Pliego de Prescripciones Técnicas para el suministro de licencias y prestación del servicio de identidad digital corporativa: plataforma para emisión y administración de certificados digitales, firma electrónica cualificada centralizada, autoridad de registro, firma mancomunada, sellado de empresa e integración con aplicaciones de Mutua Intercomarcal.

1. OBJETIVO DEL SERVICIO

Mutua Intercomarcal está inmersa en un proceso de transformación digital que lleva asociada la implantación de la identidad digital corporativa.
El objeto del presente Pliego es fijar las condiciones que deben regir contratación de los siguientes servicios:

-**Emisión de certificados electrónicos cualificados** según el Reglamento (UE) Nº 910/2014 (eIDAS), actuando la Mutua Intercomarcal como **autoridad de registro**.
-Servicio de **firma centralizada cualificada** (Reglamento (UE) Nº 910/2014 (eIDAS), incluyendo la puesta en marcha continuidad de la autoridad de registro además de la integración en las aplicaciones de Mutua Intercomarcal.
-Puesta a disposición de una **plataforma de firma mancomunada** de documentos con un proceso de firma simultánea de hasta 5 personas, con una consola de administración, roles de peticionario/control del documento y clientes de firma electrónica para los firmantes, y adicionalmente las notificaciones a peticionario y firmantes. Almacenaje y documentación de evidencias.
-Suministro y puesta a disposición de **un servicio de sellado** (con certificado de Sello de Empresa) y sellado de tiempo, para la emisión/recepción de documentos a/de usuarios de los servicios de Mutua Intercomarcal.

2. DESCRIPCIÓN DE LA SOLUCIÓN REQUERIDA Y SOLVENCIA TÉCNICA DEL LICITADOR.

2.1 Emisión de certificados electrónicos cualificados (requisito técnico)

Se requiere la emisión de los siguientes tipos de certificados:

-Certificados electrónicos cualificados de nivel alto.

-El licitador debe ser prestador de servicios electrónicos de confianza cualificados conforme al reglamento europeo eIDAS, este prestador debe estar incluido en la lista de confianza (TSL) de la Secretaría de Estado para el Avance Digital (SEAD) del Ministerio de Economía y Empresa. Además, deberá estar incluido en la lista de proveedores de servicios de certificación soportados por la plataforma @Firma.

-El licitador debe ser prestador de servicios de confianza cualificado conforme a eIDAS para ofrecer servicios de emisión de certificados cualificados de firma (QCert for Esig).

-El presente pliego contempla le emisión de certificados electrónicos cualificados para un máximo de 400 usuarios activos, de nivel alto en el entorno de producción y la provisión de 5 certificados adicionales para su uso en entornos de preproducción y pruebas.

-La validez máxima de los certificados emitidos deberá ser de 24 meses, y su renovación deberá contemplarse 30 días antes de la fecha de caducidad de los mismos.

2.2 Autoridad de registro e integración de aplicaciones

El servicio debe incluir los siguientes aspectos:

• Creación o continuidad de la **autoridad de registro para Mutua Intercomarcal** que contemple al menos los siguientes servicios web: registro de usuarios, consulta de estado de revocación de certificados por usuario, búsqueda de usuarios, revocación de certificados y borrado de usuarios.

• Se habilitará, al menos, **a cuatro personas** del departamento de Tecnologías de la Información para la supervisión y administración de la autoridad de registro.

• El licitador deberá poner a disposición de Mutua Intercomarcal una autoridad de registro de test **con las mismas funcionalidades que la autoridad de registro en el entorno de producción.**

• Servicio de estado de validación de certificados mediante CRLs, LDAP y OSCP. El peso máximo de las CRLs será menor de 150 KBs y el tiempo máximo de cada petición de validación de certificados, en cualquiera de sus tres modalidades, menor **a 1 segundo**.
Adicionalmente:
Tanto las CRLS como el OCSP deben estar firmados por **la misma autoridad de certificación** que la emisora de los certificados.
El licitador deberá poner a disposición de la Mutua un entorno para la validación de certificados emitidos por la autoridad de registro de pruebas.

