratamiento de críticos en cuanto a la política de backups, seguridad, tolerancia a errores y rendimiento.

Componentes

En el caso de paquetes y librerías externas, primero se propondrán al equipo técnico de MWCapital. Para el visto bueno se tendrá en cuenta la popularidad, solvencia contrastada y mantenibilidad de esta librería antes de dar el visto bueno a su uso.

Seguridad

A continuación, se enumera la funcionalidad de seguridad que debe cumplir el sistema:

El componente de seguridad de la plataforma debe tenerse siempre presente. La arquitectura tiene en cuenta no sólo la mejor forma de estructurar la aplicación, sino que esta estructura debe cumplir con los requisitos de seguridad del Ayuntamiento de Barcelona bajo la premisa de seguridad en el diseño. En estos momentos estos requerimientos marcan que deba diferenciarse entre el acceso a los datos externos, que se haría mediante un API y el acceso ya dentro de la red que se realizará hacia la base de datos. El objetivo de seguridad es poder controlar mejor el acceso a los datos mediante el control de los firewalls y el acceso a la base de datos.

En lo que se refiere a este documento, los requerimientos de seguridad implican ir actualizando tanto la aplicación como los módulos que se utilicen con los últimos parches de seguridad, tanto de los componentes del operativo y el software base como de los componentes de la aplicación.

- Hacer las conexiones por HTTPS.
- Asegurarse de que no existe la opción de DEBUG activada en los entornos de producción.
- Autenticación: El sistema debe comprobar que el usuario que trata de acceder al sistema es quien dice ser.
- Permisos: El sistema debe permitir acceder a las funcionalidades para las que el usuario tiene permisos. Estas funcionalidades estarán disponibles dependiendo del rol del usuario logado.
- Autorización: El sistema debe implementar mecanismos para restringir a usuarios no identificados y autorizados el acceso a la información.
- Cifrado de datos: La comunicación del usuario con el sistema se realizará únicamente mediante canales seguros (https). Los algoritmos criptográficos empleados serán los acreditados por el Centro Criptológico Nacional para su uso en el Esquema Nacional de Seguridad.

- Gestión de usuarios y sesiones: Los mecanismos de control de sesiones de usuarios autenticados contemplarán:
    - Cierre de sesión por parte del usuario.
    - Expiración automática de sesión a 60 minutos de inactividad y 12 horas de vida máxima. Estos dos parámetros deben poder modificarse desde la configuración del administrador de la plataforma.
- Gestión de errores y excepciones: Se realizará un tratamiento sistematizado y centralizado de errores y excepciones, eliminando la información interna del sistema o sensible de los mensajes mostrados al usuario.
- El nuevo sistema debe desarrollarse siguiendo patrones y recomendaciones de programación que incrementen la seguridad de los datos.
- Cualquier intercambio de datos entre servicios o aplicaciones se realizará mediante el protocolo encriptado HTTPS.

Directivas de QA

- Aunque es imposible demostrar la ausencia de errores, las buenas prácticas de calidad de código y control nos permiten tener mayor seguridad al hacer cambios y demostrar la idoneidad del programa para las tareas a realizar.
- Unit tests. Se utilizarán tests unitarios para validar las reglas de negocio y las APIs propias y de consumo de terceros (licencias).
- Rendimiento. Es conveniente comprobar las consultas que se ejecutan en la base de datos y tiempo de creación de las páginas.
- UAT. Test de aceptación de usuario final. Se requerirán los UATs para la aceptación de los desarrollos.

Plan de pruebas

Es responsabilidad del contratista la definición y realización del Plan de Pruebas incluyendo, como mínimo, las pruebas indicadas en la metodología Scrum (ver apartado 2.5.2 y Anexo 1 de este pliego).

El contratista deberá presentar a MWCapital el plan de pruebas incluyendo para cada tipología de prueba los casos de uso de los requerimientos. Una vez validado, los casos de uso definidos en el plan de pruebas serán realizados y documentados en las pruebas correspondientes.

El contratista deberá realizar la definición, planificación, organización y coordinación de las pruebas realizadas. Es responsabilidad del contratista la definición y realización de las pruebas (unitarias, de integración, de rendimiento, estrés, etc.).

Las pruebas se realizarán sobre el entorno de pruebas de preproducción, donde posteriormente validará el usuario (UAT).

Será responsabilidad del contratista la preparación de los juegos de prueba y habilitar los entornos correspondientes para las pruebas funcionales, así como los perfiles y usuarios necesarios para ejecutar estos planes de pruebas.

Para la ejecución de las pruebas deberán realizarse como mínimo las siguientes actividades:

- El contratista realizará el diseño del plan de pruebas funcionales de manera iterativa, identificando, acordando y especificando los atributos y características de calidad que se deben probar. El objetivo es diseñar las pruebas con la probabilidad de encontrar un mayor número de defectos con la mínima cantidad de esfuerzo y tiempo, demostrando que las funcionalidades son operativas, que la entrada de datos se acepta de forma correcta y que los resultados esperados son los correctos.
- Verificará que se han identificado y definido los casos de prueba necesarios para garantizar las funcionalidades de los procesos funcionales definidos, por los que se detallarán acciones a realizar y para cada uno de los casos se asociará su resultado esperado que podrá ser verificado. Durante esta misma fase, se especifican también los datos de entrada necesarios para que los casos de prueba definidos puedan ser ejecutados, ya sea buscando el éxito del resultado o bien el error.
- Se realizará la ejecución de los casos de prueba anteriormente diseñados de forma manual siguiendo el detalle del guión establecido. El analista que ejecute las pruebas debe disponer de cierta libertad y autonomía para detectar situaciones anómalas no contempladas.
- Se guardará un listado detallado de los errores encontrados en la ejecución de los casos de prueba y de su corrección.
- Se repetirá la batería de pruebas tantas veces como se estime necesario hasta la obtención del resultado correcto.

Siempre y en todo caso se deberá entregar un Informe del Resultado de la Ejecución de las pruebas, junto con la grabación de los resultados de cada prueba (posibles opciones: fichero de resultados generado por una herramienta de testing, entrega de un fichero log, captura de ventanas con el resultado de las pruebas, etc.).

La definición y ejecución del plan de pruebas será validado definitivamente por MWCapital y requerirá de su aprobación para ser admitido.

El informe contendrá, como mínimo, los siguientes elementos:

- Identificación y descripción de la prueba.
- Identificación y especificación de los atributos y características de calidad que componen la prueba.

- Resultado de la prueba, especificando si éste es satisfactorio o no, incluyendo las observaciones que se consideren necesarias para justificar el resultado.
- Informe de incidencias en el que deberá especificarse como mínimo descripción de la incidencia, fecha de apertura, fecha resolución, responsable. Este informe deberá estar actualizado diariamente y se utilizará para el seguimiento de iteraciones de las pruebas.

Directrices de documentación

Distinguimos dos tipos de documentación: la documentación del código y la documentación del aplicativo o para el usuario en el caso del desarrollo de una librería o API.

