PLIEGO DE CONDICIONES TECNICAS PARA LA RENOVACIÓN DE LAS INFRAESTRUCTURAS Y SISTEMAS OPERATIVOS DEL CPD PRINCIPAL DE MUTUA INTERCOMARCAL Y SERVICO DE MIGRACIÓN A LA NUEVA INFRAESTRUCTURA MEDIANTE CONTRATO DE RENTING

CONTENIDO

1. OBJETIVO DEL CONTRATO

El objetivo del presente contrato es el suministro, instalación y configuración de los elementos necesarios para llevar a cabo una sustitución total de la infraestructura de almacenamiento, cómputo y respaldo en el Centro de Procesamiento de Datos (CPD) principal de Mutua Intercomarcal de Barcelona.

Este contrato debe contemplar la migración de la actual infraestructura virtual al hardware y software objeto de este contrato.

Los objetivos de esta licitación son:

El detalle técnico de los materiales a suministrar, así como las acciones a realizar expuestas en este pliego, tendrán la consideración de requisitos mínimos (su incumplimiento será motivo de exclusión de la oferta).

Adicionalmente, se deberán contemplar todas las licencias necesarias para el correcto funcionamiento de la nueva infraestructura.

2. DESCRIPCIÓN DE LOS SERVICIOS E INFRAESTRUCTURA A SUMINISTRAR, INCORPORAR Y MIGRAR

Los objetivos principales del proyecto se pueden resumir de la siguiente manera:

- Actualización tecnológica del cómputo para el clúster de virtualización de producción.
- Adquisición de un nuevo sistema de almacenamiento empresarial con tecnología all-flash.
- Adquisición de un appliance de backup con características de seguridad avanzada.
- Proporcionar conectividad de 10Gb a los nuevos servidores de virtualización.
- Realizar la instalación, configuración y puesta en producción de la nueva plataforma.
- Despliegue de un nuevo entorno de backup para ofrecer inmutabilidad.
- Migración del entorno actual hacia el nuevo sistema de almacenamiento.
- Adquirir las licencias necesarias a nivel de VMware para la integración de los

nuevos servidores en el entorno productivo con capacidades de Alta Disponibilidad (HA).

- Adquirir licencias basadas en Microsoft Windows Server 2022 Datacenter.
- Ofrecer servicios de mantenimiento de la plataforma, tanto proactivos como reactivos, durante toda la duración del contrato. El soporte de la plataforma debe tener una duración de 4 años.
- Formar al equipo actual de la Organización sobre las nuevas tecnologías implantadas, mínimo 4 jornadas.

3. EQUIPAMIENTO REQUERIDO

3.1 PLATAFORMA VIRTUALIZACIÓN

Se requiere configurar un nuevo clúster de virtualización compuesto por 3 nodos para migrar toda la infraestructura virtual existente. Cada nodo debe incorporar, como mínimo, los siguientes componentes de hardware:

Requisitos de hardware genéricos por nodo:

- Servidor de 19" con una altura máxima de 1U.
- Doble procesador.
- 24 núcleos físicos (cores) con una velocidad mínima de 2,00 GHz basados en la tecnología Intel Sapphire Rapid.
- 512GB de memoria RAM DDR5.
- 2 puertos de red a 10Gb SFP+ en el slot OCP3.
- 2 puertos externos SAS de 12Gb/s en el slot PCIe.
- 1 puerto de 1GbE para la gestión remota del servidor.
- Fuente de alimentación redundante de 800W hot-plug.
- Almacenamiento para el sistema de arranque (boot) en RAID1, compuesto por dos (2) discos M.2 dedicados, con un tamaño mínimo de 480GB.
- Kit de integración en el armario rack.
- El cableado necesario para interconectar el equipo.
- Licencia para la gestión remota con funcionalidades avanzadas.
- Soporte del fabricante durante 3 años en modalidad NBD (Next Business Day).

Los nuevos servidores deben disponer de un sistema de monitorización 24x7 único con soporte técnico del fabricante a través de HTTPS.SADS

Aquí se detallan las especificaciones relacionadas con el soporte, la monitorización y la seguridad de los servidores: Este sistema debe ser accesible para el personal de IT de Mutua Intercomarcal.