• El licitador deberá suministrar una licencia de uso durante la duración del servicio de un cliente-agente CSP (Cryptographic Service Provider) para el uso de los certificados electrónicos centralizados cualificados desde el propio equipo del usuario para todos los usuarios activos. El cliente-agente permitirá al usuario visualizar y usar sus certificados centralizados de manera análoga a como si lo estuviera almacenado en local. El cliente-agente CSP **se debe integrar con el directorio corporativo de Mutua Intercomarcal** (Micrososft Active Directory) y debe permitir personalización con imagen y textos corporativos.

El cliente-agente se debe distribuir mediante un instalable MSI (Microsoft Installer) para Windows 10 y Windows 11 para todas sus versiones profesionales. El agente deberá funcionar **con los navegadores Internet Explorer,** Firefox,Google Chrome y Microsoft Edge.

• El licitador pondrá a disposición de Mutua Intercomarcal la documentación técnica y APIs, Servicios web o Componentes para integrar las aplicaciones desarrolladas por la Mutua.

• La propuesta debe incluir todas las tareas necesarias para la puesta en marcha de la emisión de los certificados cualificados, integración de las aplicaciones de Mutua Intercomarcal y la plataforma de firma centralizada.

• La propuesta debe influir un apartado de formación personalizada y manuales para el personal de Mutua Intercomarcal responsable de la autoridad de registro.

• La propuesta deberá influir soporte al equipo de desarrollo de las aplicaciones de Mutua Intercomarcal para la integración de las aplicaciones con la plataforma de firma centralizada del adjudicatario.

• En caso de pérdida de claves de acceso por parte de los usuarios o de revocación del certificado se deberá emitir un nuevo certificado sin coste adicional.

2.3 Servicio de firma electrónica cualificada centralizada.

La solución de firma centralizada **deberá estar certificada para ofrecer firma electrónica cualificada, de acuerdo al reglamento eIDAS**, debe estar basada en un certificado cualificado de firma electrónica y creada mediante un dispositivo cualificado de creación de firmas electrónicas. Este proceso/dispositivo debe estar ubicado en las instalaciones del licitador y garantizará un acceso seguro a través de Internet.

La solución de firma electrónica centralizada debe acreditar estar en posesión de la certificación como dispositivo cualificado de creación de firma remota (rQSCDev) según se establece en el Anexo II del reglamento eIDAS y figurar en la lista de dispositivos de la Comisión Europea.
https://futurium.ec.europa.eu/en

La solución propuesta debe ofrecer servicio de firma electrónica cualificados en movilidad para la firma ilimitada de documentos y transacciones tanto el entorno de producción como en el entorno de pruebas. (El tiempo máximo de cada petición de firma debe ser de 1 segundo como máximo).

La solución de firma centralizada debe ofrecer el servicio **de firma electrónica cualificada y firma electrónica avanzada**, de acuerdo al Reglamento (UE) Nº 910/2014 (eIDAS), en función de las necesidades de los procesos de negocio de las aplicaciones que se integren.

Para la firma electrónica cualificada, la solución de firma centralizada **deberá proveer de un mecanismo de segundo factor de autenticación basado en una clave temporal de un solo uso** (OTP).
La solución de firma electrónica cualificada centralizada se deberá integrar mediante componentes, servicios web o cualquier otro sistema con los desarrollos en Mutua Intercomarcal. El adjudicatario deberá facilitar los manuales de integración y muestras de código fuente para integrar el mencionado software con la solución proporcionada.

