Comunidad de Madrid

Dirección General de Sistemas
de Información y Salud Digital
Servicio Madrileño de Salud
CONSEJERÍA DE SANIDAD

PLIEGO DE PRESCRIPCIONES TÉCNICAS

RENOVACIÓN DE LAS SUPCRIPCIONES DE LAS LICENCIAS DE AUDITORÍA, ANÁLISIS FORENSE Y GESTIÓN DE DESASTRES DEL DIRECTORIO ACTIVO DEL SERVICIO MADRILEÑO DE SALUD

CONTENIDO

1. INTRODUCCIÓN

De conformidad con lo que establece el artículo 28 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público y el artículo 73 del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado por Real Decreto 1098/2001, de 12 de octubre, se exponen a continuación los fines institucionales del organismo proponente cuyo cumplimiento requiere la realización de esta contratación. Igualmente, y a tal efecto, como parte de la documentación preparatoria, se determinan con precisión la naturaleza y extensión de las necesidades que pretenden cubrirse mediante el contrato proyectado, así como la idoneidad de su objeto y contenido para satisfacerlas.

Según se dispone en el Decreto 88/2021, de 30 de junio, del Consejo de Gobierno, por el que se modifica la estructura orgánica básica de las Consejerías de la Comunidad de Madrid, modificado por el Decreto 66/2022, de 20 de julio, del Consejo de Gobierno; en el Decreto 24/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece el régimen jurídico y de funcionamiento del Servicio Madrileño de Salud; en el Decreto 2/2022, de 26 de enero, del Consejo de Gobierno, por el que se establece la estructura directiva del Servicio Madrileño de Salud (SERMAS), corresponde a la Dirección General de Sistemas de Información y Salud Digital (DGSISD) “La planificación, diseño, implantación y mantenimiento de los sistemas y tecnologías de la información para la organización y funcionamiento del Servicio Madrileño de Salud, de acuerdo con las necesidades explicitadas por las unidades directivas” y “La provisión y gestión de los servicios y equipamientos informáticos sanitarios del Servicio Madrileño de Salud”; todo ello sin perjuicio de las que correspondan a la Agencia para la Administración Digital de la Comunidad de Madrid, así como de las atribuidas a la Dirección General de Transparencia y Atención al Ciudadano y a la Dirección General de Política Digital.

De acuerdo con dichas competencias, la Dirección General de Sistemas de Información y Salud Digital, desde los Centros de Procesos de Datos (CPD) centrales del SERMAS (CPD Athene@, en Hospital Universitario 12 de Octubre, CPD de la calle Aduana y el CPD de respaldo externalizado en Tres Cantos) proporciona servicios TIC sanitarios a más de 6.800.000 ciudadanos y cerca de 90.000 profesionales de la red sanitaria pública de la Comunidad de Madrid.

Por tanto, en los CPD centrales del SERMAS se despliegan todas las aplicaciones y servicios TI de su competencia encargados de albergar los SS. II., que sustentan la operativa de gran parte de las funcionalidades del Sistema Sanitario Público. Hoy la pérdida de funcionalidad de dichos servicios TIC puede suponer poner en peligro la continuidad asistencial pública sanitaria a los ciudadanos, e incluso podría afectar a la salud de los pacientes.

El SERMAS dispone de una gestión de Usuarios basada en Directorio Activo (DA). DA es el corazón de la infraestructura de TI basado en redes Microsoft Windows. Es utilizado como maestro de usuarios de la CSCM, siendo el LDAP corporativo para el SERMAS. En dicho LDAP se recogen todos los usuarios. Además, se organizan en Unidades Organizativas (OU) en función de las aplicaciones a las que tienen acceso.

Para el cumplimiento de los requisitos de auditoría, control de accesos, securización, análisis forense y gestión de desastres en el directorio Activo, el SERMAS dispone de una serie de herramientas implantadas del fabricante QUEST SOFTWARE sobre las cuales es necesario el suministro de la renovación de las suscripciones que nos habilita la continuidad de uso y soporte de dichas licencias.

2. OBJETO DEL CONTRATO

El objeto de esta contratación lo constituye la contratación la renovación de las suscripciones de las siguientes licencias de auditoría, control de accesos, securización, análisis forense y gestión de desastres en el directorio Activo:

- Change Auditor for Active Directory.
- Change Auditor for EMC.
- Recovery Manager for AD Disaster Recovery Edition.

