

**PLIEGO DE PRESCRIPCIONES TECNICAS QUE HA DE REGIR LA CONTRATACIÓN, POR PROCEDIMIENTO ABIERTO SIMPLIFICADO SUMARIO, DEL SERVICIO DE SISTEMA DE UN SOFTWARE ITSM (LOTE 1), SERVICIO DE FIRMA EXCLAIMER (LOTE 2) Y SERVICIO DE CERTIFICADOS SSL (LOTE 3) PARA MUTUA MONTAÑESA, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 7.**

---

<b>1. INTRODUCCIÓN</b> .....	<b>2</b>
<b>2. LOTE 1: SERVICIOS Y LICENCIAS SERVICE DESK PLUS</b> .....	<b>3</b>
2.1. OBJETO .....	3
2.2. ALCANCE .....	3
2.3. REQUERIMIENTOS TÉCNICOS .....	4
2.3.1. <i>Situación actual</i> .....	4
2.3.2. <i>Nuevo sistema service desk plus</i> .....	4
<b>3. LOTE 2: SERVICIO EXCLAIMER</b> .....	<b>11</b>
3.1. ALCANCE .....	11
<b>4. LOTE 3: CERTIFICADOS SSL</b> .....	<b>12</b>
4.1. OBJETO .....	12
4.2. ALCANCE .....	12
4.3. REQUISITOS TÉCNICOS.....	12
4.3.1. <i>Aspectos generales</i> .....	12
4.3.2. <i>Entidad emisora</i> .....	13



## **1. INTRODUCCIÓN**

---

Mutua Montañesa requiere para su operativa el suministro servicios y licencias para los siguientes productos:

- Service Desk Manager Plus y servicios implantación
- Servicio Exclaimer
- Certificados SSL

La presente licitación se estructurará en lotes uno para cada uno de los productos/servicios requeridos debido a que su naturaleza es diferente, y puede ejecutarse de forma independiente, ya que no pone en riesgo la correcta ejecución de cada servicio de forma separada.

## **2. LOTE 1: SERVICIOS Y LICENCIAS SERVICE DESK PLUS**

---

Desde el área de Tecnología y Sistemas de Mutua Montañesa se coordina el SGSI (Sistema de Gestión de la Información de Mutua Montañesa). Este sistema de gestión está alineado con el Esquema Nacional de Seguridad como marco de referencia para la gestión de los servicios de TI de Mutua Montañesa.

Los procesos de gestión de incidencias, la gestión de incidentes de seguridad, configuraciones, la gestión de problemas o cambios, la gestión de la continuidad, así como otros procesos de control de las medidas de seguridad implantadas, son prioritarios para velar por el cumplimiento de este modelo de gestión.

Para el control y seguimiento de estos procesos actualmente Mutua Montañesa está utilizando una herramienta de Help Desk denominada Service Desk Plus, en su modalidad Standard, con un licenciamiento para 15 usuarios técnicos.

### **2.1. OBJETO**

---

El objeto del presente procedimiento es establecer las condiciones técnicas que regirán la contratación del suministro de las licencias de la herramienta ITSM así como los servicios profesionales para su instalación y configuración.

De manera general se solicita:

- Suministro licencias producto Service Desk Plus Enterprise
- Servicios Profesionales configuración producto.
- Instalación y Migración incidencias Helpdesk sistema actual.
- Soporte

Se pretende con esta contratación y renovación del sistema de Service Desk Plus, orientar tanto los procesos como las herramientas disponibles hacia una gestión más avanzada de los servicios TI atendiendo a las mejores prácticas en esta materia. Se pretende implantar una solución que permita gestionar una CMDB y los procesos de gestión TI habituales.

En este sentido, se debe tomar como referencia con relación al modelo de gestión, el estándar ISO 27001 y el Esquema Nacional de Seguridad.

### **2.2. ALCANCE**

---

Se estima el suministro de las siguientes licencias:

- ServiceDesk Plus Multi-Language Enterprise - Annual Subscription fee for 10 Technicians (500 nodes).

Se requiere los servicios profesionales para la instalación en un entorno on premise de la versión Service Desk Plus Enterprise más reciente.