Adicionalmente la solución de firma electrónica cualificada centralizada debe garantizar:

• Confidencialidad. La solución deberá garantizar el acceso por parte de las aplicaciones y sistemas debidamente autorizados. Se deberá ofrecer los mecanismos necesarios para evitar la suplantación de identidad y ataques que pongan en riesgo el acceso no autorizado sistema de firma centralizado.
• Integridad. El sistema debe garantizar que el proceso de firma centralizado se lleva a cabo de forma transaccional, de modo que se garantice que la información a firmar no es alterada intencionadamente o por ser incorrecta.
• Disponibilidad. El adjudicatario garantizará el acceso de las aplicaciones a integrar y la disponibilidad de los procesos de firma centralizada de acuerdo con los niveles de servicios recogidos en este pliego. El canal de comunicación utilizado para integrar las aplicaciones de Mutua Intercomarcal con el sistema de firma centralizado será a través de Internet. El adjudicatario llevará a cabo las medidas para evitar ataques de disponibilidad del servicio, como ataques distribuidos de denegación de servicio (DDoS).
Trazabilidad. El sistema llevará a cabo un registro de las operaciones de firma y de los accesos, tanto los correctos como los incorrectos.

2.3 Uso y gestión de certificados.

El adjudicatario deberá proporcionar un portal web para la gestión de la autoridad de registro de la Mutua Intercomarcal con las siguientes funcionalidades:
• Autenticación mediante datos de contraste definidos por Mutua Intercomarcal, certificado centralizado, así como de cualquier otro certificado electrónico cualificado.
- Carga masiva de usuarios de AD mediante CSV o similar.
- Gestión de titulares:
  - -Registro de usuarios
  - -Modificación de usuarios
  - -Consulta de usuarios y estado de certificados

-Emisión de certificados
-Revocación de certificados
-Baja de usuarios

- Gestión de administradores y personal de registro
- Estadística del uso de certificados (mediante portal web)

El adjudicatario debe proporcionar acceso a un portal web para la gestión de los certificados por parte de los usuarios con las siguientes funcionalidades:

- Autenticación mediante datos de contraste, certificado centralizado, así como de cualquier otro certificado electrónico cualificado.
- Revocación del certificado.
- Cambio contraseña del certificado a través del propio certificado.
- Cambio de contraseña del certificado mediante datos de contraste.
- Descarga de la clave pública del certificado
- Portal web personalizado con la imagen corporativa de Mutua.
- Acceso a través de internet y garantizando la seguridad de las comunicaciones.

2.4 Plataforma de firma mancomunada.

Preferiblemente se requiere este servicio en SaaS, con el fin de evitar gastos de mantenimiento, tiempo de gestión e inversiones en infraestructuras para la Mutua.
La plataforma que sustenta al servicio debe aportar garantías de alta disponibilidad.
La plataforma de firma mancomunada debe disponer de un módulo de administración desde donde los distintos roles de usuario puedan consultar, firmar o gestionar los documentos subidos y puestos a disposición de los firmantes.
La plataforma debe disponer de mecanismos de aviso, tanto a los firmantes como a los gestores para saber en qué momento se les requiere una firma y cuando un documento está firmado por la totalidad de los cofirmantes, para seguir con la gestión para la cual era requerida la firma.
La plataforma debe permitir el uso de forma integrada con las identidades digitales residentes en el repositorio corporativo de firmas y la utilización de los certificados digitales residentes en la mencionada plataforma para la firma de los documentos, permitiendo una gestión única de identidad ágil.
La utilidad de firma mancomunada debe proporcionar al firmante una reproducción íntegra del documento a firmar para que éste pueda validar la conformidad con el mismo.
El documento debe poder ser firmado de forma simultánea por los distintos cofirmantes y estar disponible durante, como mínimo tres años en la plataforma para su consulta y debe permitir la obtención de un certificado de autenticidad del proceso de firma acreditada por el tercero de confianza que realiza el servicio.

2.5 Plataforma de sellado de empresa.

Preferiblemente se requiere este servicio en SaaS, con el fin de evitar gastos de mantenimiento, tiempo de gestión e inversiones en infraestructuras para la Mutua.

