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

N°	REFERENCIA	CONSULTA/OBSERVACION	VECTOR	RESPUESTA
1	Pág 9 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	En las bases señalan: "El contratista deberá presentar evidencias de experiencias previas en la implementación de Programas de Ciberseguridad Industrial similares al presente en un mínimo de 25 compañías del sector Oil&Gas a nivel internacional, Con contratos superiores a 50.0 MMUS$ (acumulados en los últimos 5 años) con compañías del sector Oil&Gas. Así mismo, deberá presentar antecedentes con proyectos donde se involucren los principales Sistemas de Control de Petroperú TALARA. En aquellos casos que, por confidencialidad de la documentación, no se pueda entregar a PETROPERU, estos documentos serán exhibidos ante un notario público...." Observamos el presente requerimiento mínimo solicitado, ya que está limitando la participación a postores con experiencia en el sector Oil&Gas internacional, por lo que, solicitamos pueda haber apertura en este requerimiento a fin que exista pluralidad de postores en el presente proceso y podamos participar como un proveedor potencial con experiencia en el objetivo del servicio en el Servicio de Ciberseguridad pudiendo ser de TI o Industrial, considerando que la experiencia más enriquicedora debería enfocarse más en la experiencia del personal que el postor proponga dado que son quienes ejecutaran los servicios. Por lo que solicitamos puedan aceptar la siguiente experiencia en monto y rubro como similares: Debe contar con experiencia mínima de 10 años brindando servicios en monitoreo de equipos de seguridad en redes y eventos de ciberseguridad, y/o provisión de equipo de seguridad para la protección del perímetro de red, y/o solución de seguridad TI Licencias de seguridad y servicios de implementación, y/o tercerización de servicios de tecnología de información en seguridad informática, y/o suministros de equipos IPS, y/u Optimización de sistemas de seguridad para conexiones con Entidades Externas, y/o provisión de solución de seguridad perimetral de red y equipos balanceadores externos o internos. Para ello, el Postor deberá acreditar la experiencia por un monto mínimo de S/ 4´000,000.00 incluido IGV, acreditada mediante contratos y la respectiva conformidad por la prestación efectuada, es decir que los contratos deberán adjuntar la documentación que permita verificar que el servicio ha sido prestado. En tal sentido esta acreditación podrá también realizarse mediante comprobantes de pago cuya cancelación se acredite documental y fehacientemente (comprobantes de pago sin sello de cancelación adjuntado voucher de depósito, reporte de estado de cuenta, comprobantes de retención, boletas de depósito, entre otros documentos con los cuales se acredite el pago efectivo del servicio), comprobantes de pago cuya cancelación conste en el mismo documento, o certificación/constancia emitida por la institución/empresa donde se realizó la prestación del servicio.	Experiencia	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.
2	Pág. 5 3.1 Políticas y procedimientos de seguridad cibernética industrial	Confirmar que son políticas y procedimientos de seguridad enfocados únicamente en el ambiente OT/industrial	consultoría	Efectivamente es un ambiente OT/Industrial, diferenciado que no somos una industrial de papel, alimentos, etc. Somos una empresa cuya materia prima y productos finales son los combustibles y las consecuencias de fallos y errores son catastróficas.
3	Pág. 5 3.1 Políticas y procedimientos de seguridad cibernética industrial	Indicar la cantidad de ambientes de ingreso/salida a planta, datacenters, salas de control u otro ambientes físicos de Talara que deben ser cubiertos por el Procedimiento de control de acceso físico	consultoria	La cantidad y distribución se encuentra en el Item 3.2.1.1 "Base de Evaluación".
4	Pág. 5 3.1 Políticas y procedimientos de seguridad cibernética industrial	Indicar la cantidad y tipos de sistemas de información que deben ser cubiertos por el Procedimiento de control de acceso lógico	consultoria	La cantidad y distribución se encuentra en el Item 3.2.1.1 "Base de Evaluación".
5	Pág. 5 3.1 Políticas y procedimientos de seguridad cibernética industrial	Indicar qué sistemas operativos deben ser cubiertos por el Procedimiento de revisión del sistema operativo	consultoría	Windows 7, Windows Server 2008, Windows Server 2016 Windows 10
6	Pág. 5 3.1 Políticas y procedimientos de seguridad cibernética industrial	Indicar las marcas de antivirus que tiene implementado Petroperú y que deben ser cubiertos por el Procedimiento de gestión de parches antivirus	consultoría	Todos los servidores cuentan con el antivirus McAfee.
