SERVICIO DE FIRMA DIGITAL CERTIFICADA ONLINE DE DOCUMENTOS PARA IFEMA MADRID

EXP. 25/089 - 2000027245

PLIEGO PRESCRIPCIONES TÉCNICAS

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Madrid, Noviembre 2025

Índice

1 Introducción

IFEMA MADRID, líder en el sector de celebraciones de Ferias, Eventos y Congresos tiene como uno de sus principales objetivos el ofrecer servicios de calidad a sus empleados, organizadores, expositores y visitantes, poniendo siempre a su disposición las últimas tecnologías que faciliten su trabajo.

Para IFEMA MADRID es importante garantizar la calidad, disponibilidad, integridad, confidencialidad y seguridad de los servicios de tecnologías de la información que pone a disposición de dichos usuarios.

Por estas razones y con motivo de la renovación del servicio de Firma Digital Certificada de Documentos online para IFEMA MADRID se establece la presente licitación cuyas condiciones técnicas se describen en el presente documento.

2 Objeto

El objeto del presente contrato es el servicio de firma digital certificada online para documentos de IFEMA MADRID. Un servicio que ahorre tiempo y costes en la obtención de documentos firmados conjuntamente tanto por personas de IFEMA MADRID como por terceros, con todas las garantías jurídicas de integridad y autenticidad, equivalentes a todos los efectos a las firmas manuscritas, pero sin papel.

Este servicio debe permitir el envío de documentos a firma por internet, la obtención de las firmas válidas y la entrega de los documentos correctamente firmados a todos los interesados.

Debe ser un servicio que incorpore las medidas de seguridad solicitadas en el apartado 3.1.1 que ofrezca la máxima facilidad y conveniencia para que los partícipes puedan firmar desde cualquier lugar y con cualquier dispositivo, con la mira puesta en la eficiencia, la confidencialidad, la disponibilidad y la integridad. En particular, debe contar con medidas de seguridad que impidan el uso no autorizado de los certificados digitales de las personas de IFEMA. En definitiva, debe ser un servicio en el que IFEMA pueda depositar toda su confianza.

3 Alcance

3.1 Aplicación o portal web para el uso manual del servicio

Se solicita una aplicación, preferiblemente web, que permita a IFEMA MADRID la obtención de documentos firmados tanto por personas de IFEMA MADRID como por terceros. La solución ofrecida permitirá a los usuarios autorizados de IFEMA MADRID el acceso seguro a todas sus funcionalidades con cualquier navegador e impedirá los accesos no autorizados con medidas como las que se solicitan más adelante.

Todos los datos relacionados con IFEMA MADRID que contenga la solución tienen la consideración de datos sensibles y confidenciales de IFEMA MADRID. Por tanto, deben contar con el nivel de protección frente accesos no autorizados requeridos en este pliego. En particular, los certificados digitales de IFEMA MADRID que sea preciso configurar en la solución, deben estar protegidos de modo que no sea posible su uso no autorizado.

La solución incorporará como mínimo los procedimientos y las medidas de seguridad que se solicitan a lo largo de este documento, las que indica el apartado 3.1.1 y las que indica el documento *"Anexos Exp 25/089"* apartado *"Documentación de la dirección de tecnologías de la información_Anexo para contratos de bienes y servicios con elementos relacionados con TI"*.

La oferta indicará las medidas de seguridad y procedimientos con que cuenta la solución para impedir el acceso no autorizado a los datos y certificados digitales de IFEMA y a la propia aplicación.

Por ejemplo, indicará dónde se encuentran los datos y certificados digitales, cómo se protegen, qué impide los accesos no autorizados, qué medidas de seguridad protegen los accesos, documentos, datos y certificados, qué medidas de autenticación tiene la aplicación, qué políticas de contraseñas tales como longitud y complejidad, bloqueos por números de accesos incorrectos, caducidad de contraseñas, etc. En todo caso, esas medidas y procedimientos deberán cumplir estrictamente, como mínimo, los requerimientos contenidos en el presente pliego, pudiendo incorporar la oferta medidas o requerimientos adicionales dirigidos a garantizar la seguridad y el buen funcionamiento de la aplicación.