Conviene documentar muy bien el código, de modo que podamos utilizar las capacidades de los editores modernos de mostrarnos la documentación asociada a una librería, clase o función.

Documentación de aplicación. Para documentar cómo configurar una nueva funcionalidad a nivel de aplicación, una nueva tarea o una nueva API se requerirá uno de los dos:

- Un archivo en formato Markdown dentro del directorio docs/ en el repositorio https://github.com/factcheckingabierto/
- Un archivo en formato AsciiDoc o la herramienta Antora dentro del directorio docs/ en el repositorio https://github.com/factcheckingabierto/

Documentación APIs. En el caso de las APIs conviene documentar su utilización de forma que nos permita testear contra el entorno la utilización de la API.

Documentación Licencias. Conviene que los desarrolladores conozcan y documenten la licencia de las aplicaciones de terceros que emplean, de forma que se pueda asegurar que es compatible con el uso y distribución que se desea hacer de la aplicación y su código.

Requisitos de versionado

Se requiere que todo el código se gestione mediante un sistema de versiones, se prefiere git.

Adicionalmente, se seguirá un esquema claro de versiones que permita mantener limpia la estructura, y permita identificar claramente el contenido de cada interacción con el sistema. Hay que seguir las siguientes directrices:

- Esquema de pull requests y commit:

o Por cada commit:

• Separar título de cuerpo con una línea blanca

• Limitar el título a 50 caracteres

• Capitalizar el título

• No terminar el título con un punto

• Utilizar el modo imperativo

• Utilizar 72 caracteres para el cuerpo del mensaje

• Utilizar el cuerpo para explicar lo que se hace y el por qué contra el cómo

o Por cada pull request: habría que utilizar una plantilla en GitHub con el correspondiente número de issue de GitHub.

- Esquema de ramas: se hace seguir las directrices recomendadas por el gitflow (rama develop, release/0.x-stable, feature/xxx, fijo/xxxx, etc).

Eficiencia

A continuación, se enumeran los requerimientos de eficiencia que deben cumplir el sistema:

Toda funcionalidad del sistema y transacción de negocio debe responder al usuario en menos de 3 segundos en el 90% de las peticiones, y cumplir:

• 0,1 segundos es el límite para que el usuario sienta que el sistema reacciona instantáneamente, es decir, que no se necesita ninguna retroalimentación especial, excepto para mostrar el resultado.

• 1-3 segundos es el límite del flujo del usuario para mantenerse ininterrumpida, aunque el usuario observará el retraso. Normalmente, no se necesita ninguna retroalimentación especial durante los retrasos de más de 0,1 pero inferiores a 1,0 segundos, pero el usuario pierde la sensación de operar directamente sobre los datos.

• 10 segundos es el límite para mantener la atención del usuario centrada en el diálogo. Para retrasos más largos, los usuarios tendrán que realizar otras tareas mientras espera que acabe la petición, por lo que se les debería proporcionar información que indique cuándo se espera que la petición finalice. La retroalimentación durante el retraso es especialmente importante si el tiempo de respuesta es muy variable, puesto que los usuarios no saben qué esperar.

- El sistema debe ser capaz de operar adecuadamente hasta 250 usuarios concurrentes.
- El sistema debe ser tolerante a errores.
- El sistema debe garantizar la integridad de las transacciones.

Multilingüe

Obligatoriamente la interfaz de usuario debe estar disponible en catalán, gallego, euskera, castellano e inglés.

La totalidad de los campos/mensajes visibles por el usuario deben poder traducirse mediante la aplicación o bien en archivos de configuración, de modo que la incorporación de uno u otro idioma no suponga tener que revisar y traducir código fuente. En caso de utilizar archivos de configuración deben ser en un formato estandarizado o estándar de facto.

MWCapital requiere que la aplicación quede ya configurada inicialmente en catalán, gallego, euskera, castellano e inglés donde corresponda, y la documentación del proyecto esté disponible en inglés.

En el caso del código y toda la comunicación en el issue tracker/pull requests del GitHub, así como la documentación técnica, se hará totalmente en inglés, y también a requerimiento del MWCapital deberá hacerse en catalán.

Licencias

Los desarrollos que se realicen son propiedad de MWCapital y deben licenciarse de tal manera que MWCapital tenga la libertad de publicar el código bajo la licencia que considere más adecuada. Es necesario consultar la guía para gestionar proyectos de software libre del Ayuntamiento de Barcelona para obtener más información: https://ajuntamentdebarcelona.github.io/foss-guide/ca/Introduccio.html

2.3.5 Entorno tecnológico

Los desarrollos sobre el sitio Web se llevarán a cabo conforme a los estándares establecidos por el W3C (World Wide Web Consortium):

- Tecnologías de base: se utilizarán los estándares XHTML 1.0 y HTML5 para el marcaje de contenido y CSS 3 y SASS para el diseño visual.
- Accesibilidad: La página Web respetará las pautas de Accesibilidad de Contenidos Web 2.0 (WCAG 2.0).

2.4 INFRAESTRUCTURA DE ALOJAMIENTO

El contratista seleccionará, suministrará, gestionará y operará la infraestructura de alojamiento para la plataforma de *Fact-Checking* para toda la duración del contrato del Lote 1, garantizando la alta disponibilidad y de acuerdo con los ANS de infraestructura y los ANS de servicio detallados en este pliego, así como todas las medidas de seguridad, medidas de contingencia para recuperación del sistema y las copias de seguridad y auditorías.

2.4.1 Volumetría estimada

Se espera que la plataforma deba resolver como máximo 50K peticiones mensuales de *claim detections* y/o *claim matching*.

2.4.2 Gestión y administración de la infraestructura

El contratista se responsabilizará de las siguientes tareas de administración, mantenimiento y monitorización:

- Suministro, instalación y gestión del software o elementos de plataforma (Software as a service SaaS, Software as a Platform SaaP) necesario para el desarrollo de este contrato. Instalación y gestión del software o elementos de plataforma adicional que se pueda requerir.
- Actualización periódica de los sistemas, instalando las actualizaciones necesarias para el correcto funcionamiento y realizando aquellas configuraciones que MWCapital requiera.
- Administración integral de las bases de datos (sea cual fuere su naturaleza, relacional, no relacional, etc.) de los servidores virtuales o elementos de la plataforma incluyendo el cifrado y la seguridad de accesos.
- Configuración de servicios, plugins y/o accesorios necesarios para el funcionamiento de las aplicaciones y/o servicios que preste la plataforma.
- Instalación y configuración de certificados de seguridad.
- Gestión y monitorización permanente de los recursos y las aplicaciones de toda la infraestructura con soporte 24x7x365.
- Mantenimiento predictivo y correctivo de la infraestructura.

  Incluye por tanto la reacción a incidencias que se puedan producir (correctivo), con el diagnóstico y la solución, así como para el predictivo que en base a toda la información recogida y la monitorización permita detectar errores potenciales con el fin de resolverlos antes que se produzcan.