Se estima los servicios profesionales para la configuración de los siguientes grupos de funcionalidades:

- Service Desk: funciones para soportar la operativa de apertura de "tickets" (incidencias, peticiones, cambios) entre usuarios y soporte.
- CMDB: funciones de gestión del inventario de servicios TI y sus componentes, relaciones, atributos, etc.
- Funciones necesarias para soportar los principales procesos de gestión TI sobre los servicios IT definidos y sus componentes, según describen los estándares/modelos de referencia indicados.

- Funciones de gestión del conocimiento relativo a la resolución de problemas más típicos que ofrezcan posteriormente un sistema de autoayuda al usuario.

Entendemos que para la ejecución de estos servicios profesionales como mínimo el adjudicatario deberá dedicar 20 jornadas de trabajo.

## **2.3. REQUERIMIENTOS TÉCNICOS**

---

### **2.3.1. SITUACIÓN ACTUAL**

---

Mutua Montañesa dispone del sistema Service Desk Plus edición standard en su versión 9.0, como herramienta de ticketing para la gestión del soporte correctivo de los procesos de IT, muy vinculados a la gestión de incidencias.

Actualmente, nuestro sistema tiene una configuración del módulo HelpDesk, Usuarios, donde fundamentalmente está parametrizado la gestión de incidentes adaptado a los flujos de Mutua Montañesa con la incorporación de campos específicos y una gestión de SLA. También tenemos configurado la autenticación con el Active Directory.

Asimismo, en este entorno disponemos de un histórico de incidencias y solicitudes que necesitamos migrar al nuevo entorno. En este sentido, entendemos que es suficiente con migrar únicamente las solicitudes abiertas, y tener un backup a modo de fichero con toda la información de las incidencias cerradas, en caso de que sea requerido la revisión del histórico.

### **2.3.2. NUEVO SISTEMA SERVICE DESK PLUS**

---

#### **2.3.2.1. Aspectos Generales**

La plataforma debe estar alineada con las mejores prácticas del Esquema Nacional de Seguridad, y debe ser una herramienta capaz de gestionar, de modo general:

- La definición de los servicios y sus componentes, recogiendo sus relaciones y el significado de las mismas, de modo que sea posible registrar y posteriormente, generar informes relativos a las diferentes peticiones, cambios, incidencias, etc. en los distintos elementos y sus afecciones a los servicios o a otros elementos.
- Recoger los distintos roles asociados a los servicios y sus componentes: responsables, técnicos al cargo del mantenimiento, etc. de modo que sea posible automatizar asignaciones de ciertos tipos de tareas a los roles designados.
- Gestionar los niveles de servicio requeridos para los distintos elementos y conectar la herramienta con sistemas que permitan su seguimiento.
- Gestionar las peticiones, cambios, incidencias, problemas, etc. relativos a los servicios o sus componentes.
- Generar informes sobre todos estos aspectos

En cualquiera de los ámbitos de la solución podrán definirse campos adicionales, que serán dinámicos en función del registro (ítem CMDB, registro de Service Desk o inventario). La

configuración de estos campos deberá poder realizarse desde el interface web, sin necesidad de programación. Podrá adjuntarse cualquier fichero de información adicional.

El sistema contará con métodos de generación de métricas o indicadores configurables, que permita realizar un análisis de situación actual y pasada, así como análisis de tendencias. Las métricas deberán ser parametrizables, y accesibles desde el interface web.

El sistema contará con un conjunto de reportes por defecto, ofreciendo facilidades para adaptar dichos reportes, modificándolos según las necesidades corporativas, y añadiendo nuevos reportes específicos. Los reportes deberán admitir visualización on-line, así como exportación al menos a formatos abiertos, PDF, texto u hojas de cálculo que permitan su tratamiento externo.

Las diferentes pantallas (listados, informes,..) admitirán exportación a formatos abiertos (csv, pdf, imágenes,..) para su posterior utilización. En su generación admitirán filtrado por los campos comunes (fechas, categoría del registro, tipo del registro, cliente, prioridad,...).

