PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE REGIRÁ LA ADJUDICACIÓN MEDIANTE PROCEDIMIENTO ABIERTO SIMPLIFICADO LA CONTRATACIÓN DEL SERVICIO DE MANTENIMIENTO PLATAFORMA GESTIÓN CLAVES CENTRALIZADAS Y FIRMA DE DOCUMENTOS PARA MUTUA MONTAÑESA.

Mutua Montañesa
Mmuy fácil

Índice

1. INTRODUCCIÓN

Mutua Montañesa posee una solución de centralización de certificados, firma digital y biométrica aportada por la empresa Ivnosys que da servicio a distintos procesos de la organización. El presente pliego recoge la necesidad de mantenimiento y evolución de dicha solución

1.1. OBJETIVOS DEL PROYECTO

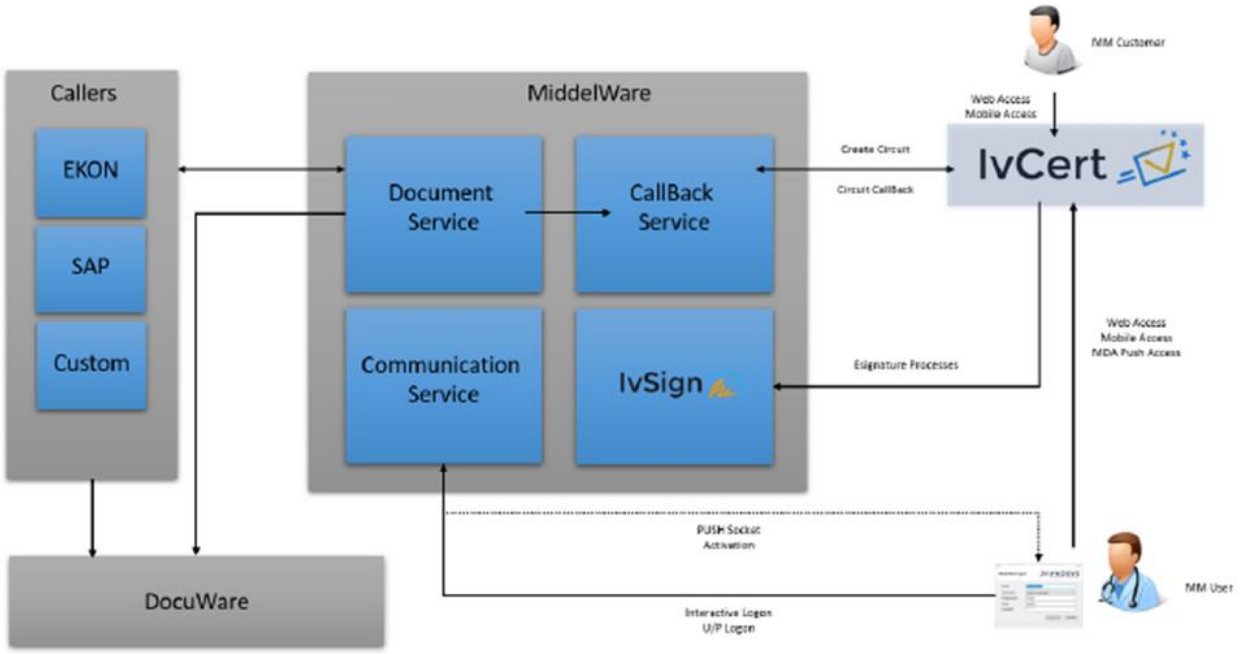
Servicio de mantenimiento de las licencias y desarrollos que dan cobertura funcional al sistema de firma y certificados digitales de mutua montañesa.

1.2. ALCANCE DEL PROYECTO

Contratación de un servicio de mantenimiento de los elementos recogidos en el presente documento.

2. SITUACIÓN ACTUAL

Mutua Montañesa, posee un sistema de centralización de certificados, firma digital y biométrica basada en la integración mediante un middleware de desarrollo a medida de que integra las diferentes herramientas estándar del fabricante de SW SignaturIT GROUP, como son IvCert e IvSign con los elementos corporativos de Mutua Montañesa. El Siguiente esquema recoge la estructura general de la solución:



2.1. CENTRALIZACIÓN DE CERTIFICADOS

Mutua Montañesa posee un sistema de Control de Certificados Centralizado (Central Key Control, en adelante CKC), sobre el que pivotan las diferentes soluciones de firma existentes en la organización en el que se almacenan la totalidad de los certificados que emplean los usuarios de Mutua Montañesa tanto a nivel de firma como de autenticación ante las diferentes entidades con las que interactuamos.

