

**PLIEGO DE CLÁUSULAS TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS RELACIONADOS CON LA GESTIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN, ISO 27001 Y ESQUEMA NACIONAL DE SEGURIDAD. AUDITORIA INTERNA DE SEGURIDAD, LOPDGDD Y SERVICIOS DE DELEGADO DE PROTECCIÓN DE DATOS.**

**1- OBJETO DEL SERVICIO Y DESCRIPCIÓN.**

El objeto de este servicio es el conseguir los siguientes objetivos:

- Establecer las bases de relación entre Mutua Intercomarcal y el Adjudicatario con respecto a la SERVICIOS RELACIONADOS CON LA GESTIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN, Y PROTECCIÓN DE DATOS, mediante la contratación de un servicio de consultoría de seguridad y consultoría legal. Para colaborar en la consecución y/o renovación de las certificaciones de 27001 y ENS, evolución de las soluciones tecnológicas de seguridad, así como para proveer de un servicio de Delegado de Protección de Datos a la Organización y garantía de derechos digitales y consultoría legal asociada.

**EN CUANTO A GESTION DE LA SEGURIDAD – PLAN DE CONTINGENCIAS (ASPECTOS VINCULADOS A LA LEGALIDAD APLICABLE):**

- Evolución del plan de Continuidad de negocio, que contemple los aspectos del actual mapa de red y las modificaciones referentes al CPD de contingencia y entorno Cloud. Liderazgo del proyecto de migración e implantación de los cambios.
- Documentación de todos los procesos de recuperación de los servicios en caso de contingencia grave que implique el cambio de centro de proceso.
- Definir procedimientos y calendario de pruebas del Plan de Contingencia T.I.
- Definición de roles y responsabilidades: Formación del personal involucrado en el Plan de Contingencia T.I.

**GESTION DE LA SEGURIDAD – EN BBDD Y APLICACIONES:**

- Establecer, proponer y mantener mecanismos de auditoría sobre las BBDD en producción que permitan el cumplimiento de la LOPDGDD y un mejor control de accesos a nivel de registro.
- Establecer mecanismos de auditoría de procesos de entrada de datos para garantizar la legitimación de los mismos, su correcta protección y/o legalización cuando proceda.
- Establecer mecanismos de auditoría de aplicaciones que permita la detección de debilidades de éstas respecto a posibles ataques o procesos relacionados de transmisión de datos a través de redes públicas. (incluyendo pentesting)

- Establecer mecanismos de auditoría y control de las comunicaciones.
- Proponer un sistema de auditoría de usuarios a nivel de red, sistema operativo, aplicaciones y sistemas basado en un modelo asumible para Mutua Intercomarcal e integrado dentro del SGSI.

#### **EN CUANTO A GESTION DE LA SEGURIDAD – ISO-27.000 – ISO 20.000: → ENS**

- Consultoría, Auditoria y soporte para certificar las auditorías internas o externas de seguimiento o renovación de la ISO 27000 y ENS
- Soporte para la elaboración de un plan anual de gestión de servicios, sistemas y comunicaciones (T.I. En general) y elaboración de los objetivos departamentales.
- Gestión y control en relación con los contratos con terceros y contratos internos relacionados con los sistemas anteriormente descritos (seguridad y gestión del servicio).
- Ampliación y mantenimiento de todos los indicadores necesarios para el control de los sistemas de gestión (tanto de proceso como de operación), así como las medidas y los procedimientos asociados.
- Seguimiento y mejora de la gestión, soporte y evolución del nivel de la gestión de problemas, articulando las vías adecuadas para su tratamiento, resolución, documentación y procedimiento.
- Seguimiento y mejora, mantenimiento, y colaboración con la Evaluación y Gestión del Riesgo en todas sus dimensiones (5 dimensiones).
- Seguimiento y mejora, mantenimiento de control de gestión de la disponibilidad de los activos de T.I. de forma alineada a los activos de negocio y directrices del plan estratégico de Mutua Intercomarcal.
- Seguimiento y mejora de la gestión, soporte e implantación de todos los procesos de renovación tecnológica y gestión del cambio tanto de hardware como de software en los temas relacionados con la seguridad.
- Seguimiento y mejora, soporte y control de la gestión de la configuración de todos los sistemas y aplicaciones.
- Seguimiento y mejora, soporte e implantación de la gestión del conocimiento para una correcta transferencia de lo mismo a los usuarios y gestores de TI.
- Seguimiento y mejora, soporte y evolución de la gestión de incidencias y peticiones de cambio, incluyendo los mecanismos de control asociados.
- Seguimiento y mejora, soporte y evolución de la gestión de la capacidad, integrado en mecanismos de monitorización y control, de las aplicaciones, de los servicios y de las infraestructuras.
- Seguimiento y mejora, soporte y evolución de la gestión de las relaciones con el negocio entre los servicios prestados como proveedor de servicios de la Organización.