7	Pág. 5 3.1 Políticas y procedimientos de seguridad cibernética industrial	Favor de indicar el alcance del procedimiento de Gobernanza USB (actividades que debería cubrir)	consultoría	Se aclara que debe cubrir todas las actividades que impidan el ingreso de ataques informáticos por medio del empleo de memorias USB o dispositivos que utilicen conexiones USB, así como la salida de información confidencial. Lo cual debería estar contemplado dentro de los procedimientos propios a desarrollarse en el servicio.
8	Pág. 5 3.2Evaluación de la seguridad cibernética	Favor de indicar si cuentan con un SGSI (sistema de gestión de seguridad de la información) en PETROPERU bajo qué normas se encuentra alineado. De ser posible indicar su nivel de madurez. Caso contrario compartir la documentación que sustente la operación de los controles de seguridad en PETROPERU y Talara	consultoria	PETROPERU cuenta con un SGSI para sector TI. Para el caso de redes OT y DCS esta concebido y construido bajo ciertos lineamientos de ciberseguridad, los mismos que se adjuntan.
9	Pág. 6 3.2.2.1Reunión de Inicio	Confirmar si la reunión inicial podrá realizarse de manera remota	consultoria	Debe realizarse de manera presencial.
10	Pág 6 Alcance de la Evaluación de Seguridad. 3.2.1.1 Base de evaluación	Favor aclarar el inventario total a nivel de OT involucrado, incluyendo marcas y modelos de las distintas tecnologías.	COE	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.

11	Pág 6 Alcance de la Evaluación de Seguridad. 3.2.1.1 Base de evaluación	Agradecemos se suministre la arquitectura actual a nivel de OT	COE	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.
12	Pág. 7 3.2.2.2Evaluación in situ	Indicar el proceso de ingreso a la planta, costos asociados referidos a traslados, viáticos, estadía y otros	consultoria	El ingreso a planta son los estipulados por ley y referidos a la Seguridad y Salud Ocupacional, SCTR, Pruebas COVID (si aun es vigente en la ejecución), etc. los mismos que serán coordinados con el postor ganador de la Buena Pro. Sin embargo, los gastos de viáticos, entre otros son responsabilidad del contratista.
13	Pág. 7 3.2.2.2Evaluación in situ	Indicar los requisitos exigibles que deben cumplir los consultores para el ingreso a planta (seguros médicos, pruebas covid, exámenes médicos, equipo de protección personal específico por planta, inducción u otros) que no hayan sido especificados en el TDR.	consultoria	Serán coordinados con el postor ganador de la Buena Pro previo al inicio del servicio.
14	Pág. 7 3.2.2.2Evaluación in situ	Confirmar si las "políticas y procedimientos de seguridad actuales." podrán ser compartidos de manera virtual o sólo podrán ser revisados insitu	consultoria	No se dispone de Políticas ni procedimientos de seguridad OT.
15	Pág. 7 3.2.2.2Evaluación in situ	Indicar la cantidad de plantas y sus ubicación donde se espera que se realice la revisión insitu	consultoria	Las Unidades de la Planta se indican en el numeral 3.2.1.1 de las Condiciones Técnicas. Asimismo, se adjunta Arquitectura de Red para complementar la información y las mismas se encuentran en la ciudad de Talara.
16	Pág. 7 3.3Capacitación en seguridad cibernética	Confirmar si las capacitaciones podrán realizarse de forma remota, considerando que el capacitador podrá estar en otro país distinto al de Perú.	consultoria	Las capacitaciones deberán ser presenciales.
17	Pág 8 3.4 Gestión de Medios Extraíbles (Gobierno de Puertos USB)	Se requiere confirmar el fabricante, versiones de software y tipo de sistema operativo de los sistemas de contro endpointl, a fines de validar la compatibilidad con la solución de Gestión de medios USB.	cyber	Referirse a lo indicado en la respuesta 5 y 10 del presente pliego absolutorio.
18	Pág 8 3.4 Gestión de Medios Extraíbles (Gobierno de Puertos USB)	Se tiene la siguiente duda, por un lado se menciona que la solución este certificada para uso en sistemas de control, pero por otro lado menciona que debe estar basado en tablet DELL, puntualizando a un solo fabricante de dispositivo. Confirmar que el alcance solo aplica para endpoints del tipo Tablet DELL, mas no otros dispositivos como HMI, PLC.	cyber	En las especificaciones Técnicas no se esta haciendo referencia a ninguna marca en particular.