El objetivo principal es proporcionar una gestión predictiva a través de la monitorización de los elementos y entornos que componen la infraestructura, así como las auditorías periódicas que permitirán detectar las situaciones de riesgo reales o potenciales e iniciar las acciones necesarias, de forma proactiva, para su gestión y resolución en el menor tiempo posible, garantizando la máxima disponibilidad de la plataforma. MWCapital dispondrá de acceso para visualizar las métricas de todos los servicios utilizados y podrá requerir incorporar nuevas y/o alarmas sobre las aplicaciones que se ejecuten en la infraestructura.

- Las tareas de mantenimiento que puedan afectar al funcionamiento de los diferentes servidores o elementos de la plataforma se realizarán en horario nocturno y con previa comunicación y aceptación de MWCapital, pues probablemente se produzcan reinicio de servicios.
- Mantenimientos programados (mínimo de una vez al mes). Aparte de las actuaciones bajo demanda y/o por problemas técnicos, mensualmente se realizará un mantenimiento para asegurar que todos los servidores o elementos de la plataforma tienen los parches de seguridad actualizados y que disponen por ejemplo de la última versión estable del sistema operativo instalada y de las librerías y programas base en ejecución, etc. También se deberá revisar el rendimiento y consumo de la arquitectura para ajustar los recursos. En caso de que fuera necesario el reinicio de elementos de la plataforma para instalar parches de sistema y/o nuevas versiones de librerías o programas, se programará en la ventana de tiempo aprobada por MWCapital.
- Se incluirán las ampliaciones de recursos de las instancias de los elementos de la plataforma que se harán cuando sea necesario como resultado de la monitorización o por indicación expresa de MWCapital. Se deberán monitorizar y detectar aquellas situaciones que puedan suponer una ampliación temporal de recursos, que deberá realizarse de forma automatizada para mantener la calidad de servicio de la plataforma.
- Monitorización de servicios TCP estándar y también de servicios de aplicación y software (URL concretas, login a servicios, núm de peticiones, consultas o actividad que suponga consumo de recursos en la plataforma). En caso de detectar cualquier incidencia en la monitorización, el proveedor lo notificará a MWCapital inmediatamente (por correo electrónico y por teléfono) y, en coordinación con MWCapital, deberá llevar a cabo determinadas acciones para solucionar el problema, como la ampliación de recursos del servicio, el reinicio del elemento afectado y/o el arranque o parada de un determinado servicio.
- Resolución de problemas o fallos que afecten al correcto funcionamiento de los servicios instalados.
- Programación y verificación de copias de seguridad y de instantáneas (snapshots) si las hubiere.

- La restauración de copias de seguridad (completos o a nivel de ficheros y/o de bases de datos) y la restauración de snapshots en respuesta a un requerimiento de MWCapital o de sus desarrolladores.
- Servicios de auditoría y análisis forense para averiguar las causas ante cualquier incidencia que afecte a los sistemas, como caídas de rendimiento, problemas de funcionamiento o con la sospecha, detectada o reportada, de cualquier intrusión o infección en los sistemas objeto de este contrato.
- En caso de que sea patente una infección o intrusión ya sea por evidencia constatada o por el resultado de una auditoría o análisis forense, el contratista debe realizar la limpieza y/o desinfección de los sistemas objeto de este contrato, así como implementar las acciones requeridas para evitar nuevas infecciones y por tanto resuelvan la vulnerabilidad.
- La empresa adjudicataria entregará un informe mensual de las actuaciones realizadas que incluya, además de la relación de incidencias y su estado de resolución (sistema de tickets), una lista de comprobaciones (*check list*) hechas a cada uno de los servidores o elementos de la plataforma: versiones de sistema, consumos (CPU, memoria RAM, espacio libre, media del ancho de banda consumido, número de conexiones, estado de las copias de seguridad). Este informe incluirá, por cada uno de los dominios: el número de ataques bloqueados por el WAF, una estadística detallada del número de solicitudes, ancho de banda, uso de la memoria u otros elementos que indique MWCapital.
- Generar y mantener actualizada toda la documentación referente a la infraestructura.

2.4.3 Gestión de usuarios y permisos

El proveedor deberá ocuparse de la gestión de usuarios garantizando el cumplimiento de todas las medidas de seguridad, añadiendo aquellos que se soliciten para el acceso a través de una determinada VPN y gestionando sus permisos de acceso a su área de consumo del recurso o recursos concretos.

En cuanto a la política de contraseñas se trabajará con claves de un mínimo de 8 caracteres que contengan números y símbolos. Se deberá solicitar a los usuarios un cambio de contraseñas con una periodicidad máxima de 12 meses.

2.4.4 Gestión de VPNs

Gestión y configuración de conexiones VPN Site-to-site entre las redes de MWCapital o las empresas desarrolladoras o colaboradoras y los servicios correspondientes de la plataforma.

Se configurarán VPNs Site-to-site para garantizar la conectividad con protocolos de seguridad desde la propia red de MWCapital y desde las redes de los diferentes colaboradores de MWCapital hasta un máximo de 10 empresas con unos 20 usuarios conectados con sus servidores de trabajo en cualquier horario.

2.5 ORGANIZACIÓN

La metodología de desarrollo está basada en el marco de gestión y trabajo Scrum (ver *ANEXO 1. Metodología SCRUM*), tanto en sus roles como en su única fase (el *sprint*) y las reuniones estándar que contiene. Los roles del equipo Scrum se repartirán entre la Dirección de Innovación de MWCapital y el contratista de la siguiente manera:

Dirección de Innovación de MWCapital:

- Product Owner.
- Scrum Master.
- Enlaces.

Contratista:

- Proxy Product Owner.
- Equipo de Desarrollo Scrum que dispondrá de todas las capacidades necesarias para el análisis, construcción, prueba, despliegue, soporte y mantenimiento del producto.
- Responsable del contrato que será el interlocutor único entre el contratista y MWCapital para todos los temas relacionados con la gestión y ejecución del contrato.

Los interlocutores de MWCapital serán el Product Owner, el Proxy Product Owner, el Scrum Master y los enlaces, y facilitarán la información necesaria y el acceso a los interlocutores oportunos para garantizar la productividad del equipo y su correcta toma de decisiones informadas.

Con carácter general, MWCapital velará, mediante las figuras del Product Owner y Scrum Master, el cumplimiento de los plazos acordados, así como la calidad y la adecuación de los servicios objeto de este contrato y la ejecución del desarrollo según la metodología y los estándares ágiles Scrum.

Igualmente MWCapital proporcionará enlaces para las diferentes disciplinas del proyecto que sean necesarias:

- Comunidad de *fact-checkers*.
- Arquitectura.
- Telecomunicaciones.

- Helpdesk.
- Seguridad.
- Protección de datos.
- Mantenimiento de Aplicaciones.

