

PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20606052112	Fecha de envío :	09/05/2024
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	20:40:09

Observación: Nro. 1

Consulta/Observación:

En el numeral IV del literal g) de los DOCUMENTOS DE PRESENTACION OBLIGATORIA y se exige lo siguiente: Documentación sustentatoria que evidencie al equipo CSIRT propuesto, como miembro del FIRST esta documentación debe estar a nombre del postor.

Esta exigencia es arbitraria y atenta contra los principios de: Libertad de Concurrencia, Competencia e Igualdad de Trato. Se supone que el postor o los postores en caso de consorcios, serán finalmente los que ejecuten la prestación objeto de la convocatoria y sobre ellos recaerá cualquier tipo de responsabilidad que se suscite, por lo que no se entiende porque se exige que el personal propuesto sea miembro del FIRST, la cual no es una organización certificada, es solo es un grupo de personas que se unen para tratar medidas de desarrollo preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

Una disposición como esta no hace sino evidenciar una discriminación con la finalidad de restringir la pluralidad de postores. Si el área usuaria esta interesada en contratar a una empresa que pueda desarrollar la prestación objeto de la convocatoria deberá solicitar que esta cuente con la experiencia en el rubro y la experiencia se sustenta con la facturación, la cual demuestra objetivamente la EXPERIENCIA EN LA ESPECIALIDAD.

En base a lo señalado SOLICITÓ que el requerimiento de ser miembros del CSIRT que ante un incidente de seguridad digital ayudarán a OSIPTTEL a mitigar, contener y dar solución, sea RETIRADO por ser restringir la pluralidad de postores o en su defecto sea colocado como OPCIONAL o como un CRITERIO DE EVALUACION, de lo contrario se estaría vulnerando los principios que inspiran la contratación estatal.

Acápite de las bases : Sección: Especifico Numeral: 2.2.1.1.

Literal: G

Página: 17

Artículo y norma que se vulnera (En el caso de Observaciones):

Artículo 2, literal a, b y e de la Ley 30225

Análisis respecto de la consulta u observación:

No se acoge la observacion, por cuanto es necesario para el OSIPTTEL que el equipo CSIRT este acreditado por el FIRST, ya que esto demuestra el respaldo al mismo ante una comunidad reconocida mundialmente en la respuesta a incidentes de seguridad, el cual es el objeto de la presente contratación. Así mismo, en la "Guía para la Conformación e Implementación del Equipo de Respuestas ante Incidentes de Seguridad Digital" normada por la Secretaría de Gobierno y Transformación Digital (Ente rector de las entidades públicas en materia de seguridad digital) el FIRST es mencionado repetidas ocasiones como una comunidad de referencia.

Así mismo, no se estan infringiendo los principios de libertad de concurrencia ni competencia ni igualdad de trato, toda vez que actualmente existen más de 10 organizaciones con CSIRT acreditados (<https://www.first.org/members/teams/>), cabe resaltar que en las actuaciones preparatorias para el presente procedimiento de selección se verificó la pluralidad de postores.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20606052112	Fecha de envío :	09/05/2024
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	20:40:09

Observación: Nro. 2

Consulta/Observación:

En el numeral IV del literal g) de los DOCUMENTOS DE PRESENTACION OBLIGATORIA y se exige lo siguiente: Copia de la certificación ISO/IEC 27001 donde se detalle el alcance e incluya los procesos del CyberSOC. Exigir una certificación ISO/IEC 27001 constituye una grave irregularidad porque se pretende introducir dentro de los DOCUMENTOS DE PRESENTACION OBLIGATORIA y por ende dentro de los Términos de Referencia ya que hace referencia al servicio que se va a prestar, evaluaciones o certificaciones internacionales que estarían dirigidas a evaluar la calidad de los bienes-servicios a contratarse o las empresas, LO CUAL ESTA PROHIBIO. Quiero señalar, con respecto a la formulación de las EETT o TDR elaboradas por el área usuaria, que el Órgano Supervisor de las Contrataciones Estatales en reiterados documentos ha señalado que en estos no pueden exigirse certificaciones o evaluaciones internacionales pues no son una condición determinante para la operatividad de estos y podría restringir el principio de libre competencia. En el portal web del OSCE se encuentra un documento titulado Instructivo: Formulación de Especificaciones Técnicas para la Contratación de Bienes y Términos de Referencia para la Contratación de Servicios y Consultorías en General, emitido mediante Resolución N°423-2013-OSCE/PRE, en el cual se establece que: En las EETT o TDR no se deben requerir certificaciones internacionales sobre la calidad de los bienes o servicios a contratarse como, por ejemplo, las certificaciones ISO, pues no son una condición determinante para la operatividad de estos y podrían restringir la libre competencia (Resolución N°423-2013-OSCE/PRE, página 10).

