Comunidad de Madrid | Dirección General de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN

RESPUESTAS A LAS ACLARACIONES SOLICITADAS POR EMPRESAS PARA EL EXPEDIENTE PA SER–42/2023 (A/SER-047045/2023):"OFICINAS DE SEGURIDAD Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN DEL SERVICIO MADRILEÑO DE SALUD – 2 LOTES"

Pregunta	Fecha Pregunta	Respuesta
PPT apartado 3.1.2.1 Gestión del portfolio y de los proyectos de ciberseguridad ¿Cuál es la herramienta actual de GRC?	29/02/2024	Aun no tenemos ninguna adquirida. Esperamos disponer de la herramienta en este año.
PPT apartado 3.1.2.13 Integración en el ciclo de vida seguro de los proyectos de la Consejería de Sanidad Dentro de los servicios mencionados dentro del paradigma DevSecOps: 1.- ¿Cuales serían las herramientas esperadas dentro del ciclo de DevOps? 2.-¿Se espera que los servicios se den como parte del ciclo automático o que sea un servicio dedicado on-demand por parte de los proyectos?	29/02/2024	Herramientas para hacer análisis estáticos de código, de calidad reconocida. Y análisis dinámico de código para la búsqueda de vulnerabilidades en las aplicaciones, de calidad reconocida. Lo ideal sería automatizar el servicio, pero de momento se tendrá que hacer bajo demanda y priorizando aquellas aplicaciones que son más críticas.
PPT apartado 3.1.2.14. Comunicación, concienciación y formación en seguridad de la formación En el punto 3.1.2.14, página 26, se habla de un Plan anual de Formación, pero en la fase 4: Mejora continua (pág.27) de este apartado, habla de Plan bianual de formación, ¿qué quiere decir?	29/02/2024	Se trata de un error material. Se publica una corrección de errores en el pefil del contratante.
PPT apartado 3.1.2.8 Mantenimiento y cumplimiento de objetivos normativos ¿SERMAS posee actualmente la certificación del ENS?	29/02/2024	Actualmente hay un único hospital con certificación de cumplimiento en ENS. Hay ya realizado un trabajo previo de implantación de medidas y desarrollo del marco normativo, para la implantación del ENS en distintas áreas de los servicios centrales del SERMAS.
PPT apartado 3.1.2.11 Servicio multidisciplinar en materia de seguridad Cuando se refiere a "Aplicación de planes de continuidad de negocio alineados con las tareas definidas", ¿Nos podrían indicar cuál es la tipología de tareas definidas?	29/02/2024	Se refiere a las tareas que defina la DGSD. Por ejemplo, realización de plan de continuidad de negocio ante incidentes de alto impacto que afecten a un servicio asistencial, a un centro de procesamiento de datos, un sistema de información centralizado…
PPT apartado 3.1.2.17. Apoyo ante incidentes de alto impacto o cibercrisis Atendiendo a la naturaleza y características de este servicio, pero tambien al matiz especificado de que es un servicio de apoyo, ¿hay que considerar este servicio como uno más a prestar dentro del horario regular de los servicios o se requiere este en particular con mayor disponibilidad?	29/02/2024	Se requiere una mayor disponibilidad, y se cubriría con los servicios específicos de la línea variable detallados en el PCAP y el punto 8.2 "Modelo de Gestión de la línea variable del lote 1".
El apartado 3.1.5. del PPT establece que "la adjudicataria garantizará la integridad de los sistemas". Entendemos que "garantizará", no significa o implica que el adjudicatario deberá asegurar y mantener la integridad en todo momento y que cualquier fallo en dicha integridad, sea por la razón que sea, podrá implicar responsabilidad y/o penalizaciones exigidas a la adjudicataria, sino que se hayan aplicado las medidas conducentes a la protección de la información y dichos sistemas, objeto de este pliego. ¿Es correcto nuestro entendimiento dado que no existe la seguridad 100%?	29/02/2024	Así es, se refiere a que la adjudicataria será diligente en sus actos.