Mutua Montañesa tiene este CKC conectado con la entidad de emisión de certificados de Camerfirma, de la que somos RA (Agentes de Registro), lo que permite mejor eficiencia a nuestra organización, ya que no se hace necesaria el traslado de sus empleados a oficinas autorizadas del emisor de certificados para la validación y obtención de los certificados, sino que son emitidos autónomamente por nuestro departamento de RRHH existiendo un componente de integración entre Camerfirma y el sistema CKC que permite la recepción automática e integrada con nuestro directorio activo de los certificados emitidos.

En la actualidad existen:

- 270 certificados de Persona Física y pertenencia a empresa activos con una validez de 2 años
- 1 sello de entidad
- 12 certificados de representación de entidad Jurídica
- 1 certificado de encriptación.

2.2. FIRMA DIGITAL

Mutua montañesa a través de un middleware diseñado específicamente para nuestras necesidades tiene integrado mediante APIRest con sus sistemas de backend y con las soluciones de IvSign e IvCert una solución de firma digital que comprende la firma mediante certificado de los empleados de mutua y la firma biométrica (Tablet/Movil) por parte de pacientes de la entidad.

Dicho middelware contiene la lógica de los flujos de firma a disparar, los catálogos documentales, y aspectos relativos al comportamiento de los documentos con funciones como:

- Número de firmas requerida y tipo de las mismas (Empleado, paciente, ambos)
- Personalización de la marca de firma por tipo de documento.
- Ubicación del grafo de firma
    - Por Coordenadas
    - Por patrón de texto (ancla)
    - Múltiples marcas
    - Numero de paginas a incluir el grafo o datos de firma
- CSV: Generación e impresión de un código CSV a cada documento generado cuyo tipo tenga activada la función. Permite la consulta de documentos a partir de dicho código CSV para la validación electrónica de originales.
- Imprimir al finalizar
- Callbacks a transaccionales para actualizar estado de firma
- ….

En la actualidad tenemos implementados diversos tipos de firma: biométrica, electrónica con certificado digital centralizado, firma OTP avanzada. La plataforma dispone de múltiples mecanismos adicionales que Mutua Montañesa podrá ir incluyendo en su catálogo de servicios paulatinamente.

La plataforma también esta dotada de un portafirmas y de un agente de escritorio que están diseñados para agilizar los procesos de firma y facilitar al usuario la gestión de los documentos que puede tener pendientes.

Así mismo se ha desarrollo un entorno web de administración de la solución que permite la monitorización de todas las actividades de firma llavadas a cabo a través del middelware, gestión de callbacks, cambios de estado de documentos,…

En el Anexo I se describe algo más en profundidad los circuitos básicos de firma.

2.2.1. FIRMA ELECTRÓNICA

Se emplea este tipo de firma para su uso por parte de los profesionales de la organización sobre todos los documentos oficiales emitidos por nuestros sistemas de backend (Sap y Ekon actualmente)

Sobre el soporte de IvCert, la plataforma permite la firma de documentos mediante certificado digital alojado en el almacén centralizado identificando el usuario Windows validado y dándole acceso exclusivo para la firma de documentos a sus certificados asignados, ya sea por usuario a por reglas de pertenencia y visibilidad a grupos.

Así mismo el sistema permite la derivación de firma entre profesionales y el acceso a portafirmas para la gestión de documentos pendientes de firmar. Dichos documentos también cuentan con un sello de tiempo que la propia plataforma gestiona de manera automática.

El volumen de firma aproximado de los últimos años de uso de la herramienta es:

ARCHIVADOR	2021	2022	2023	2024	Total general
HHCC	90680	118452	106768	75827	391727
SAPREST	53546	62706	48649	33901	198802
Total general	**144226**	**181158**	**155417**	**109728**	**590529**

2.2.2. FIRMA BIOMÉTRICA

Se emplea para la firma de documentos por parte de pacientes. En la actualidad esta firma esta implantada para documentos asistenciales (consentimientos informados, declaraciones de datos de accidente, confirmación de citas, …).