El sistema dispondrá de distintos niveles de acceso configurables por perfiles, permitiendo controlar qué perfiles de usuarios o técnicos pueden visualizar los diferentes ítems de información o realizar ciertas acciones.

Se valorará que el sistema cuente con la opción de registrar la actividad de accesos (quién y cuándo se accede a cada registro) así como cambios en los campos de los registros.

### **2.3.2.1. Arquitectura de la solución**

La solución se instalará en un entorno on premise de Mutua Montañesa, que se suministrará con el sistema operativo instalado, y la empresa adjudicataria será la encargada de realizar la instalación de la solución. Es requerido que, en la oferta, el licitador nos indique las características mínimas para la implantación de la solución.

Mutua Montañesa facilitará una maquina virtual Windows Server 2022 o inferior, instalada y configurada con todos los parches de S.O. actualizados y la solución de EDR existente en la organización. El resto de las configuraciones, productos, licencias, etc. deberán ser aportados por el proveedor y acordados con Mutua Montañesa en el arranque del proyecto.

La plataforma debe contar con una interface 100% web, tanto para la administración del sistema como para su uso, sin necesidad de instalar software adicional en los equipos, salvo el destinado a la recolección de datos de inventario para equipos cliente windows. El portal web de los usuarios deberá ser compatible con los principales navegadores web (IE, Firefox, Chrome,..). La validación de usuarios y la gestión de los mismos deberán estar integrados con el DA de la organización. El interfaz web ofrecerá:

1. Portal de usuarios.
2. Portal de técnicos encargados de la resolución de las peticiones o incidencias.
3. Portal de gestores con cuadro de mando y funciones de generación de informes relativos al servicio, elementos o procesos de los que sean responsables.
4. Portal de administradores de la herramienta. El portal de usuarios podrá ser totalmente configurable, con la opción de añadir los logotipos corporativos, mensajes de bienvenida y alertas/avisos. Desde el portal de usuario podrán publicarse distintos links configurables, para acceder a otros sistemas web corporativos, o incluso a enlaces externos.

### **2.3.2.1. Service Desk (Helpdesk)**

El software de Service Desk **gestionará las incidencias, peticiones, problemas, cambios y entregas relativas a elementos de inventario y/o CMDB de forma totalmente integrada**. Este punto de integración es muy importante, y una mejora sustancial para tener recogido el ciclo de vida de una incidencia y su afectación al inventario.

El flujo deberá poder parametrizarse para adaptarse a las necesidades concretas de la organización, y deberá cubrir todo el ciclo de vida, desde el registro inicial, hasta el cierre final. Las incidencias o peticiones podrán relacionarse con otras incidencias, peticiones, problemas, RFCs o tópicos de conocimiento. Cualquiera de los módulos de gestión de incidencias, peticiones, problemas, cambios o entregas deberá estar integrado y tener acceso directo a cualquiera de los CIs almacenados en el módulo de gestión de la configuración (CMDDB). Las relaciones deberán ser bidireccionales.

La herramienta incorporará métodos para clasificar las incidencias en distintos tipos y categorías. Se podrán configurar las categorías de incidencias necesarias, enlazarlas jerárquicamente en los niveles necesarios y asociar categorías o tipos a tipos de CIs.

Las incidencias y peticiones podrán priorizarse en base al impacto y urgencia de las mismas. Se valorará la existencia de algún mecanismo que permita establecer las reglas de prioridad lo más amplio posible utilizando los campos disponibles (tipos, categorías, elementos afectados, intervalos de tiempo transcurridos, campos propios que indiquen prioridades o impactos,..).

#### **Flujos de autorización**

En función de la clasificación de la incidencia o petición, el sistema será capaz de gestionar un flujo de autorizaciones previo a la atención del registro. Los perfiles autorizadores no serán necesariamente personal técnico de soporte.

#### **Sistemas Autoayuda**

Además, la aplicación gestionará las comunicaciones con el usuario a través de un portal web para que cualquier usuario de la organización pueda conocer el estado de sus incidencias dadas de alta. El portal de los usuarios contará con opciones de autoayuda, permitiendo a los usuarios la consulta de FAQs o tópicos de conocimiento previamente publicados por el personal de soporte, y que permita la resolución rápida de incidencias o peticiones sin necesidad de contactar con el personal de soporte.