Cuando se utiliza la palabra "velar" (e.g. apartados 3.1.5; 3.1.2.8. primer párrafo; 3.1.2.9.c. del PPT) o "supervisar" (o "supervisión") (e.g. 3.1.2.9; 3.1.2.10 del PPT), entendemos que se quiere decir que el adjudicatario proporcionará el asesoramiento necesario para que la DGSD, el CISO o el DPD, según sea el caso, puedan cumplir o supervisar, y controlar que se cumple, con sus funciones de aseguramiento de la seguridad y cumplimiento (o compliance) con la normativa que le es aplicable. ¿Es correcto nuestro entendimiento? Asimismo, se dice que el adjudicatario "velará por el correcto cumplimiento de la normativa aplicable en materia de seguridad y protección de datos". Entendemos que aplicaría sólo al ámbito de los sistemas de información del SERMAS. ¿Es correcto nuestro entendimiento?	29/02/2024	1ª Pregunta: así es 2 ªPregunta: en lo relativo a la protección de datos, el ámbito sería el SERMAS y el resto de la administración de la Consejería de Sanidad.
En relación con la Seguridad de la información y el servicio, el apartado 3.1.5 del PPT, establece que "la adjudicataria deberá velar porque los servicios implantados cumplen con (…) aquella normativa de seguridad que le sea de aplicación obligatoria". Entendemos que la normativa de seguridad será la indicada por el poder adjudicador y que el adjudicatario podrá proporcionar asesoramiento en esta materia pero que no tendrá responsabilidad en cuanto decidir cuál es la normativa aplicable. ¿Es correcto nuestro entendimiento?	29/02/2024	Únicamente seria así en el caso de que hubiera una concurrencia normativa entre normas de igual rango. Para el resto de casos, el asesoramiento debería incluir también qué normativa es la de aplicación preferente, aunque la decisión última frente a terceros sea la del adjudicador
En relación con la elaboración del PESI, el apartado 3.1.2.7.FASE TO-BE: Se habla de los "Objetivos que deberá cubrir, entre otros: (…) Aseguramiento del IOTM, Aseguramiento del Servicio digital, Aseguramiento de los entornos de Cloud, Aseguramiento y gestión de la calidad de los datos, Aseguramiento de la inteligencia artificial, Aseguramiento en la divulgación de la información" (…). Con "aseguramiento", como objetivo, entendemos que se quiere decir que el PESI deberá incluir la identificación y definición de las medidas de protección aplicables a las áreas descritas. ¿Es correcto nuestro entendimiento?	29/02/2024	Es correcto

En relación con el apoyo al CISO, el apartado 3.1.2.9 del PPT establece que “dicho apoyo contará con las siguientes actividades:” a. “Establecimiento de medidas de seguridad en el SERMAS y en la DGSD, de acuerdo con la normativa vigente de las actividades de tratamiento que contengan datos de carácter personal, y la realización de auditorías en el ámbito de protección de datos de carácter personal”. Entendemos que esto quiere decir que el adjudicatario proveerá el asesoramiento necesario para que la DGSD puede decidir qué medidas se deben implementar por el adjudicatario. ¿Es correcto nuestro entendimiento? b. “Establecimiento de mecanismos para garantizar el acceso y la autenticación de los usuarios a los sistemas de información en el SERMAS”: Entendemos que esto quiere decir que el adjudicatario deberá proponer los mecanismos en cuanto a acceso y autenticación y que el poder adjudicador deberá decidir su implementación, que será llevada a cabo por el adjudicatario. ¿Es correcto nuestro entendimiento? c. “Definir la normativa de seguridad y velar por su cumplimiento”, entendemos que quiere decir que el adjudicatario proporcionará la asesoría jurídica necesaria para que la DGSD pueda definir la normativa aplicable en cada momento y pueda así, velar por su cumplimiento. ¿Es correcto nuestro entendimiento? d. “Dar apoyo a procesos de contratación de la DGSD, si así lo requiere”. Entendemos que se trataría de apoyar y asesorar sobre las medidas de seguridad que deberían aplicar en el servicio o suministro a contratar. ¿Es correcto nuestro entendimiento?	