PLIEGO DE CLÁUSULAS TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS INFORMÁTICOS RELACIONADOS CON EL CENTRO DE SOPORTE AL USUARIO (SAU), SOPORTE DE 1ER, 2º Y 3ER. NIVEL, ADMINISTRACIÓN DE SISTEMAS, GESTIÓN DE PROYECTOS EVOLUCIÓN, PARCHEADO Y MEJORAS DE SISTEMAS Y BBDD, Y SERVICIO DE GUARDIAS 24X7

CONTENIDO

1. OBJETIVO DEL SERVICIO

Implantación de servicios expertos de técnico de sistemas de Infraestructuras TIC y Seguridad de tercer nivel. La misión del servicio es administrar los sistemas virtualizados a nivel de hardware, storage, software y firmware de TIC's así como las redes e infraestructuras de red de comunicaciones que lo soportan. Aportar una visión experta a la implantación, mantenimiento de nuevas soluciones y herramientas de software y seguridad, generando una mejora continua de su eficacia respondiendo y potenciando la estrategia de la Mutua y la legislación vigente.

Servicio de soporte de atención al usuario de nivel 1, 2 y 3, dando respuesta remota y/o "in situ" a incidencias, peticiones de servicio y acciones periódicas de mantenimiento de sistemas y microinformática y sobre todas las aplicaciones en producción y desarrollo gestionadas por la organización y la Oficina de proyectos. Así como gestionando las alarmas y escalando posibles eventualidades de forma profesional y rigurosa. Gestión del inventario físico de elementos de TI. Coordinación entre la organización y terceros vinculados a proyectos o incidencias relacionadas con TI.

Gestión del Equipamiento de infraestructura hardware de la organización, gestión de inventario, resolución de averías e incidencias, gestión de garantías, almacenamiento, retirada y certificación de destrucción segura del material obsoleto.

Implantación de servicio de guardias 24x7x365 y monitorización de sistemas, con asistencia presencial, gestión de alarmas y evolución y mejora de las herramientas de colección de logs.

Colaboración en el desarrollo de nuevos proyectos tecnológicos aportando know how en todos los aspectos relevantes como arquitectura de sistemas, dimensionamiento, seguridad, etc ...

2. DESCRIPCIÓN DE LOS SERVICIOS

2.1 SERVICIO TÉCNICO EXPERTO EN INFRAESTRUCTURAS TIC Y SEGURIDAD

2.1.1 Condiciones de la jornada laboral:

Grupo de Soporte Remoto 5 días a la semana de 9 a 18h, con posibilidad de desplazamiento a dependencias de la organización, frente a respuesta de incidentes que lo requieran en un tiempo máximo de 2h durante toda la jornada laboral.
Posibilidad de desarrollar tareas de mantenimiento de sistemas fuera de la jornada laboral de forma esporádica, ya sea entre semana o fines de semana para evitar la parada del servicio. (servicios pactados fuera del presente contrato)

2.1.2 Solvencia Técnica profesional requerida:

- Técnico de sistemas experto con 10 años de experiencia en servicios de Ingeniero de sistemas y comunicaciones.
- Experto en seguridad redes y comunicaciones. (CCNA CISCO o similar)
- Conocimientos de Sistemas de Gestión de Seguridad de la Información y políticas de Seguridad. (ISO 27001)
- Conocimientos de Análisis forense digital.
- Conocimientos de Administración de Microsoft Security Administration.
- Conocimientos de Microsoft Azure
- Especialista en Veeam Backup.
- Conocimientos de Network security Firewall (Fortinet o similar)
- Conocimientos de Pentesting, (Nessus o similar)
- Conocimientos de EDR (Especialmente en FortiEMS)
- Conocimientos de Virtualización (Vmware y AHV Nutanix)
- Conocimientos de gestión y dimensionamiento de almacenamiento.
- Conocimientos de ITIL (ISO 20.000)
- Conocimientos de herramientas de tiqueting (Preferiblemente ProjectOffice)

Aquellas ofertas que no reúnan los requisitos mencionados, se considerará que no pueden acreditar los aspectos de solvencia técnica o profesional, por lo que serán excluidas.