- **Repositorio de firmware y drivers:** Cada servidor debe mantener un repositorio local de versiones de firmware y controladores que permita restablecer niveles de firmware seguros o aplicar parches en caso de riesgo potencial. También debe ser posible restaurar directamente al nivel de firmware cargado y probado en fábrica.
- **Gestión remota del sistema:** Cada servidor debe ofrecer un sistema/controladora de gestión remota del sistema integrada en el equipo con redirección gráfica independiente de las CPU de producción. Debe incluir software de consola de KVM virtual con las siguientes características:
    - Gestión a través de una interfaz web.
    - Capacidad para compartir hasta 6 sesiones simultáneas para tareas colaborativas en el servidor.
    - Seguridad basada en roles que admita autenticación de dos factores.
    - Lista de componentes del servidor y descripción de su estado.
    - Acceso remoto al estado y registros integrados del servidor.
    - Regulación dinámica de la energía del servidor.
    - Gráficos en 3D de la temperatura de las partes del servidor.
    - Montaje remoto de carpetas, CD, DVD, disquetes, USB, etc.
    - Carga de imágenes del sistema operativo.
    - Apagado y encendidos remotos del servidor, independientemente del sistema operativo.
    - Soporte para la monitorización SNMP sin necesidad de agentes en el sistema operativo.
    - Envío de eventos a un servidor syslog.
    - Sincronización NTP.
    - Soporte para la automatización mediante una API Rest conforme con Redfish.
- **Tarjeta de gestión:** La tarjeta de gestión (y el software asociado) debe venir activada y completamente operativa para cada nodo. El servidor debe contar con un puerto dedicado de 1GbT RJ45 para este propósito.
- **Seguridad de firmware:** Para mejorar la seguridad del equipo y prevenir ataques a través de firmware modificado, el chip de gestión debe tener una huella digital

inmutable incrustada en el silicio, lo que impide el arranque a menos que la clave digital del firmware crítico coincida con la huella digital incrustada en el silicio. Esta tecnología debe ser proporcionada por el fabricante del servidor y no puede basarse en soluciones de terceros.

- **Validación periódica de firmware:** El sistema, durante su operación, debe realizar una validación periódica de los niveles de firmware en busca de código comprometido. En caso de una infracción, se llevará a cabo una restauración automática a un estado de confianza conocido. Esta capacidad de restauración automática debe incluir al menos los componentes esenciales de firmware del servidor: chip de gestión, UEFI, dispositivos lógicos programables simples (SPLDs), management engine (ME) e innovation engine (IE).
- **Bloqueo de configuración:** Para evitar la alteración no deseada de la configuración del hardware del servidor, se debe bloquear su estado, de manera que se monitoree y se emitan alertas en caso de un cambio en la configuración del servidor. Deben detectarse cambios en al menos los siguientes elementos: DIMMs de memoria, procesadores, dispositivos PCIe, configuraciones en el estado de seguridad del servidor y errores de autenticación para deshabilitar esta funcionalidad.
- **Borrado seguro de discos y memoria NAND:** Los servidores deben incorporar un sistema de borrado seguro de discos y memoria NAND para que puedan restablecerse a un estado inicial garantizando que todos los datos almacenados se eliminen por completo.
- **Designación de producto "Cyber CatalystSM":** Los servidores propuestos deben contar con la designación de producto "Cyber CatalystSM" según el programa "Cyber CatalystSM by Marsh" (https://www.marsh.com/us/campaigns/cyber-catalyst-by-marsh.html). (La designación "Cyber CatalystSM" dentro del programa "Cyber Catalyst by Marsh" indica que ciertos productos y servicios de seguridad han sido identificados por las principales aseguradoras del mercado como efectivos para reducir el riesgo cibernético. Las organizaciones que adoptan estas soluciones pueden ser consideradas para recibir términos y condiciones mejorados en las pólizas de seguro cibernético.)

3.2 CABINA DE ALMACENAMIENTO PRIMARIO

A continuación, se describen las especificaciones para la cabina de almacenamiento primario que se requiere:

- **Capacidad:** Se requiere un sistema de almacenamiento basado en tecnología all-flash, para garantizar un rendimiento óptimo en los servicios corporativos de Mutua

Intercomarcal con una capacidad neta de almacenamiento en SSD mínima de 34TB (sin contar con técnicas de reducción de datos).

- **Disponibilidad y Tolerancia a Fallos:**
  - El sistema de almacenamiento debe incluir al menos 2 controladoras con acceso en modo bloque.
  - La conectividad del nuevo almacenamiento será de tipo 12Gb/s SAS.
  - El sistema debe proporcionar doble camino de acceso al almacenamiento desde los servidores para garantizar alta disponibilidad en el sistema.
  - El sistema RAID debe permitir la falla de 2 discos de forma simultánea sin afectar la integridad de los datos.
  - El sistema RAID debe incorporar 2 discos en modo de repuesto integrados y con la posibilidad de ampliar la cantidad si es necesario.
  - El sistema debe ser capaz de soportar la falla de una controladora sin afectar el entorno productivo.
  - En caso de fallo en la alimentación, el sistema debe contar con un sistema de protección para garantizar la integridad de la información.
  - Las actualizaciones de firmware deben poder realizarse en caliente sin interrupción del servicio.

