INDAGACIÓN DE MERCADO N° IM-001-2023
SERVICIO DE CIBERSEGURIDAD INDUSTRIAL PARA LOS SISTEMAS DE CONTROL DE REFINERÍA TALARA
CÍA.: AXUS S.A.C.

N°	Sección	Párrafo	Dice	Consulta	Respuesta
1	ALCANCE DEL SERVICIO	3.f	Implementar un sistema para el gobierno de puertos USB que permita el monitoreo en tiempo real sobre el uso de medios extraíbles. Debe considerar la funcionalidad de detección de extracción de información.	Esta funcionalidad solo es implementada por Honeywell. En aras de la multiplicidad de marcas y de aprovechar otras funcionalidad importantes para la ciberseguridad con que no cuenta Honeywell, sugerimos colocar como opcional la funcionalidad de detección de extracción de información.	Tenemos entendido que un sistema de detección de amenazas de los medios extraibles, puede ser suministrado por otros vendors; se solicita que exista un mitigación de la propagación de virus/ransomware/malware, etc a traves de los dispositos USB/Harddrives.
2	ALCANCE DEL SERVICIO	3.f	Implementar un sistema para el gobierno de puertos USB que permita el monitoreo en tiempo real sobre el uso de medios extraíbles. Debe considerar la funcionalidad de detección de extracción de información.	Sírvase definir a qué se refiere con "monitoreo en tiempo real".	Se refiere a que el análisis de medios USB es analizado y reportado al SOC.
3	ALCANCE DEL SERVICIO	3.h	Implementación del servicio de endurecimiento de la totalidad de la infraestructura OT con aplicación de las políticas de ciberseguridad de Petroperú.	Es necesario indicar que la ejecución del endurecimiento debiera ser solo en aquellos equipos que permitan ser actualizados por proveedores distintos al fabricante del DCS	El proveedor a su costo debe garantizar durante la etapa de endurecimiento el conocimiento de la tecnología del DCS (Ya que el licenciante tiene sus propios procedimientos). Se entiende que durante esta etapa no se debe afectar el proceso continuo de la Planta.
4		3.i	Implementar un servicio de Test de Penetración con personal propio, experto en la ejecución de estos servicios que complemente el programa de remediación emitido según Estudio Diagnóstico previamente ejecutado.	El servicio de Pentesting es altamente especializado. En aras de contar con los mejores profesionales para brindar el servicio, se sugiere eliminar la restricción de que sea personal propio, pudiendo ser subcontratado.	Solicitud rechazada. Apreciaremos ceñirse a lo indicado en las Condiciones Técnicas.
5	ALCANCE DEL SERVICIO	3.4	El contratista debe implementar mediante un Gateway orientado a la gestión de Medios extraíbles, el gobierno de los puertos USB. Debe contar con un servicio de soporte complementario para la identificación en tiempo real de hashes basado en la nube. El equipo debe poder generar sus propios agentes de control a ser instalados en los nodos del Sistemas de Control y nodos de la PCN.	El que el sistema esté en nube implica una conexión permanente a Internet, lo cual introduce un factor de riesgo. El utilizar un sistema on-premise, que se actualice periódicamente mediante una conexión temporal a internet es más seguro. Sugerimos omitir el requerimiento de que sea exclusivamente en nube.	Nos referimos a que la base de datos de nuevos virus y las actualizaciones deben tener la posibilidad de actualizarse desde la nube hacia los dispositivos de escaneo de memorias USB.
6	ALCANCE DEL SERVICIO	3.4	El contratista debe implementar mediante un Gateway orientado a la gestión de Medios extraíbles, el gobierno de los puertos USB. Debe contar con un servicio de soporte complementario para la identificación en tiempo real de hashes basado en la nube. El equipo debe poder generar sus propios agentes de control a ser instalados en los nodos del Sistemas de Control y nodos de la PCN.	Con respecto al "generar sus propios agentes de control a ser instalados en los nodos",existen otras tecnologías y procedimientos que pueden brindar un grado de control similar o superior a lo plantedo. Sugerimos ampliar el alcance.	Sugerencia rechazada puesto que no se propone cuales son esas otras tecnologías similares o superiores.