2.1.3 Funciones del servicio:

- Implementar nuevas soluciones de infraestructuras y seguridad, realizando propuestas de forma proactiva.
- Integrar las aplicaciones en la metodología de trabajo de la organización
- Escalar el conocimiento mediante el desarrollo de manuales y procedimientos de los nuevos proyectos, en línea con las políticas de documentación de la organización.
- Mantener durante el desarrollo de su actividad, el nivel de riesgo de la organización por debajo del nivel de riesgo aceptado por la misma.
- Realizar la gestión de las Infraestructuras TIC, comunicaciones y *networking*, seguimiento, control y operación de dispositivos asociados.
- Realizar la recepción, seguimiento y gestión de incidencias, imputar horas trabajadas en el sistema de gestión de Incidencias de la Organización.
- Evaluar la gestión del cambio para los nuevos proyectos implantados. Dimensionamiento, afectación de sistemas relacionados, formación a técnicos o usuarios de la organización.
- Realizar la recepción, seguimiento y gestión de proyectos, así como imputar horas trabajadas en los diferentes proyectos en el sistema de gestión de proyectos propio de la organización
- Implementar documentación, manuales y procedimientos de los nuevos proyectos implantados, en línea con las políticas de documentación de la organización.
- Asistencia “in situ” cuando se requiera a todas las dependencias de la Organización.
- Mantener los equipos de la organización, correctamente dimensionados, configurados y actualizados.

- Implementar pruebas periódicas de *Pentesting* de seguridad. (Caja Negra/ Caja blanca)
- Colaborar con la concienciación en seguridad mediante ataques de simulación de suplantación de identidad. (phishing)
- Gestionar EDS de servidores y equipos finales.
- Mantener ultimas distribución y parches en sistemas operativos.
- Realizar el control y seguimiento de los procesos de copias de seguridad. Así como implementar optimización y gestión de calendarización de estas.
- Revisar periódicamente logs de aplicaciones y seguridad para evidenciar posibles riesgos.
- Colaborar en procesos de migración de infraestructuras de la organización incluso fuera del horario laboral, con el fin de garantizar la mínima afectación del servicio.
- Colaborar con las pruebas de implantación de nuevos sistemas, incluso fuera de horario laboral, con el fin de garantizar la mínima afectación del servicio.
- Realizar las medidas de los indicadores de calidad y de seguridad de la información asociadas al servicio.
- Colaborar de forma proactiva con los técnicos de nivel 2 y con el equipo de la organización.
- Colaborar con el responsable de Seguridad en la gestión de la Seguridad de la Información en la Organización. (Controles ISO 27001)
- El personal asociado al servicio adquirirá las funciones de oficina técnica y de calidad y ayudará al responsable de Infraestructuras y seguridad, así como a la Dirección de TI a desarrollar las estrategias de servicio del departamento.
- Reportar periódicamente al responsable de Infraestructuras, estado de la red, resultados de prueba de intrusión, monitorización y optimización proactiva de recursos.

2.2 SERVICIO DE SOPORTE DE ATENCION AL USUARIO NIVEL 1 y 2

2.2.1 Condiciones de la jornada laboral:

Recurso de soporte presencial en las instalaciones de la Organización, en horario de tardes de 9.30h a 18.30h, de lunes a viernes.

En caso de ausencia por periodo vacacional o enfermedad será substituido por una persona con un perfil de las mismas características.