- **Escalabilidad y Rendimiento:**
  - El sistema debe permitir la ampliación de la capacidad mediante la adición de nuevos discos o boxs.
  - La cabina debe permitir el cambio en caliente de las controladoras.
  - Cada controladora debe incluir al menos 4 puertos SAS a 12Gb/s.
  - El sistema debe tener la capacidad de agregar discos de diferentes tecnologías (SAS, SATA) para cubrir posibles necesidades futuras.
  - El sistema debe permitir la posibilidad de *tiering* automático, lo que implica la capacidad de mover datos automáticamente entre diferentes niveles de almacenamiento según su uso y necesidades de rendimiento.

- **Integración.**
  - En cuanto a la integración, el nuevo sistema de almacenamiento debe ser compatible con los sistemas operativos líderes de la industria, que incluyen:
    - Microsoft Windows Server 2016, 2019 y 2022.

        - VMWare, incluyendo la versión vSphere 8.0.
    - Además, el nuevo sistema de almacenamiento debe proporcionar capacidades de integración con el sistema de virtualización actual (VMWare vSphere) ofreciendo las siguientes funcionalidades:
        - VASA (vSphere Storage APIs for Storage Awareness): Esto permite una mayor visibilidad y control de los recursos de almacenamiento en el entorno de virtualización.
        - VAAI (vStorage APIs for Array Integration): Proporciona una mayor eficiencia en las operaciones de almacenamiento, permitiendo que las tareas de almacenamiento sean realizadas directamente por el almacenamiento subyacente.
        - SRM (Site Recovery Manager): Esta funcionalidad está relacionada con la recuperación ante desastres y la migración de máquinas virtuales entre sitios, lo que es fundamental para la continuidad del negocio y la gestión de la recuperación de datos en caso de fallos.

- **Soporte y Monitorización:** En cuanto al soporte y monitorización del sistema de almacenamiento propuesto, se consideran los siguientes aspectos:
    - Se valorará que el sistema de almacenamiento propuesto disponga de una herramienta de monitorización para supervisar el rendimiento del sistema en tiempo real.
    - Se valorará que cuente con una herramienta de alertas para prevenir que los administradores deban estar pendientes de posibles problemas, como fallos de hardware o pérdida de conexión.
    - Todas las funcionalidades requeridas deben estar licenciadas de forma independiente del número de discos o terabytes, de manera que cualquier ampliación no suponga un aumento de costos.
    - La garantía del almacenamiento, software y licencias mínima será de 24x7 durante 3 años. Durante este período, el fabricante se compromete a realizar reparaciones en caso de avería y a reemplazar el material propuesto para el correcto funcionamiento del sistema sin costos adicionales.
    - El adjudicatario debe garantizar que el equipo propuesto no quedará obsoleto por parte del fabricante durante al menos los próximos 5 años.
    - El adjudicatario debe contar con un equipo técnico de soporte in situ autorizado por el fabricante en Barcelona o su área metropolitana.
    - El adjudicatario debe ser un Servicio Técnico Oficial del fabricante para

poder realizar los servicios de instalación y proporcionar el mantenimiento postventa in situ según los Acuerdos de Nivel de Servicio (SLAs) acordados.

- Los servicios de implementación de la cabina deben ser realizados por técnicos certificados por el fabricante, además, el fabricante validará la correcta instalación del nuevo sistema y emitirá un certificado de implementación exitosa.

- **Protección de datos y eficiencia:** En lo que respecta a la protección de datos y la eficiencia, se requiere que el sistema de almacenamiento cumpla con las siguientes características:
  - El sistema debe admitir copias físicas consistentes (clones).
  - El sistema debe permitir la creación de copias virtuales de LUN consistentes (snapshots). (Los snapshots son instantáneas del estado de los datos en un momento dado y deben ser consistentes y confiables.)
  - El sistema debe ser capaz de replicar volúmenes a otro sistema con las mismas características y garantizar la consistencia de los datos. Esto es fundamental para la alta disponibilidad y la recuperación ante desastres.
  - La cabina de almacenamiento debe permitir la recuperación del espacio asignado una vez que se elimina el contenido (storage reclaim). Esto implica la capacidad de liberar espacio que no se está utilizando de manera eficiente.
  - El sistema de almacenamiento debe admitir técnicas de reducción de datos en línea, como Thin Provisioning. (Thin Provisioning permite asignar espacio de almacenamiento de manera eficiente, asignando solo el espacio físico necesario a medida que los datos se escriben, lo que ayuda a optimizar el uso de recursos de almacenamiento)

Estas características contribuyen tanto a la protección de datos como a la eficiencia en el uso de la capacidad de almacenamiento.

