MEMORIA JUSTIFICATIVA DE LA NECESIDAD E IDONEIDAD DEL CONTRATO DE SERVICIOS DE OFICINAS DE SEGURIDAD Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN DEL SERVICIO MADRILEÑO DE SALUD – 2 LOTES

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 76/2023, de 5 de julio, del Consejo de Gobierno, por el que se establece la estructura orgánica básica de las Consejerías de la Comunidad de Madrid, y la Consejería de Digitalización en la que se crea la Dirección General de Salud Digital a la que le corresponde la asunción de competencias de la extinta Dirección General de Sistemas de Información y Salud Digital del Servicio Madrileño de Salud, según Decreto 02/2022, de 26 de Enero por el que se establece la estructura directiva del Servicio Madrileño de la Salud: “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 Atención al Ciudadano y Transparencia y a la Dirección General de Estrategia Digital. Todo lo anterior según las disposiciones adicionales del Decreto que contemplan que en todo aquello que suponga cambio de centro presupuestario y en lo relativo a la adaptación de los procesos de estructuras orgánicas, presupuestarias y contables deberá quedar adecuado, como máximo, el día 1 de enero de 2024.

ANTECEDENTES Y JUSTIFICACIÓN

La asistencia sanitaria está cada vez más conectada, ya que las empresas de tecnología médica fabrican actualmente más de 500.000 tipos diferentes de productos sanitarios; por ejemplo, los llamados wearables (dispositivos digitales vestibles), los dispositivos implantables y los dispositivos médicos estacionarios. Al mismo tiempo, un estudio demostró que los hospitales estadounidenses tenían, en promedio, entre 10 y 15 dispositivos conectados por cama, lo que da una idea de cómo la proliferación de soluciones de tecnología médica ha cambiado por completo el panorama de las TIC en las organizaciones sanitarias de todo el mundo. Todos estos dispositivos los fabrican diferentes empresas, y todos deben comunicarse eficazmente entre sí para brindar atención al paciente. La creciente interconexión de los productos sanitarios y el uso de conexiones remotas para su mantenimiento; la necesidad de vigilar continuamente a los pacientes (incluso a los que no están ingresados en el hospital); el uso de teléfonos inteligentes para que pacientes y médicos accedan a la información sobre la salud; junto con la incapacidad de los departamentos informáticos (TI) para aplicar parches y la habitual falta de presupuesto

para los servicios y soluciones de ciberseguridad hacen que el sector de la atención sanitaria sea especialmente vulnerable. La ciberseguridad debe tenerse en cuenta en toda la vida útil de los diferentes activos (infraestructura, programas informáticos, sistemas, dispositivos, etc.) para las instituciones sanitarias.

En los últimos años, el sector sanitario ha sufrido una presión constante y en auge porque ha estado en el punto de mira de los cibercriminales, especialmente en los últimos meses como consecuencia del conflicto ruso. Desde que comenzó la crisis sanitaria, se han ido sucediendo los ataques al sector salud españoles, hospitales, servicios de salud y aseguradoras. Situación no exclusiva a España, como dejaron patente las agresiones similares, algunas de ellas con efectos graves sufridas por muchos otros países.

La Dirección General de Salud Digital (DGSD), dentro de su estructura organizativa, cuenta con un Área de Seguridad, cuyo cometido es la gestión de la seguridad de los sistemas de información en el ejercicio de sus competencias.

La amplia red asistencial del SERMAS conlleva la existencia de sistemas de información con una alta diversificación y heterogeneidad, distribuidos en diferentes centros, por lo que se hace imprescindible disponer de los mecanismos adecuados para garantizar la seguridad en todos los ámbitos de actuación y con el máximo alcance.

A medida que la ciberseguridad se convierte en una prioridad para los hospitales, es esencial que se integre de manera global en los diferentes procesos, componentes y fases que influyen en el ecosistema de las TIC de la asistencia sanitaria. La consolidación de una oficina de seguridad, de una oficina para la continua auditoría y verificación de cumplimiento normativo, así como contar con un centro de operaciones de seguridad especializado, son factores clave para configurar un seguro entorno TIC de los hospitales modernos a la vanguardia para alcanzar los objetivos de ciberseguridad.

Fuentes:

https://www.enisa.europa.eu/publications/report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/procurement-guidelines-full-version-es.pdf

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

El Esquema Nacional de Seguridad (ENS) es un Real Decreto de obligado cumplimiento para el sector público. Nace con el fin de especificar las medidas de seguridad necesarias para salvaguardar los distintos ámbitos de la organización que son susceptibles de ser atacados. Para ello, se detallan una serie de medidas organizativas y operativas (técnicas), que, al ser integradas en la Administración, mejoran exponencialmente el nivel de seguridad.

El ENS establece un planteamiento común de seguridad para la protección de la información que manejan y los servicios que prestan las administraciones públicas, fundamentalmente. Impulsa la gestión continuada de la seguridad, imprescindible para la transformación digital en un contexto donde las ciberamenazas surgen en el día a día. Además, facilita la cooperación y

proporciona un conjunto homogéneo de requisitos a la Industria, por lo cual también constituye un referente de buenas prácticas en el ámbito digital.