29/02/2024	a. Correcto b. Correcto c. Correcto d. Además de las medidas de seguridad, el soporte deberá abarcar la redacción de todas las cláusulas y anexos relacionados con la normativa sobre seguridad y protección de datos que procedan, así como un análisis, en este mismo ámbito de los diferentes documentos administrativos que se presenten
En relación con el apoyo al delegado de protección de datos de la Consejería de Sanidad de la Comunidad de Madrid, conforme al apartado 3.1.2.10 del PPT, se establece que “dicho apoyo contará con las siguientes actividades: (…) Estudiar la viabilidad de las iniciativas del SERMAS, proponiendo cambios para el correcto cumplimiento de la legislación en materia de protección de datos y seguridad.” Entendemos que se trata de apoyar al DPD y asesorarle en el cumplimiento de la normativa aplicable para que el DPD pueda tomar una decisión informada. ¿Es correcto nuestro entendimiento?	29/02/2024	Sí, aunque como se indica en el texto, en los casos en los que se requiera, el apoyo consistirá en presentar textos alternativos que se considere que cumplen con la normativa.
En cuanto al servicio multidisciplinar en materia de seguridad, el apartado 3.1.2.11 primer párrafo del PPT establece que el asesoramiento “tiene como objetivo (…), asegurar la continuidad del servicio (…)”. En relación con ello, teniendo en cuenta que no se puede asegurar la continuidad del servicio al 100%, en especial, en caso de desastres o de situaciones imprevistas, entendemos que lo que se solicita es que se diseñen e implementen unos procesos y un plan de continuidad para poder recuperar a la mayor brevedad posible, los sistemas críticos (y, finalmente, todos los sistemas), en el caso de una eventualidad que afecte a los sistemas. ¿Es correcto nuestro entendimiento?	29/02/2024	Correcto
En cuanto al apoyo a las auditorías como parte las funciones del Lote 1, tal y como se describe en diversos apartados del Pliego de Prescripciones Técnicas, entendemos que ello no supone asistir como peritos o proporcionar soporte en litigios o de otro modo actuar como expertos como parte de una actividad regulada o que requiera algún tipo de licencia de actividad específica (contable, fiscal, etc.). ¿Es correcto nuestro entendimiento?	29/02/2024	Correcto
En relación con todos los servicios incluidos en los pliegos, entendidos de forma holística, entendemos que el propósito es establecer las medidas encaminadas a: (i) detectar o mitigar las vulnerabilidades y violaciones de seguridad, (ii) evitar las intrusiones o cualquier daño a los sistemas del SERMAS u otras instalaciones, activos u operaciones, (iii) cumplir o ayudar al SERMAS o a DGSD a cumplir los estándares del sector o cualquier otro requisito, sin que en ningún caso pueda garantizarse evitar el 100% de las casuísticas posibles. ¿Es correcto nuestro entendimiento?	29/02/2024	Correcto
En el documento 04-ppt, página 7, se menciona lo siguiente: “hay que indicar que en la actualidad la DGSD ya dispone de la certificación ISO/IEC 27001 para la Oficina de Seguridad de Sistemas de la Información, por lo que el adjudicatario del presente lote deberá mantener dicha certificación” La pregunta es la siguiente, ¿ El mantenimiento de la certificación incluye el coste asociado a la realización de las auditorías de mantenimiento/renovación que sucedan durante la vigencia del contrato?	01/03/2024	Así es, el coste recaerá en la empresa adjudicataria del contrato