La solución contará al menos con los siguientes roles principales para sus usuarios:

a. Rol de administradores para los usuarios Administradores de Sistemas de IFEMA MADRID que realizan las tareas de configuración y administración de sistemas de la solución.
b. Rol para usuarios que desencadenan manualmente los procesos de firma, especificando los documentos y los firmantes. En adelante usuarios remitentes.
c. Rol para los usuarios internos de IFEMA MADRID que firman los documentos con su propio certificado digital de persona física o jurídica. En adelante, usuarios firmantes internos.
d. Rol para resto de usuarios, excluyendo firmantes internos, que deban firmar documentos. En adelante, terceros firmantes.
e. Rol para grupos de usuarios internos de IFEMA MADRID que consultan el estado de envíos a firma en los que se les haya configurado como grupo interesado en dicho estado. En adelante, usuarios interesados.

Se solicitan la realización de las actividades técnicas necesarias para el establecimiento, activación y configuración del servicio para IFEMA MADRID hasta el punto de que permita iniciar su utilización por parte de los usuarios en las condiciones de seguridad descritas a lo largo de este documento y el acceso de los usuarios a instrucciones, ejemplos, material formativo y procedimientos de resolución de dudas e incidentes.

Asimismo, el adjudicatario debe estar abierto a realizar modificaciones y mejoras en un tiempo aceptable (una jornada) en el funcionamiento de la aplicación, que sean razonables y de interés para IFEMA MADRID. Por ejemplo, cambios que faciliten la usabilidad o que mejoren la imagen de IFEMA MADRID y de sus documentos firmados ante terceros. **Toda modificación que supere una jornada de esfuerzo se valorará aparte**: el adjudicatario presentará presupuesto que deberá ser aprobado por IFEMA MADRID.

3.1.1 Seguridad

La oferta describirá las medidas de seguridad que permiten acceder, autenticar y autorizar a los usuarios de cualquier tipo: remitentes, firmantes internos, terceros firmantes, interesados, administradores, etc. junto con las medidas que impiden el acceso ilícito a la plataforma, que deberán cumplir todos los requerimientos contenidos en el presente pliego. Las medidas deberán poder ser configuradas adecuadamente por el servicio de soporte del adjudicatario solo a petición de IFEMA MADRID o de conformidad con IFEMA MADRID.

El adjudicatario incorporará a la solución, con la conformidad de IFEMA, las medidas de seguridad necesarias para garantizar la seguridad frente a nuevas amenazas.

La aplicación propuesta debe permitir configurar, el número de reintentos tras los cuales se bloquea el acceso, la longitud y la complejidad de las contraseñas, el uso de un segundo factor de autenticación, y cualquier otro elemento necesario para lograr el equilibrio adecuado entre seguridad y usabilidad. La aplicación propuesta debe contar con un procedimiento y unas medidas de seguridad adecuadas para impedir el acceso no autorizado a cualquiera de sus elementos tales como los documentos que contenga, los certificados digitales de los usuarios de IFEMA, sus funcionalidades, sus logs, etc.

En particular, sin que sea una enumeración cerrada, la oferta debe contener, al menos:

* Medidas de seguridad específicas para el acceso autenticado a la plataforma. Por ejemplo, políticas de longitud mínima de las contraseñas, complejidad y tiempo de validez de las mismas o la exigencia de doble factor de autenticación. En particular, terceros firmantes y/o Administradores de Sistemas.

* Medidas de seguridad adecuadas para impedir el acceso ilícito, los intentos de adivinar contraseña y los ataques de diccionario. La aplicación permitirá configurar el número de reintentos no válidos de autenticación y el período entre los mismos, tras los cuales se debe bloquear la cuenta del usuario relacionada. En particular, para terceros firmantes y/o Administradores de Sistemas.

