

INFORME DE NECESIDAD DE CONTRATACIÓN DEL “SERVICIO DE OPERACIÓN Y MANTENIMIENTO DE LAS HERRAMIENTAS DE CIBERSEGURIDAD IMPLANTADAS PARA PROTECCIÓN DE LOS SISTEMAS DE CONTROL INDUSTRIAL “

El artículo 116 de la Ley de Contratos del Sector Público dispone que la celebración de contratos por parte de las Administraciones Públicas requerirá la previa tramitación del correspondiente expediente, que se iniciará por el Órgano de Contratación motivando la necesidad del contrato en los términos previstos en el artículo 28 de la citada Ley y que deberá ser publicado en el perfil del contratante.

Con la finalidad de dar cumplimiento a los artículos 28 y 116 de la LCSP (Ley 9/2017), se emite el siguiente informe de necesidad:

Las razones que justifican la necesidad de contratación del “SERVICIO DE OPERACIÓN Y MANTENIMIENTO DE LAS HERRAMIENTAS DE CIBERSEGURIDAD IMPLANTADAS PARA PROTECCIÓN DE LOS SISTEMAS DE CONTROL INDUSTRIAL”, contempladas en el procedimiento objeto del informe, son las siguientes:

EMUASA forma parte del grupo de empresas AGBAR, compartiendo los sistemas centrales de ciberseguridad y las infraestructuras tecnológicas corporativas dedicadas a este desempeño.

El Departamento de Seguridad del Área de Sistemas de Información de EMUASA tiene entre sus funciones la Gestión, Conservación-Mantenimiento y Mejora de los sistemas de protección de ciberseguridad.

La necesidad de contratar un “Servicio de mantenimiento herramientas de ciberseguridad” es para cumplir con la obligación de cumplir correctamente con las medidas de protección descritas en los PPE’s asociados a sus infraestructuras críticas, así como, con las obligaciones impuestas por la legislación que atañe a las empresas designadas como Servicio Esencial por la administración.

Dada la especificidad y la magnitud de los trabajos a realizar que requiere de unos medios materiales y humanos de los que no dispone EMUASA para destinarlos a tal fin, es necesaria la contratación de dicho Servicio, y así se puedan cumplir con plenas garantías los objetivos de esta licitación.

El escenario actual del ciberdelincuencia en todos sus modelos de actuación ha exigido la necesidad de adoptar complejas medidas tecnológicas para prevenir sus amenazas. La diversidad de modelos de posibles ataques a las infraestructuras y equipos de las redes informáticas en los servicios esenciales, exigen, por un lado, aplicar soluciones independientes que traten de dar respuesta a las distintas tipologías de amenazas, por otro, el seguimiento continuo de la información facilitadas por las herramientas aplicadas y acciones de respuesta acordes con las situaciones concretas detectadas mediante estas, sin obviar la responsabilidad de vehicular de manera eficiente hacia las autoridades nacionales, aquellas que supongan un riesgo grave o una realidad no deseada, con la mayor claridad, conocimiento, visión global orientada a la actividad del servicio esencial que protegen y celeridad.

Estos requerimientos nos sitúan en un marco en el cual la defensa de las infraestructuras críticas y los servicios esenciales, no pueden plantearse, como la propia administración recomienda, desde un plano de actuación independiente, fuera de un marco colaborativo, con la inclusión, en el modelo de protección, de equipos humanos especializados, dedicados 24/7, de manera exclusiva, a la gestión de la información obtenida por los sistemas tecnológicos implicados en éste cometido.

Es por todo lo anterior por lo que EMUASA, ha decidido contratar los servicios de un gabinete externo cuyo objeto principal sea supervisar el correcto funcionamiento de los sistemas de Ciberseguridad aplicados ya o en un futuro, a sus sistemas de control industrial (SCI/ OT), la vigilancia de la información del estado de las amenazas evaluadas, la toma de acciones destinadas a mitigar estas o contener y responder a ataques, así como informar de la evolución y día a día de sistemas, amenazas, vulnerabilidades, ataques, estado del arte y soluciones aplicables.

Si bien las soluciones tecnológicas adoptadas por EMUASA, provienen del espectro general de medidas ofrecidas en el mercado, la adaptación de los atacantes a las particularidades del negocio de sus posibles víctimas, aconsejan, que el equipo dedicado a la supervisión y acciones en tiempo real frente a éstos, dispongan de conocimientos y experiencia en la protección de infraestructura y servicios del sector del agua, en el cual está encuadrado el negocio de EMUASA. La transversalidad de escenarios, modus operandi, riesgos, amenazas y medidas adoptables para minimizar el impacto, dentro de un mismo sector industrial, dan relevancia a la proximidad o experiencia de los equipos de detección y respuesta al sector del agua.

En la presente licitación se ha optado por un procedimiento de tramitación negociado sin publicidad debido a los requerimientos técnicos de exclusividad por la conectividad a las consolas centrales de software de ciberseguridad, el nombramiento de EMUASA como servicio esencial del estado con fecha 22 de julio de 2019, las indicaciones de la “Guía Nacional de Notificación y Gestión de Incidentes” del INCIBE y las del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el Artículo 2. Ámbito de aplicación y ANEXO II Medidas de Seguridad “Selección de medidas de seguridad”, tal y como se detalla en el informe de exclusividad.

No se ha considerado conveniente la división en lotes del presente servicio en base a los siguientes hechos:

La contratación debe hacerse en un solo lote pues el licitador debe dar el servicio de una forma integral, sin obviar ninguna de las herramientas y o actuaciones necesarias devenidas de la vigilancia y resultados de los análisis obtenidos en cada una de ellas. La correcta ejecución de esa complementariedad, es clave para que los sistemas actuales continúen operando sin problemas ni interferentes dotando a EMUASA de una mayor efectividad en las soluciones de defensa existentes.

El contrato derivado de esta licitación no requiere la cesión de datos personales por parte de EMUASA al contratista.

Por tanto, la necesidad de contratación de este servicio queda plenamente justificada, dándose cumplida razón de los motivos que se proponen al Órgano de Contratación para llevar a cabo la licitación mediante procedimiento negociado sin publicidad y posterior contratación del “SERVICIO DE OPERACIÓN Y MANTENIMIENTO DE LAS HERRAMIENTAS DE CIBERSEGURIDAD IMPLANTADAS PARA PROTECCIÓN DE LOS SISTEMAS DE CONTROL INDUSTRIAL ”

Fdo.: Francisco Alarcón Ros