Contará con opciones de integración de chat para que los usuarios contacten con los técnicos de soporte. El portal podrá ser configurable, permitiendo ordenar, acumular, filtrar las pantallas de datos en función de los campos de los registros (categorías, tipos, prioridades,... o bien los campos personalizados definidos) sin necesidad de programación. El sistema permitirá configurar plantillas. Debe poder definirse que perfil de usuarios pueden utilizar ciertas plantillas o haber modelos diferentes para usuarios o técnicos.

#### **Alta incidencias o peticiones automáticas**

El sistema admitirá el alta de nuevas incidencias o peticiones realizadas directamente por los técnicos de soporte en su nombre de los usuarios. Debe poder configurarse qué perfiles de técnicos pueden dar de alta dichos registros. El sistema admitirá el alta de nuevas incidencias o peticiones mediante el envío de correos electrónicos a cuentas de e-mail (POP3, IMAP). Deberán poderse configurar distintas cuentas asociadas a la creación de distintos tipos o categorías o reglas para la creación en función de los campos que incluya el

mensaje. También admitirá el alta de nuevas incidencias o peticiones directamente a partir de cambios detectados en la infraestructura. El sistema registrará el origen de la notificación de la incidencia o petición, admitiendo distinguir al menos la recepción de incidencias desde el portal web de usuarios (registro de origen automático), origen en correos electrónicos, origen mediante llamada telefónica o cualquier otro origen configurable. Los cambios de estado en la incidencia o petición podrán ser notificados de manera automática por la herramienta vía correo electrónico, dirigido tanto a los usuarios finales como a los técnicos de soporte. Deben poder manejarse distintos mensajes para los usuarios o internos entre los técnicos de soporte. El sistema deberá contabilizar de manera automática el tiempo invertido en cada etapa del ciclo de vida, así como guardar el histórico de dicho ciclo de vida.

### **Notificaciones automáticas, escalado y SLAs**

El sistema permitirá notificar a los técnicos cuando existan registros en su bandeja de entrada que hayan excedido un umbral de tiempo (configurable) sin haber sido atendidos. Permitirá configurar reglas para el escalado jerárquico de incidencias / peticiones que superen un umbral configurable del SLA asignado así como enviar notificaciones automáticas como aviso.

En función de la clasificación de la incidencia o petición, el sistema será capaz de calcular automáticamente SLAs basados en tiempos de atención, escalados o resolución. Deberán tenerse en cuenta diferentes calendarios y horarios de servicio en estos cálculos. Cualquiera de las acciones documentadas por los técnicos de soporte podrá ser marcada para ser visible al usuario final o privada, para uso interno de los técnicos de soporte. El cierre podrá realizarse por el propio usuario una vez validado. En el momento del cierre de las incidencias o peticiones, el usuario podrá contestar una encuesta de valoración (global y/o vinculada a tipos concretos de incidencias/peticiones) totalmente configurable por parte de los técnicos de soporte. Los registros podrán ser confirmados y cerrados por el usuario directamente desde el interface web, momento en el que el sistema podrá ser configurado para realizar una encuesta de satisfacción.

Ante la circunstancia de que el usuario final no cierre la incidencia o petición en un tiempo razonable, el sistema deberá ofrecer mecanismos configurables para su cierre automático. En el momento del cierre de la incidencia o petición, el sistema deberá calcular de manera automática al menos:

- tiempo real de resolución
- tiempo real de cierre
- horas invertidas en las acciones realizadas
- grado de cumplimiento del SLA establecido

### **2.3.2.1. C MDB**

El módulo de gestión de configuración (C MDB) deberá estar integrado con el módulo de inventario permitiendo el alta automática de CIs tecnológicos detectados por el inventario y con los módulos de gestión de incidencias, problemas, peticiones, cambios.

El nivel de automatización para la gestión de CIs a partir del inventario, deberá ser configurable, permitiendo indicar qué tipos de activos deben ser automáticamente catalogados como CIs vinculados y dispondrá de opción de bloquear la modificación de CIs si no existen RFCs vinculadas. Se deberán poder definir reglas para configurar qué tipos de CIs se pueden dar de alta, tipos de relaciones entre tipos de CIs.