En la página 9, se menciona lo siguiente: “La información sobre los requisitos de esta herramienta (refiriéndose a la de Project and Portafolio Management) está en el apartado 3.1.2.3. Cuadro de Mando y Reporte” Sin embargo, en este apartado no se hace referencia explícita a los requisitos de una herramienta. La pregunta es la siguiente, ¿es posible que falte información sobre la herramienta y los requisitos o debemos entender que la herramienta está asociada a un cuadro de mando que permita a la OSSI la correcta gobernanza del servicio en tiempo real?	01/03/2024	La herramienta está asociada a un cuadro de mando que permita a la OSSI la correcta gobernanza del servicio en tiempo real

El alcance del pliego “abarca a los sistemas de información que dan soporte al tratamiento de datos/información del SERMAS en su ámbito de actuación, tales como: informática médica, gestión sanitaria, y otros relativos al sistema sanitario con los ciudadanos, profesionales sanitarios, oficinas de farmacia, sanidad privada y cualesquiera personas físicas o jurídicas” o ¿Podemos cuantificar este número de sistemas y entidades? o ¿Cuántos servicios/información afectada? o ¿Esos servicios/información cuantos sistemas y subsistemas disponen?	05/03/2024	Cuantificar los sistemas de información con sus subsistemas, es uno de los primeros ejercicios que tiene que hacer la empresa adjudicataria.
¿Cuántos centros presenciales tiene la comunidad de Madrid? Para la parte de Auditoría de Protección de datos se estipula una auditoria con alcance mínimo de 51 centros y 430 tratamientos. ¿Correcto?	05/03/2024	Se trata de un alcance mínimo. La CSCM tiene 59 responsables de tratamiento y 597 tratamientos en la actualidad
En la parte de adecuación al ENS se hace referencia al cumplimiento del ENS, pero no se determina el nivel de cumplimiento (alto, medio, bajo). Entendemos que dicha adecuación es a nivel alto, ¿correcto?	05/03/2024	A día de hoy el CCN ha publicado un perfil de cumplimiento específico para Salud (CCN-STIC 891). Se trataría de cumplir con las medidas que este perfil indica.
¿Las herramientas que se hace mención, son responsabilidad en cuanto a licenciamiento del adjudicatario?	05/03/2024	Las licencias de las herramientas serán responsabilidad en cada caso: • Project and Porfolio Management, del adjudicatario • GRC, de la DGSD • Del CCN-CERT, de la DGSD • Ciberejercicios, del adjudicatario • Pruebas integradas en el ciclo de desarrollo, del adjudicatario
¿Tiempo mínimo de incorporación de los perfiles tras la firma del contrato?	05/03/2024	Tal como se especifica en el apartado 5.1. Organización general del PPT, el equipo de trabajo ofertado por cada lote se incorporará tras la formalización del contrato para la ejecución de los trabajos.
En relación al PCAP queríamos aclarar la siguiente duda: • En el punto 9.3.4 se indica que la puntuación será en función del número de personas con DPD por encima del mínimo exigido en el PPT (en este caso 3) Sin embargo, en el PPT (página 49) se indica que se debe de reunir, entre el equipo de trabajo “en su conjunto”: Certificación DPD según el esquema de la agencia de protección de datos. Pero no vemos dónde se indica que deba de haber, al menos, 3 personas con esta certificación. A nuestro parecer, sería suficiente con 1 persona.	06/03/2024	Se trata de un error material. Se publica una corrección de errores en el pefil del contratante.
En la pág. 27 del PCAP rectificado se indica: Se incluirán los documentos necesarios que permitan acreditar la oferta realizada. ¿Para acreditar las personas adicionales con certificado de Delegado de protección de datos por encima del número exigido en el PPT es suficiente una declaración responsable o es necesario adjuntar a la oferta los propios certificados?	12/03/2024	Para acreditarlo tienen que adjuntar copia de los certificados.