19	Pág 8 3.5Monitoreo de Redes OT	Al mencionar servicio de monitoreo de la red OT , confirmar si hace referencia a una solución de monitoreo de eventos de seguridad que se alimenta de las distintas plataformas IT/OT, o hace referencia a una solución propia de monitoreo de amenazas y vulnerabilidades en tiempo real de forma segura y pasiva en la red OT	cyber	El punto 3.5 hace referencia a un Centro de Operaciones de Ciberseguridad externo y propio del postor el cual mediante hardware, software y enlaces VPN monitorea la red operativa.
20	Pág 8 3.5Monitoreo de Redes OT	de ser el escenario 1. Se solicita brindar listado de marca, modelo y tipo de plataformas que se esperan monitorear en redes OT, incluyendo tipo y versión del sistema operativo en caso deba contemplarse tambié servidores/ estaciones de trabajo.	cyber	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.
21	Pág 8 3.5Monitoreo de Redes OT	Existen tiempos de retención histórico y en caliente para el registro y eventos derivados del monitoreo SOC?	cyber	EL SOC debe trabajar en tiempo real.
22	Pág 8 3.5 Monitoreo de Redes OT para la totalidad de la infraestructura de Refinería TALARA (SOC OT)	Favor aclarar si Talara ejecutara las contenciones que dictamine el servicio de respuesta a incidentes, o si espera que dentro del servicio de respuesta a incidentes se incluya la ejecucion de las configuraciones para realizar las contenciones ante un incidente, de ser asi, favor aclarar con qué elementos de control a nivel de seguridad OT cuenta Talara para ejecutar las contenciones pertinentes.	COE	EL SOC o el personal de la contratista debe de realizar las configuraciones. Refinería Talara no cuenta con SOC.
23	Pág,. 8 3.5Monitoreo de Redes OT para la totalidad de la infraestructura de Refinería TALARA (SOC OT)	Confirmar si actualmente cuentan con un Procedimiento de respuestas a incidentes de seguridad industrial y el alcance del mismo, indicar si cuentan además con Playbooks u otra documentación relacionada al proceso de respuesta a incidentes	consultoria	No se cuenta con la información indicada.
24	Pág,. 8 3.5Monitoreo de Redes OT para la totalidad de la infraestructura de Refinería TALARA (SOC OT)	Favor de indicar el alcance del del Procedimiento de Respuesta a Incidentes vigente y bajo qué norma se encuentra alineada	consultoria	No se cuenta con la información indicada.
25	Pág,. 8 3.5Monitoreo de Redes OT para la totalidad de la infraestructura de Refinería TALARA (SOC OT)	Confirmar si se espera que la revisión y mejora del Procedimiento de Respuesta a Incidentes sea ejecutado durante los 3 primeros meses de inicio del servicio	consultoria	Se aclara que el SOC debe entrar en operación durante los 3 primeros meses.

26	Pág 8 3.6 Servicio de Endurecimiento de nodos de la infraestructura crítica.	Favor aclarar la cantidad y tipos de activos considerados como infraestuctura critica	COE	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.
27	Pág. 8 3.6Servicio de Endurecimiento de nodos de la infraestructura crítica.	Indicar el alcance del Servicio de Endurecimiento de nodos de la infraestructura crítica (es decir se podría considerar la evaluación del estado de endurecimiento, definición del plan de acción para la implementación y mejora de hardening, diseño de políticas, procedimientos y plantillas de hardening, e implementación de hardening)	consultoria	El alcance debe estar acorde a las recomendaciones vigentes del CIS Benchmark.
28	Pág. 8 3.6Servicio de Endurecimiento de nodos de la infraestructura crítica.	¿Con qué periodicidad se espera que sea implementado el Servicio de Endurecimiento de nodos de la infraestructura crítica?	consultoria	Se realizará bajo demanda, cuando se detecten falencias de la ciberseguridad o 2 veces por año.
29	Pág. 8 3.6Servicio de Endurecimiento de nodos de la infraestructura crítica.	Indicar la cantidad de activos, tipo, marca, modelo, y sistema operativo que formarían parte del alcance del Servicio de Endurecimiento de nodos de la infraestructura crítica.	consultoria	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.
30	Pág 9 3.7 Servicio de Test de Penetración.	¿Hay entorno de preproducción o laboratorio para llevar a cabo la explotación de las vulnerabilidades?	cyber	No.