- Seguimiento y mejora, soporte y evolución de la gestión de la entrega de servicios, infraestructuras, hardware o software, procedimientos, planificación acuerdos entre las partes y mecanismos de seguimiento y validación asociados.

## 2- DEFINICION DE PROCEDIMINETOS Y METODOLOGIA DE GESTION.

Definir y documentar de acuerdo con la realidad existente y los requisitos legales para Mutua Intercomarcal los siguientes aspectos:

- Metodología de Gestión del proyecto (Gestión de la Seguridad de la Información).
- Metodología de gestión de servicios de seguridad de la información.
- Definición de la Estructura Operativa para los servicios prestados a Mutua Intercomarcal.  
Estructura organizativa
- Modelo Operativo de seguridad de la información (gestión del proceso del cambio, resolución de problemas ...)
- Procedimientos de Escalados de incidencias de seguridad.
- Toma de requerimientos que contemplen todos los aspectos de seguridad en proyectos de desarrollo.

Definición, evolución y mantenimiento de políticas **de seguridad** de la Organización para la Gestión y Operación de los Sistemas de Información:

- Definición de políticas por entornos.
- Políticas de renovación de infraestructura Hardware.
- Políticas de entorno Infraestructura ofimática (AD, Correo, FileServer).
- Políticas de Infraestructura de comunicaciones LAN, WAN, SDH, Telefonía
- Políticas de Infraestructura de seguridad (seguridad perimetral, FW)
- Políticas de Copias de Seguridad
- Procedimientos de Contingencia menor (recuperación por entornos)
- Políticas de Informes de SLA
- Etc. ...

### 3 – CONDICIONES DE EJECUCIÓN.

Este servicio se llevará a cabo en las dependencias propias de Mutua Intercomarcal.

#### 3.1. Condiciones de ejecución básicas:

- Toda la documentación y resultados del proyecto tendrán que estar en lengua catalana y/o castellana.
- El Adjudicatario tendrá que demostrar su competencia en actividades parecidas, aportando referencias de servicios que esté prestando actualmente.

#### 3.2. Marco temporal del proyecto.

Fases y plazos máximos para la entrega de resultados:

Fase de transición del servicio	Siete días naturales después de la firma del contrato.
Fase de transformación/adequación	Catorce días naturales, después de finalizar la fase de transición.
Fase de operación	Resto del contrato, dependiendo de las posibles prórrogas.
Fase de entrega del servicio a nuevo proveedor si procede	15 días una vez finalizado el contrato.

#### 3.3. Equipo mínimo para la ejecución del contrato:

El adjudicatario tendrá que adscribir a la ejecución del contrato como mínimo los siguientes perfiles:

- 1 Consultor de Sistemas de Gestión de la Seguridad ISO 27000 y de ENS.
- 1 Delegado de Protección de Datos
- 1 Auditor Interno de ISO 27001 / ENS /LOPDGDD

Se valorará el grado de dedicación de personal a la seguridad de los servicios objeto de este contrato, así como su dedicación según sus funciones.

### **JORNADAS DE CONSULTORIA:**

- Trabajo de consultoría. (25 jornadas año)
- Trabajos de renovación de 27/ENS (7 jornadas)
- Realización Auditoría Interna. (8 jornadas)
- Participación en la auditoría Externa (7 jornadas)
- Consultoría sobre acciones correctivas y de mejora. (4 jornadas)

### **JORNADAS de DPD para atender todas las funciones propias del cargo:**

- Reunión mensual de seguimiento sobre estado y desarrollo de la LOPDGDD (12 jornadas).
- Ejercer como DPD de la Mutua Intercomarcal, esto es: Soporte a incidencias, supervisión y colaboración en análisis de impacto para nuevos tratamientos, ayudas jurídicas a reclamaciones y ejercicio de derechos de los interesados, defensa jurídica ante la Agencia, validación y control de auditorías internas de protección de datos, redacción de cláusulas de protección de datos en contratos y leyendas, supervisión y control de la parte jurídica de los incidentes de seguridad y comunicación de brechas a la AEPD, etc. ... (12 jornadas).