La firma biométrica se realiza mediante tablets microsoft Surface con windows 11 dotadas de sistemas capacitivos y pantallas superiores a 8" capaces de almacenar datos biométricos tales como la presión velocidad y orientación del trazo. Dichos datos son cifrados con un certificado cuya clave privada está depositada ante notario (tercero de confianza) lo que impide la reutilización o modificación de dichos datos biométricos, con el fin sustentar dicha firma como legitima con carácter legal.

Los usuarios tienen asociadas la(s) Tablet(s) de firma en la que se activará el agente de firma para que el trabajador mutualista pueda leer el documento completo que va a firmar y una vez de acuerdo procederá a realizar su firma manuscrita sobre la pantalla del dispositivo.

2.2.3. FIRMA SMS AVANZADA

Permite el envío de documentos al terminal móvil del mutualista/paciente para la firma de documentos. El proceso envia un SMS con un enlace al documento de Firma, solicitándole para la validación de acceso el NIF del destinatario por medidas de seguridad. Una vez leído el documento el usuario puede firmarlo desde su terminal móvil, recibiendo un SMS con un código OTP y realizando un grafo sobre la pantalla del terminal.

2.2.4. FIRMA OTP

Actualmente Mutua Montañesa cuenta con un proceso de firma de documentos de RRHH externalizado en una plataforma Cloud mediante un servicio externo denominado c-Office. Mutua Montañesa este trabajando con el actual proveedor para usar las opciones de firma de IvCert para internalizar este servicio, que se basa en la firma de contratos laborales por parte de los profesionales de Mutua montañesa. En este servicio se remite un SMS con una password de un solo uso (One Time Password – OTP) que sirve para la firma del documento y que junto con el resto de evidencias que guarda la plataforma da validez legal al acto de firma.

3. REQUERIMIENTOS

La presente licitación presenta los siguientes requerimientos técnicos y de suministro que Mutua Montañesa necesita en el ámbito de la firma electrónica a lo largo del tiempo establecido en el PPD que compone esta licitación.

Estará dentro del alcance de esta licitación los siguientes elementos:

- **Mantenimiento integral de la solución** de firma on-premise/cloud con derecho de uso de toda la suite de productos IvSign, IvCert incluidas todas las licencias, motor e integraciones necesarias de producto para 300 usuarios.
- **Uso de servicios de firma.** Uso ilimitado de firma por certificado digital y firma biométrica.
- **Mantenimiento y evolución del middelware** que orquesta la solución entre los transaccionales y gestor documental de Mutua y las soluciones de firma.
- **Soporte y/o implementación de otros flujos de firma** en integraciones con otros sistemas de la organización (EJ: Pixelware - Contratación Pública, RRHH) u otros desarrollos menores que sean requeridos en relación a la firma durante el periodo de vida del contrato. (Ej soporte a la adición de un flujo de firma nuevo, implementación de un tipo documental nuevo con necesidades específicas,)
- **Oficina de registro R.A.** que permite a Mutua Montañesa ser autónoma en la emisión de certificados a sus empleados en nombre de una entidad de certificación válida que este reconocida por las administraciones públicas y se encuentre dentro del catálogo de entidades certificadores de aFirma, evitando así costes de desplazamiento y pérdida de productividad de estos. Dicha oficina de Registro deberá permitir a los operadores de Mutua Montañesa la generación de certificados de manera autónoma, siempre siguiendo los procedimientos de calidad y seguridad indicados por la RA. El acceso al entorno de generación de certificados deberá ser web, permitiendo aspectos tales como:
    - Gestión de operadores y administradores del sistema.
    - Gestión de peticiones, emisión, renovación y revocación de certificados.
        - Carga por lotes de peticiones de certificados
        - Aprobación/revocación masiva de certificados
        - Listado de certificados emitidos y estado de los mismos
    - Consulta pública de claves públicas de certificados.
    - Políticas de certificación, documentación y formación.
    - Emisión de certificados en soporte software, hardware y centralizados.

  La RA permitirá al operador la emisión de los diferentes tipos de certificados de PF indicados en el pliego, así como su integración automática con el almacén de certificados de la organización.