Las relaciones entre CIs asociados a activos del inventario podrán gestionarse de manera automática. Se admitirá la creación de relaciones manuales. Se valorará que contemplen un valor que refleje el peso, importancia o impacto de la relación.

Se deberá poder definir el ciclo de vida para cada tipo de CI y los estados compatibles con cada tipo.

Se deberán poder configurar distintos niveles de profundidad (detalle de información) en función del tipo de CI, y campos de información diferenciados en función del tipo de CI seleccionado. El conjunto de tipos de datos para los campos de información deberá ser amplio para permitir los usos más comunes (textos, listas desplegables, opciones,...).

Las relaciones, bien sean automáticas o manuales, deberán visualizarse en modo de listados y en representación gráfica. El modo gráfico de relaciones permitirá moverse entre los distintos CIs, mostrando el grado de importancia o impacto de cada una de las relaciones y su tipo y soportará búsquedas filtradas por tipos de CIs, de relaciones, profundidad a partir de un CI inicial.

El modo gráfico deberá visualizar de manera rápida aquellos CIs en los que existan cambios sobre la situación monitorizada, en situación de fallo, con incidencias,..

El sistema admitirá modificar el estado (disponible/no disponible) de elementos de la CMDB desde herramientas externas que miden la disponibilidad de la infraestructura.

Se valorará que la herramienta incorpore herramientas para la gestión de la seguridad de la información o los servicios alineada con los requisitos del Esquema Nacional de Seguridad:

- Gestión del valor de los ítems de información y servicios.
- Propagación de valores hacia elementos inferiores a través de las relaciones entre CIs.
- Análisis de riesgos de los sistemas de información definidos o enlace a herramientas que lo permitan

## **2.4. SERVICIOS PROFESIONALES**

---

La contratación del servicio llevará asociadas una serie de tareas para el desarrollo del proyecto que estimamos que deberá realizarse en 3 meses de duración desde la adjudicación del servicio.

En primer término, se requiere la instalación del nuevo entorno y migración de las incidencias abierta del actual sistema de Mutua Montañesa. En este punto será requerida la configuración inicial del producto para poder poner en funcionamiento el módulo de help desk (gestión incidencias, problemas y gestión de cambios), así como las funcionalidades básicas del CMDB para dar soporte a la gestión de incidencias y éstas puedan estar relacionadas.

Asimismo, se requiere la revisión en más profundidad de los procesos IT relacionados con el control de medidas de seguridad del ENS y su aplicación a las medidas de control implantadas en Mutua Montañesa.

Para la configuración el entorno, a continuación, enumeramos el volumen de elementos de configuración (CIs): hardware, aplicaciones software, servicios, y personas que forman parte del sistema TI.

Además, identificaremos los atributos principales de cada elemento de configuración que entendemos mínimos para su puesta en marcha.

A modo de referencia actualmente gestionamos en nuestro inventario la siguiente cantidad de dispositivos. En verde se marca los dispositivos que entendemos como Nodos en el cómputo de licencias.

Resumen de elementos inventario actual.

<b>Etiquetas de fila</b>	<b>Activo</b>	<b>Srv. Tecnico</b>	<b>STOCK</b>	<b>Total general</b>	
Armario		1	2	3	
Cabina de Discos		5	1	6	
Cinta		1		1	
Compartidor		5	13	18	
Controlador			1	1	
Disco Duro		4	15	19	
Firewall		3	2	5	
Gestor Correo			2	2	
Grabadora DVD		4		4	
Hub		1	1	2	
Impresora		1		1	
Impresora Multifunción B/N		55	1	56	
Impresora Multifunción Color		36		36	
Lector Cód. Barras		1		1	
<b>PC</b>		<b>27</b>	<b>2</b>	<b>32</b>	
<b>Portátil</b>		<b>59</b>	<b>9</b>	<b>68</b>	
Maquina Virtual		80		80	
Proyector Informático		2	4	6	
Router		3	30	33	
SAI		1		1	
Scanner		1	1	2	
Semáforo		1		1	
Serv. Dedic.		13	3	16	
Sistema Sonido		25	1	26	
Switch		51	19	70	
Tablet		53	2	10	65
TFT		293	4	82	379
<b>ThinClient</b>		<b>227</b>	<b>18</b>	<b>137</b>	<b>382</b>
Transceiver		3	7	10	
Unidad de Cintas		1	6	7	
WebCam		35	2	37	
Lector Tarjetas			1	1	
PDU		6		6	
Proxy			1	1	
Antena Wifi		10		10	
Monitor		3		3	
TV		28		28	
Telefono Movil		15	15	30	