NOTA: (las jornadas serán consideradas de 8 horas)

### **3.4. Infraestructura necesaria para llevar a cabo el proyecto:**

- En el momento de la prestación del servicio el adjudicatario tendrá que aportar las licencias de renovación de las herramientas asociadas al servicio y cualquier otro componente o medio técnico necesario para la realización de los trabajos.
- Mutua Intercomarcal pondrá a disposición del adjudicatario aquella información que considere necesaria para el desarrollo del proyecto, y que el adjudicatario tendrá que haber solicitado previamente.

### **3.5. Descripción de la metodología a utilizar:**

- El adjudicatario tendrá que presentar la metodología que utilizará para desarrollar y hacer el seguimiento del proyecto.
- En la parte referente al seguimiento de la evolución del proyecto, independientemente de la metodología utilizada, el adjudicatario se tendrá que ajustar a los requerimientos de Mutua Intercomarcal.

### **3.6. Requerimientos de seguridad:**

- Confidencialidad, privacidad y publicidad del servicio o de la información.
- El adjudicatario está obligado a guardar secreto respecto 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 o privada, ningún tipo de información de los contenidos, entregables, evolución y progreso de este proyecto o actuaciones que sean llevadas a cabo, sin el consentimiento explícito, formal y por escrito de Mutua Intercomarcal.

#### **3.6.1 Propiedad intelectual:**

Toda la documentación que se genere a lo largo del servicio es propiedad exclusiva de Mutua Intercomarcal. El licitador no la podrá utilizar para otras finalidades sin el consentimiento expreso de Mutua Intercomarcal.

#### **3.6.2 Seguridad y protección de datos:**

El adjudicatario de los servicios se compromete a cumplir los requerimientos de seguridad y continuidad aplicables al objeto del contrato especificados en:

- La familia de normas ISO /IEC 27000, que ampara una implementación efectiva de la seguridad de la información.
  - ISO/IEC/UNE 27001, de gestión de seguridad de la información, adaptada a la estructura administrativa, personal y de entorno tecnológico de Mutua Intercomarcal y aplicada de forma proporcional a los riesgos reales.

- ISO/IEC/UNE 27002, de buenas prácticas y recomendaciones (controles) de la parte 2 de la norma 27001.
- **Real Decreto 311/2022 de 3 de mayo**, por el que se regula el Esquema Nacional de Seguridad.

Adicionalmente, el adjudicatario se compromete a:

- Cumplir con las directivas tecnológicas y de seguridad y calidad que establezca Mutua Intercomarcial.
- Implementar las medidas, procesos, y requerimientos que Mutua Intercomarcial solicite con esta finalidad y le propondrá los que considere necesarios para mejorar las soluciones.
- Facilitar toda aquella información que Mutua Intercomarcial requiera a fin de que éste pueda dar cumplimiento a la legislación y normativa referida en este apartado.

### **3.7. Facturación de los servicios:**

El servicio se facturará en cuotas mensuales vencidas en importes proporcionales al total.

MUTUA INTERCOMARCAL, dispone de una página web de proveedores, donde se deberán depositar las facturas en formato PDF, o en FACE.

## **4. DURACION DEL CONTRATO.**

El plazo de duración del contrato será de **un año**, contando a partir del día de la firma del contrato.

## **5. PRORROGAS.**

Este contrato podrá ser prorrogado por **1 + 1 (2) años adicionales**, facultativos para MUTUA INTERCOMARCAL y obligatoria para el adjudicatario.

## 6. PRESUPUESTO BASE LICITACIÓN.

- El precio máximo de licitación de este servicio es de .....**35.000 € + IVA**
- Valor estimado del contrato ..... **105.000 € + IVA**

## 7. REVISION DE PRECIOS.

- No procede

## 8. GARANTIA PROVISIONAL.

- No procede

## 9. GARANTIA DEFINITIVA.

- No procede

## 10. OBLIGACIONES ESPECÍFICAS DE LAS PARTES.

- El Adjudicatario, tiene la obligación de presentar un Plan de Trabajo o memoria técnica para evaluar su capacidad para llevar a cabo el proyecto.