7	ALCANCE DEL SERVICIO	3.4	La solución debe estar certificada para su uso con Sistemas de Control afines a los implementados en Refinería TALARA. Así mismo deberán presentarse casos previos de implementación satisfactoria con el equipo elegido.	Esto excluiría a todos los fabricantes distintos a Honeywell. Sugerimos revisar, en aras de obtener una pluralidad de ofertas.	Existen en el mercado soluciones de ciberseguridad por terceros que son compatibles y soportan el Experion PKS.
8	ALCANCE DEL SERVICIO	3.4	Deberá estar basado en Tablet estándar que garantice su uso en ambientes tipo industriales (equipos rugged).	Existen otras tecnologías y procedimientos diferentes a Tablet que pueden brindar un grado de control similar o superior. Sugerimos eliminar la restricción en aras de obtener una pluralidad de ofertas.	Solicitud rechazada, debido a que no detalla cuales son esas tecnologías superiores o similares.
9	ALCANCE DEL SERVICIO	3.5	El servicio a considerar será tipo 7x24hs, por Centros independientes uno del otro que operen en forma conjunta	Un Centro de Operaciones de Seguridad (SOC) basado en servicios en nube, no requiere redundancia de centros, ya que ofrece por diseño, alta disponibilidad y no está asociada necesariamente a una locación física. Sugerimos eliminar esta restricción, en aras de la racionalidad de recursos.	Solicitud rechazada, el SOC debe tener redundancia de ubicación geográfica.
10	ALCANCE DEL SERVICIO	3.5	Se pretende contar con un servicio de monitoreo de Redes OT, que actualmente esté en funcionamiento, sea estáble y al menos tenga tres años de operación continua durante los últimos cuatro años.	Confirmar que el monitoreo se refiere a un monitoreo continuo durante los últimos 3 años.	El monitoreo de Redes OT debe tener al menos tres años de operación continua durante los últimos cuatro años. Asimismo, nos referimos a los SOC del proveedor.
11	ALCANCE DEL SERVICIO	3.5	Se pretende contar con un servicio de monitoreo de Redes OT, que actualmente esté en funcionamiento, sea estable y al menos tenga tres años de operación continua durante los últimos cuatro años.	Confirmar que el servicios de monitoreo durante los últimos 3 años sea en redes OT y/o IT.	Para el presente servicio sólo se consideran servicios en redes OT.
12	ALCANCE DEL SERVICIO	3.6	El contratista debe implementar un servicio periódico de endurecimiento de nodos críticos de la infraestructura de Refinería TALARA.	Por favor, proporcionar un listado de los nodos críticos de la infraestructura de Refinería TALARA, indicando marca, modelo y versión.	Se adjunta la Arquitectura de Red. La misma que apreciaremos se maneje con carácter confidencial y sólo debe ser utilizada para la presente Indagación de Mercado.
13	ALCANCE DEL SERVICIO	3.6	El contratista debe implementar un servicio periódico de endurecimiento de nodos críticos de la infraestructura de Refinería TALARA.	Es necesario indicar que la ejecución del endurecimiento debiera ser solo en aquellos equipos que permitan ser actualizados por proveedores distintos al fabricante del DCS	El proveedor bajo su propio costo deberá buscar las alianzas con la casa matriz del DCS que permitan garantizar la mencionada actividad.

14	REQUERIMIENTOS TÉCNICOS MÍNIMOS	10	El contratista deberá presentar evidencias de experiencias previas en la implementación de Programas de Ciberseguridad Industrial o servicios similares en materia de Ciberseguridad en un mínimo de 25 compañías del sector Oil&Gas a nivel Nacional e internacional.	En los términos en que está planteado, se excluyen a la gran mayoría de especialistas de ciberseguridad industrial peruanos. Se sugiere racionalizar la solicitud de experiencia considerando la cantidad de empresas del sector que existen en el pais. En este sentido, la experiencia es más valiosa por el número de años atendiendo a empresas en el sector, que el número de empresas en sí. Se sugiere también ampliar los sectores para incluir minería, energía y manufactura.	El proyecto de modernización de la refinería Talara ha implicado una inversión de mas de 5000 millones de dólares, el sistema de control y redes OT constituye el centro neurálgico de la operación y producción de la refinería. En tal sentido, es nuestro fin asegurar nuestra inversión con la participación de empresas con experiencia en ciberseguridad en el sector de Oil &Gas, por ello lamentamos no poder acceder a su solicitud.