3. ESPECIFICACIONES DE LOS PRODUCTOS INCLUIDOS EN EL SUMINISTRO DE RENOVACION DE LAS SUSCRIPCIONES.

3.1 Descripción de los productos incluidos en la renovación de suscripciones

En la actualidad el SERMAS dispone de los siguientes productos instalados del fabricante QUEST SOFTWARE.

- Change Auditor for Active Directory:

Permite llevar a cabo auditorías completas del área de IT en tiempo real, un análisis forense detallado y una monitorización integral de la seguridad de todos los cambios clave del administrador, del usuario y de la configuración para Active Directory y Azure AD.

Realiza un seguimiento en detalle de las actividades del usuario durante los inicios de sesión, las autenticaciones y otros servicios clave para mejorar la detección de las amenazas y la monitorización de la seguridad.

Se gestiona a través de una consola central, la cual elimina la necesidad y la complejidad de múltiples soluciones de auditoría del área de TI. Se obtiene una vista única y correlacionada de todas las actividades de AD y Azure AD, con visibilidad de todos los cambios, ya sean locales o en la nube.

En un entorno tan complejo como el actual del SERMAS, los administradores no suelen ser conscientes de los problemas hasta que es demasiado tarde y esto suele ir asociado al incumplimiento de las normativas, resultando imposible presentar informes, y/o búsqueda específica de un evento. Se trata de un proceso que consume mucho tiempo, por tanto, tener una visión global de todos los cambios y registros de sucesos hace que se convierta en un proceso muy complejo.

Una de las características claves de Quest Change Auditor for AD es que de un solo vistazo se obtiene la información necesaria para identificar el suceso, ya que se aglutina en un único evento todo el proceso sin necesidad de tener que correlacionar como nos ocurre con el método nativo. Los datos representados por el suceso son:

- Quién ha realizado el cambio.
- Qué objeto se cambió (antes y después).

- Dónde se ha producido el cambio.
- Cuándo se hizo el cambio.
- Por qué se hizo el cambio.
- Equipo desde dónde se originó el cambio.

La ventaja de tener toda la información almacenada en un repositorio único, permite tener una visión global de todo lo que sucede en el entorno corporativo. Esto hace reducir tiempo en la resolución de problemas ya que no es necesario acceder al servidor dónde ocurrió el suceso, incrementar la seguridad de cada una de las plataformas y presentar informes para el cumplimiento de GDPR, LOPD, SOX, HIPAA, GLBA y los marcos y normas, tales como Esquema Nacional de Seguridad, COBIT, FISMA y SAS 7.

- Change Auditor for EMC.

Éste módulo de Change Auditor permite integrar la auditoría realizada, sobre las cabinas disponibles en los DC centrales del SERMAS, para la consolidación y centralización de sistemas de ficheros Windows (carpetas departamentales y de usuario) basadas en equipos UNITY del fabricante DELL-EMC, junto con el resto de auditorías realizadas. De esta forma, es posible disponer de un repositorio centralizado con toda la información necesaria para realizar el análisis forense de qué ha sucedido en los entornos del cliente. En el caso concreto de la auditoría sobre las cabinas de DELL-EMC, se obtendrán los eventos relacionados con la auditoría sobre ficheros y sobre carpetas. Por ejemplo, es posible saber quién ha accedido a un fichero, quién lo ha modificado o borrado, y lo mismo para las carpetas, incluyendo los cambios en los permisos de acceso.

- Recovery Manager for AD Disaster Recovery Edition

Permite recuperar el entorno de Directorio Activo ante cualquier desastre que pueda producirse, llegando a recuperarlo incluso sobre un entorno completamente nuevo si fuera necesario. Incluye las siguientes características:

- Reducir el tiempo de inactividad, restaurando cualquier objeto en AD y haciendo que los usuarios afectados vuelvan a trabajar rápidamente sin necesidad de reiniciar las controladoras de dominio.

- Restaurar el bosque completo y el sistema operativo de los controladores de dominio ante cualquier ataque ransomware que pudiera haberlos dejado inutilizados.
- Acelerar la recuperación identificando rápidamente los objetos o atributos que se cambiaron o eliminaron.
- Flexibilidad de restauración: recuperación por fases, recuperación del AD sobre "Clean OS" o sobre backups de tipo baremetal.
- Protección ante malware de los backups del AD por medio de un almacenamiento seguro.
- Estatus y visibilidad del proceso actual de restauración del bosque y siguientes pasos a ejecutar.
- Gestión de cualquier escenario de desastres sobre el AD: desde cambios en atributos, corrupción del SYSVOL hasta desastres totales sobre el bosque del AD.
- Recuperación de contraseñas y SID History.
- Informes comparativos que resalten las diferencias entre el contenido de backups de producción y entre distintos backups.