3.3 NUEVA PLATAFORMA DE BACKUP

El Sistema de almacenamiento de backup empresarial debe cumplir con las siguientes características técnicas:

- **Requerimientos Generales de la Controladora Base:**
  - Mínimo de dos (2) CPU AMD con 8 núcleos cada una.
  - Mínimo de 512GB de RAM, tipo DDR4-3200.

- Mínimo de dos (2) puertos de 10/25Gb Ethernet (PCIe).
- Mínimo de dos (2) puertos de 1/10GBase-T Ethernet (integrados en placa).
- Mínimo de dos (2) discos dedicados para contener el sistema operativo.

- **Características Generales del Sistema de Almacenamiento:**
  - Debe admitir el etiquetado de VLAN.
  - Debe admitir la agregación de puertos (port bonding) en los puertos IP del mismo tipo.
  - Debe ofrecer un mínimo de 80TB de espacio local bruto (RAW), distribuido en discos de 8TB.
  - Debe ser escalable hasta al menos 250TB de espacio local bruto (RAW).
  - Debe ser escalable hasta al menos 200TB de capacidad neta local y aproximadamente 400TB adicionales de capacidad neta utilizando almacenamiento en la nube, como AWS, Azure o un objeto de almacenamiento S3. (La capacidad neta local se define como el resultado de restar la capacidad bruta local del sistema (RAW) menos el espacio necesario para la implementación de la protección de la información, que incluye grupos de RAID y discos de hot spare. No se aplica ninguna técnica de ahorro de disco, como la deduplicación o la compresión, en el cálculo del espacio local. La capacidad externa que se pueda consumir en un entorno de nube pública o privada no se considera en el cálculo del espacio local.)

- **Arquitectura de Almacenamiento:**
  - Debe tener una única capa de almacenamiento local activa para operar con los datos. No se permiten configuraciones con movimiento interno o archivo de información a una capa secundaria de disco dentro del almacenamiento local del mismo repositorio.

- **Rendimiento:**
  - Debe ofrecer un rendimiento sostenido de escritura de al menos 25TB por hora.

- **Licencias:**
  - Debe incorporar todas las licencias necesarias para implementar las funcionalidades de deduplicación/compresión y réplica optimizada, permitiendo la transmisión de bloques únicos no duplicados.

- **Eficiencia del almacenamiento de las copias de seguridad:** En cuanto a la eficiencia del almacenamiento de copias de seguridad, se requiere que el sistema cumpla con las siguientes características:
    - El sistema debe integrar un motor de deduplicación obligatoriamente en línea, lo que significa que optimiza el espacio antes de escribir en los discos físicos. No se permiten dispositivos que utilicen deduplicación en un proceso posterior.
    - El algoritmo de deduplicación debe ser capaz de trabajar con tamaños de bloque variables en los datos de copia de seguridad de forma obligatoria. Esto permite reconocer un mayor número de patrones repetidos y garantizar la máxima eficiencia en la transmisión y el almacenamiento de datos en el mismo repositorio.
    - Además de la deduplicación, el sistema debe integrar obligatoriamente la compresión en línea de los datos, es decir, antes de escribir en los discos físicos. No se permiten dispositivos que utilicen compresión en un proceso posterior.

  Estas características aseguran una alta eficiencia en la optimización del espacio de almacenamiento y la reducción del espacio necesario para almacenar las copias de seguridad. La deduplicación y la compresión in-line garantizan que los datos se almacenen de la manera más eficiente posible en el repositorio de copias de seguridad.

- **Protección de la información y seguridad:** En lo que respecta a la protección de la información y la seguridad, el sistema propuesto debe cumplir con las siguientes características:
    - El sistema debe proteger los datos mediante un RAID 6 hardware, que estará configurado de fábrica y no requerirá manipulaciones adicionales durante la fase de instalación. En caso de necesidad de escalar el tamaño, se incorporarán discos en grupos RAID 6 adicionales.
    - Adicionalmente, el sistema debe incorporar al menos un (1) disco en el rol de hot spare por cada grupo RAID.
    - Debe disponer de mecanismos de revisión y verificación continuos durante la ingesta de la información, y periódicamente, sobre los datos ya almacenados para asegurar la consistencia de la información.
    - Debe admitir la funcionalidad de encriptación de datos en reposo (data-at-rest encryption), que cumpla con la validación FIPS 140-2. El cifrado de los datos debe realizarse después del procedimiento de deduplicación y puede

ejecutarse en la totalidad del repositorio o en volúmenes parciales.