* Un procedimiento para desbloquear las cuentas bloqueadas, que permita que los usuarios legítimos puedan trabajar con pocas molestias pero que impida eficazmente los accesos no autorizados. En caso de incidencias con el acceso (bloqueo de cuenta, olvido de contraseña, etc.), un usuario legítimo debe poder acceder a la plataforma en menos de cuatro horas. En particular, la plataforma debe contar con procedimientos tales como desbloqueo automático tras un tiempo prudencial configurable de 15 minutos o más, email para la activación de la cuenta bloqueada a la dirección predefinida del usuario, teléfono de soporte, preguntas de seguridad con respuestas predefinidas, o cualquier procedimiento con una agilidad y eficiencia similar.

* Autenticación de múltiples factores para terceros firmantes.

El adjudicatario deberá incorporar, sin coste para IFEMA, lo antes posible las mejoras en asuntos de seguridad que surjan en el futuro y que sean necesarias y adecuadas para impedir las amenazas y los ataques que puedan surgir de forma destacada y que ahora mismo no se pueden prever.

La aplicación funcionará en infraestructura que cuente con medidas que garanticen la confidencialidad de todos los elementos de la aplicación, datos, configuraciones, certificados, etc. respecto de otros clientes y usuarios de la misma infraestructura; medidas para recuperar la integridad de todos los elementos de la aplicación en caso de borrado, corrupción, o pérdida. Medidas para garantizar una disponibilidad elevada y recuperarla lo antes posible en caso de incidente que impida su funcionamiento. El licitante incluirá en su oferta las explicaciones y evidencias que acrediten la conformidad y adecuación de su oferta en materia de seguridad a lo solicitado en este párrafo. Estas medidas y procedimientos deben poder recuperar en menos de 4 horas la disponibilidad y consistencia de la solución a una situación existente como máximo 24 horas antes del incidente.

La solución ofertada deberá incluir la monitorización de los logs de accesos para identificar ataques y la adopción de medidas para mitigarlos. En particular y a modo de ejemplos, los intentos ilícitos de acceso y las medidas para mitigarlos. O también, a modo de ejemplo, la detección de los ataques de diccionario - tras lo que se averiguará la ubicación geográfica de las direcciones IPs y, si procede, se impedirá la comunicación desde dichas IPs-. O los intentos de explotar vulnerabilidades en la aplicación web, así como la adopción de todas las medidas necesarias para mitigarlas.

3.1.2 Conformidad jurídica de la firma

La oferta asimismo describirá los diversos mecanismos que permiten a la solución ofrecida la obtención de firmas electrónicas avanzadas por parte de terceros, con validez y aceptación jurídica.

Asimismo, la oferta describirá también el mecanismo que permita la obtención de firmas electrónicas cualificadas por parte de terceros, con validez y aceptación jurídica.

3.1.3 Usuarios remitentes

Los usuarios remitentes son los que tramitan los documentos que han de firmar los usuarios firmantes, tanto internos como terceros. A continuación, se describen las funciones y el modo de funcionamiento que debe tener la aplicación que se solicita para los miembros del rol de usuarios remitentes.

Se solicita una aplicación, preferiblemente web, para los usuarios remitentes.

La aplicación contará con las funcionalidades necesarias para realizar envíos de documentos a firma, consultar el estado de los envíos realizados e incluso cancelar los envíos cuando su estado así lo permita.

La aplicación ofrecida debe permitir al usuario remitente configurar con facilidad el envío correcto del documento a la firma, tanto en lo que se refiere a los elementos principales, tales como la identificación de los documentos que forman parte del envío o quiénes son los destinatarios con sus datos de contacto, como en lo que se refiere a los detalles de aspecto y usabilidad que se solicitan a continuación.