2.2.2 Solvencia Técnica profesional requerida:

- Experiencia previa, mínima de 10 años, en soporte de sistemas informáticos Windows o Linux, diagnóstico análisis y resolución de problemas, preferiblemente en mutua de accidentes de trabajo.
- Conocimientos de Administración de servidores y EndPoints Microsoft.
- Conocimientos de Administración o gestión de usuarios en *Active Directory*
- Conocimientos en Telefonía IP (Asterisk)
- Conocimientos de Gestión e Integración de MDM
- Soluciones de *Printing*
- Gestión de Base de datos de inventario. (Linux)
- Conocimientos en redes y comunicaciones. (CCNA CISCO o similar)
- Conocimientos de herramientas de virtualización (*Vmware*)
- Conocimientos de Gestión de sistema de copias (Preferiblemente Veeam backup)
- Conocimientos de configuración de switches-routers.
- Conocimientos de Microinformática
- Conocimientos de ofimática de Microsoft (Office 365, Azure AD)
- Conocimientos de EDR
- Conocimientos de software antivirus.
- Conocimientos de cartelería digital
- Conocimientos de buenas practicas de gestión de controles de Seguridad, Norma ISO 27002.

2.2.3 Funciones del servicio:

- Aportar un soporte técnico informático de calidad a todo el personal de la organización.
- Realizar la recepción, seguimiento, categorización y gestión de incidencias de los usuarios de la organización en todas las sucursales de la organización, Sede Social y centro de contingencia, alineado con las buenas prácticas y los protocolos de comunicación y atención al usuario, establecidos en la organización (evitar el máximo el tiempo de espera al usuario, evitar el no contestar por falta de recurso o asistencia física en el lugar de atención, asistencia in situ cuando se requiera por parte de la organización...).
- Gestionar Peticiones de Servicio.
- Gestionar Actividades periódicas de Checklist
- Documentar Incidencias de Seguridad.
- Monitorizar el correcto funcionamiento de los dispositivos de la red.
- Las personas asociadas a este servicio tendrán el conocimiento necesario con el fin de poder dar de alta cualquier dispositivo nuevo que requiera monitorización, siempre que este dispositivo se interrogue con herramientas ya establecidas en el sistema de monitorización.
- Las personas asociadas a este servicio deberán ser capaces de mantener los grupos de aviso, así como los períodos de este y los medios para canalizar dichos avisos en el sistema implantado.
- Las personas asociadas al servicio serán capaces de mantener actualizada la BD con el fin de dar de baja aquellos dispositivos que lo sean y evitar en todo momento falsos positivos.
- Las personas asociadas al servicio recibirán y canalizarán las alarmas asociadas a su perfil y escalarán aquéllas que no tengan asignadas. Dispondrán de un mecanismo de visualización de dispositivos que permita gestionar de forma visual los sistemas.

- Fruto del registro de los datos en la herramienta de monitorización podrán emitir informes de cargas de utilización o de ocupación para prever futuras acciones.
- El sistema de monitorización guardará uno histórico con el fin de sacar datos sobre disponibilidad de los sistemas y para poder gestionar la capacidad de estos con interfaces que permitan una visualización fácil e interpretable de los resultados.
- El personal asociado al servicio deberá operar y gestionar las herramientas de colección de logs y las de explotación de estos, evolucionando los cuadros de mando asociados a la explotación de los datos recogidos.
- El sistema de cartelería digital se tratará como un cliente más y se incluirá en los mecanismos de gestión y monitorización de los sistemas.
- Gestionar altas, bajas, modificaciones de usuarios de Active Directory.
- Gestionar altas, bajas, modificaciones y licencias de usuarios de Office 365.
- Gestionar provisionamiento de usuarios de Azure AD hacia las aplicaciones integradas en la organización.
- Las personas asociadas al servicio gestionarán los dispositivos de seguridad perimetral y los limitadores de contenidos, filtros anti spam, IDS, EDR y demás elementos que componen la mencionada seguridad perimetral.
- Gestionar proyectos de implantación de aplicativos en colaboración con el responsable de Infraestructuras.
- Dar soporte a reuniones, video conferencias y ponencias vía telemática.
- Imputar horas trabajadas en el sistema de gestión de Incidencias de la Organización.
- Realizar la Interlocución y registro de incidencias escaladas a terceros fabricantes u operadoras y seguimiento de estas hasta su cierre.
- Realizar el seguimiento de proyectos, así como imputar horas trabajadas en los diferentes proyectos en el sistema de gestión de proyectos propio de la organización.