Estos interlocutores tendrán la responsabilidad de validar las partes del sistema que estén bajo su responsabilidad y según la metodología descrita en el *ANEXO 1. Metodología SCRUM* de este pliego, aportando requisitos funcionales y no funcionales y facilitando el trabajo dentro de sus áreas. Es posible que algunos de estos interlocutores pertenezcan a otros proveedores de MWCapital que presten servicios relacionados con las diferentes disciplinas que rodean el proyecto. Esto no debe comportar ningún problema ni entorpecer la ejecución del contrato. MWCapital reforzará la idea de equipo multidisciplinario sin importar la pertenencia a uno u otro proveedor.

Con carácter general, la interlocución de los roles de MWCapital asignados al contrato (Product Owner y Scrum Master) será indistintamente con todos los miembros del equipo. Es necesario que esta organización incluya la figura del Responsable de contrato del proveedor, que será el interlocutor único entre el contratista y MWCapital para todos los temas relacionados con la gestión y ejecución del contrato. Las funciones y responsabilidades del Responsable de contrato del contratista están detalladas en el apartado 2.*6.1 Funciones por perfil* de este pliego.

La organización del contrato deberá ajustarse a los requisitos mínimos que se especifican en los siguientes apartados.

2.5.1 Comité de dirección

Sus funciones son las de supervisar la marcha del contrato y la toma de decisiones que afectan al objetivo y alcance del mismo. El Responsable de contrato del contratista asistirá a las reuniones de este Comité siempre que sea requerido por cualquiera de sus miembros.

Resultado de todas las reuniones: se redactará un acta con los temas tratados y los acuerdos tomados. Si el Responsable de contrato del contratista asiste a las reuniones, será el encargado de la elaboración de la documentación de seguimiento del contrato necesaria para tal fin y también de levantar el acta de las reuniones. Esta acta se hará llegar en la mayor brevedad posible a todos los destinatarios que el Comité de Dirección considere oportuno.

Se reúne normalmente cada 2 sprints, aunque se podrá convocar con carácter extraordinario siempre que se considere necesario. Forman parte:

- Dirección de Innovación de MWCapital o en quien delegue.

- Product Owner.
- Proxy Product Owner.
- Scrum Master.
- Responsable de contrato del contratista (según requerimientos).

2.5.2 Eventos de seguimiento

El día a día del proyecto lo gestionan los roles del Equipo Scrum (Product Owner, Proxy Product Owner, Enlaces, el Equipo de desarrollo y el Scrum Master). Los diferentes eventos sirven para gestionar el estado del desarrollo al resto de actores de MWCapital, así como apoyar al Product Owner en la toma de decisiones para definir los siguientes sprints.

A continuación, se describen los diferentes eventos de seguimiento:

Planificación del sprint (sprint Planning)

La Planificación del Sprint es la reunión inicial donde el equipo Scrum determina qué ítems del Backlog se harán durante esta iteración. Esta reunión tiene dos objetivos principales:

- Determinar qué se hará: se seleccionan los ítems más prioritarios desde el punto de vista de negocio y técnico, de manera colaborativa entre todo el equipo Scrum.
- Determinar cómo se hará: el Equipo analiza técnicamente cómo se harán los ítems, p.e. haciendo un diseño de alto nivel y desglosando las tareas técnicas.

Es muy importante que los ítems estén previamente analizados (estado ready) para que esta reunión sea eficiente y se generen pocas dudas que puedan causar problemas dentro del Sprint.

Aspectos básicos de la Planificación del Sprint:

- Asistentes: Product Owner, Proxy Product Owner, Enlaces, el Equipo de desarrollo y el Scrum Master.
- Entradas: Backlog de producto y metas de negocio del Product Owner.
- Salidas: Backlog de sprint y meta del sprint.

Scrum diario (Reunión diaria)

El Scrum diario es una reunión que se realiza todos los días para que el Equipo de desarrollo haga seguimiento del Sprint, se coordine y decida acciones correctivas en caso de que sea necesario. Participarán el Scrum Master de MWCapital y el equipo de desarrollo con participación puntual de los diferentes enlaces.

El formato habitual de la reunión consiste en los miembros del Equipo utilizando estas preguntas para coordinarse y tomar decisiones:

- ¿Qué he hecho desde la última reunión para cumplir la meta del Sprint?
- ¿Qué haré hoy para cumplir la meta del Sprint?
- ¿Qué riesgos o problemas veo para que el equipo cumpla la meta del Sprint?

Aspectos básicos

- Equipo de desarrollo, enlaces (opcional) y Scrum Master (opcional).
- Duración máxima: 15 minutos.
- Entradas: Backlog de sprint y meta del sprint.
- Salidas : Backlog de sprint y decisiones.

La revisión del sprint (Sprint Review)

La Revisión del sprint es una reunión de gestión donde el equipo Scrum revisa qué se ha conseguido la entrega del incremento previsto y piensan qué queda por hacer a los futuros sprints. A esta reunión puede asistir cualquier otro rol de la organización que quiera saber el estado del desarrollo.

Durante esta reunión se puede hacer una demo general para identificar mejoras para próximos sprints, pero esta demo no sirve para validar las funcionalidades entregadas. La validación de los ítems entregados debe hacerse durante el siguiente sprint.

Aspectos básicos:

- Asistentes: Equipo Scrum.
- Duración máxima aproximada: 1h por cada semana de sprint.
- Entradas: Backlog del producto y meta del sprint.
- Salidas: Backlog del producto.

La retrospectiva del sprint (Sprint Retrospective)

La Retrospectiva del sprint es la última reunión del sprint, donde el Equipo Scrum identifica mejoras al funcionamiento del equipo para próximos sprints.

Un formato básico de reunión es donde cada miembro del Equipo valora el sprint pasado y hace propuestas para el siguiente, respondiendo a las preguntas:

- ¿Qué ha ido bien en este sprint?
- ¿Qué ha ido mal en este sprint?
- ¿Qué acciones concretas de mejora podríamos hacer en los próximos sprints?

Es conveniente que el Scrum Master haga también propuestas de mejora, que la totalidad de las propuestas de mejoras se incluyan en el backlog y que realice un seguimiento de las mejoras propuestas durante los sprints.

Aspectos básicos:

- Asistentes: Equipo Scrum
- Entradas: Información de la ejecución del sprint
- Salidas: Backlog de ideas de mejora.

Equipo de integración

Dado que hay dependencias directas con los equipos del Lote 2 y el Lote 3, tanto técnicas como de planificación, los equipos implicados deberán establecer un equipo de integración, tal y como se indica en el framework Scrum.

Este equipo de integración será de carácter virtual, es decir, que sus miembros formarán parte de los equipos de los contratos implicados y tendrán una dedicación parcial y variable al equipo de integración. La dedicación necesaria la decidirán sprint a sprint en función del grado de dependencias y de su complejidad.

Las funciones básicas del equipo serán:

- Revisar conjuntamente los Backlogs para anticipar y minimizar posibles dependencias.
- Preparar la planificación de los sprints para identificar y planificar las dependencias a gestionar durante el sprint.
- Gestionar durante el sprint el tratamiento de las dependencias para minimizar los conflictos.
- Mejorar de manera continua la coordinación entre los equipos.

El equipo de integración dispondrá del Scrum Master que le apoye en la organización.