Por defecto, el envío a firma se producirá en cuanto esté completamente bien configurado.

El formato de los documentos a firmar será PDF en general. Se prevé que la mayoría de ellos tendrán concretamente formato PDF generados con MS Word de Office 365.

Aspecto, usabilidad:

La aplicación debe cumplir los siguientes requerimientos de aspecto y usabilidad:

Debe ser configurable el número de mensajes de recordatorio que recibirán los usuarios firmantes que no hayan firmado transcurrido un período, también configurable.

Debe ser configurable también la posición de las firmas en los documentos. Es decir, el usuario remitente debe poder especificar la ubicación en la que aparecerán en los documentos una vez firmados los detalles identificativos de los firmantes y de sus firmas.

Debe permitir que la cantidad de firmantes de un envío sea variable: uno o más, tanto internos como terceros firmantes. El caso previsto más frecuente son los envíos para dos firmantes: uno interno y otro externo, si bien la plataforma debe admitir la firma sea cual sea el número de firmantes.

El orden de firma debe ser configurable en los envíos con varios firmantes: los firmantes internos se podrán configurar como los últimos para que no reciban notificación ni documento pendiente de firma alguno hasta que todos los firmantes externos hayan firmado correctamente.

Debe ser sencillo para el usuario remitente encontrar los datos más relevantes que faciliten su trabajo habitual. En particular y a modo de ejemplo, Debe ser sencillo consultar y encontrar los datos de los terceros firmantes de alta más reciente o conocer el estado de los envíos pendientes, cuántas notificaciones ha recibido cada firmante, si llegaron o no a su destinatario y el motivo -email o teléfono incorrecto-, etc.

Los mensajes de error de la aplicación para el usuario remitente deben ser claros y permitirle identificar y corregir por sí mismo la causa del error.

Las notificaciones de documentos pendientes de firma a terceros deben repetirse automáticamente tras un período configurable o razonable de tres días, por ejemplo.

Los envíos a firma deben poder ser editados o cambiados para rectificaciones. Por ejemplo, para cambiar el o los documentos enviados o para cambiar a los destinatarios firmantes del envío.

El remitente podrá descargar el documento firmado correctamente y con las firmas válidas disponibles realizadas aun cuando no lo hayan firmado todos sus destinatarios.

Tanto remitentes como interesados podrán consultar con facilidad el estado del envío con el detalle de la cantidad, método y momento de las notificaciones que ha enviado el sistema al tercero firmante.

3.1.4 Usuarios firmantes internos

Los usuarios firmantes internos son los usuarios de IFEMA MADRID, normalmente altos cargos de la organización, que deben firmar los documentos que se les remita a firmar con su propio certificado digital de persona física o de persona jurídica.

Se solicita una aplicación, preferiblemente web, para los usuarios firmantes internos a la que accederán de forma segura para realizar su cometido.

Se requiere que la aplicación sea sumamente sencilla y que presente una usabilidad elevada para el usuario firmante interno. Para ello, debe cumplir, al menos, los requerimientos que se identifican a continuación:

La aplicación deberá mostrar al usuario firmante interno la lista de los documentos que tiene pendientes de firmar nada más acceder, sin pantallas intermedias ni requerimientos de claves adicionales.

En el caso de que en un envío a firma se haya configurado al usuario firmante interno como el último en firmar, lo cual será el caso más habitual, la aplicación no le mostrará los documentos pendientes de firmar por parte de otros usuarios. No obstante, la aplicación debe garantizar el acceso por los usuarios autorizados a esta documentación.

El usuario firmante interno podrá leer detenidamente uno por uno los documentos pendientes de firma cuantas veces sea necesario, accediendo en cuantas ocasiones lo necesite y con el dispositivo o navegador moderno que prefiera. Por ejemplo, PC, iPad, Chrome, Safari, etc.