**Mutua  
Montañesa**  
Muy fácil

**Expediente nº 2022-002-022**

### **3. LOTE 2: SERVICIO EXCLAIMER**

---

Mutua Montañesa posee una infraestructura de correo electrónico basado en Microsoft Exchange 2007, sobre el que hay implementado un sistema de firma al pie de correos electrónicos Exclaimer Signature Manager Exchange.

Dentro del plan de contratación de Mutua Montañesa para este 2022, está prevista la implantación de un nuevo sistema de correo basado en Office 365 por lo que el uso de este sistema de firma onpremise dejara de tener efecto. Sin embargo, hasta que dicha actualización se produzca, algo que en ningún caso será más tarde de un año, es necesario seguir manteniendo el actual sistema de firma por lo que se requiere la contratación del mantenimiento del sistema de firma actual Exclaimer Signature Manager Exchange para 500 buzones durante un año.

#### **3.1. ALCANCE**

---

Se estima el suministro del producto Exclaimer Signature Manager Exchange para 500 buzones por 12 meses de servicio.

## **4. LOTE 3: CERTIFICADOS SSL**

---

Mutua Montañesa necesita contar con un servicio de suministro de certificados web, que se utilizan para establecer una conexión segura a los sitios web de la organización.

Los certificados SSL son un elemento imprescindible para garantizar la seguridad en el intercambio de información entre los sitios Web, siendo el medio que permite el cifrado de las comunicaciones entre ambos extremos, para garantizarse su privacidad e integridad.

En la actualidad es necesario disponer de certificados web. Las páginas que no disponen de un certificado web se muestran como "no seguras" en los navegadores principales, como pueden ser Chrome o Firefox.

### **4.1. OBJETO**

---

El objeto del presente procedimiento es establecer las condiciones técnicas que regirán la contratación de suministro de certificados SSL para comunicaciones.

En este pliego técnico se recogen los requisitos mínimos tanto de la entrega inicial como de los pedidos posteriores, bajo demanda en función de las necesidades.

De manera general se solicita:

- Suministro de certificados web.
- Portal de Gestión del Servicio.
- Contacto telefónico y/o por correo electrónico 24x7 con un asesor técnico personalizado.

### **4.2. ALCANCE**

---

Se estima el suministro para 3 años de los certificados de la siguiente tipología y cantidad:

- 1 certificado Wildcard OV.
- 1 Certificado QWAC.

### **4.3. REQUISITOS TÉCNICOS**

---

#### **4.3.1. ASPECTOS GENERALES**

---

Todos los requisitos enumerados son de cumplimiento obligatorio. Las ofertas que ofrezcan características que no se ajusten a estos requisitos no serán tomadas en consideración en el presente procedimiento de licitación.

Se debe disponer de un panel de gestión web de la entidad emisora en el que visualizar las unidades de certificado disponibles, así como descargar los certificados emitidos, CSR y certificados de CA.

El servicio debe permitir la validación/aprobación de dominios sobre los que se solicitarán los certificados necesarios. Esta prevalidación debe permitir la emisión más ágil, o incluso instantánea, de los certificados de los dominios preaprobados.

El servicio debe disponer de un asesor técnico personalizado, con contacto telefónico y/o por correo electrónico en español, así como disponer de soporte técnico 24x7.

Debe ser posible o bien solicitar al asesor la emisión de los certificados, enviando el correspondiente CSR o poder hacer la gestión directamente a través de la web de la entidad emisora. La emisión de certificados deberá ser automática o semiautomática en el caso de certificados de dominios previamente validados/aprobados.