- Adicionalmente, debe admitir la funcionalidad de Secure Erase, con el objetivo de garantizar que los datos no puedan ser recuperados de manera no autorizada. Debe cumplir con NIST SP800-88 y realizar un mínimo de siete (7) sobreescrituras aleatorias.
- Debe incluir mecanismos de seguridad para garantizar la protección total contra ataques de ransomware y otros malware.
- Estas características aseguran que los datos almacenados estén protegidos tanto en términos de integridad como de confidencialidad y que el sistema esté preparado para hacer frente a amenazas de seguridad, incluyendo la encriptación de datos, la destrucción segura de información y la prevención de ataques de malware.
- El sistema requerirá un sistema de autorización dual mediante un usuario específico de seguridad para validar la ejecución o no de las operaciones críticas sobre el sistema. Esto incluye la capacidad de modificar y/o eliminar un volumen, todo el almacenamiento, realizar cambios en la fecha/hora y desactivar la funcionalidad de autorización dual. La autorización dual es un proceso de seguridad que requiere la aprobación de al menos dos usuarios autorizados antes de llevar a cabo acciones críticas.
- El sistema deberá permitir la configuración de un período de inmutabilidad, al menos a nivel de volumen. La inmutabilidad se refiere a la incapacidad de cambiar o eliminar datos durante un período de tiempo especificado, lo que garantiza la preservación de los datos en su estado original durante ese tiempo.

Estas características aseguran que los datos almacenados estén protegidos tanto en términos de integridad como de confidencialidad y que el sistema esté preparado para hacer frente a amenazas de seguridad, incluyendo la encriptación de datos, la destrucción segura de información y la prevención de ataques de malware.

- **Tipos de acceso.** En cuanto a los tipos de acceso y funcionalidades que se requieren del sistema de almacenamiento de backup, se deben cumplir las siguientes especificaciones:
  - El sistema propuesto debe admitir acceso VTL FC (Fibre Channel), VTL iSCSI, NFS exports y SMB shares como repositorios de backup, con acceso concurrente para cada uno de ellos.
  - Debe ser capaz de emular al menos los formatos de cintas LTO-5, LTO-6 y

LTO-7.

- Debe tener la capacidad de configurar al menos una combinación de 64 bibliotecas de cintas y objetivos NAS, junto con 100,000 o más ranuras de cartuchos en un solo dispositivo.
- Debe tener inteligencia para comprender tanto la deduplicación basada en origen como en destino y debe integrarse con el software de backup en producción, como Veeam Backup & Replication.
- Además, debe estar certificado para trabajar con otros principales proveedores del mercado, como CommVault, Zerto y otros, además del software de backup actual.
- Se valorará positivamente si el dispositivo también dispone de software o complementos para realizar copias directas (sin software de copia de seguridad) desde Oracle RMAN, SQL Server y SAP HANA.
- El dispositivo propuesto debe ser capaz de ofrecer su almacenamiento de forma directa e integrada a las aplicaciones de backup, optimizando las transferencias de datos y eliminando la necesidad de utilizar modos VTL o NAS. Se requiere la integración de esta funcionalidad con el software de backup actualmente en producción en Mutua Intercomarcal. Esta capacidad permitirá realizar tareas de deduplicación en origen utilizando el mismo algoritmo implementado en el dispositivo de disco.
- Para el software de backup actualmente implementado en Mutua Intercomarcal (Veeam), se deben incorporar las siguientes integraciones:
    - Capacidad para realizar copias virtuales sintéticas integradas con la cabina, lo que agiliza los procesos de backup sintético y reduce la necesidad de leer nuevamente los backups completos e incrementales.
    - Integración de las funcionalidades de Instant Recovery, recuperación de archivos y recuperación de elementos de aplicaciones a través de Veeam Explorers para lograr una recuperación más rápida y eficiente.
    - Posibilidad de configurar una tarea de tipo "Backup Copy Job" que los dispositivos de copias comprenderán y realizarán de forma autónoma.

Estas especificaciones aseguran una flexibilidad y versatilidad en las operaciones de backup, así como la capacidad de trabajar con una variedad de formatos y aplicaciones de backup para garantizar la eficiencia y la capacidad de recuperación de datos.