El usuario firmante interno debe poder seleccionar con facilidad uno, varios o todos los documentos de su lista de documentos pendientes para rechazar o firmar todos los documentos seleccionados con una sola operación, tras la cual, desaparecerán de su lista de documentos pendientes. La operación más frecuente prevista es la de seleccionar varios o todos los documentos de la lista de pendientes y firmarlos de una sola vez, independientemente del número de documentos que contenga la selección. Es decir, firmar muchos documentos a la vez al final no debe ser una operación tediosa ni que requiera mucho más esfuerzo por parte del usuario firmante interno que firmar sólo un documento.

La plataforma permitirá con facilidad y de forma segura la incorporación o supresión de los certificados de firma electrónica operativos.

Seguridad de los certificados

Los certificados digitales de persona física o jurídica de los usuarios firmantes internos deben contar con la máxima protección frente a un uso no autorizado.

En el caso en que la solución propuesta requiera que el certificado digital de persona física o jurídica del usuario firmante interno se instale en la plataforma del adjudicatario, se indicarán en la oferta las medidas de seguridad que impiden el acceso, el uso y la obtención de copias de dicho certificado digital. IFEMA considerará aceptable la solución ofrecida en el caso que dichas medidas de seguridad sean adecuadas y no dejen lugar a dudas que se ha mitigado la amenaza del uso ilícito del certificado digital de persona física de un usuario firmante interno. Se consideran medidas adecuadas y suficientes, entre otras:

- Que no hubiese nunca copia del certificado digital en la plataforma del adjudicatario.
- En el caso de que haya copia del certificado en la plataforma del adjudicatario, que el uso de la clave privada esté protegido por su propio PIN o contraseña y sin almacenarlo junto con el certificado.

En el caso de que las medidas de seguridad propuestas sean diferentes de las dos anteriores sugeridas, el ofertante deberá, a requerimiento de IFEMA, completarlas o sustituirlas a su satisfacción.

3.1.5 Terceros firmantes

La plataforma ofrecida permitirá que los terceros puedan firmar con cualquiera de los siguientes tipos de firma electrónica, que deberán cumplir, en todo caso, los requisitos legalmente establecidos para su validez:

1. Con una firma electrónica avanzada basada en un certificado expedido por un prestador de servicios de certificación conforme a la Ley 59/2003, de firma electrónica (LFE).

En este caso, la aplicación ofrecida deberá ser capaz de realizar las comprobaciones necesarias para asegurar que la firma es correcta. En particular comprobará, al menos:

• Que el certificado procede de un prestador de servicios de certificación cuya información conste en la correspondiente dirección de internet de la Administración General del Estado a la que se refiere el artículo 30.2 LFE

• Que el propio certificado digital sea válido, que no esté revocado, que no haya expirado su período de validez.

El fallo de cualquiera de estas comprobaciones es un evento de seguridad del que IFEMA MADRID debe tener en seguida un dictamen del adjudicatario con todos los detalles para comprender si se trata de un fallo de operación o de un intento delictivo de fraude en el acto de la firma.

2. Con otro tipo de firma electrónica que pueda considerarse avanzada, de conformidad con la LFE que la define como la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control. En particular, ha de ser una firma electrónica con autenticación de doble factor, email y mensaje en el móvil.

Cualquiera que sea el tipo de firma electrónica utilizado, la plataforma debe garantizar que el contenido de los documentos a firmar no puede ser modificados en forma alguna una vez incorporados a la plataforma y hasta el momento en que se firman.

La plataforma propuesta deberá permitir la tramitación de la firma por un tercero de acuerdo con el procedimiento que se expone a continuación:

El tercero firmante recibirá un email de notificación que le indicará con claridad que se encuentra ante un envío de documentos para firmar procedentes de IFEMA MADRID y le permitirá acceder con cualquier dispositivo a los documentos cuya firma se solicita. El caso habitual es que sea un solo documento.

El tercero firmante podrá leer y examinar el contenido de los documentos cuantas veces necesite y desde el navegador moderno y dispositivo de su preferencia.