El principal objetivo de estas medidas de seguridad es proteger la información y los datos de la organización, de forma que no pueda ser interceptada por terceros, manipulada, inaccesible o eliminada, entre otras posibles amenazas. Para medir el grado de cumplimiento de estas medidas se basa en un modelo de auditoría continua.

ENS: "Anexo II: Medidas de seguridad de protección de las aplicaciones informáticas y protección de los servicios y aplicaciones web". *Se deben realizar auditorías de seguridad y pruebas de penetración a los servicios y aplicaciones web, incluyendo auditorías al código fuente de programas, con la periodicidad que la organización establezca internamente tomando en cuenta la criticidad de dichos servicios/aplicativos y el tipo de datos que traten.*

ENS: "Artículo 9: Reevaluación periódica". *Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.*

DESCRIPCIÓN GENERAL DE LAS NECESIDADES

El objeto del presente expediente es el de proporcionar los servicios de:

- Oficina de Seguridad de Sistemas de la Información (OSSI)
- Servicio de cumplimiento normativo en materias de protección de datos y seguridad

que son necesarios para abordar y ejecutar los trabajos destinados a impulsar y adquirir un escenario base que mejore la ciberresilencia global.

La OSSI se constituye como un instrumento de prevención, detección, respuesta a amenazas y riesgos de seguridad, así como órgano responsable de la coordinación e implantación de políticas y medidas de seguridad de la organización, prestando a la Consejería de Sanidad una serie de servicios tanto reactivos, como preventivos, con el objeto de impulsar y dar soporte a la implantación de las medidas de seguridad en sus distintos Centros.

Los principales objetivos que se persiguen con la contratación de estos servicios pueden resumirse en los siguientes puntos:

- Modelo de servicio de gestión de la seguridad alineado con las necesidades actuales de la CSCM.
- Prestar apoyo experto en materia de seguridad en los proyectos de desarrollo, mantenimiento y evolución de los sistemas de información que dan servicio a los entornos sanitarios de la CSCM.
- Prestar apoyo experto en materia de seguridad para la gestión de infraestructuras y servicios.

- Mejorar las medidas de seguridad existentes y prestar apoyo al desarrollo de la función TIC.
- Optimizar los costes asociados a la gestión de la seguridad en el SERMAS.
- Disponer de flexibilidad ante necesidades no previstas.
- Contribuir a que el área de seguridad pueda disponer de una visión global de la seguridad del conjunto de la organización que permita trabajar de forma más eficiente, con mejor capacidad de respuesta y garantía de la continuidad del servicio.

Entre las principales tareas y servicios que se deben prestar desde la OSSI de la DGSD, se encuentran los siguientes

- Cumplimiento legal y normativo, orientado al desarrollo de actividades de asesoría y consultoría para el cumplimiento de la legislación vigente y normativa relacionada con las tecnologías de la información, incluyendo actividades relacionadas con administración electrónica.
- Asesoría y auditoría de controles de seguridad de TI, para velar por un adecuado grado de madurez de la seguridad de los sistemas de información en los centros del SERMAS, que asegure la continuidad del servicio y prevenga otros riesgos como perdida de datos o confidencialidad. Este proceso se basa en la asesoría y el seguimiento de la normativa aplicable, así como de estándares y códigos de buenas prácticas, relacionados con la seguridad de los sistemas de información.
- Análisis de software y hardware. La Oficina de seguridad es responsable del establecimiento del modelo de seguridad dentro del ciclo de vida de desarrollo de aplicaciones informáticas, dentro del cual desarrolla la función de verificación de los niveles de seguridad reales de los sistemas de información, aplicaciones y dispositivos hardware del SERMAS, así como de los nuevos que se quieran implantar o adquirir. Se trata de evitar potenciales pérdidas de información confidencial o indisponibilidad de los sistemas, entre otros.
- Comunicación y formación en seguridad de la información, orientado a la concienciación y formación en materia de seguridad de la información, y al entendimiento de la legislación y normativa que les aplica a todos los entes del SERMAS.
- Servicio de seguridad y privacidad para la gestión de incidentes y riesgos para garantizar la continuidad del negocio, protegiendo los activos críticos.

El expediente se dividirá en dos lotes, para facilitar la obtención de los objetivos. Se enumeran a continuación:

- Lote 1: Oficina de Seguridad de los Sistemas de Información (OSSI).
- Lote 2: Oficina de Auditoría Interna.

CONCLUSIÓN

Para dar cumplimiento a las necesidades descritas, se propone la contratación del servicio de OFICINAS DE SEGURIDAD Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN DEL SERVICIO MADRILEÑO DE SALUD – 2 LOTES, en los términos previstos en los pliegos de referencia, por el plazo de vigencia allí indicado y con el coste detallado en la memoria económica.

Madrid,
LA DIRECTORA GENERAL DE SALUD DIGITAL

Firmado digitalmente por: RUIZ HOMBREBUENO NURIA
Fecha: 2023.11.17 13:25