- **Monitorización y Gestión Remota.** En cuanto a la monitorización y gestión remota del sistema propuesto, se deben cumplir las siguientes especificaciones
    - El sistema propuesto debe admitir la monitorización local y en la nube, que muestre información sobre:
        - Licencias
        - Configuración detallada del hardware instalado
        - Información global y parcial sobre la capacidad actual, eficiencia de almacenamiento por volumen de datos y predicción automática de la capacidad futura del sistema.
        - También debe proporcionar una lista de casos abiertos con soporte (solo en la nube) y notificaciones de actualizaciones disponibles para el sistema (solo en la nube).
    - Debe ser integrable en una plataforma de monitorización basada en el protocolo SNMP.
    - Debe ofrecer una interfaz gráfica de usuario (GUI) que permita una gestión cómoda y que también tenga la capacidad de gestionar otros dispositivos del mismo tipo (si existen).
    - Además, desde la GUI del sistema propuesto, debe poder mostrar información agregada de los demás sistemas de backup con el mismo sistema operativo o superior en el entorno.
    - Debe incluir una herramienta de gestión, monitorización y generación de informes integrada en un procesador dedicado (ASIC) dentro de la placa base del equipo.
        - El acceso se realizará mediante un puerto 1GBase-T dedicado (OOBM, fuera de banda) y proporcionará una API REST de gestión de acuerdo con la especificación Redfish DMTF.
        - Debe cumplir con estándares de seguridad como FIPS 140-2, CNSA, SSL/TLS de 256 bits y autenticación en dos factores (2FA).
        - Debe admitir alertas de componentes críticos de hardware, como CPU, memoria y disco, y tener funcionalidad de actualización de firmware.

Estas especificaciones garantizan una monitorización efectiva y una gestión remota del sistema, lo que facilita el mantenimiento y el diagnóstico de problemas, y permite tomar decisiones basadas en datos precisos y actualizados sobre el estado del sistema y la capacidad futura. La integración con protocolo SNMP

facilita la interoperabilidad con otras soluciones de gestión de la red.

Para facilitar la instalación, mantenimiento y diagnóstico de incidencias durante el período de garantía, es un requisito que los servidores y el almacenamiento sean del mismo fabricante.

4. LICENCIAS Y SOFTWARE

En cuanto a las licencias de software requeridas, se necesitan las siguientes:

4.1 Plataforma de Virtualización (VMWare vSphere ESXi)

- Licencia nueva con soporte de 3 años para el producto.
    - vSphere Essentials Plus Kit.

4.2 Sistemas Operativos de Servidores (MS Windows Server 2022)

- Se requieren nuevas licencias de Windows Server 2022 Datacenter para poder implementar un número ilimitado de máquinas virtuales, cubriendo todos los núcleos físicos de los equipos ofrecidos.
- Además, se deben contemplar licencias de CAL (Licencias de Acceso de Cliente) de Windows Server 2022 para accesos de usuario.

5. INSTALACIÓN Y CONFIGURACIÓN

La oferta debe incluir los siguientes elementos relacionados con la instalación y configuración del proyecto

- Instalación de la nueva infraestructura (servidores, almacenamiento...) en un rack de servidores.
- Actualización del firmware, instalación y configuración del sistema operativo hipervisor en los nuevos servidores.
- Instalación y configuración del nuevo sistema de almacenamiento primario.
- Implementación y configuración del nuevo servidor vCenter en formato appliance.
- Configuración del clúster vSphere y licenciamiento del mismo.
- Despliegue y configuración del nuevo dispositivo de backup.
- Instalación de la última versión disponible de Veeam Backup, configuración y verificación del correcto funcionamiento.
- Realización de las tareas necesarias para la seguridad del entorno de backup

(consolas de Veeam, repositorios de backup, entre otros).

- Migración de datos y servicios al nuevo entorno.
- Limpieza de todo el cableado reemplazado durante las operaciones descritas.
- Gestión de las licencias y provisión de estas durante la ejecución del proyecto.
- Documentación detallada relacionada con todos los cambios mencionados, incluyendo todas las configuraciones aplicadas para poder gestionar todos los elementos posteriormente.

El proceso de instalación y configuración se llevará a cabo según las directrices del responsable de sistemas de Mutua Intercomarcal y siempre por personal calificado, técnicos e ingenieros de sistemas y redes certificados por los fabricantes involucrados en el proyecto.

Las ofertas deben incluir un cronograma que contemple todas las actividades previstas y la posible afectación de cada una de ellas.

Las tareas que puedan afectar el trabajo diario de los usuarios se llevarán a cabo en fechas y horas acordadas con el personal de IT de Mutua Intercomarcal. Del mismo modo, todas las tareas a realizar se programarán teniendo en cuenta el objetivo de minimizar al máximo el impacto en los usuarios y preservar la información existente.

En cuanto a los elementos de seguridad perimetral y acceso remoto, Mutua Intercomarcal acordará con el adjudicatario el método apropiado de soporte remoto, de acuerdo con la tecnología disponible en el momento de la ejecución.

6. FORMACIÓN Y CAPACITACIÓN AL PERSONAL DE SISTEMAS DE LA ORGANIZACIÓN

Para lograr garantizar una comprensión adecuada y una gestión efectiva de la nueva tecnología implementada es crucial proporcionar formación y capacitación al personal técnico de la organización. Se deberán garantizar un mínimo de 4 jornadas presenciales de formación. Dicha formación garantizará:

- La adopción efectiva de la nueva tecnología: La formación ayuda a los empleados a comprender cómo utilizar y administrar la nueva solución de manera efectiva. Esto asegura que puedan sacar el máximo provecho de las capacidades de la tecnología.