- Implementar documentación, manuales y procedimientos de los nuevos proyectos implantados, en línea con las políticas de documentación de la organización.
- Colaborar con la concienciación y formación a los usuarios en buenas prácticas globales, seguridad, sistemas, infraestructuras, de los equipos y redes.
- Mantener el parque informático de la organización actualizado, aplicando últimas distribuciones y parches en sistemas operativos de los usuarios finales.
- Mantener el aplicativo de MDM correctamente actualizado.
- Mantener el stock de material informático de la organización.
- Gestionar el stock y recambio de fungibles de impresoras departamentales de la organización.
- Gestionar garantías con fabricantes.
- Instalar nuevo software en los equipos finales.
- Colaborar de forma proactiva con los técnicos de nivel 3 y con el equipo de la organización, escalando la información requerida.
- Alimentar la Base de Datos de conocimiento de la organización con los procedimientos de aquellos procesos que se consideren más relevantes y que puedan aportar valor al servicio cuando se produzcan incidencias o peticiones relacionadas con dicha información.
- Realizar Análisis de cumplimiento de las tareas programadas.
- Realizar estadísticas mensuales de explotación de los servicios definidos en los SLA's. (de igual forma para RFC's)
- En caso de que las aplicaciones sufran procesos de cambio, las personas de soporte deberán formarse y adaptarse a la evolución tecnológica para poder desempeñar sus tareas.
- Las personas que prestan el servicio deberán mantener actualizado y controlado todo el stock de hardware y software de la Organización mediante una herramienta automática y la asociación de la misma en la CMDB de la Organización.

- Las personas asociadas al servicio tendrán que mantener un stock asignado en cada centro, así como el del repositorio central, con el fin de garantizar una operativa mínima en caso de avería en cada sito en la que den servicio.
- Las personas asociadas al servicio deberán mantener actualizada la información contenida en la CMDB en cuanto a los IC's que forman parte, incluyendo los datos administrativos (contrato de renting, finalización de garantías, service packs asociados y condiciones de los mismos).
- Las personas asignadas al servicio deberán mantener una BD de licencias con el fin de garantizar los requisitos legales en esta materia.
- El licitador brindará mecanismos para el control de los activos con el fin de acercarse a la gestión de una CMDB basada en las buenas prácticas de ITIL.
- Las personas asociadas al servicio gestionarán el "Portal Personal" de la Organización en cuanto a alta de usuarios, baja de usuarios y administración de permisos de acceso, pertenencia a grupos, etc ..., según las especificaciones del SGSI y las directrices de la dirección de T.I. de la Organización.
- El equipo deberá dar soporte presencial a actos institucionales (incluso fuera de las sedes de Mutua y en algunos casos en horario no laboral) con el fin de resolver cualquier incidencia durante el desarrollo del acto.

2.3 GESTIÓN DE LA INFRAESTRUCTURA DE HARDWARE.

2.3.1 Solvencia Técnica profesional requerida:

- Experiencia y conocimiento de gestión licenciamiento Microsoft y Google
- Experiencia en gestión de ciclo de vida de activos.
- Experiencia en gestión de garantías.
- Disponer de Certificación o capacidad de destrucción certificada de equipos y/o documentación confidencial.
- Gestión de monitorización de activos y servicios.