Enlace:
<https://cdn.www.gob.pe/uploads/document/file/3143698/INSTRUCTIVO%20ELABORACION%20EETT%20Y%20TDR%20.pdf.pdf?v=1653422891>

En base a lo señalado SOLICITÓ que el requerimiento de contar con una certificación ISO/IEC 27001 donde se detalle el alcance e incluya los procesos del CyberSOC., sea RETIRADO por ser restringir la pluralidad de postores o en su defecto sea colocado como OPCIONAL o como un CRITERIO DE EVALUACION, de lo contrario se estaría vulnerando los principios que inspiran la contratación estatal.

Acápite de las bases : **Sección:** Especifico **Numeral:** 2.2.1.1 **Literal:** h **Página:** 17

Artículo y norma que se vulnera (En el caso de Observaciones):

Artículo 2, literal a, b y e de la Ley 30225

Análisis respecto de la consulta u observación:

No se acoge la obsrevacion, por lo que se requiere que el postor que proveera servicios de seguridad, el mismo que tendra acceso a activos críticos de la institución, cuente con una acreditación que garantice que los procesos del CYBERSOC se realizan de forma segura. Así mismo, no se estan infringiendo los principios de libertad de concurrencia ni competencia ni igualdad de trato, toda vez que actualmente existen varias organizaciones con CYBERSOC que cuentan con certificación ISO/IEC 27001, cabe resaltar que en las actuaciones preparatorias para el presente procedimiento de selección se verificó la pluralidad de postores.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20606052112	Fecha de envío :	09/05/2024
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	20:40:09

Observación: Nro. 3

Consulta/Observación:

El presente procedimiento de selección es un SERVICIO DE GESTION DE EVENTOS E INCIDENTES DE SEGURIDAD DIGITAL, sin embargo, no se entiende por qué se pretende incluir de contrabando la adquisición o empleo de hardware (servidor de recolección, servidor de monitoreo u otros componentes). Se dice en los términos de referencia que el hardware provisto por el contratista debe poder ser instalado en un rack de 19 y debe contar con fuentes redundantes, etc.

Finalmente lo que importa en este tipo de servicios es el monitoreo, la recolección de eventos y la respuesta ante incidentes y estos pueden ser realizados con el uso de softwares especializados que no necesitan de un soporte físico tipo servidor, sino solo del uso de un software especializado desarrollado sobre una arquitectura basada en agente ligero, lo cual permitiría menores y mejores tiempos de respuesta y contención activa ante un ciberataque.

Por lo que se solicita considerar como alternativa una plataforma basada en agente que libere del uso de infraestructura específica para su normal desempeño.

Acápite de las bases : Sección: Especifico Numeral: 3.1 Literal: G Página: 24

Artículo y norma que se vulnera (En el caso de Observaciones):

Artículo 2, literal a, b y e de la Ley 30225

Análisis respecto de la consulta u observación:

No se acoge la observacion por cuanto el OSIPTEL ha establecido los componentes mínimos para el servicio a contratar en base a su experiencia, necesidades de seguridad y capacidades técnicas, por lo que no se considera la alternativa propuesta por el postor.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20606052112	Fecha de envío :	09/05/2024
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	20:40:09

Consulta: Nro. 4

Consulta/Observación:

En el literal C denominado Experiencia del Postor en la Especialidad, se indica que se consideraran como servicios similares: a) Servicios de CyberSOC y/o b) Servicios de Ciberinteligencia y/o c) Servicios de Seguridad Informática Gestionada y/o d) Servicios de Administración y monitoreo de plataformas de seguridad.