- **Sellado de tiempo**: Servicio que añade una marca de veracidad de tiempo a todos los actos de firma que se llevan a cabo. Dicho servicio de sellado implicará el suministro anual de 200.000 Sellos de tiempo. Dicha bolsa de sellos no caducará quedando para años sucesivos el remanente anual que se pudiera producir.
  El proveedor en su oferta económica deberá incluir el precio unitario de sello de tiempo adicional en bloques de 10.000 sellos, lo que llegado el caso de superar el máximo requerido servirá como tarifa para facturar los excesos de sellado producidos. El proveedor deberá informar a Mutua Montañesa cuando haya consumido el 75% y el 90 % de los sellos del año para permitir a Mutua Montañesa analizar el desvío y poder tomar las medidas adecuadas.
- **Suministro Certificados cualificados de persona física y pertenencia a entidad** (o certificado equivalente que pueda aparecer en el tiempo de vida del contrato) para 300 empleados activos de la organización, mediante el suministro de certificados con una validez mínima de 2 años. Dicha bolsa de certificados no caducará quedando para años sucesivos el remanente anual que se pudiera producir.

  El proveedor en su oferta económica deberá incluir el precio unitario de certificado adicional, lo que llegado el caso de superar el número requerido servirá como tarifa para facturar los excesos de certificados generados, hasta un máximo de 150 certificados adicionales año. El

proveedor deberá informar a Mutua Montañesa cuando haya consumido el 75% y el 90 % de los certificados suministrados para permitir a Mutua Montañesa analizar el desvío y poder tomar las medidas adecuadas.

- **Suministro anual de 12 Certificados cualificados de representante de persona Jurídica ante AAPP** (o certificado equivalente que pueda aparecer en el tiempo de vida del contrato) con una validez mínima de 2 años. Dicha bolsa de certificados no caducará quedando para años sucesivos el remanente anual que se pudiera producir. El proveedor en su oferta económica deberá incluir el precio unitario de certificado adicional, lo que llegado el caso de superar el máximo requerido servirá como tarifa para facturar los excesos de certificados generados.
- **Un Certificados Cualificado de Sello de Entidad** a nombre de Mutua Montañesa con una validez mínima de 2 años. Sera por cuenta del proveedor el mantenimiento/renovación de este certificado activo mientras el contrato asociado a esta licitación este en vigor.
- **Un certificado Cualificado de Cifrado** a nombre de Mutua Montañesa con una validez mínima de 2 años. Sera por cuenta del proveedor el mantenimiento/renovación de este certificado activo mientras el contrato asociado a esta licitación este en vigor.
- **Servicio de tercero de confianza** basado en la custodia externa ante notario o similar de la clave privada de dicho certificado de cifrado.
- **Servicio de firma OTP**. El proveedor deberá suministrar dentro del precio de su oferta un mínimo de 3000 firmas OTP anuales. Dicha bolsa de firmas no caducará quedando para años sucesivos el remanente anual que se pudiera producir. El proveedor en su oferta económica deberá incluir el precio unitario de firma OTP adicional, lo que llegado el caso de superar el máximo anual fijado servirá como tarifa para facturar los excesos de certificados generados. El proveedor deberá informar a Mutua Montañesa cuando haya consumido el 75% y el 90 % de los certificados del año para permitir a Mutua Montañesa analizar el desvío y poder tomar las medidas adecuadas.

3.1. EVOLUCIÓN DE LA PLATAFORMA

El proveedor deberá garantizar la evolución de la plataforma manteniéndose vigilante de las posibles actualizaciones de producto que el fabricante de la solución pueda publicar. Estará incluido dentro de este alcance cualquier modificación o adaptación de los desarrollos que estas actualizaciones o parches de seguridad pudieran provocar en el resto de los componentes o desarrollos que pudieran verse afectados, así como las actualizaciones provocadas por descatalogación de versiones o requerimientos de parches de actualización y seguridad que en las infraestructuras de soporte (S.O y BBDD) se pudieran producir.

Así mismo se incluirá en la oferta un mantenimiento evolutivo funcional basado en bolsa de horas, en las que, ante una necesidad de evolución de las personalizaciones realizadas para Mutua Montañesa y tras una definición clara de alcance funcional y esfuerzo se proceda a aceptar de común acuerdo un alcance de esfuerzos. Se estima en 120 horas anuales el esfuerzo asignado a la evolución de la plataforma. Para queda necesidad funcional nueva o solicitud de modificación, el proveedor llevará acabo un análisis de esfuerzo e indicara a Mutua una estimación que deberá ser consensuada por ambas entidades. El modelo de facturación será en modo de Pago por uso no pudiéndose exceder las horas máximas indicadas en el contrato.