15	REQUERIMIENTOS TÉCNICOS MÍNIMOS	10	El monto contractual acumulado de las experiencias comprendidas en los últimos 5 años deberá ser superiore a 50.0 MMUS$ (sumatoria de servicios de los últimos 5 años) con compañías del sector Oil&Gas	En los términos en que está planteado, se excluyen a la gran mayoría de especialistas de ciberseguridad industrial peruanos. Se sugiere racionalizar la solicitud de experiencia a US$ 250,000 Se sugiere también ampliar los sectores para incluir minería, energía y manufactura.	El proyecto de modernización de la refinería Talara ha implicado una inversión de mas de 5000 millones de dólares, el sistema de control y redes OT constituye el centro neurálgico de la operación y producción de la refinería, en tal sentido es nuestro fin asegurar nuestra inversión con la participación de empresas con experiencia en ciberseguridad en el sector de Oil &Gas, por ello lamentamos no poder acceder a su solicitud. En las condiciones tecnicas integradas se ha actualizado el monto.
16	11 PERSONAL Y APÉNDICE N 02: PERSONAL DEL SERVICIO	- Un (01) Líder del Proyecto de Ciberseguridad - Un (01) Gerente del Proyecto		Las descripciones difieren en varios puntos. Por favor confirmar: - El título, "Líder" o "Gerente" - Confirmar que la formación puede ser en una profesión universitaria afín a: Procesos industriales (industrial, química, mecánica), Informática (computación, informática, sistemas) o Electrónica (electrónica, eléctrica, de control industrial). - La presencialidad sería requerida durante los periodos de implementación del contrato, no durante los períodos de operación contínua.	* Si, al referirse al líder del proyecto de ciberseguridad, nos referiamos al gerente del proyecto. Se realiza la modificación en las Condiciones Técnicas Integradas. Al referirse al cargo de Líder se entiende por el Ingeniero a cargo del mencionado servicio, motivo por el cual no se aceptarán certificados con términos de asistente o supervisión. Debido que el Líder del Proyecto y el Gerente es la misma persona, se unifica la formación solicitada en las Condiciones Técnicas Integradas. * La presencia del Lídeo o Gerente será durante todo el plazo de ejecución del servicio.
17	11 PERSONAL Y APÉNDICE N 02: PERSONAL DEL SERVICIO	- Un (01) Consultor Líder en Seguridad Cibernética	a) Formación Académica Ingeniero titulado, en las especialidades de Ingeniería Electrónica, Sistemas, industrial u otras ingenierías afines colegiado y habilitado por el CIP (o equivalente si fuera extranjero). Tendrá al menos una certificación de Ciberseguridad (CCNA, CISSP, CCIE, CCSP, CCNP), o certificado de entrenamientos / cursos en Ciberseguridad realizado en los últimos 5 años.	Las descripciones difieren en varios puntos. Por favor confirmar: - Confirmar que la formación puede ser en una profesión universitaria afín a: Procesos industriales (industrial, química, petroquímica, mecánica), Informática (computación, informática, sistemas) o Electrónica (electrónica, eléctrica, de control industrial). - Debido a la esepcialización y responsabilidad de la función, se sugiere aceptar sólo las certificaciones internacionales mencionadas, no cursos, que podrían ser no evaluados.	* Se unifica la formación solicitada para el Consultor Líder en Seguridad Cibernética en las Condiciones Técnicas Integradas. * Ceñirse a lo solicitado en las Condiciones Técnicas Integradas.