Los certificados tendrán una duración mínima de 1 año, y se podrán renovar anualmente. En el caso de renovaciones, el año deberá ser adicional y empezar a contar a partir de la fecha de vencimiento del certificado en cuestión.

A la caducidad de un subdominio QWAC (ej:xxxxx.mutuamontanesa.es) se podrá emitir un nuevo certificado QWAC de iguales características pero para otro subdominio o SAN (Ej: yyyyy.mutuamontanesa.es) específico sin coste adicional

#### **4.3.2. ENTIDAD EMISORA**

---

Tanto si la oferta es presentada por la entidad emisora, como si es presentada a través de un partner, reseller o similar, todos los certificados deben ser de la misma entidad emisora de certificados, o de la misma marca.

Se requiere que la entidad emisora de certificados pueda emitir certificados del tipo QWAC (Qualified Website Authentication Certificate), en conformidad con el reglamento europeo eIDAS, por lo que será una información que deberá aportarse antes de la adjudicación.

El licitador debe indicar en su oferta la entidad emisora o marca que propone para los certificados, que se comprobará que se encuentra en alguno de los siguientes:

- Listado de QTSPs (Qualified Trust Service Providers) de España (<https://webgate.ec.europa.eu/tl-browser/#/tl/ES> // <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/ES>) para el servicio **QWAC - Qualified certificate for website authentication.**
- Relación de prestadores de servicios electrónicos de confianza cualificados (<https://sedeaplicaciones.minetur.gob.es/Prestadores/>), en el apartado Servicios electrónicos de confianza cualificados  Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web.

Se deberá poder preaprobar la validación del dominio mutuamontanesa.es de cara a agilizar la posterior emisión y renovación de certificados bajo ese nombre de dominio y los subdominios que de él se requiera

Adicionalmente la entidad emisora deberá cumplir con las siguientes características/servicios:

- Notificación de expiración.
- Certificados con cumplimiento X.509.
- Reediciones ilimitadas gratuitas, que se podrán realizar con o sin renovación de las claves.
- Certificados con número ilimitado de instalaciones/servidores.
- Certificados web compatibles con navegadores Internet Explorer, Firefox y Chrome sin requerir la instalación de certificados raíz adicionales.
- Portal de Gestión del Servicio directo de la Entidad Emisora, no se admitirá la gestión a través de un portal intermedio del partner.
  - El portal de gestión del servicio debe ser proporcionado dentro del portal de gestión de la entidad emisora, o de la empresa perteneciente a la marca de la entidad emisora, con las máximas medidas de seguridad.

- Se valorará que sea posible disponer de varios usuarios gestores.
- Soporte técnico, telefónico y/o por correo electrónico, 24x7.
- Asesor técnico personalizado en español que podrá formar parte de la organización de la entidad emisora o del reseller/partner que se presente a la licitación

#### **4.3.2.1. Características específicas de certificados Wildcard**

El certificado Wildcard ofertado deberá cumplir las siguientes características mínimas

- Certificados con validación de organización (OV), en los que se verifica la identidad de organización.
- Cifrado de 256 bits.
- Algoritmo SHA-2 de clave pública RSA (al menos, compatible con funciones hash: 256)
- Criptografía de clave pública ECC (al menos, compatible con funciones hash: 256)
- Compatible con cifrado de clave pública de 2048 bits o superior.
- Asegurar un dominio y todos sus subdominios de primer nivel. (mutuamontanesa.es y \*.mutuamontanesa.es)

#### **4.3.2.2. Características específicas de certificados QWAC**

El certificado Wildcard ofertado deberá cumplir las siguientes características mínimas

- Certificados cualificados (QWAC), que cumplen con el Reglamento eIDAS.
- Cifrado de 256 bits.
- Algoritmo SHA-2 de clave pública RSA (al menos, compatible con funciones hash: 256)
- Compatible con cifrado de clave pública de 2048 bits o superior.
- Posibilidad de cambiar/sustituir los CN y SAN de los certificados QWAC sin cargo