3.2. CALIDAD DE LOS DESARROLLOS

El conjunto de desarrollos realizados han de cumplir con los niveles de calidad exigidos por Mutua Montañesa, tanto por lo que respecta a los procesos que rigen su construcción, como los procedimientos utilizados para validar que el producto está libre de defectos.
Se requiere la definición del proceso y conjunto de procedimientos asociados que el licitador realizará para asegurar:

- Que el conjunto de procesos durante la fase de desarrollo cumple con buenas prácticas en la gestión de proyectos
- Que el conjunto de procedimientos definidos cubre cada uno de los aspectos para validar la calidad de producto respecto a la:

  - Utilidad
  - Garantía de uso
  - Sencillez
- Que existen un conjunto de indicadores que permitan comprobar el nivel de utilidad y garantía de la aplicación, y que ayuden a la toma de decisiones sobre:
  - Si el producto se ha desarrollado correctamente, es decir, si se han cumplido con todos los procedimientos definidos en el pliego
  - Si el producto está libre de defectos funcionales
  - Podemos realizar el despliegue a entorno productivo
  - Tenemos un nivel de calidad suficiente para su uso en entorno productivo.
- Seguridad. Todos los desarrollos realizados deberán estar orientados a la seguridad, siendo este aspecto una premisa clave en cualquier desarrollo.
  - Vulnerabilidades
  - Nuevas vulnerabilidades
  - Esfuerzo de corrección de vulnerabilidades

Mutua Montañesa, será propietaria de todos los desarrollos realizados adhoc para la organización (principalmente los que tengan que ver con el middelware) y tendrá en todo momento acceso como mínimo de solo lectura a los códigos fuente/bases de datos/parametrizaciones que se realicen específicamente para Mutua Montañesa.

3.3. PUESTA EN PRODUCCIÓN

El proveedor deberá disponer de los medios necesarios para realizar pruebas unitarias de modificaciones y puestas en producción que minimicen los posibles fallos o defectos de funcionamiento. Para este fin, Mutua Montañesa pondrá, en la medida de lo posible, a disposición del proveedor de entornos de test sobre los que poder evaluar y verificar el correcto funcionamiento de los nuevos desarrollos a implantar. En caso de no poder garantizar dicho entorno de test para alguno de los elementos que constituyen el entorno productivo de mutua montañesa, se facilitará los medios para garantizar que las pruebas se puedan desarrollar de la manera más fiable posible dependiendo como es lógico de la naturaleza de los propios desarrollos. El proveedor deberá indicar para cada puesta en producción los módulos afectados por dicho cambio de manera que los juegos de pruebas a realizar sean lo mas objetivos posibles y evitando así la necesidad de realizar test de validación completos de la solución en cada iteración de puesta en producción de una modificación.

4. SOPORTE TECNICO PLATINUM

El proveedor deberá garantizar un soporte técnico de calidad para todas las soluciones que componen el presente pliego. Para ello deberá designar a un especialista de soporte con conocimientos técnicos relativos a las particularidades de Mutua Montañesa, nominado, que sirva de canal de comunicación directo entre Mutua Montañesa y el proveedor, con capacidad ejecutiva e influencia en la interlocución con las áreas internas del proveedor. Así mismo ante incidencias generales del producto, se deberá garantizar un enrutamiento prioritario de las incidencias de Mutua Montañesa.

Otros perfiles designados a disposición del proyecto deberán ser como mínimo:

- Especialista Onboarding para los nuevos despliegues
- Customer Success

Así mismo, se pondrá a disposición de Mutua, un canal de información directo a traves de mail y chat para agilizar la interlocución entre el proveedor y el adjudicatario.

El proveedor deberá poner a disposición de mutua los siguientes canales de comunicación para la interlocución en lo que a soporte técnico respecta:

- **Portal de Incidencias**. Deberá permitir el acceso a los usuarios que Mutua Montañesa designe. Este portal permitirá la apertura y seguimiento de tickets activos así como el acceso al histórico de incidencias de la organización.
- **Teléfono**. Mutua Montañesa dispondrá de un canal directo telefónico para la gestion de incidencia con el interlocutor nominado como Especialista de Soporte.
- **Reuniones**. Reuniones periódicas de seguimiento del servicio en la que se analicen las incidencias del periodo y se tomen decisiones para la mejora integral del servicio.