2.3.2 Funciones del servicio:

- Disponer del **servicio propio** de gestión y reparación de todo el equipamiento (hardware) con material y mano de obra incluida (incluyendo gestión de garantías).
- Disponer de un **servicio de substitución y depósito del hardware** en caso de retirada por avería de máquina.
- Las personas asignadas al servicio deberán mantener una BD de licencias con el fin de garantizar los requisitos legales en esta materia.
- Mantener actualizado y controlado todo el stock de hardware y software de la Organización.
- Las personas asociadas al servicio tendrán que controlar todos los movimientos de este hardware desde la llegada de este a la Organización hasta su baja por cualquier motivo al final de su vida útil. También tendrán que controlar su proceso de compra cuando así se les requiera
- Disponer de **servicios de retirada y destrucción certificada** de equipos obsoletos. (equipos y discos duros)
- El licitador establecerá unos circuitos adecuados con el fin de que la gestión de las peticiones de material se informe de forma adecuada a los receptores del servicio.

- El licitador establecerá mecanismos ágiles de comunicación para la gestión de llegada, retirada y/o traslado de material en los diversos centros y personas.
- El licitador brindará mecanismos para el control de los activos con el fin de acercarse a la gestión de una CMDB basada en las buenas prácticas de ITIL.

2.4 SERVICIO DE GUARDIAS 24X7 Y MONITORIZACIÓN DE SISTEMAS Y ALARMAS.

2.4.1 Condiciones de la jornada laboral:

Soporte Remoto 24x7, con posibilidad de desplazamiento a dependencias de la organización, frente a respuesta de incidentes que lo requieran en un tiempo máximo de 4 h.

2.4.2 Solvencia Técnica profesional requerida:

- Técnico de sistemas experto con más de 10 años como Ingeniero de Sistemas.
- Experto en seguridad redes y comunicaciones. (CCNA CISCO o similar)
- Conocimientos de Sistemas de Gestión de Seguridad de la Información y políticas de Seguridad. (ISO 27001)
- Conocimientos de Análisis forense digital.
- Conocimientos de Administración de Microsoft Security Administration.
- Conocimientos de Microsoft Azure
- Especialista en Veeam Backup.
- Conocimientos de Network security Firewall (Fortinet o similar)
- Conocimientos de Pentesting, (Nessus o similar)
- Conocimientos de EDR (FortiEMS)
- Conocimientos de Virtualización (Vmware)
- Conocimientos de gestión y dimensionamiento de almacenamiento.
- Conocimientos de ITIL (ISO 20.000)
- Conocimientos de herramientas de tiqueting (Preferiblemente ProjectOffice)
- Conocimientos de automatización y gestión de alarmas para el control de clima y humedad (Tecnología Schneider)
- Certificados de Ethical Hacking

2.4.3 Funciones del servicio:

- El personal asociado a este servicio recibirá las notificaciones de incidencias que proporcione el equipo de monitorización y asumirá las funciones correctivas fuera de las horas de actividad de Sistemas, (de 20:00h en 8:00 h), dará soporte en todo momento al equipo de personas de Sistemas con el fin de gestionar aquellas incidencias que, por su naturaleza o problemática, no sea posible resolver en horario laboral.
- Responder de forma proactiva a las incidencias que puedan surgir fuera del horario laboral, dando repuesta de las urgentes en un máximo de 60' y de las críticas en un máximo de 30'.
- Coordinar y colaborar en la solución de las posibles incidencias, junto al esponsable de Infraestructuras de la organización.
- Desplazarse en caso necesario a la Sede Social, CPD, o CPD de contingencias en un máximo de 3h desde el aviso, para solucionar o colaborar con la solución de las incidencias.
- Colaborar con el tramite o gestión de garantías en caso de substitución de equipos.
- Facilitar soporte técnico especializado, mediante un teléfono de contacto 24x7, al responsable de Infraestructuras de la organización.

2.5 BOLSA DE HORAS TECNICOS DE SISTEMAS DE NIVEL 3

2.5.1 Condiciones de la Jornada laboral

- Servicio remoto o presencial según proyecto requerido
- Bolsa de 100 horas anuales.