Las actividades de este equipo serán paralelas a los sprints de los equipos, con los eventos habituales:

- Planificación previa de los sprints.
- A discreción, Scrum diario con los representantes de cada uno de los equipos.
- Revisión global del sprint.
- Retrospectiva global del sprint.

2.6 RECURSOS HUMANOS

2.6.1 Funciones por perfil

El contratista proporcionará un equipo de trabajo adecuado en número y preparación para la ejecución de los servicios.

MWCapital estima que los perfiles mínimos necesarios del contratista para la prestación de los servicios de esta licitación son los que se detallan a continuación.

Estos perfiles pueden ser compartidos por una misma persona, siempre que cubra todos los requerimientos expuestos, o bien repartidos entre varias personas del equipo, indicando por cada una de ellas el porcentaje de dedicación y el número de personas de cada perfil que se proponen.

1) Coordinador del contrato y Jefe de proyecto: Función de gestión del proyecto y los recursos humanos asignados, velar por la calidad del servicio, convocar a los comités y tareas de interlocución principal con MWCapital. Como coordinador del contrato asiste a los comités de dirección y se ocupa de los aspectos contractuales. Experiencia profesional o conocimientos mínimos requeridos:

    - Diez (10) años experiencia en proyectos tecnológicos.
    - Ocho (8) años experiencia en proyectos del ámbito TIC WEB.
    - Cinco (5) años experiencia como Responsable de Contrato con administración pública o sector privado.
    - Cinco (5) años experiencia como Jefe de Proyecto con administración pública o sector privado.
    - Disponer de Un (1) certificado Scrum de scrum.org.

2) Arquitecto principal: Diseño de la infraestructura, implementación de la automatización, directrices tecnológicas, rendimiento, solidez y escalabilidad de la plataforma. Participación en Divos. Experiencia profesional o conocimientos mínimos requeridos:

    - Siete (7) años experiencia en proyectos tecnológicos.
    - Participación en Cinco (5) proyectos de administración de aplicativos LAMP (Linux, Apache, Misal/MariaDB PHP).
    - Disponer de un mínimo de Nueve (9) conocimientos de los enumerados a continuación:
        - Cloud público: Google Cloud y AWS.
        - Gestión de contenedores: Docker o Kubernetes

- Infraestructura como Código: SALTstack o Packer o Terraform u Opsworks
- Servidores Web: Nginx, Apache, PHP FPM,
- Sistemas de memoria caché http: Varnish o CDNs – Akamai o Cloudflare, Redis o Memcache.
- Lenguajes / frameworks desarrollo: PHP y Bash.
- Bases de datos: MySQL/MariaDB, Postgresql.
- Sistema operativo: Linux (CentOS o Debian o Ubuntu)
- Gestión de versiones: GIT o GitLab
- Monitorización: Nagios o Grafana o Cloudwatch
- Conocimiento de protocolos de red: HTTP y TLS y TCP/IP y DNS y HTTPS+SSL.

3) Soporte al usuario: Encargado de atender las peticiones y los avisos, mediante las herramientas y canales de apoyo, aclarar dudas de las peticiones, velar para que el estado de las peticiones esté puntualmente informado y organizar los repositorios de documentación publicada del proyecto. Experiencia profesional o conocimientos mínimos requeridos:

    - Tres (3) años experiencia profesional de soporte al usuario o gestión del cliente en proyectos tecnológicos.

4) Analista Programador PHP: Encargado de realizar los análisis, el diseño, la codificación y los mantenimientos de los aplicativos web, incidencias de seguridad, conflictos de configuración en cuanto a la plataforma, aplicación de cambios masivos los aplicativos o webs gestionadas en el contrato (ej: inclusión de Cloudflare para acelerar el rendimiento, subidas de versión ante la publicidad de vulnerabilidades graves). Participación en DevOps. Experiencia profesional o conocimientos mínimos requeridos:

    - Diez (10) años experiencia profesional
    - Experiencia en al menos Diez (10) proyectos de aplicaciones LAMP (Linux, Apache, MySQL/MariaDB y PHP)
    - Experiencia en Cinco (5) proyectos en con frameworks PHP (Laravel, Phalcon...)
    - Orientado a la gestión de Movilidad (Mobile First)

5) Otros especialistas SEO/SEM, UX, Analítica y métricas, RRSS, Inbound marketing

- SEO/SEM: especialista en posicionamiento en buscadores y en anuncio en buscadores con una experiencia mínima de Tres (3) años.
- Analítica y métricas: especialista en analítica y métricas para sitios web. Realización de informes que incluya los resultados cuantitativos y cualitativos para la extracción de aprendizajes e identificación de mejoras. Creación de cuadros (dashboards) de indicadores digitales con Google Analytics y Google Data Studio. Con experiencia mínima de Tres (3) años.
- UX: especialista en experiencia de usuario, maquetación y diseño gráfico con una experiencia mínima de Cinco (5) años.
- RRSS: especialista en RRSS que incluya como mínimo Linkedin, X (Twitter), Youtube e Instagram con una experiencia mínima de Tres (3) años.

2.7 ACUERDOS DE NIVEL DE SERVICIO - ANS

Para la gestión y el seguimiento de los servicios prestados para el contratista, se definen una serie de Acuerdos de Nivel de Servicio (ANS) que los licitadores pueden complementar y/o mejorar. Estos permiten monitorizar y evaluar la calidad y la gestión de los servicios mediante indicadores que parametrizan el grado de logro acordado para cada servicio.

Los indicadores tendrán la siguiente estructura en común:

- Descripción: definición del indicador y objeto de medida.
- Cálculo: fórmula para el cálculo del indicador.
- Criticidad: grado de criticidad para las incidencias o las solicitudes.
- Valor límite: valor mínimo/máximo a partir del cual el indicador cumple el nivel de servicio acordado. El valor indicado en las tablas será el valor requerido para el contrato.

Criticidad	Definición
Grave	Interrupciones o disfunciones en el funcionamiento de los servicios y/o procesos en producción que den lugar a una completa inoperatividad del sistema, de un servidor, o de cualquier servicio o elemento en particular requerido para la operativa normal de la arquitectura. Impacta un número alto o es una operativa de negocio crítica. Incidencias que afecten a la integridad, confidencialidad y disponibilidad de la información. No hay ninguna solución alternativa. La incidencia debe ser atendida de manera urgente con el objetivo de recuperar el servicio lo antes posible. Las actividades por la resolución pueden incluir: Actuaciones ante cualquier ataque a cualquiera de los equipos o dispositivos de la infraestructura de la plataforma. Actuar a un servidor o servicio para solucionar problemas de saturación o rendimiento. Resolución de problemas o fallos que afecten al correcto funcionamiento de los servidores y/o elementos y/o servicios instalados. Ajustar los recursos en producción en caso necesario (como resultado de la monitorización o en respuesta a una alarma) o por solicitud de MWCapital. Desactivar los accesos mediante filtros y reglas en caso de sospecha de intrusión a bases de datos o cualquier información protegida. Configuración de servicios, plugins y/o accesorios necesarios para el funcionamiento de las aplicaciones y/o servicios. Restauración de copias de seguridad (completos o a nivel de ficheros y/o de bases de datos) y la restauración de snapshots en respuesta a un requerimiento de MWCapital. Actuaciones de *Disaster Recovery* Servicios de auditoría y análisis forense para averiguar las causas ante cualquier incidencia que afecte a los sistemas, como descensos de rendimiento, problemas de funcionamiento o con la sospecha, detectada o reportada, de cualquier intrusión o infección en los sistemas de la plataforma. Limpieza y desinfección de sistemas o software base infectados.