El email de notificación contendrá las instrucciones sencillas necesarias para que el tercero firmante pueda por sí mismo acceder al documento y proceder a su firma. También contendrá un medio de contacto con el servicio de ayuda del adjudicatario en caso de duda o dificultad. Dicho servicio le ofrecerá los consejos e indicaciones oportunas para resolver su duda y para acceder y firmar correctamente los documentos del envío.

En caso de error al proceder a la firma de un documento, la aplicación de firma ofrecerá al tercero firmante mensajes claros de la causa del error para que pueda resolverlo por sí mismo, sin perjuicio de ofrecerle también el medio de contacto con el servicio de ayuda.

El tercero firmante podrá optar por utilizar cualquiera de las dos formas de firma electrónica indicadas, la firma electrónica avanzada basada en un certificado expedido por un prestador de servicios de certificación o la firma electrónica avanzada no basada en un certificado sino en una autenticación de doble factor: email y contraseña de un solo uso OTP enviada al teléfono móvil del firmante. En esta última, se recogerá el trazo, su velocidad y, si el dispositivo lo permite, su presión e inclinación. Se procederá finalmente a firmar los documentos con el certificado digital válido proporcionado por el adjudicatario.

Podrá existir varios firmantes dentro de la misma empresa (firma mancomunada) o en varias empresas (en caso de UTE).

3.1.6 Usuarios interesados

Usuarios internos de IFEMA MADRID que pueden consultar el estado de los envíos a firma en los que hayan sido configurados como interesados. Podrán consultar detalles como la fecha del envío, los datos de los destinatarios, cuáles de los destinatarios han firmado y qué destinatarios tienen pendiente aún la firma de la documentación enviada.

3.1.7 Usuarios administradores

La aplicación ofertada deberá permitir a IFEMA realizar tareas de sistemas tales como, por ejemplo:

✓ Verificar la disponibilidad de las funcionalidades de la solución.

✓ El alta, la baja y la configuración de cuantos usuarios remitentes y usuarios firmantes internos sean necesarios.

✓ Bloqueo y desbloqueo de las cuentas de los tipos usuario remitente, firmante interno, usuarios administradores.

✓ Consulta de indicadores clave de la actividad de plataforma relevantes para el seguimiento del cumplimiento adecuado del presente contrato y consulta de los datos que necesita habitualmente un administrador de sistemas para elevar internamente a otras instancias el estado del servicio de firma digital certificada de IFEMA. Por ejemplo, datos de consumos, de tiempos de disponibilidad. Datos de uso tales como cantidad de documentos enviados a firma por período, cantidad de documentos efectivamente firmados por firmantes internos, por terceros firmantes, firmados conjuntamente, etc. Cantidad de documentos enviados por remitente o por API por período, etc. Cantidad de documentos rechazados. Consumos de espacio, de ancho de banda, etc.

Consulta de logs con información útil que contribuyan a la resolución de incidencias de cualquier tipo, en particular de incidencias relacionadas con en el uso del API.

✓ Reconfiguración de los parámetros de la interfaz API.

✓ Vinculación de grupos de seguridad del Directorio Activo de IFEMA MADRID a grupos de usuarios de la solución.

✓ Cualesquiera otras tareas de configuración de sistemas relacionadas con este servicio.

IFEMA deberá poder solicitar al proveedor realizar algunas de estas tareas de sistemas en horario laboral mediante un procedimiento ágil y sencillo, basado en el acceso a soporte por medio de una dirección de email y número de teléfono sin tarificación adicional. No se requiere una aplicación web de autoservicio para que los usuarios administradores puedan realizar por sí mismos alguna de las tareas de sistemas descritas. No obstante, en el caso que esté disponible tal aplicación en la oferta o lo estuviera durante la duración del contrato, IFEMA la utilizaría para realizar algunas de las tareas de sistemas en que recurrir a dicha aplicación de autoservicio resulte más sencillo, ágil y eficiente que el procedimiento basado en email y teléfono, a criterio de IFEMA. Sin perjuicio de la posibilidad de realizar siempre las tareas de sistemas por email y por teléfono.