La plataforma que sustenta al servicio debe aportar garantías de alta disponibilidad y se dimensiona en un máximo de 200.000 documentos anuales.
El entorno de operación debe de estar dedicado y/o segmentado para el uso exclusivo Mutua Intercomarcal siendo imposible cualquier incidente de seguridad por motivo de compartición del servicio con otras entidades.

-La función de sellado con certificado de Sello de Empresa debe englobar operaciones criptográficas siguiendo los estándares de la industria como xmldsig, XAdES, etc, así como operaciones criptográficas básicas como hashes (SHA-256), algoritmos de cifrado simétrico y de clave pública.
-La función de Custodia Segura de Claves debe ser implementada en un módulo HSM (Hardware Security Module) lo que garantiza la custodia de las claves asociadas a los certificados de representación o corporativos.
-Los módulos criptográficos deben proporcionar las funcionalidades de generación de firma electrónica, verificación, cifrado y descifrado de datos, generación de sellados de tiempo, etc., accesibles mediante APIs.
-Se requiere Sello de Tiempo Cualificado y se utilizará en procesos masivos de firma, para garantizar la integridad documental y el momento exacto en que se firma el documento, mostrando inequívocamente que el contenido no ha sido alterado y que proceden de un único proceso trazable, desde la generación del documento, y hasta la recepción final del mismo una vez todos los actores del proceso han tramitado y firmado ese mismo documento único.
- El mecanismo de integración es a través de API o WebServices.
- Formatos de firma que debe suportar la plataforma:

-XMLDSig: Firma digital sobre documentos estructurados de tipo XML.

-XAdES: Formato de firma que extiende a XMLDSig a través del estándar europeo XAdES (“XML Advanced Electronic Signatures”) definido por ETSI a nivel europeo en su especificación ETSI TS 101 903. Dentro de los tipos de documentos XAdES existentes, protocolo TSP (“Time-Stamp Protocol”) en el caso de autoridades de sellado de tiempo.

-PDF: Los documentos PDF que permita realizar además sellado de tiempo y representar gráficamente las firmas.

-PAdES: Firma basada en el estándar avanzado de firma sobre PDFs PAdES, desde los formatos básicos hasta el formato LTV que permita almacenar/conservar las firmas a lo largo del tiempo mediante la adición de Document TimeStamps.

-PKCS#7: El formato de firma PKCS#7, permite contar con compatibilidad respecto a firmas realizadas con anterioridad. Debe permitir añadir sellado de tiempo a este tipo de firma.

-CAdES: Formato de firma CMS Advanced Electronic Signatures, que es una firma avanzada basada en el formato CMS, que a su vez es una actualización del formato PKCS#7. Este formato añade la posibilidad de generar firmas en serie, añadir distintos tipos de TimeStamp, incluir los certificados correspondientes a las diferentes cadenas de certificación, así como incluir toda la información de verificación (CRLs y OCSPs) en el

documento. Este tipo de firma es adecuado para ser almacenada en repositorios de firmas que deban tener validez durante un tiempo prolongado sin los problemas que puedan ocasionar la caducidad o estado de revocación de los certificados.
-SMIME: Siendo MIME el formato de correo electrónico, SMIME como método para enviar y recibir mensajes MIME seguros. SMIME usa el formato de datos definido para PKCS#7.

Sellado de Tiempo Cualificado

TimeStamp con sellos de tiempo cualificados según eIDAS y conforme al RFC3161.
Sello de tiempo emitido mediante protocolo HTTP en formato ASN1 conforme al RFC3161. La fuente de tiempo de la TSA debe estar sincronizada con el ROA (Real Instituto y Observación de la Armada), de conformidad con lo previsto sobre la hora legal en el RD 1308/92 de 23 de octubre, por el que se declara el Laboratorio del Real Instituto y Observación de la Armada como laboratorio depositario del patrón nacional del tiempo, Orden PRE/1551/2003 de 10 de junio, por el que se desarrolla el RD 209/2003 de 21 de febrero.