2.5.2 Solvencia Técnica profesional requerida:

- Técnico de sistemas experto con más de 10 años de experiencia en sistemas.
- Experto en seguridad redes y comunicaciones. (CCNA CISCO o similar)
- Conocimientos de Sistemas de Gestión de Seguridad de la Información y políticas de Seguridad. (ISO 27001)
- Conocimientos de Análisis forense digital.
- Conocimientos de Administración de Microsoft Security Administration.
- Conocimientos de Microsoft Azure
- Especialista en Veeam Backup.
- Conocimientos de Network security Firewall (Fortinet o similar)
- Conocimientos de Pentesting, (Nessus o similar)
- Conocimientos de EDR (FortiEMS)
- Conocimientos de Virtualización (Vmware)
- Conocimientos de gestión y dimensionamiento de almacenamiento.
- Conocimientos de ITIL (ISO 20.000)
- Conocimientos de herramientas de tiqueting (Preferiblemente ProjectOffice)
- Conocimientos de automatización y gestión de alarmas para el control de clima y humedad (Tecnología Schneider)
- Certificados de Ethical Hacking

El Adjudicatario deberá demostrar su competencia en actividades parecidas, aportando como mínimo 3 referencias de servicios que esté prestando actualmente.

Aquellas ofertas que no reúnan los requisitos mencionados, se considerará que no pueden acreditar los aspectos de solvencia técnica o profesional, por lo que serán excluidas.

2.5.3 Funciones del servicio:

- Implementar nuevas soluciones de infraestructuras y seguridad, realizando propuestas de forma proactiva.
- Integrar las aplicaciones en la metodología de trabajo de la organización
- Escalar el conocimiento mediante el desarrollo de manuales y procedimientos de los nuevos proyectos, en línea con las políticas de documentación de la organización.
- Mantener durante el desarrollo de su actividad, el nivel de riesgo de la organización por debajo del nivel de riesgo aceptado por la misma.
- Realizar la gestión de las Infraestructuras TIC, comunicaciones y *networking*, seguimiento, control y operación de dispositivos asociados.
- Realizar la recepción, seguimiento y gestión de incidencias, imputar horas trabajadas en el sistema de gestión de Incidencias de la Organización.
- Evaluar la gestión del cambio para los nuevos proyectos implantados. Dimensionamiento, afectación de sistemas relacionados, formación a técnicos o usuarios de la organización.
- Realizar la recepción, seguimiento y gestión de proyectos, así como imputar horas trabajadas en los diferentes proyectos en el sistema de gestión de proyectos propio de la organización
- Implementar documentación, manuales y procedimientos de los nuevos proyectos implantados, en línea con las políticas de documentación de la organización.
- Asistencia “in situ” cuando se requiera a todas las dependencias de la Organización.
- Mantener los equipos de la organización, correctamente dimensionados, configurados y actualizados.
- Implementar pruebas periódicas de *Pentesting* de seguridad. (Caja Negra/ Caja blanca)

- Colaborar con la concienciación en seguridad mediante ataques de simulación de suplantación de identidad. (phishing)
- Gestionar EDS de servidores y equipos finales.
- Mantener ultimas distribución y parches en sistemas operativos.
- Realizar el control y seguimiento de los procesos de copias de seguridad. Así como implementar optimización y gestión de calendarización de estas.
- Revisar periódicamente logs de aplicaciones y seguridad para evidenciar posibles riesgos.
- Colaborar en procesos de migración de infraestructuras de la organización incluso fuera del horario laboral, con el fin de garantizar la mínima afectación del servicio.
- Colaborar con las pruebas de implantación de nuevos sistemas, incluso fuera de horario laboral, con el fin de garantizar la mínima afectación del servicio.
- Realizar las medidas de los indicadores de calidad y de seguridad de la información asociadas al servicio.
- Colaborar de forma proactiva con los técnicos de nivel 2 y con el equipo de la organización.
- Colaborar con el responsable de Seguridad en la gestión de la Seguridad de la Información en la Organización. (Controles ISO 27002)
- El personal asociado al servicio adquirirá las funciones de oficina técnica y de calidad y ayudará al responsable de Infraestructuras y seguridad, así como a la Dirección de TI a desarrollar las estrategias de servicio del departamento.
- Reportar periódicamente al responsable de Infraestructuras, estado de la red, resultados de prueba de intrusión, monitorización y optimización proactiva de recursos.