A modo ilustrativo, en los últimos seis meses IFEMA sólo ha solicitado UNA actividad de administración de sistemas al proveedor actual.

3.1.8 Autenticación y autorización de usuarios internos

Tanto la autenticación como la autorización de los usuarios internos estará integrada con el Azure Active Directory de IFEMA MADRID. Los usuarios internos son los usuarios remitentes, usuarios firmantes internos, usuarios interesados y usuarios administradores.

3.1.9 APIS para integración con Salesforce, SAP y otras plataformas

La plataforma deberá contar con una API REST amplia y robusta que permita integrar de manera eficiente con los sistemas y procesos existentes en la organización. De esta forma, deberá permitir la automatización de firmas de documentos generados y gestionados por distintas plataformas como por ejemplo Salesforce, SAP, ServiceNow o cualquier otra que IFEMA MADRID determine. En general, la API deberá permitir exponer todas las operaciones que puedan realizarse desde la web de la plataforma o desde los dispositivos móviles en relación con lo solicitado en el presente pliego. En cuanto a seguridad, la API deberá cumplir con los estándares establecidos por IFEMA MADRID (mínimo exigido actualmente Oauth), garantizando únicamente los accesos legítimos de IFEMA MADRID e impidiendo los accesos ilícitos.

3.1.10 Otras funcionalidades y características

El adjudicatario debe adoptar medidas para que los emails que envía la solución no sean considerados como spam. A petición de IFEMA MADRID, el remitente de estos emails se cambiará por una dirección personalizada para IFEMA MADRID.

Las instrucciones para los terceros firmantes externos serán claras y suficientes para que puedan decidir correctamente a su conveniencia firmar con su propio certificado digital o por los demás métodos que ofrezca la plataforma.

4 Situación Actual

4.1 Volumetría de referencia)

a. 2000 envíos al año a firma
b. 1 grupo de usuarios, con Un solo usuario, el Vicepresidente, que hace algunos envíos en su propio nombre y que principalmente accede para buscar envíos pendientes de su propia firma y proceder a firmarlos o rechazarlos según proceda.
c. 1 grupo de remitente, con 2 usuarios que hacen envíos en nombre del Presidente y/o Vicepresidente. Es de prever que se alcancen hasta 15 remitentes que realizarán envíos en nombre de otros tantos firmantes internos, durante la vigencia del presente contrato.
d. 1 grupo de firmantes, con 1 usuario. Es de prever se alcancen hasta 15 firmantes, durante la vigencia del presente contrato.
e. 30 grupos de 200 usuarios en total interesados en el estado de los envíos que pueden consultarlo en función de su pertenencia a uno de los 30 grupos diferentes.

5 Documentación técnica a entregar en el sobre número 2

5.1 CRITERIOS DE ADMISIBILIDAD. CONTENIDO OBLIGATORIO QUE DEBEN INCLUIR LAS OFERTAS NO SUJETO A VALORACIÓN

Se deberá aportar la documentación técnica que se requiere en este apartado, para la admisión de su oferta técnica. En caso de no incluir algún apartado/contenido la oferta será excluida.

La documentación que debe presentar el ofertante en este sobre tendrá el objetivo concretar su propuesta para el servicio solicitado. Es decir, debe explicar como pretende acometer el servicio que requiere IFEMA MADRID explicando cada parte del mismo. Se tendrá en cuenta la claridad expositiva, la concreción y adecuación efectiva a los servicios solicitados.

Documento expositivo de la propuesta, de **extensión máxima no superior a 20 páginas** sin incluir la portada ni el índice, con tipo de letra de tamaño entre 10 y 12 (excepto títulos).