A continuación, se detalla el alcance de los productos implantados en el SERMAS sobre los que se requiere la contratación de la renovación de las suscripciones de las licencias por un periodo **de tres años**.

Producto	P/N	Cantidad	Descripción	Periodo de renovación de las suscripciones y soporte asociado
CHANGE AUDITOR FOR AD PER MANAGED PERSON TERM LICENSE/MAINT	EAQ-NPO-TB	90.000	Número de Usuarios	Tres Años
CHANGE AUDITOR FOR EMC PER MANAGED PERSON TERM LICENSE/MAINT	CHU-NPO-TB	90.000	Número de Usuarios	Tres Años
RECOVERY MANAGER FOR ACTIVE DIRECTORY DISASTER RECOVERY EDITION PER MANAGED PERSON PREMIER TERM LICENSE/MAINT	DRF-ATA-TB-PRE	90.000	Número de Usuarios	Tres Años

4. SERVICIOS DE GARANTÍA, SOPORTE Y ACTUALIZACIÓN

Las renovaciones de las suscripciones de las licencias incluyen los servicios de soporte y actualización del fabricante del producto asociados al uso de estas, por un periodo unificado común y Cotérmino con fecha de finalización el 30/4/2026 en modalidad 24x7 para las suscripciones de Recovery Manager for AD Disaster Recovery Edition y en modalidad (soporte estándar 8x5) para las suscripciones de Change Auditor for AD y Change Auditor for EMC.

Los servicios de Soporte y Actualización deben incluir la intervención correctiva necesaria para resolver todos los incidentes, de software base, que pudieran causar una interrupción del servicio.

4.1 Condiciones de los servicios de garantía, soporte y actualización

Estos servicios tienen las condiciones siguientes:

- Asignación de un responsable del servicio del fabricante con funciones de apoyo en la tramitación de los problemas urgentes y asistencia especializada para reforzar las medidas en base a incidentes de seguridad.
- El adjudicatario deberá proporcionar el derecho de actualización a nuevas versiones del producto y la disponibilidad de parches y revisiones menores, siempre y cuando sea necesario, en cualquiera de las plataformas para las que esté disponible el producto, durante todo el plazo de la garantía, sin sobrecoste adicional. Se incluye:
    - Acceso a los recursos de auto-servicio de las bases de datos de incidencias del fabricante en la modalidad establecida.
    - Acceso al portal web de soporte del fabricante
    - Acceso a las nuevas versiones de cualquier componente de la solución cuando estén disponibles. El adjudicatario deberá efectuar la entrega de las nuevas versiones por los medios electrónicos adecuados. Previamente, el adjudicatario entregará una lista de las nuevas funcionalidades de la versión, que incluirán mejoras generales, nuevas funcionalidades y/o correcciones a bugs de la solución.
    - Soporte para la puesta en producción de las nuevas versiones y parches del software de cualquier componente de la solución propuesta. Comprende todos los procesos

de parametrización, pruebas y validación de las nuevas funcionalidades, en los diferentes entornos afectados. Este soporte deberá llevarse a cabo en todas las instalaciones donde se encuentre implantada la solución objeto de este pliego. Los procesos de puesta en producción se deberán ajustar al procedimiento establecido por el SERMAS vigente en cada momento.

  - Se incluirán informes de valoración de niveles de revisión de firmware y de software anuales, a realizar en las fechas elegidas por SERMAS

- El adjudicatario estará en disposición de recibir comunicaciones de avería o incidencias con una disponibilidad de 24x7. Este procedimiento contemplará, al menos, la apertura de incidencias por vía telefónica, mail, página web o SMS.
- En el caso de que se produzca una incidencia, el adjudicatario asignará un técnico especializado en las soluciones que llevará el caso hasta la completa resolución de la incidencia.
- El adjudicatario deberá proveer el servicio de garantía en castellano.
- El adjudicatario realizará informes preventivos sobre el estado de la configuración y los enviará periódicamente. Así mismo, tendrá disponible asesoramiento técnico especializado para revisar las conclusiones de cada informe preventivo y aportar directrices sobre cómo llevarlos a cabo.
- El SERMAS podrá realizar un número ilimitado de accesos al servicio de apertura de incidencias.
- Tratamiento específico para incidencias prioridad 1 (prioridad CRÍTICA).
- Escalado y resolución de incidentes.