Normal	Impacta un número alto de usuarios, pero la afectación a la operativa de negocio no es crítica, o afecta a un número bajo de usuarios y hay una solución de contingencia aceptable. Las tareas asociadas a la operativa de negocio se pueden seguir desarrollando. Incidencias en los servicios en pre-producción. Solicitudes de cambios de la configuración de la infraestructura. Apoyo técnico en general. La incidencia debe ser atendida de manera ágil para recuperar el servicio normal en un tiempo razonable. Las actividades por la resolución pueden incluir: Creación y configuración de nuevos servidores o elementos instalando el sistema operativo y/o el software adicional que se pueda requerir. Ajustar los recursos de los servicios en caso necesario (como resultado de la monitorización o en respuesta a una alarma) o por solicitud de MWCapital. Solicitudes de cambios o incorporaciones de registros a los DNS. Solicitudes de cambio en las reglas de filtrado del Firewall y/o del WAF y/o de otros elementos o dispositivos de seguridad. Creación, eliminación de usuarios. Asignación y/o cambio de los permisos de los usuarios Solicitudes de gestión de VPNs o equivalentes (Ztrust...): añadir nuevos usuarios, creación de nuevas VPNs Requerimientos de información o verificación sobre el funcionamiento de cualquier dispositivo de la infraestructura de MWCapital. Instalación, configuración y renovación de certificados de seguridad. Solicitudes de creación de nuevas métricas o de alarmas de monitorización Informes de incidencias en el funcionamiento de un determinado servicio de la infraestructura objeto del contrato.
Leve	Disfunciones en el funcionamiento de los servicios y/o procesos en producción que no afecten a la calidad del servicio. Solicitudes de asesoramiento. Las actividades por la resolución pueden incluir: Asesoramiento general a MWCapital. Proyectos de implantación de servidores y/o nuevos elementos y/o nuevos servicios. Realización de informes especiales requeridos por MWCapital. Instalación de parches de sistema y/o nuevas versiones de librerías o programas en la ventana de tiempo aprobada previamente por MWCapital.

	Criticidad/Tipo		
	Leve	**Normal**	**Grave**
Tiempo de contacto	<= 6h	<= 2h	<= 10min
Tiempo de análisis y planificación	<= 12h	<= 8h	<= 1h
Tiempo de resolución	<= Planificado y aprobado por MWCapital	<= 16h	<= 4h
Alcance horario	10x5*	10x5*	24x7x365*
Volumen de incidencias reabiertas		<= 4	<= 3

Ver apartado 2.8.2 *Horarios de prestación de los servicios

Indicador	Descripción	Cálculo
Tiempo de contacto	Tiempo que ha transcurrido entre la solicitud y la respuesta de recepción por parte del contratista.	***Timestamp* de la respuesta de recepción – *Timestamp* de la solicitud**
Tiempo de análisis y planificación	Tiempo que ha transcurrido entre la comunicación de una solicitud y la planificación de la resolución	***Timestamp* de la entrega del análisis y la planificación – *Timestamp* de la solicitud**
Tiempo de resolución	Tiempo que ha transcurrido entre la comunicación de una solicitud y la resolución efectiva	***Timestamp* de la resolución efectiva – *Timestamp* de la solicitud**

Volumen de incidencias reabiertas	Número de incidencias reabiertas por resolución incorrecta	Número de incidencias reabiertas mensualmente

Por otra parte, los ANS de la infraestructura de sistemas y comunicaciones suministrada será del 99,99%.

El cumplimiento de los ANS será revisado de manera bimensual. En el comité de dirección se deberá realizar una presentación del estado de cumplimiento de los ANS y posibles desviaciones que se hayan dado.

3 LOTE 2. API DEL CLAIM DETECTION Y SERVICIOS PARA LA INTEGRACIÓN EN LA PLATAFORMA

3.1 OBJETO

El objeto de este lote es:

- La provisión de las licencias para el uso de las funcionalidades específicas de *Claim Detection* y el *middle software* (API) para su exposición al consumo por parte de la plataforma.
- Gestión, desarrollo y construcción de todos los elementos *middle software* (API).
- Gestión del lote y coordinación con los otros lotes del contrato.
- Puesta en marcha, *go live*, y mantenimiento del *middle software* (API) y las licencias para toda la duración del contrato.

3.2 CARACTERÍSTICAS TÉCNICAS Y ALCANCE

Indicadores y métricas requeridos

Las nuevas herramientas de Inteligencia Artificial están permitiendo la generación de nueva desinformación, en más modalidades (imagen, audio, vídeo...), facilitando la creación de campañas de desinformación más precisas. Sin embargo, las posibilidades de la Inteligencia Artificial (IA) y el Machine Learning (ML) siguen siendo mucho más amplias, y ayudar a contrarrestar la desinformación es una de ellas.

Una de las aplicaciones en las que los modelos de IA están jugando un papel clave es en el desarrollo de sistemas automáticos de verificación de la desinformación. No obstante, debido al volumen sustancial de información, las complejidades asociadas con el discernimiento de dichos datos y la utilización de algoritmos de IA/ML, que, si bien son

notablemente potentes, no están exentos de problemas y sesgos que pueden obstaculizar el desarrollo de sistemas resilientes, confiables y eficientes para abordar de manera efectiva el problema de la desinformación. Por ello es requisito del contrato disponer de los indicadores y métricas para evaluar cuantitativa y cualitativamente estos sistemas de verificación (automática o semiautomática).

Son 3 los grupos de indicadores:

1. Modalidades de información
2. Métricas de calidad
3. Métricas de rendimiento

Estos indicadores están detallados en el A*nexo 2 Relativo al contrato para el suministro de una Plataforma de Fact-checking para la comunidad española*, y a la vez se indica si son adecuados para *claim detection* (CD), *claim matching* (CM) o ambos (CD-CM), aunque que sea parcialmente.

Detección y Recopilación de Claims (*Claim Detection*)

a) El contratista deberá proporcionar APIs que permitan la integración de la plataforma con repositorios abiertos de fact-checking existentes o previstos (hasta un máximo de 10 APIs)
b) Los algoritmos de claim detection subyacentes a las licencias deben ser capaces de identificar y recolectar afirmaciones a verificar a partir de una amplia variedad de fuentes abiertas como RSS, URLs, redes sociales accesibles, aplicaciones de mensajería privada, e incluso de archivos de base de datos en diferentes formatos (CSV, JSON, etc.).
c) Los algoritmos de claim detection subyacentes a las licencias deben estar dentro de los rangos y condiciones de los indicadores del Anexo 2 anteriormente mencionado.
d) Los algoritmos de claim detection subyacentes a las licencias deben ser capaces de detectar de manera efectiva las afirmaciones dentro de un conjunto de datos proporcionado por los evaluadores y de acuerdo a los rangos y condiciones de los indicadores del Anexo 2 anteriormente mencionado.