4.1. ACUERDOS DE NIVEL DE SERVICIO

El mantenimiento de estos servicios cubrirá evoluciones menores de la plataforma de firma, tales como adaptaciones a nuevos formatos de documentos o la agregación de algún campo de información adicional, así como la corrección de bugs detectados durante el periodo de vida del presente contrato.

4.1.1. RESOLUCIÓN DE INCIDENCIAS

Definiciones:

- **Tiempo respuesta**: Es el tiempo que ha transcurrido desde que se notificó una incidencia hasta que el proveedor ha contactado por primera vez con MM. En este instante el proveedor comenzará a trabajar en la resolución de la incidencia.
- **Tiempo restauración**: Es el tiempo que ha transcurrido desde que se notificó una incidencia hasta que el proveedor ha dado una primera solución al problema, siendo previamente aceptada por el cliente y recuperándose el servicio.
- **Tiempo solución definitiva**: Es el tiempo que ha transcurrido desde que se notificó una incidencia hasta que el proveedor ha dado una solución definitiva al problema, previamente aprobada por MM.
- **Solución definitiva**: Está orientada a una solución final del problema, que se podrá conseguir volviendo a dejar el sistema como estaba antes de la incidencia o incorporando aquellas mejoras que eviten una reincidencia del mismo problema.

Los problemas que se puedan producir estarán catalogados en las siguientes categorías, según su prioridad:

- **Nivel 1-CRITICA:** Fallo total del sistema, impidiendo el acceso a la plataforma o servicio e imposibilidad de hacer uso de cualquiera de sus servicios

- **Nivel 2-ALTA**: Fallo de una o varias funcionalidades clave del servicio funcionalidades principales del servicio, y no secundarias), que afecta gravemente al correcto funcionamiento del servicio para todos los usuarios.
- **Nivel 3-BAJA**: Fallo de una o más funcionalidades del servicio sin presentar un efecto significativo inmediato en la calidad del servicio a todos los usuarios, como un fallo ergonómico, gráfico, editorial, etc.

El adjudicatario pondrá a disposición de Mutua Montañesa un soporte prioritario a través de teléfono y correo electrónico en horario laboral español (Lunes a Jueves: 8:00 a 17:30 Viernes: 8:00 a 15:00 exceptuando fiestas a nivel Nacional). Así mismo, para incidencias de Nivel 1 deberá existir un servicio de monitorización y de soporte técnico en modalidad de 24x7.

4.1.2. SLA

Dentro del ámbito de los servicios definidos en el presente documento, el proveedor asegurará a MM su disponibilidad de acuerdo con los tiempos y condiciones sobre el nivel de servicio (SLA) requerido.

Como norma general y de cara a la medida de los tiempos de nivel de servicio definidos a continuación, de las penalizaciones y cualquier otro aspecto en el que sea relevante, la prioridad de cada incidencia será acordada entre el proveedor y MM en cada caso.

La siguiente tabla se muestran los tiempos con el nivel mínimo de servicio requerido:

	Tiempo Respuesta	Tiempo Resolución
Nivel 1	0,5 hora laborable	4 horas laborables
Nivel 2	0,5 hora laborable	8 horas laborables
Nivel 3	0,5 hora laborable	24 horas laborables

No se considerarán, a efectos de SLAs, los "cortes programados" de los servicios acordados por las partes y causados por:

- Trabajos que implican corte del servicio y que son necesarios para mejorar el funcionamiento de este.
- Trabajos de mantenimiento preventivo de infraestructuras.
- Actualizaciones de Software.

Los cortes programados de servicio serán notificados con al menos 48 horas de antelación por los canales de comunicación establecidos.

4.1.3. PENALIZACIONES

El SLA de respuesta se medirá según una asignación de pesos a cada incidencia que no cumpla con los tiempos de resolución en base al siguiente baremo:

- Nivel 1 --> 10 puntos
- Nivel 2 --> 5 puntos
- Nivel 3 --> 1 punto

Las penalizaciones por aplicar se calcularán mensualmente con los siguientes %:

- Hasta 10 puntos --> 2% del precio de facturación correspondiente al mes de la incidencia
- Entre 11 y 20 puntos --> 5 % del precio de facturación correspondiente al mes de la incidencia
- 21 puntos o más --> 10 % del precio de facturación correspondiente al mes de las incidencias