Características generales a tener en cuenta:

- Que permita la generación de sellos de tiempo conforme a los RFCs 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) y RFC 5816.
- Que permita el funcionamiento simultáneo de distintas Políticas de Timestamp, pudiendo elegir, por política, el OID que la identifica, algoritmos hash aceptados, algoritmo hash usado para la firma del sello de tiempo, clave y certificado usados para generación de TimeStamps.
- Que disponga de una Política de Timestamp **por defecto** para las peticiones que no indican una política de timestamp concreta.
- Que permita la administración independiente desde consola o módulo de administración.
- Que disponga de la posibilidad de activación/desactivación temporal de cada política de timestamp.
- Que permita el uso de listas blancas por ip.
- Que permita el uso de claves de firma contenidas en almacenes software PCKS#12 o en los HSM soportados.
- Debe disponer de un registro de auditoría de sellos de tiempo generados.
- Debe disponer de un mecanismo de firma de trazas de auditoría de sellos generados y herramienta para verificación de integridad.

- Generación de sellos de tiempo en formato ASN1 conforme al RFC3161
- Funcionamiento alternativo en modo proxy contra una TSA externa.

3. FASES DEL PROYECTO Y MODELO DE RELACIÓN

3.1 Fase de Implantación

El objetivo de esta fase es la definición de requerimientos, parametrización e instalación del objeto del contrato, la puesta en marcha del servicio con las máximas garantías y calidad del servicio.
En esta fase se facilitará la documentación técnica y componentes para la integración de las aplicaciones corporativas con la plataforma de firma centralizada del adjudicatario. Además, se resolverán posibles dudas para la correcta integración.
El prestador del servicio personalizará y configurará los portales web para la gestión de la autoridad de registro y para la gestión de los certificados por parte de los usuarios autorizados de Mutua Intercomarcal.
El adjudicatario impartirá la formación para la puesta en marcha del sistema de acuerdo con la planificación acordada con Mutua Intercomarcal.
Esta fase se iniciará en el momento de la firma del contrato y tendrá una duración máxima de 2 meses.

3.2 Fase de servicio regular

Fase de operación regular del servicio circunscrito al cumplimiento de los ANS establecidos.
En esta fase el adjudicatario debe garantizar la correcta prestación del servicio.
Durante esta fase se incluye la generación de un número ilimitado de firmas cualificadas en dispositivo HSM ubicado en las instalaciones del adjudicatario y accesible de forma segura a través de Internet.
Se incluye dentro del alcance del contrato las actualizaciones del sistema de firma centralizada y de creación de certificados que incluye la resolución de incidencias y mejoras de seguridad. También se incluye dentro del contrato el soporte y consultas al adjudicatario que permita garantizar la correcta prestación del servicio.

3.3 Fase de devolución del servicio

La devolución del servicio tendrá lugar por cualquiera de las siguientes causas:

- ✓ Terminación del contrato por finalización del período contractual acordado y liquidación de este.
- ✓ Resolución del contrato de forma anticipada por incumplimiento del objeto del contrato y liquidación del mismo, o cualquier otra causa que suponga causa de resolución.

En todos los casos, existirá un periodo de devolución del servicio para garantizar la transferencia del conocimiento adquirido o generado durante la prestación del servicio por parte del

adjudicatario a Mutua Intercomarcal, o hacia el nuevo adjudicatario, sin que ello repercuta en una pérdida del nivel de calidad del servicio.

En esta fase, el adjudicatario deberá traspasar los servicios, simultaneándose los trabajos de devolución con los de prestación del servicio regular, sin coste adicional.
El adjudicatario deberá colaborar activamente con la Mutua Intercomarcal y con el futuro proveedor durante este proceso para facilitar la transferencia del conocimiento y la responsabilidad sobre los servicios.
El traspaso se realizará en un plazo acordado previamente o bien establecido de 6 semanas desde la finalización del contrato.