4 LOTE 3. API CLAIM MATCHING Y SERVICIOS PARA LA INTEGRACIÓN EN LA PLATAFORMA

4.1 OBJETO

El objeto de este lote es:

- Gestión del lote y coordinación con los otros lotes del contrato

- Gestión, desarrollo y construcción de todos los elementos de software necesario
- La provisión de las licencias para el uso de las funcionalidades específicas de *Claim Matching* y el *middle software* (API) para su exposición al consumo por parte de la plataforma.
- Puesta en marcha y *go live*.

4.2 CARACTERÍSTICAS TÉCNICAS Y ALCANCE

Indicadores y métricas requeridos

Las nuevas herramientas de Inteligencia Artificial están permitiendo la generación de nueva desinformación, en más modalidades (imagen, audio, vídeo...), facilitando la creación de campañas de desinformación más precisas. Sin embargo, las posibilidades de la Inteligencia Artificial (IA) y el Machine Learning (ML) siguen siendo mucho más amplias, y ayudar a contrarrestar la desinformación es una de ellas.

Una de las aplicaciones en las que los modelos de IA están jugando un papel clave es en el desarrollo de sistemas automáticos de verificación de la desinformación. No obstante, debido al volumen sustancial de información, las complejidades asociadas con el discernimiento de dichos datos y la utilización de algoritmos de IA/ML, que, si bien son notablemente potentes, no están exentos de problemas y sesgos que pueden obstaculizar el desarrollo de sistemas resilientes, confiables y eficientes para abordar de manera efectiva el problema de la desinformación. Por ello es requisito del contrato disponer de los indicadores y métricas para evaluar cuantitativa y cualitativamente estos sistemas de verificación (automática o semiautomática).

Son 3 los grupos de indicadores:

1. Modalidades de información
2. Métricas de calidad
3. Métricas de rendimiento

Estos indicadores están detallados en el Anexo N, y a la vez se indica si son adecuados para *claim detection* (CD), *claim matching* (CM) o ambos (CD-CM), aunque que sea parcialmente.

Etiquetado de Claims y Correspondencia con Fact-Checks Existentes (Claim Matching)

a) El contratista deberá proporcionar APIs que permitan la integración de la plataforma con repositorios abiertos de fact-checking existentes o previstos (hasta un máximo de 10 APIs)

b) Los algoritmos de *claim matching* subyacentes a las licencias deben ser capaces de comparar eficazmente las afirmaciones detectadas con una base de datos de afirmaciones existentes para encontrar coincidencias
c) Los algoritmos de *claim matching* subyacentes a las licencias deben estar dentro de los rangos y condiciones de los indicadores del Anexo anteriormente mencionado
d) Los algoritmos de *claim matching* subyacentes a las licencias deben ser capaces de comparar eficazmente las afirmaciones dentro de un conjunto de datos proporcionado por los evaluadores y de acuerdo a los rangos y condiciones de los indicadores del A*nexo 2 Relativo al contrato para el suministro de una Plataforma de Fact-checking para la comunidad española*.

5 LOTE 4 TESTING Y EVALUACIÓN PLATAFORMA

5.1 OBJETO

El objeto de este lote es la realización de los test, la validación funcional y de sistemas de la plataforma en su conjunto.

5.2 CARACTERÍSTICAS TÉCNICAS Y ALCANCE

Es responsabilidad del contratista la definición y realización de las pruebas de test y evaluación de la plataforma, incluyendo como mínimo, las métricas e indicadores indicadas en el A*nexo 2 Relativo al contrato para el suministro de una Plataforma de Fact-checking para la comunidad española* de este pliego.

El contratista deberá presentar a MWCapital, el plan de pruebas, incluyendo para cada tipología de prueba, los casos de uso de los requerimientos. Una vez validado, aprobado y admitido, los casos de uso definidos en el plan de pruebas serán realizados y documentados en las pruebas correspondientes.

El contratista deberá realizar la definición, planificación, organización y coordinación de las pruebas realizadas. Es responsabilidad del contratista la definición y realización de las pruebas.

Las pruebas se realizarán sobre el entorno de pruebas de preproducción y una vez validadas se realizarán en el entorno de producción en las ventanas de tiempo que no supongan una alteración del servicio de la plataforma y previa aprobación por parte de MWCapital

Será responsabilidad del contratista la preparación de los juegos de prueba y habilitar los entornos correspondientes para las pruebas funcionales, así como los perfiles y usuarios necesarios para ejecutar estos planes de pruebas.

Para la ejecución de las pruebas deberán realizarse como mínimo las siguientes actividades:

- El contratista realizará el diseño del plan de pruebas de manera iterativa, identificando, acordando y especificando las métricas, indicadores, atributos y características de calidad que se deben probar. El objetivo es diseñar las pruebas a fin de validar que las funcionalidades son operativas de acuerdo con las métricas e indicadores, que la entrada de datos se acepta de forma correcta y que los resultados esperados son los correctos.
- Verificará que se han identificado y definido los casos de prueba necesarios para garantizar las funcionalidades y rendimiento de la plataforma, por lo que se detallarán acciones a realizar y para cada uno de los casos se asociará su resultado esperado que podrá ser verificado. Durante esta misma fase, se especifican también los datos de entrada necesarios para que los casos de prueba definidos puedan ser ejecutados, ya sea buscando el éxito del resultado o bien el error.
- Se realizará la ejecución de los casos de prueba anteriormente diseñados de forma manual siguiendo el detalle del guion establecido. El analista que ejecute las pruebas debe disponer de cierta libertad y autonomía para detectar situaciones anómalas no contempladas.
- Se guardará un listado detallado de los errores encontrados en la ejecución de los casos de prueba y de su corrección.
- Se repetirá la batería de pruebas tantas veces como se estime necesario hasta la obtención del resultado correcto.

Siempre, y en todo caso, se deberá entregar un Informe del Resultado de la Ejecución de las pruebas, junto con la grabación de los resultados de cada prueba (posibles opciones: fichero de resultados generado por una herramienta de testing, entrega de un fichero log, captura de ventanas con el resultado de las pruebas, etc.).

La definición y ejecución del plan de pruebas será validado definitivamente por MWCapital y requerirá de su aprobación para ser admitido.

El informe contendrá, como mínimo, los siguientes elementos:

- Identificación y descripción de la prueba.
- Identificación y especificación de las métricas, indicadores, atributos y características de calidad que componen la prueba.
- Resultado de la prueba, especificando si éste es satisfactorio o no, incluyendo las observaciones que se consideren necesarias para justificar el resultado.