3. PROCEDIMINETOS Y METODOLOGIA DE GESTIÓN:

- El licitador deberá realizar una descripción detallada de la Metodología de Gestión de la transición del servicio para garantizar la continuidad del servicio.
- El licitador deberá realizar una descripción detallada de la Metodología de gestión de los servicios a prestar.
- Definición de la Estructura Operativa que aplicará para el servicio a Mutua Intercomarcal.
    - Estructura organizativa
    - Modelo Operativo (gestión local, gestión remota, guardias ...)
    - Escalados y aprobaciones para peticiones, incidencias y problemas.
    - Escalados de seguridad
    - Toma de requerimientos

- Definición de los procedimientos operativos para la Gestión y Operación de los Sistemas de Información de Mutua Intercomarcal:
    - Definición de procedimientos por entornos.
    - Infraestructura Hardware
    - Entorno Infraestructura ofimática (AD, Correo, FileServer)
    - Infraestructura de comunicaciones LAN,WAN, SDH, Telefonía
    - Infraestructura de seguridad (seguridad perimetral, FW)
    - Copias de Seguridad, backup y recuperación.
    - Procedimientos de Contingencia menor (recuperación por entornos)
    - Informes de SLA.

4. CONDICIONES DE EJECUCIÓN.

Este servicio se llevará a cabo en las dependencias propias de Mutua Intercomarcal, pudiéndose realizar en remoto algunos de los servicios, como por ejemplo el de monitorización o el de soporte 24x7.

4.1 Condiciones de ejecución básicas

- Toda la documentación y resultados del proyecto deberán redactarse en lengua catalana y/o castellana.

4.2 Marco temporal del proyecto

Fases y plazos máximos para la entrega de servicios:

- Fase de transición del servicio: Quince días naturales, después de la firma del contrato.
- Fase de transformación/adecuación: Catorce días después de finalizar la fase de transición
- Fase de operación: Resto del contrato, dependiendo de las posibles prórrogas.
- Fase de devolución del servicio a un nuevo proveedor:
  15 días laborables post vencimiento del contrato.

4.3 Equipo mínimo para la ejecución del contrato

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

- 1 Jefe de Proyecto, responsable del servicio e interlocutor con Mutua Intercomarcal.
- Técnico de Sistemas de Nivel 1 y 2. (se requiere garantizar el servicio en periodos vacacionales o de baja por enfermedad)
- Grupo Técnico de Sistemas de Nivel 3. (pueden requerirse más de un técnico servicio + bolsa de horas de forma simultánea)
- Grupo Técnicos para el soporte 24x7x365 (Guardias)
- Infraestructura para la gestión de material, hardware y garantías.

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

4.4 Infraestructura y volumetría del proyecto

En el momento de la prestación del servicio el adjudicatario tendrá que aportar las licencias 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.

Con el fin de facilitar el dimensionamiento del servicio aportamos los siguientes datos:

▪ Nº de solicitudes de servicio Total atendidas en 2024 (tickets) por el Servicio de Atención al Usuario y sistemas : 7.263. (**2.104 atendidas por el servicio objeto del contrato**)

▪De las cuales han sido incidencias: 3.972. De ellas, **atendidas por el servicio objeto del contrato: 1.121 (18 de ellas atendidas por el servicio de guardias 24x7)**

▪De las cuales han sido RFCs: 3.291. De ellas, **atendidas por el servicio objeto del contrato: 983**

4.5 Nivel de servicio (SLA)

El adjudicatario debe presentar, como parte de la oferta, su mejor propuesta sobre los niveles de servicio a satisfacer, acordes con las necesidades a tal efecto de Mutua Intercomarcal.

