INDAGACIÓN DE MERCADO N° IM-001-2023

SERVICIO DE CIBERSEGURIDAD INDUSTRIAL PARA LOS SISTEMAS DE CONTROL DE REFINERÍA TALARA

CÍA.: KYDRIL PERÚ S.A.C.

N°	CONSULTA	RESPUESTA
1	Mencionado Centro (SOC – Security Operation Center) debe tener capacidad de detección de amezas, monitoreo de redes proveer conexión remota segura de grado industrial, soporte a la planificación del patching de los sistemas operativos de las estaciones de control y los antivirus Consulta: Por favor indicar si es necesario implementar cada una de estas soluciones, o solo requiere que el SOC OT sea capaz de gestionar soluciones que ya utilice PetroPerú.	EL SOC del postor debe tener todas esas funcionalidades solicitadas, Petroperú Refinería Talara no dispone en la actualidad de ningún SOC OT.
2	El servicio a considerar será tipo 7x24hs, por Centros independientes uno del otro que operen en forma conjunta. Debe considerar así mismo, un servicio de Respuesta a Incidentes para áreas industriales brindado por personal experto en Infraetructuras Industriales. Consulta: Entendiendo que según la definición de personal calificado, dentro de los requisitos, debe tener experiencia y certificaciones en el ámbito de ciberseguridad industrial, ¿Se requiere esta expertiz para solucionar incidentes operacionales, o para otorgar una revisión desde el punto de vista de la ciberseguridad? Favor especificar.	Se esta solicitando experiencia desde el punto de vista de la ciberseguridad.
3	¿Es posible detallar los fabricantes y protocolos industriales utilizados en la red industrial?	Principalmente Experion PKS, Allen Bradley, Siemens, Schneider Electric, ABB, protocolos y redes como FTE, SafeNet, Modbus TCP, IEC61850, entre otros.
4	Para la gestión de medios extraíbles, existe una estimación del total de endpoints que requieren de este control?	Será determinado por el Contratista, alineado a la política y aprobado por Petroperú S.A. durante la Ejecución del Servicio, pudiendo ser mínimo 8.
5	Sobre el monitoreo de las redes OT, ¿Puede efectuarse en modo pasivo (escucha de tráfico), activo (consulta a los ciberactivos), o puede ser híbrido (ambas opciones previas)?	Hibrido, sin que afecte la performance y latencia de la red OT.
6	Sobre la ejecución de Test de Penetración, ¿Existe una metodología específica a considerar para su desarrollo?	No existe metodología, pero preferentemente deseamos una prueba minuciosa tipo white box.
7	Para el servicio de endurecimiento de nodos, se entiende que cualquier medida que implique la configuración de servidores pueden impactar la operación (Ej: Reinicio de máquinas, afectación de aplicaciones, entre otros). ¿Se entiende como recomendaciones para su implementación? Considerando que un cambio operacional sin notificación y revisión de los equipos internos, puede generar un impacto.	El proveedor bajo su propio costo deberá buscar las alianzas con la casa matriz del DCS que permitan garantizar la mencionada actividad.
8	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. Consulta: Se solicita que se acepte que la experiencia solicitada pueda ser tambien de programas de ciberseguridad en industrias en general, para permitir mayor participacion de postores especialistas .	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.

9	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 aquellos casos que, por confidencialidad de la documentación, no se pueda entregar a PETROPERU, estos documentos serán exhibidos ante un notario público. Consulta: Para mayor participacion de empresas especialistas se solicita que se permita presentar facturacion de soluciones de ciberseguridad en general ya que actualmente en el mercado Peruano no hay muchas empresas del sector mencionado (Oil&Gas). La solicitud corresponde al cumplimiento del Articulo 7 inciso i del reglamento de contrataciones de PetroPerú donde se pide: "*i) La calificación debe ser objetiva y congruente con el objeto de la convocatoria y con las condiciones que ofrece el mercado, debiendo sujetarse a criterios de racionalidad y proporcionalidad* "	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.
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 aquellos casos que, por confidencialidad de la documentación, no se pueda entregar a PETROPERU, estos documentos serán exhibidos ante un notario público. Consulta: Para mayor participacion de empresas especialistas se solicita que se permita presentar facturacion de soluciones de ciberseguridad en general con un monto minimo de 5 millones de dolares en los ultimos 5 años. La solicitud corresponde al cumplimiento del Articulo 7 inciso i del reglamento de contrataciones de PetroPerú donde se pide: "i) La calificación debe ser objetiva y congruente con el objeto de la convocatoria y con las condiciones que ofrece el mercado, debiendo sujetarse a criterios de racionalidad y proporcionalidad"	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.
11	El contratista deberá contar con Centros de Operación de Ciberseguridad propios que puedan proveer un servicio 7x24hs. Como mínimo el servicio deberá considerar: el monitoreo de las infraestructuras de procesos de planta, la detección de vulnerabilidades y eventos y el servicio de respuesta a incidentes. Mencionado Centro (SOC – Security Operation Center) debe tener capacidad de detección de amezas, monitoreo de redes proveer conexión remota segura de grado industrial, soporte a la planificación del patching de los sistemas operativos de las estaciones de control y los antivirus. Acreditar con certificados vigentes emitidos de empresa auditora bajo ISO 20000 e ISO 27001 Consulta: Para permitir mayor participacion de proveedores especializados en servicios de ciberseguridad, se solicita que se permita presentar ISO 9001 en reemplazo de alguno de los ISOs solicitados	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.
12	APÉNDICE N° 02: PERSONAL DEL SERVICIO Un (01) GERENTE DEL PROYECTO a) Formación Académica Ingeniero titulado, en las especialidades de Ingeniería Electrónica, Sistemas , industrial u otras ingenierías colegiado y habilitado por el CIP (o equivalente si fuera extranjero). Consulta: Por favor confirmar que se aceptará que el especialista cuente con grado de bachiller para permitir mayor participación de proveedores.	Ceñirse a lo indicado en las Condiciones Técnicas Integradas.
13	APÉNDICE N° 02: PERSONAL DEL SERVICIO Un (01) GERENTE DEL PROYECTO El Postor deberá adjuntar una Constancia en la cual acredite que el Especialista participó directamente en la ejecución de proyectos y servicios de Ciberseguridad industrial en los sectores de Oil&Gas y Minería, implementando y realizando actividades en materia de Ciberseguridad con cargos de Lider. Consulta: Para permitir mayor participación de especialistas se solicita que se pueda sustentar la participacion en proyectos de servicios de ciberseguridad en todos los sectores del mercado.	Ceñirse a lo indicado en las Condiciones Técnicas Integradas.