Si durante un año el proveedor penaliza en durante 3 meses consecutivos o 4 meses alternos, esto podrá motivar la rescisión del contrato por parte de Mutua Montañesa sin lugar a ningún tipo de contraprestación económica más allá del pago de los servicios de pago por uso disfrutados hasta el momento de la rescisión

5. CESE DEL SERVICIO

El proveedor en el momento de cese del servicio ya sea producido por el fin de fecha del contrato o por cualquier otra causa imputable o no al proveedor, deberá garantizar el traspaso de conocimiento y la cesión completamente operativa del servicio al departamento de Sistemas de Mutua Montañesa o quien este designe como nuevo responsable del servicio. Dicho traslado incluirá toda la documentación existente de la solución mantenida, incluyendo como mínimo:

- Credenciales.
- Código fuente de los desarrollos específicos de Mutua Montañesa.
- Claves de Cifrado.
- Documentación técnica de la solución.
- Instalables y programas necesarios para el correcto funcionamiento de la plataforma.

Los ítems descritos como mínimos anteriormente deberán estar en un repositorio común, a acordar entre las partes durante la totalidad de la vigencia del contrato, y se deberá facilitar por parte del proveedor la cesión/exportación operativa de los mismos en caso de que estos se alberguen en infraestructuras de pago a nombre del proveedor.

En ningún caso el proveedor podrá anular ningún componente de la solución (EJ: revocación de certificados) o cualquier otra acción que desemboque en una perdida de servicio para Mutua Montañesa

6. CUMPLIMIENTO ENS

El adjudicatario deberá garantizar la seguridad, disponibilidad, confidencialidad e integridad de la información de Mutua Montañesa a la que tenga acceso en el desarrollo del proyecto mediante el cumplimiento de las siguientes normas básicas:

- Cumplir con los estándares y políticas de seguridad de Mutua Montañesa.
- Garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y transmitida por su red.
- Informar a Mutua Montañesa acerca de su política de seguridad, así como de la implementación y seguimiento por parte de su organización.
- Informar por escrito a Mutua Montañesa tan pronto como se detecten riesgos reales o potenciales de seguridad en su red o en el equipamiento del cliente.
- Acceso a cualquier equipamiento de red y/o sistemas de información mediante un control de acceso lógico, garantizando la restricción a los usuarios autorizados.
- Garantizar la estricta aplicación de las normas de seguridad por parte de su personal.

El adjudicatario deberá desarrollar en materia de seguridad todas las modificaciones requeridas que cumplan con la normativa en LOPD, RGPD y ENS (Nivel Alto), ya que la naturaleza de la información gestionada es de carácter ALTO.
El sistema objeto de esta licitación está encuadrada en la siguiente categorización ENS de nuestros sistemas:

Tipo	ID	Servicio / Información	Disponibilidad	Auntenticidad	Integridad	Confidencialidad	Trazabilidad
		Valor Maximo de los servicios	ALTO	ALTO	ALTO	ALTO	MEDIO
Información	IN_03_14	Gestión Documental Asistencial/Prestaciones	A	A	A	A	M

Por tanto, el adjudicatario deberá tener en cuenta como mínimo los requisitos de seguridad y compliance recogidos en la siguiente tabla:

Codigo ENS	Título	BAJA	MEDIA	Alta
op	**Marco operacional**			
[op.pl]	Planificación			
[op.pl.5]	Componentes certificados			Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas. Una instrucción técnica de seguridad detallará los criterios exigibles.
[op.acc]	Control de acceso			

Codigo ENS	Título	BAJA	MEDIA	Alta
[op.acc.1]	Identificación	1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación. 2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad. 3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que: a) Se puede saber quién recibe y qué derechos de acceso recibe. b) Se puede saber quién ha hecho algo y qué ha hecho. 4. Las cuentas de usuario se gestionarán de la siguiente forma: a) Cada cuenta estará asociada a un identificador único. b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario. c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.		