Dicha propuesta de niveles de servicio debe contemplar los siguientes ANS (Acuerdos de Nivel de Servicio), para cada uno de los ámbitos del servicio: incidencias o RFC, en función de su nivel de criticidad (crítica, urgente y no urgente):

ANS	INCIDENCIAS		
HORARIO	No Urgente	Urgente	Crítica
9:00-18:30			
Respuesta:	8 horas	2 horas	45 minutos
Solución:	24 horas	8 horas	3 horas

ANS 24x7	INCIDENCIAS		
HORARIO	No Urgente	Urgente	Crítica
20:00-08:00			
Respuesta:	-	30 Minutos	15 Minutos
Solución:	-	8 horas	6 horas

ANS	RFC (peticiones)		
HORARIO	No Urgente	Urgente	Crítica
09:00-18:30			
Respuesta:	-	4 horas	30 minutos
Solución:	-	Planificada	24 horas

4.6 Descripción de la metodología de seguimiento del proyecto.

El licitador deberá presentar una descripción de la metodología que utilizará para desarrollar y hacer el seguimiento del proyecto.

En cuanto la adaptación a la evolución en T.I. liderada por Mutua Intercomarcal, el licitador, independientemente de la metodología utilizada, deberá ajustarse a los requerimientos de dicha evolución y ajustar el servicio a los cambios que se vayan produciendo sin deteriorar la calidad de este.

4.7 Requerimientos de seguridad

El licitador deberá manifestar su compromiso para preservar la confidencialidad, privacidad y no publicidad del servicio o de la información a la que se tenga acceso gracias a la prestación del servicio.

El adjudicatario está obligado a guardar secreto respecto 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 cualquiera 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 se sean llevados a cabo, sin el consentimiento explicito, formal y por escrito de Mutua Intercomarcal.

4.7.1 Propiedad intelectual

Toda la documentación, código o parametrización 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 como Mutua Intercomarcal.

4.7.2 Seguridad y protección de datos

El adjudicatario deberá acreditar disponer de la ISO 27001 (con un epígrafe concordante a los servicios relacionados con el presente contrato) y deberá presentar el documento de aplicabilidad referido en el epígrafe.

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

- Las normas ISO/IEC/UNE 27002 de mejores prácticas de seguridad de la información y ISO/IEC/UNE 27001 de gestión de la seguridad de la información, adaptadas en la estructura administrativa, personal y entorno tecnológico de Mutua Intercomarcal y aplicadas de forma proporcional a los riesgos reales.

Adicionalmente, 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 ésta pueda dar cumplimiento a la legislación y normativa referida en este apartado.
- El adjudicatario deberá cumplir con todo lo dispuesto en la Ley Orgánica de Protección de Datos y en la LSSICE, así como con todos los requisitos que se le

van a exigir de forma contractual como “Encargado del tratamiento” con acceso a los datos propiedad de Mutua Intercomarcal “Responsable del Tratamiento”.

4.8 Prestaciones superiores o complementarías en las exigidas (Mejoras)

Se valorará principalmente la propuesta de servicio que se adapte mejor a la naturaleza propia de las Mutuas colaboradoras con la Seguridad Social, sus funciones, herramientas y aplicaciones establecidas como válidas y las mejoras a aportar como resultado del proyecto.

4.9 Facturación de los servicios

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

En función del importe deberá utilizarse la plataforma FACE.

5. CRITERIO DE VALORACIÓN

En Anexo al pliego Administrativo.

46581544N
ANTONIO SERRA
(R:G60328796)
FIRMA

Digitally signed by 46581544N ANTONIO SERRA (R:G60328796) FIRMA
Date: 2025.02.18 13:23:52 +01'00'