14	Un (01) CONSULTOR LÍDER EN SEGURIDAD CIBERNÉTICA El consultor líder en seguridad cibernética tiene como función principal el desarrollo y ejecución de todos los procesos, políticas y procedimientos del programa de cumplimiento que se incluyen en el alcance de trabajo definido. El consultor líder podra desempeñar las funciones de ingeniero residente a) Formación Académica Ingeniero titulado, en las especialidades de Ingeniería Electrónica, Sistemas , industrial u otras ingenierías afínes colegiado y habilitado por el CIP (o equivalente si fuera extranjero). Consulta: Por favor confirmar que se aceptará que el especialista cuente con grado de bachiller para permitir mayor participación de especialistas calificados.	Ceñirse a lo indicado en las Condiciones Técnicas Integradas.
15	Un (01) CONSULTOR LÍDER EN SEGURIDAD CIBERNÉTICA El consultor líder en seguridad cibernética tiene como función principal el desarrollo y ejecución de todos los procesos, políticas y procedimientos del programa de cumplimiento que se incluyen en el alcance de trabajo definido. El consultor líder podra desempeñar las funciones de ingeniero residente b) Experiencia Experiencia acreditada por un periodo de 5 años de servicio en soporte , asesoramiento, consultoria comicionamiento , en áreas de ciberseguridad, network , Tecnología Informática. Deberá acreditar su participación en al menos 5 proyectos relacionados con el objeto del presente. Consulta: Por favor confirmar que se aceptara que la participacion solicitada de los 5 proyectos de servicios de ciberseguridad.	Ceñirse a lo indicado en las Condiciones Técnicas Integradas.
16	Un (01) Consultor Líder en Seguridad Cibernética : -Experiencia genérica de cinco (05) años (constancias de trabajo a partir de grado obtenido) -Experiencia especifica tres (03) años ocupando posiciones similares (acreditar con constancias; suma a la experiencia genérica). Experiencia especifica en Industrias de Minería o petróleo (Oil & Gas) Consulta: Para mayor participación de profesionales que tienen experiencia en Servicios de Ciberseguridad, se solicita que la experiencia especifica de 3 años sea para las industrias en general, no solo de mineria o petroleo	Ceñirse a lo indicado en las Condiciones Técnicas Integradas.
17	Un (01) Consultor Líder en Seguridad Cibernética : -Experiencia genérica de cinco (05) años (constancias de trabajo a partir de grado obtenido) -Experiencia especifica tres (03) años ocupando posiciones similares (acreditar con constancias; suma a la experiencia genérica). Experiencia especifica en Industrias de Minería o petróleo (Oil & Gas) -La educación formal del profesional es: Ingeniero en electrónica, Electricidad, informática, industrial y analista de sistemas. (acreditado con Grado Obtenido) -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. Consulta: Se solicita que se confirme que sera aceptada certificaciones como ITIL, COBIT para permitir mayor participacion de especialistas.	Se acepta la solicitud y se procede a incluir las certificaciones ITIL y COBIT solicitadas para el Consultor Líder en Seguridad Cibernética en las Condiciones Técnicas Integradas.

18	Un (01) Consultor Líder en Seguridad Cibernética : -Experiencia genérica de cinco (05) años (constancias de trabajo a partir de grado obtenido) -Tendrá una amplia experiencia en cumplimiento normativo (IEC 62443, NIST). (Adjuntar Certificado) Consulta: Se solicita que se confirme que tambien sera aceptada la certificacion de Gerente Certificado de Seguridad de la Información (CISM - Certified Information Security Manager). Quedando el requerimiento de la siguiente manera: -Tendrá una amplia experiencia en cumplimiento normativo (IEC 62443, NIST) (Adjuntar Certificado) o experiencia en gerencia de seguridad de la informacion (adjuntar certificado)	Se incluirá para el Consultor Líder en Seguridad Cibernética el Certificado de Seguridad de la Información (CISM) en las Condiciones Técnicas Integradas.