4.2 Nivel de servicio de la garantía

Además de las condiciones indicadas previamente para el soporte del software, el adjudicatario deberá cumplir con el Acuerdo de Nivel de Servicio establecido en este apartado. Como tiempo máximo de resolución (T. máx.) se considera el periodo máximo que transcurre desde la comunicación de la incidencia hasta la resolución de la misma.

A efectos de los tiempos de respuesta a los incidentes, se tendrán en cuenta la siguiente clasificación por prioridades:

Nivel de gravedad	DESCRIPCIÓN DE LA SEVERIDAD DEL INCIDENTE	Respuesta inicial de Soporte Estándar	Respuesta inicial de Soporte 24x7
Nivel 1	Todas las funciones o una proporción sustancial de las funciones del software no están disponibles y no hay una solución provisional posible, o el sistema va tan lento que los tiempos de respuesta lo hacen inutilizable, y/ o hay un problema que ha causado o tiene el potencial de provocar un impacto crítico en el funcionamiento de los servicios de los sistemas de Información	Dentro de 1 Hora (Disponible durante el horario de atención local.)	Dentro de 1 Hora (Cobertura las 24 horas, los siete días de la semana)
Nivel 2	Las funciones o una proporción sustancial de las funciones del software no están disponibles y hay una solución provisional posible, o el software ha disminuido su rendimiento de tal forma que los tiempos de respuesta hacen muy difícil su uso y/o hay un problema que causa o tiene potencial de provocar un impacto significativo en los servicios de los sistemas de Información	Dentro de 2 Horas	Dentro de 2 Horas
Nivel 3	Cualquier función del software que no está disponible o el software ha disminuido su rendimiento, o no funciona de la forma documentada, de tal forma que impacta en una reducción de eficiencia que tiene un impacto medio o bajo en los servicios de los sistemas de Información. Una solución provisional puede ser aceptable y se propone e implementa por la empresa adjudicataria.	Dentro de 4 Horas	Dentro de 4 Horas
Nivel 4	Cualquier petición de incremento de funcionalidades que tenga mínimo o ningún impacto en los servicios de los sistemas de Información y para las que no se requiere una solución inmediata. Solicitudes de información o consultas	Dentro de 1 Día Hábil	Dentro de 1 Día Hábil

5. TRATAMIENTO DATOS PERSONALES

El presente contrato basado no requiere tratamiento de datos personales.

Se prohíbe expresamente el acceso o cualquier otro tratamiento de datos personales por parte del contratista. Éste deberá aplicar las medidas técnicas y organizativas necesarias para garantizar tal fin.

Si se produjera una incidencia durante la ejecución del contrato que conllevase un acceso o cualquier otro tratamiento accidental o incidental de datos personales, el contratista deberá ponerlo en conocimiento del responsable del contrato en el plazo de 72 horas de haberse producido o evaluado el alcance y consecuencias, facilitando toda la información a la oficina de seguridad de la DGSISD. En estos supuestos el contratista permitirá y contribuirá a la realización

de auditorías, incluidas inspecciones por parte del correspondiente responsable del tratamiento de datos o auditor autorizado por el mismo.

Se requiere la manifestación expresa del sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos conforme a los artículos 35.1d y 122.2 de la LCSP modificados por el artículo 5 del Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

En el caso de que por necesidades del contrato fuese preciso que el contratista accediera a datos personales, se formalizará, con anterioridad a que se produzca dicho acceso, una adenda al objeto de adaptar el contenido del contrato a la normativa nacional y de la Unión Europea en materia de protección de datos personales.

En todo caso, el contratista deberá respetar la normativa vigente en materia de protección de datos.

6. OFERTA TÉCNICA Y DOCUMENTACIÓN A ENTREGAR

El contratista elaborará una propuesta técnica donde defina el detalle del suministro de renovación de las suscripciones, condiciones de la garantía, y las mejoras ofertadas para los criterios de valoración, teniendo en cuenta los requerimientos recogidos en el presente pliego.

La oferta Técnica deberá ajustarse a las necesidades expresadas y no incluir información genérica que no se relacione directamente con los objetivos aquí descritos.

La documentación de la Oferta Tecnica se presentará en castellano.

EL DIRECTOR GENERAL DE SISTEMAS
DE INFORMACIÓN Y SALUD DIGITAL

Firmado digitalmente por: LOPEZ VALVERDE ARGUESO MIGUEL
Fecha: 2023 02 13 10:23