- Prevención de errores: Un personal bien capacitado es menos propenso a cometer errores en la configuración, administración y uso de la tecnología, lo que puede reducir el riesgo de problemas y fallos.
- Optimización del rendimiento: La capacitación permite a los técnicos aprender cómo optimizar la solución para el mejor rendimiento y eficiencia posibles, lo que puede ahorrar tiempo y recursos.
- Gestión de problemas: Con la capacitación adecuada, los técnicos pueden diagnosticar y resolver problemas más rápidamente, minimizando el tiempo de inactividad y garantizando un funcionamiento fluido del sistema.
- Seguridad: La capacitación también puede incluir pautas y mejores prácticas de seguridad, lo que es fundamental en la protección de datos y activos críticos.
- Actualización de habilidades: La capacitación continua ayuda a mantener actualizadas las habilidades y conocimientos del personal técnico.
- Gestión del cambio: La implementación de nuevas soluciones puede generar resistencia al cambio. La formación puede ayudar a superar esta resistencia y fomentar una transición más suave.

7. TERMINOS DE EJECUCIÓN

El plazo de ejecución del contrato será de un máximo de 3 meses a partir de la fecha de notificación de la adjudicación, de acuerdo con el calendario que se establezca por parte de Mutua Intercomarcal.

8. PLAZO DE GARANTIA

Todo el hardware incluido en la propuesta tendrá una garantía mínima de 4 años proporcionada por el fabricante, que incluirá cobertura total para piezas de repuesto, mano de obra y desplazamiento.

Todo el material debe ser adquirido directamente al fabricante del país de instalación a través del canal oficial de distribución. Además, el fabricante del país de instalación debe brindar soporte oficial en garantía para el hardware.

9. REQUERIMIENTOS DE SEGURIDAD Y PROTECCIÓN DE DATOS.

9.1 Requerimientos de seguridad y privacidad

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

9.1.1 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.

9.1.2 Seguridad y protección de datos

Se valorará 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:

- 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.
- 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 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 de los ficheros”.

9.1.3 Solvencia Técnica profesional requerida:

- Certificación Partner de fabricante:
  - Gold Partner o equivalente del fabricante.
  - Aruba: Platinum Partner (por temas de integración)
  - VMware: Select Partner (por temas de integración)
  - Veeam: Gold Partner (por temas de integración)

- Jefe de Proyecto:
  - Project Management Professional (PMP)
  - ITIL Managing Professional v4

- Ingeniero de Sistemas:
  - VMware: VMware Certified Professional DCV

10. PROCEDIMIENTOS Y METODOLOGIA DE GESTIÓN:

- El licitador deberá realizar una descripción detallada de la Metodología de Gestión del proyecto de transición. (captación del servicio).
- El licitador deberá realizar una descripción detallada de la Metodología de gestión de los servicios a prestar.
- El licitador deberá definir 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 e incidencias
  - Escalados de seguridad
  - Toma de requerimientos

10.1 Condiciones de ejecución básicas

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

10.2 Marco temporal del proyecto

Fase de Suministro	6 semanas
Fase de Implantación / Configuración	1 semana tras la fase de suministro
Fase de Migración	2 semanas tras la fase de Implantación
Fase de Formación	1 semana tras la fase de migración

Fases y plazos máximos para la entrega de resultados:

- Fase de suministro: De 6 semanas tras finalizar la fase de transición
- Fase de implantación - Configuración: 1 semanas tras la fase de suministro
- Fase de migración: 2 Semanas tras la fase de Implantación
- Fase de formación: 1 Semana tras la fase de Migración, in situ.

10.3 Equipo mínimo para la ejecución del contrato

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

- 1 Project Manager
- 1 ingeniero de Sistemas
- 1 Account manager

10.4 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.

10.5 Descripción de la metodología de seguimiento del proyecto.

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.

10.6 Prestaciones superiores o complementarías en las exigidas

Se valorará principalmente la propuesta de servicio que se ajuste más a la realidad actual

con respecto a las herramientas y aplicaciones que Mutua Intercomarcal ha establecido como válidas y las mejoras a aportar como resultado del proyecto.

10.7 Facturación de los servicios

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

MUTUA INTERCOMARCAL, dispone de una plataforma de gestión de facturas de proveedores, donde se deberán depositar.