31	Pág 9 3.7 Servicio de Test de Penetración.	¿Cuántas líneas de producción hay que auditar en cada test?	cyber	El DCS es transversal a todas las unidades de producción por tanto el test de penetración no se realiza por líneas de producción aisladas. Revisar arquitectura de Red adjunta.
32	Pág 9 3.7 Servicio de Test de Penetración.	¿El alcance de cada test será siempre el mismo? Por ejemplo los 69 servidores y 68 controladores y PLC´s serán el mismo objetivo en cada test? , ¿o se requerirá hacer foco cada vez en unos diferentes?	cyber	El test de penetración es general a todos los componentes del sistema.
33	Pág 9 3.7 Servicio de Test de Penetración.	¿El enfoque de estos test será de caja negra (sin aportar información de la línea de producción) o se aportará información (cuentas de usuario, u otro)?	cyber	Se debe aportar información.
34	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	De ser necesario, confirmar que PETROPERU contará con un circuito de datos y un equipo de comunicación local en sus instalaciones como parte de los requisitos previos para instaurar una conexión VPN SITE to SITE estable entre el centro de operaciones del postor (SOC) y la red OT de refinería	cyber	Se confirma.
35	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	Indicar el alcance del servicio avocado a la detección de vulnerabilidades (es decir se podría considerar escaneo a nivel de dispositivos en la red, estaciones de trabajo, servidores, aplicaciones web, servicios web) y cantidades por tipo.	cyber	EL alcance esta resumido en el numerla 3.2.1.1 de las Condiciones Técnicas.
36	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	Respecto a la detección de vulnerabilidades, indicar la periodicidad de escaneo esperada.	cyber	La detección de vulnerabilidades debe ser constante y autónomo basándose en el monitoreo continuo del trafico de red.
37	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	Respecto al servicio de detección de vulnerabilidades, confirmar si PETROPERU dispone o facilitará de una herramienta de gestión/detección de vulnerabilidades.	cyber	Petroperú no dispone de la herramienta indicada, la misma que debe estar contemplado dentro del presente servicio, siendo entera responsabilidad del Contratista.
38	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	Confirmar en qué etapa del RFI se espera elaborar el inventario de los activos?	cyber	Debe realizarse en las primeras etapas del servicio.
39	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	Confirmar en que etapa del programa de ciberseguridad se espera realizar el soporte a la planificación del patching? Y cual es la periodicidad?	cyber	Se realizará bajo demanda, cada vez que se descubran vulnerabilidades.
40	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	Confirmar qué se quiere decir con capacidad para elaborar la conexión remota segura de grado industrial? Si hace referencia a elaborar procedimientos para el mismo o al aprovisionamiento de una solución tecnológica? De ser este último se necesita brindar mayor detalle del alcance esperado.	cyber	La conexión de acceso remoto del SOC a la red OT debe ser muy segura y debe contemplar procedimientos y soluciones tecnológicas que garanticen la protección de la infraestructura OT, siendo de entera responsabilidad del Contratista.
41	Pág 10 9.REQUERIMIENTOS TÉCNICOS MÍNIMOS	Cuantos usuarios se conectan de forma remota segura a la red industrial?	cyber	No esta definido aún, pudiendo ser un máximo de 10 concurrentes.
42	Pág 11 10PERSONAL (Describir a la persona que estara presente en Talara)	Favor de indicar el régimen de trabajo del Consultor Líder en Seguridad Cibernética (horarios, días, modalidad en sitio) ,del residente responsable y del personal adicional que considere el postor en planta de acuerdo a los lineamientos en TALARA.	consultoria	De acuerdo a lo indicado en el literal f) y g) del numeral 21 de las Condiciones Técnicas.
43	Pág 11 10PERSONAL (Describir a la persona que estara presente en Talara)	Confirmar que se valorará otras certificaciones de seguridad o ciberseguridad	consultoria	Afirmativo, siempre que sean estándares de ciberseguridad.

44	Pág 14 17. FACTURACION Y FORMA DE PAGO	Respecto a la estructura de costos del Apéndice 4. No se muestra ninguna apendice 4, solo apendice 3 con estructura de costos incompleto para el total de sub partidas. Se tiene un formato de estructura completo?	cyber	Adecuarse a las Condiciones Técnicas Integradas adjuntas.
45	Pág 17 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Respecto al listado de repuestos críticos, solicitamos se brinde mayor detalle de las plataformas (marca, modelo, tipo de plataforma) que solicitan disponibilidad de repuestos a cargo del proveedor. sección I	cyber	Detalles del equipamiento será en la etapa del ejecución del contrato; sin embargo, el postor puede identificar equipos críticos de las planos de las arquitecturas de red.