- Informe de incidencias en el que deberá especificarse como mínimo descripción de la incidencia, fecha de apertura, fecha resolución, responsable. Este informe deberá estar actualizado diariamente y se utilizará para el seguimiento de iteraciones de las pruebas.

Se realizarán como mínimo cuatro (4) evaluaciones completas durante el período de ejecución del contrato. Cada evaluación deberá entregar dentro de un máximo de dos (2) semanas desde la solicitud por parte MWCapital.

5.3 RECURSOS HUMANOS

5.3.1 Funciones por perfil

El contratista proporcionará un equipo de trabajo adecuado en número y preparación para la ejecución de los servicios.

MWCapital estima que los perfiles mínimos necesarios del contratista para la prestación de los servicios de esta licitación son los que se detallan a continuación.

Estos perfiles pueden ser compartidos por una misma persona, siempre que cubra todos los requerimientos expuestos, o bien repartidos entre varias personas del equipo,

1) Coordinador del contrato y Jefe de proyecto: Función de gestión del proyecto y los recursos humanos asignados, velar por la calidad del servicio, convocar a los comités y tareas de interlocución principal con MWCapital. Como coordinador del contrato asiste a los comités de dirección y se ocupa de los aspectos contractuales. Experiencia profesional o conocimientos mínimos requeridos:

    - Diez (10) años experiencia en proyectos tecnológicos.
    - Tres (3) años experiencia en proyectos del ámbito *fact-checking*.
    - Cinco (5) años experiencia como Responsable de Contrato con administración pública o sector privado.

2) Analista: Encargado de realizar los análisis, el diseño, la configuración y parametrización de las herramientas de análisis. Experiencia profesional o conocimientos mínimos requeridos:

    - Cinco (5) años experiencia profesional como analista
    - Experiencia en al menos Tres (3) proyectos de *fact-checking*

6 CONDICIONES GENERALES

6.1 LUGAR DE PRESTACIÓN DEL CONTRATO

EL SERVICIO NO SE PRESTARÁ EN LAS OFICINAS DE MWCAPITAL SALVO QUE ASÍ SE REQUIERA EXPRESAMENTE.

En las ocasiones que lo requieran, se podrá solicitar el desplazamiento a las oficinas de MWCapital para la prestación del servicio que sea necesario, siendo obligación del contratista la aportación de las herramientas que sean necesarias para la prestación de este.

Las reuniones se realizarán en las oficinas de MWCapital o telemáticamente por videoconferencia siempre que MWCapital así lo solicite.

6.2 HORARIOS DE LA PRESTACIÓN DE LOS SERVICIOS

El contratista deberá garantizar que el horario de prestación de los servicios sea como mínimo coincidente con el horario laboral de MWCapital: 10 x 5 (días laborales en la ciudad de Barcelona, de lunes a viernes de 8 h a 18 h).

Excepcionalmente, y con aviso previo de 24 horas, se podrá requerir la ejecución de determinados servicios fuera del horario estipulado (emergencias, desarrollos urgentes, incidencias críticas...) sin que la prestación de los mismos suponga un coste excepcional por MWCapital respecto al precio/hora habitual.

6.3 GARANTÍA

Durante el periodo de garantía el contratista se compromete a resolver todas las incidencias o defectos detectados en los desarrollos entregados que le sean imputables a él por acción o por omisión, sin ningún tipo de coste por MWCapital.

Las acciones de mantenimiento correctivo que resulten como causa de una acción previa realizada por el propio contratista en el desarrollo de cualquiera de los servicios definidos en el presente pliego de prescripciones técnicas, se tratarán como actividades sujetas a garantía de 12 meses, y por lo tanto estarán incluidas sin ningún coste adicional en el servicio.

Las actuaciones sujetas a garantía deberán ser incorporadas como información del estado de los servicios en los comités de seguimiento indicando su periodo de finalización por servicio.

El periodo de garantía deberá ejecutarse en los términos estipulados en el presente punto, aunque el contratista no continúe con la prestación del servicio.

6.4 SEGURO DE RESPONSABILIDAD PROFESIONAL

El contratista deberá disponer de una póliza de seguro de responsabilidad civil por riesgos profesionales asociados a la actividad objeto del contrato por un importe mínimo de **20.000 euros**.

6.5 SEGURIDAD

En cuanto a los aspectos propios de seguridad, se tendrá especial cuidado de prever que los productos finales cumplan con lo establecido en el RD 3/2010 de 8 de enero por el que se regula la Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica.

El contratista se obliga a velar por el cumplimiento de la legislación vigente aplicable al objeto del contrato y especialmente en lo que se refiere a la protección de datos de carácter personal (GDPR) y la Ley Orgánica 3/2018, de 5 de diciembre, de Datos de Carácter Personal y Garantía de los Derechos Digitales.

6.6 CONFIDENCIALIDAD

La empresa contratada se obliga a no difundir y guardar el más absoluto secreto de toda la información a la que tenga acceso en cumplimiento del presente contrato y en suministrarla sólo al personal autorizado por la MWCapital.

El contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer como consecuencia de la participación en la presente licitación, o, con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrán copiar o utilizar como finalidad diferente a las que la información tiene designada.

Cuando el objeto del contrato sea la construcción y / o mantenimiento de Sistemas de Información y / o Infraestructuras Tecnológicas, el deber de secreto incluye los componentes tecnológicos y medidas de seguridad técnicas implantadas en los mismos.

La empresa contratada será responsable de las violaciones del deber de secreto que se puedan producir por parte del personal a su cargo. Asimismo, se obliga a aplicar las medidas necesarias para garantizar la eficacia de los principios de mínimo privilegio y necesidad de conocer, por parte del personal participante en el desarrollo del contrato.

Una vez finalizado el presente contrato, la empresa contratada se compromete a destruir con las garantías de seguridad suficientes o devolver toda la información facilitada por MWCapital, así como cualquier otro producto obtenido como resultado del presente contrato.

6.7 CLÁUSULA DE PROPIEDAD INTELECTUAL

La propiedad intelectual de los trabajos realizados al amparo de este contrato pertenece a MWCapital de forma exclusiva. Los productos o subproductos derivados no podrán ser utilizados sin la debida autorización previa.

El acceso a información y/o productos protegidos por la propiedad intelectual, propiedad de MWCapital, necesarios para el desarrollo del producto o servicio contratado no presupone en ningún caso la cesión de esta.

La empresa contratada acepta expresamente que los derechos de explotación de los productos derivados de este pliego corresponden única y exclusivamente a MWCapital. En consonancia, el contratado cede, con carácter de exclusividad, la totalidad de los derechos de explotación de los trabajos objeto de este pliego, incluidos los derechos de comunicación pública, reproducción, transformación o modificación y cualquier otro derecho susceptible de cesión en exclusiva, de acuerdo con la legislación sobre derechos de propiedad intelectual.

Barcelona, a 12 de abril de 2024

Eduard Martín
Chief Innovation Officer
Fundació Barcelona Mobile World Capital Foundation