Codigo ENS	Título	BAJA	MEDIA	Alta
[op.acc.2]	Requisitos de acceso	Los requisitos de acceso se atenderán a lo que a continuación se indica: a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema. c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.		
[op.acc.3]	Segregación de funciones y tareas		El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita. En concreto, se separarán al menos las siguientes funciones: a) Desarrollo de operación. b) Configuración y mantenimiento del sistema de operación. c) Auditoría o supervisión de cualquier otra función	

Codigo ENS	Título	BAJA	MEDIA	Alta
[op.acc.4]	Proceso de gestión de derechos de acceso	Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios: a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada. b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones. c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.		
[op.exp]	Explotación			

Codigo ENS	Título	BAJA	MEDIA	Alta
[op.exp.2]	Configuración de seguridad	Se configurarán los equipos previamente a su entrada en operación, de forma que: a) Se retiren cuentas y contraseñas estándar. b) Se aplicará la regla de "mínima funcionalidad": 1. El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad, 2. No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible. 3. Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue. c) Se aplicará la regla de "seguridad por defecto": 1. Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. 2. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes. 3. El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.		
[op.exp.3]	Gestión de la configuración		Se gestionará de forma continua la configuración de los componentes del sistema de forma que: a) Se mantenga en todo momento la regla de “funcionalidad mínima? ([op.exp.2]). b) Se mantenga en todo momento la regla de “seguridad por defecto? ([op.exp.2]). c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]). d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]). e) El sistema reaccione a incidentes (ver [op.exp.7]).	

Codigo ENS	Título	BAJA	MEDIA	Alta
[op.exp.4]	Mantenimiento	Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente: a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas. b) Se efectuará un seguimiento continuo de los anuncios de defectos. c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.		
[op.exp.8]	Registro de la actividad de los usuarios	Se registrarán las actividades de los usuarios en el sistema, de forma que: a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información. b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema. c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados. d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema		

Codigo ENS	Título	BAJA	MEDIA	Alta
[op.exp.11]	Protección de claves criptográficas	Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final. a) Los medios de generación estarán aislados de los medios de explotación. b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.	a) Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5]. b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.	
[mp.com.3]	Protección de la autenticidad y de la integridad	a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (ver [op.acc.5]). b) Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos: 1. La alteración de la información en transito 2. La inyección de información espuria 3. El secuestro de la sesión por una tercera parte c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación.	a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad. b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional. c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.	a) Se valorará positivamente en empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual. b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5]. c) Se aceptará cualquier mecanismo de autenticación de los previstos en normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias altas en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.
[mp.si]	Protección de los soportes de información			

Codigo ENS	Título	BAJA	MEDIA	Alta
[mp.si.5]	Borrado y destrucción	La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos. a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.	b) Se destruirán de forma segura los soportes, en los siguientes casos: 1. Cuando la naturaleza del soporte no permita un borrado seguro. 2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida,. c) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].	
[mp.sw]	Protección de las aplicaciones informáticas			
[mp.sw.1]	Desarrollo		a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción. b) Se aplicará una metodología de desarrollo reconocida que: 1. Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida. 2. Trate específicamente los datos usados en pruebas. 3. Permita la inspección del código fuente. 4. Incluya normas de programación segura. c) Los siguientes elementos serán parte integral del diseño del sistema: 1. Los mecanismos de identificación y autenticación. 2. Los mecanismos de protección de la información tratada. 3. La generación y tratamiento de pistas de auditoría. d) Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.	
[mp.info]	Protección de la información			

Codigo ENS	Título	BAJA	MEDIA	Alta
[mp.info.1]	Datos de carácter personal	Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.		
[mp.info.3]	Cifrado			Para el cifrado de información se estará a lo que se indica a continuación: a) La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella. b) Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en [mp.com.2]. c) Para el uso de criptografía en los soportes de información, se estará a lo dispuesto en [mp.si.2].

Codigo ENS	Título	BAJA	MEDIA	Alta
[mp.info.4]	Firma electrónica	Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.	a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados. b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional. c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin: d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación: 1. Certificados. 2. Datos de verificación y validación. e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2 del apartado d). f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.	

Codigo ENS	Título	BAJA	MEDIA	Alta
[mp.s.2]	Protección de servicios y aplicaciones web	Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias. a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos: 1. Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado. 2. Se prevendrán ataques de manipulación de URL. 3. Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies". 4. Se prevendrán ataques de inyección de código. b) Se prevendrán intentos de escalado de privilegios. c) Se prevendrán ataques de "cross site scripting". d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés". Se emplearán "certificados de autenticación de sitio web" acordes a la normativa europea en la materia.		Se emplearán "certificados cualificados de autenticación del sitio web" acordes a la normativa europea en la materia.

Mutua Montañesa

Mmuy fácil