46	Pág 17 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Respecto al listado de repuestos críticos, confirmar si PETROPERU provisionará algun almacen o espacio dentro de la refineria TALARA?	cyber	Si se proporcionará.
47	Pág 17 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Solicitamos confirmar si los equipos críticos del sistema tienen contrato de soporte vigente gestionado por PETROPERU? e indicar el número serial de los mismos para fines de validación de condición actual. Sección I.	cyber	Sera provisto en la etapa de ejecución del contrato con el postor ganador de la Buena Pro.
48	Pág 17 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	En el punto g) Piden enviar un personal en sitio bajo un tiempo de respuesta de doce horas en caso no sea solucionado remotamente, sin embargo hay un personal residente dedicado que piden en bases en el punto f), el mismo que haría las manos remotas de ser el caso, en ese sentido solicitamos aclarar bajo que situaciones u horarios se requiere cubrir esta atención en sitio?	cyber	EL horario de trabajo es el de oficina en días laborables (lunes a viernes), los fines de semana o feriados cuando el personal viaja se da un plazo de 12 horas para apersonarse de no haberse solucionado el problema de manera remota.
49	Pág 17 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Aclarar qué se entiende por largo tiempo de entrega (indicado en sección I)?	cyber	Se refiere a estimar el peor escenario de tiempo de entrega de repuestos.
50	Pág 18 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Confirmar bajo qué casuísticas no consideraría PETROPERU como idóneo al personal del postor. sección m)	cyber	Sin ser limitativo: Desempeño bajo, no muestre capacidad de resolución de problemas o taltan de conocimientos del tema, sin claridad en sus comunicaciones, baja apertura al dialogo y transferencia de conocimientos del sistema, entre otros, que dificulten la resolución e identificación de problemas de ciberseguridad.
51	Pág 18 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Agradeceremos nos puedan reconfirmar que el presente requerimiento hace referencia a que el equipo de trabajo o personal presentado como parte de la propuesta presentada por el postor deberá ser el mismo que ejecute el servicio adjudicado. sección q)	cyber	Se confirma.
52	Pág 18 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Confirmar si la custodia de equipos se refiere a plataformas existentes que dispone PETROPERU en su red OT? De ser así, Se solicita brindar el listado de todas las plataformas (tipo de plataforma, serial numbers, tipo de licencias, marca, modelo, fecha de cese de contrato de soporte/licencia con los fabricantes) que requieren custodia a cargo del proveedor a fines de determinar los riesgos que incurren en los mismos. Sección t)	cyber	El numeral t) de Obligaciones y responsabilidades del contratista, se refiere a los equipos de propiedad del contratista, como Laptops, Teléfonos celulares intrínsecos, entre otros.
53	Pág 18 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Se necesita brindar mayor detalle del alcance esperado en la custodia de equipos, si el mismo implica delegar todas las actividades en la administración de cada plataforma (incidentes/requerimientos)? mantenimiento preventivo? monitore de salud de los equipos? monitorear los contratos de soporte/licencia del fabricante para cada plataforma durante el servicio? entre otros que describa PETROPERU. Sección t)	cyber	El numeral t) de Obligaciones y responsabilidades del contratista, se refiere a los equipos de propiedad del contratista, como Laptops, Teléfonos celulares intrínsecos, entre otros.
54	Pág 18 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Dentro de la custodia de los equipos, se necesita aclarar si será responsabilidad de PETROPERU los gastos incurridos ya sea por concepto de renovación de contrato de soporte/licencia con los fabricantes y/o por actualización tecnológica ante obsolecencia (fin de ciclo de los equipos). sección t)	cyber	El numeral t) de Obligaciones y responsabilidades del contratista, se refiere a los equipos de propiedad del contratista, como Laptops, Teléfonos celulares intrínsecos, entre otros.
55	Pág 18 20.OBLIGACIONES Y RESPONSABILIDADES DEL CONTRATISTA	Favor aclarar que queda excluido del servicio cualquier ampliación de las plataformas (ya sea nuevas licencias, componentes o tarjetas del equipo) dentro de la custodia de los equipos de PETROPERU. En ese sentido sería tratado como será tratado mediante un proyecto especial fuera del alcance	cyber	El numeral t) de Obligaciones y responsabilidades del contratista, se refiere a los equipos de propiedad del contratista, como Laptops, Teléfonos celulares intrínsecos, entre otros.