3.3 Interlocución, responsabilidades y modelo de relación

Mutua Intercomarcal aportará a un jefe de Proyecto, que será el responsable de supervisar los Acuerdos de Nivel de Servicio y será el encargado de dirigir y coordinar la relación con el proveedor del mismo.

El adjudicatario deberá adscribir a la ejecución del contrato como medios personales, y de conformidad con lo establecido en el artículo 76.2 de la LCSP, un jefe de Proyecto que se encargará de la, supervisión y cumplimiento de los Acuerdos de Nivel de Servicio, así como de coordinar y garantizar el cumplimiento de los requisitos del contrato, asignando los medios y personal adecuados para la correcta prestación de este.

El licitador debe incluir en su propuesta un modelo de relación, calendario de reuniones de seguimiento y modelo de explotación de datos de evaluación del servicio, identificación de riesgos de este, plan de calidad y modelo de gestión de incidencias.

El servicio deberá estar activo en horario 24x7, y el soporte de este, en horario laboral.

4. CONDICIONES DE EJECUCIÓN.

4.1 Condiciones de ejecución básicas

- Se requiere que para todos los bienes y servicios a contratar exista una permanente actitud proactiva por parte del adjudicatario. Se desea que éste sea realmente un socio tecnológico de MUTUA INTERCOMARCAL.
- MUTUA INTERCOMARCAL es una entidad con vocación de mejora continua, lo que puede representar la expansión y apertura de nuevos centros, cambios en las comunicaciones en centros actuales, situaciones de emergencia que pueden derivar en necesidades adicionales.

- Correrán por cuenta del adjudicatario **todos los gastos derivados del transporte de material hasta su ubicación definitiva** y el acceso hasta las dependencias de MUTUA INTERCOMARCAL.
- El adjudicatario deberá mantener una actitud proactiva y diligente en los **procesos de transferencia de servicio (si aplica)**, tanto cuando lo recibe de un tercero como cundo deba transferirlo al final del contrato, respetando los compromisos adquiridos en su propuesta.
- El adjudicatario estará obligado a garantizar la disponibilidad, seguridad, integridad y confidencialidad de los datos a los que tenga acceso, considerándolo desde Mutua Intercomarcal como una figura de "Encargado de Tratamiento" (Según Ley Orgánica 03/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales, y del Reglamento Europeo de Protección de Datos).
  Sus principales obligaciones en cuanto a **seguridad de la información** serán:

  a) Garantizar la estricta aplicación de las **normas de seguridad** por parte de su personal. (Basadas en la aplicación de la ISO 27001 implantada en Mutua Intercomarcal).
  b) **Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información a la que se tenga acceso (si aplica)** para el desarrollo del servicio, respetando los compromisos adquiridos.
  c) Garantizar que toda la información que es transmitida por MUTUA INTERCOMARCAL no es almacenada ni interceptada, de extremo a extremo en la red.
  d) Cumplir con los estándares y políticas de seguridad de MUTUA INTERCOMARCAL.
  e) Informar a MUTUA INTERCOMARCAL de **manera inmediata**, de las **incidencias de seguridad**, y cuando se detecten riesgos reales o potenciales de seguridad en su red o equipamiento.
  f) Ejecutar todas las operaciones de servicio siguiendo procedimientos pactados con Mutua Intercomarcal y propios del licitador que contemplen las normas de seguridad jurídicas y normativas establecidas.
  g) Permitir a Mutua Intercomarcal realizar **controles periódicos y auditorías** sobre el servicio.
  h) Poseer los mecanismos necesarios que garanticen que **el acceso** a cualquier equipamiento de red o sistemas de información **sea única y exclusivamente para los usuarios autorizados** a ello (si aplica).
  i) A nivel general, cumplir con todas las obligaciones que establece la Ley Orgánica 03/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales y el Reglamento Europeo de Protección de Datos (GDPR) ; así como la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios(si es de aplicación al servicio).
  j) Descripción de los **mecanismos de cifrado de datos** que utiliza el servicio, como requisito indispensable **para dar cumplimiento reglamentado a las comunicaciones de datos sensibles** (si aplica al servicio).