11. CRITERIO DE VALORACIÓN

Mutua Intercomarcal ha establecido la siguiente tabla de valoración para las propuestas:

Puntos desglosados por criterios de valoración objetiva/ subjetiva:

CRITERIOS VALORACIÓN OBJETIVA (AUTOMÁTICA/FÓRMULAS)	**64 PUNTOS**
CRITERIOS VALORACIÓN SUBJETIVA	**36 PUNTOS**
TOTAL	**100 PUNTOS**

Puntos desglosados por competencias técnico/económicas del licitador:

OFERTA ECONÓMICA	**50 PUNTOS**
CERTIFICACIONES SEGURIDAD Y GESTIÓN DE PROYECTOS	**14 PUNTOS**
CALIDAD Y CARACTERÍSTICAS DEL SERVICIO, PRODUCTO Y SLA PROPUESTO	**36 PUNTOS**
TOTAL	**100 PUNTOS**

11.1 Cuadro de puntuación:

Ítem Criterio	CRITERIOS DE VALORACIÓN	Valoración Automática	PUNTOS
	OFERTA ECONÓMICA	SI	**50**
	CERTIFICACIONES		
1	Certificado ISO 27001 (Gestión de Seguridad de la Información)	SI	5
2	Certificado ENS (Nivel Medio o Alto)	SI	6
3	Certificado ISO 9001(Gestión de Calidad)	Si	1
4	Certificado ISO 45001 (Seguridad y Salud en el trabajo)	SI	1
5	Certificación ISO 14001	Si	1
	SERVICIO		**Hasta 36**
6	Planteamiento global y calidad del servicio acorde con los requisitos del pliego, adecuación de la solución de servicio al entorno de Mutua Intercomarcal	No	Hasta 14
7	Metodología, planificación, organización y configuración del proyecto	No	Hasta14
8	Propuesta de acuerdos de nivel de servicio SLA de acuerdo con las necesidades del proyecto y plan de gestión de riesgos asociado.	No	Hasta 8

Los criterios señalados en la tabla anterior como de valoración automática, esto es, señalados como un SÍ, deberán incluirse dentro del SOBRE 3, el resto de los criterios señalados como un NO valoración automática deberán incluirse en el SOBRE 2.

Valoración Económica (de 0 a 50 puntos):

La obtención de la puntuación respecto a la propuesta económica se obtendrá de la siguiente fórmula:

- Px= Oe * Pe / Ox
- Px= Puntuación de la oferta valorada.
- Pe= Puntuación de la oferta más económica
- Oe= Precio de la oferta más económica
- Ox= Precio de la oferta valorada.

La puntuación de la oferta más económica será de 50 puntos.

Baja temeraria: En relación con el criterio de la oferta económica, cuando una oferta sea inferior al 15% de la media de las ofertas presentadas, y de acuerdo con lo establecido en el artículo 152 LCSP, Mutua Intercomarcal apreciará, que esta proposición no puede ser cumplida como consecuencia de la inclusión de valores anormales o desproporcionados. En este supuesto, se pedirá a la empresa afectada un informe justificativo de la viabilidad de su oferta, que deberá ser entregado en el plazo máximo de tres días hábiles desde la notificación. A la vista de este informe y del que elaborarán los servicios técnicos propios, Mutua Intercomarcal podrá declarar la oferta de anormalmente baja y, por tanto, la excluirá de la valoración, según establece el artículo 152.4 TRLCSP. Las ofertas que no sean calificadas desproporcionadas o temerarias serán puntuadas recibiendo la máxima puntuación la oferta más baja y disminuyendo la puntuación proporcionalmente al aumento de los respectivos presupuestos, de acuerdo con la fórmula anterior.

El licitador que presente una oferta económica igual al presupuesto de licitación obtendrá 0 puntos. Aquellas ofertas económicas, que sobrepasen el importe del presupuesto máximo de licitación quedarán excluidas.

12. PLAZO DE DURACION DEL CONTRATO.

El plazo de duración del contrato será de cuatro años, contando a partir del día de la firma del contrato.

13. PRORROGA DEL CONTRATO.

No aplica

14. PRESUPUESTO BASE LICITACIÓN.

El precio máximo de licitación anual de este servicio es de 154.000€ + IVA (La propuesta debe incluir los importes de financiación correspondientes **al renting**.

Debe indicarse el importe mensual del mismo + IVA **(renting a 48 MESES)**

15. OBLIGACIONES ESPECÍFICAS DE LAS PARTES.

- El Adjudicatario, tiene la obligación de presentar un Plan de Trabajo.

15.1 Cuadro de puntuación

Los criterios señalados en la tabla anterior como de valoración automática, esto es, señalados como un **SÍ**, deberán incluirse dentro del **SOBRE 3**, el resto de los criterios señalados como un **NO** valoración automática deberán incluirse en el **SOBRE 2**.