El ofertante deberá tener en cuenta que la documentación presentada en este apartado que exceda del número límite de páginas indicado, debiendo cumplir, además, tamaño de fuente, no será revisada en la parte que resulte excedida y deberá contener estrictamente los apartados indicados. En caso de no incluir algún apartado/contenido la oferta será excluida.

El contenido del documento es el siguiente:

1. Descripción de las Medidas de seguridad y procedimientos con que cuenta la solución para impedir el acceso no autorizado a los datos y certificados digitales de IFEMA y a la propia aplicación (De acuerdo a lo indicado en el PPT, apartado "3.1 Aplicación o portal web para el uso manual del servicio").
2. Descripción de las medidas de seguridad que permiten acceder, autenticar y autorizar a los usuarios de cualquier tipo.
3. Descripción y detalle de los aspectos de seguridad comentados en el PPT apartado "3.1.1 Seguridad".
4. Descripción y detalle de los aspectos de seguridad comentados en el PPT apartado "3.1.2 Conformidad jurídica de la firma".
5. Indicar expresamente que la solución ofertada cumple con el "Reglamento eIDAS UE nº 910/2014" (Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014).

6 Normativa y reglamentación técnica

Será de aplicación la normativa técnica vigente, así como la actual Ley de Prevención de Riesgos Laborales.

Todos los informes, estudios y documentos, así como los productos y subproductos elaborados por el proveedor como consecuencia de la ejecución del contrato serán propiedad de IFEMA MADRID, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el proveedor autor de los trabajos.

El proveedor renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los informes, estudios y documentos elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de IFEMA MADRID.

Específicamente todos los derechos de explotación y titularidad de los servicios y productos elaborados durante la ejecución del contrato corresponden únicamente a IFEMA MADRID y, particularmente, a IFEMA MADRID.

El proveedor no adquiere ningún derecho sobre el hardware (material), software (aplicativos) e infraestructuras propiedad de IFEMA MADRID, salvo el de acceso indispensable al mismo para el cumplimiento de las tareas que se desprenden de las obligaciones dimanadas del contrato.

La información almacenada en las aplicaciones, así como la utilizada para la mecanización de incidencias y soluciones propias del servicio objeto del contrato, quedarán bajo propiedad y uso de IFEMA MADRID.

El proveedor no podrá utilizar la información obtenida en la actividad desarrollada como consecuencia de la ejecución del contrato (en particular las bases de datos de incidencias y soluciones), no pudiendo transmitir dicho conocimiento, sin el consentimiento expreso y escrito de IFEMA MADRID. Asimismo, deberá contar con consentimiento expreso y escrito para realizar modificaciones de hardware, aplicativos o infraestructuras.

7 Personas de contacto

Les recordamos que, para cualquier consulta o aclaración de carácter administrativo, técnico o económico sobre este expediente, deben proceder conforme a lo previsto en los apartados 5.- CONSULTAS y 6.- PRESENTACIÓN DE LAS PROPOSICIONES. NOTIFICACIONES Y COMUNICACIONES- del cuadro de características-.

Igualmente, les recordamos que, para aquellas cuestiones que puedan afectar a la operativa / funcionalidad del portal de licitación electrónica de IFEMA MADRID, existe un área de soporte y consulta a licitadores dentro de la web:

1. Preguntas frecuentes: https://licitaciones2.IFEMA MADRID.es/html/preguntas-frecuentes
2. Manual de uso de la plataforma: https://licitaciones2.IFEMA MADRID.es/resources/Guia_Licitadores.pdf
3. Soporte y contacto con plataforma: https://pixelware.com/servicios-soporte-licitadores/

El contacto telefónico con el encargado de la gestión del expediente perteneciente a la Dirección de Compras y Logística de IFEMA MADRID, que se cita a continuación, se limitará a cuestiones meramente informativas no vinculantes sobre el propio proceso de licitación:

Técnico de Compras: 676.132.048.