k) Considerar la gestión asociada a la implantación y mantenimiento del proyecto en aspectos como:

   i. **Modelo de relación**.
   ii. **Gestión de cambios**, gestión e inventario de los cambios del material suministrado y control de licencias (caducidad).
   iii. **Elaboración de informes** de incidencias del servicio y de SLA's comprometidos: periódicamente, o a petición expresa de MUTUA INTERCOMARCAL.

4.2 Marco temporal del proyecto.

El servicio se realizará **durante el período de un año, alcanzándose o no la cifra límite de licitación del concurso** en función de los términos y condiciones del contrato.

4.3 Requisitos de Seguridad específicos.

4.3.1 Confidencialidad, privacidad y publicidad del servicio o de la información.

- El adjudicatario está obligado a guardar secreto respeto a los datos o información previa que no siendo públicos o notorios estén relacionados con el objeto del contrato. Cualquier comunicado de prensa o inserción a los medios de comunicación que el proveedor realice referente al servicio que presta a la Mutua Intercomarcal tendrá que ser aprobado previamente por Mutua Intercomarcal.
- No se podrá tratar con cualquier otra persona física, ente, organismo o empresa pública privada ningún tipo de información de los contenidos, entregables, evolución y progreso de este proyecto o actuaciones que se lleven a cabo, sin el consentimiento explicito, formal y por escrito de Mutua Intercomarcal.

4.3.2 Seguridad y protección de los datos

- El adjudicatario se compromete a:
  - Cumplir con las directivas tecnológicas y de seguridad y calidad que establezca Mutua Intercomarcal.
  - Implementar las medidas, procesos, y requerimientos que Mutua Intercomarcal solicite con esta finalidad y le propondrá los que considere necesarios para mejorar las soluciones.

- Facilitar toda aquella información que Mutua Intercomarcal requiera a fin de que éste pueda dar cumplimiento a la legislación y normativa referida en este apartado.
- Cumplir con todas las obligaciones respecto a la LOPD–GDD y RGPD establecidas en el pliego Administrativo del contrato.

4.5. Facturación de los servicios

- Se facturará mensualmente y de acuerdo con la distribución proporcional de importes acordada.
- La facturación se realizará a través de la plataforma FACE.
- No se aceptará ninguna factura sin referencia al contrato adjudicado.

4.6. Service Level Agreement (SLA):

Tiempo de resolución de incidencia en período de garantía

Se define tiempo de resolución de incidencias como el tiempo trascurrido desde que una incidencia es notificada hasta su completa resolución.

Ante la aparición de una incidencia que afecte al servicio, se establece un tiempo **máximo de resolución de 8 horas laborables.**

Penalizaciones por incumplimiento de los acuerdos de nivel de servicio.

Cada licitador deberá proponer los mecanismos de penalización que crea más adecuados en la propuesta que presente.

La Mutua evaluará cada propuesta de SLA's y penalización (por incumplimiento) dentro de los aspectos de valoración sujeta a juicio de valor en el cuadro de puntuación.

4.7. Mejoras

Se indicarán todas aquellas características que los licitadores consideren como mejoras técnicas.

4.8. Presentación de ofertas

Las ofertas presentadas deberán guardar el siguiente formato, o similar, dejando la documentación complementaria requerida en anexos (si aplica). Para ello, los licitadores limitarán su oferta técnica de acuerdo con el índice detallado a continuación:

En Barcelona a fecha de la firma electrónica

Director de Organización y T.I.

46581544N ANTONIO SERRA (R:G60328796) FIRMA

Digitally signed by 46581544N ANTONIO SERRA (R:G60328796) FIRMA
Date: 2025.11.17 11:45:46 +01'00'