Al respecto, es importante tener presente que el presente proceso de selección tiene por objeto la contratación del, SERVICIO DE GESTION DE EVENTOS E INCIDENTES DE SEGURIDAD DIGITAL

Como se puede observar, el área usuaria ha hecho una redundancia innecesaria entre los servicios similares al objeto de la convocatoria, generando con ello un obstáculo para la mayor participación de postores. Es decir, si interpretamos literalmente el texto descrito como servicios similares al objeto de la convocatoria, nos percataremos que ella hace referencia a los servicios de un SOC. Entonces, si el objeto de la convocatoria hace referencia a un servicio de SOC y los servicios similares también AMBOS TEXTOS NO SON SIMILARES, SINO IGUALES y por ello existe una redundancia innecesaria que restringe la participación de una mayor cantidad de postores.

Por ello en aras de fomentar la más amplia, objetiva e imparcial concurrencia, pluralidad y participación de postores solicitamos incluir dentro del concepto de similares, los servicios de:

Análisis de riesgos y/o análisis y remediación de riesgos, servicios de prestación de antivirus y/o antispam y/o soluciones de ciberseguridad.

Acápite de las bases : Sección: Especifico Numeral: 3.2 Literal: C Página: 33

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Los servicios de Análisis de riesgos y/o análisis y remediación de riesgos son términos generales y usan una metodología que comprende aspectos diferentes sobre probabilidad e impacto, siendo que la gestión de eventos e incidentes evalúan las situaciones reales que suceden sobre la infraestructura tecnológica a monitorear.

Los servicios de prestación de antivirus y/o antispam y/o soluciones de ciberseguridad son componentes de software para tareas específicas siendo que el servicio de gestión de eventos e incidentes de seguridad monitorea eventos de seguridad relacionados a estos componentes por lo cual los servicios de prestación de antivirus y/o antispam y/o soluciones de ciberseguridad no pueden ser considerados como similares

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 5

Consulta/Observación:

COntirmar que se puede presentar propuesta del servicio de empresas que cuenta con la infraestructura fisica de su SOC fuera del Perú, teniendo en cuenta que es un servicio remoto.

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: j Página: 24

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

En los TDR, no se ha especificado que los CYBERSOC deban estar ubicados solo en PERÚ, solo existe la precisión de que "Los CyberSOC deben ubicarse geográficamente distante uno del otro, con una distancia mínima de 8 kilómetros entre ambos".

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 6

Consulta/Observación:

Parrafo: El alcance del servido comprende la gestión de eventos e incidentes de seguridad de los siguientes activos:

Consulta:

Teniendo en cuenta que para brindar el servicio de SOC se tienen que implementar sondas o colectores. Confirmar que desde el Datacenter donde se instalará el colector, se tiene conectividad a todos los activos onpremise

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: VII Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se confirma que desde el Datacenter se tiene conectividad a los activos a monitorear

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Se agregara en las bases lo siguiente:

(...)

G. HARDWARE Y SOFTWARE PARA LA PRESTACION DEL SERVICIO

(...)

El hardware provisto por el contratista debe poder ser instalado en un rack de 19" y debe contar con fuentes redundantes, las conexiones electricas con del tipo C-13 y C14 y la conexion a la red sera con conexion ethernet RJ45.

Cabe resaltar que desde el Datacenter se tiene conectividad a los activos a monitorear.

(...)

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 7

Consulta/Observación:

Parrafo:
El alcance del servido comprende la gestión de eventos e incidentes de seguridad de los siguientes activos:

Consulta:

¿Cual es el throughput del NDR?

Acápite de las bases : Sección: Especifico Numeral: VII Literal: VII Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

El throughput del NDR es 12MB

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Se agregara en las bases lo siguiente:

(...)
VII. DESCRIPCIÓN DEL SERVICIO
(...)
01 NDR (12 MB)
(...)

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 8

Consulta/Observación:

Consulta:

- 1.- ¿Cuántos usuarios tienen 0365 ?
- 2.-¿ En el uso de 0365 se tiene en más de un tenant ?

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: VII Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

750 Usuarios y un solo tenant

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Se agregara en las bases lo siguiente:

- (...)
- VII. DESCRIPCIÓN DEL SERVICIO
- (...)
- Microsoft 365 (750 Usuarios y 01 tenant)
- (...)

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 9

Consulta/Observación:

Consulta:

¿Cuales son las capacidades tecnológicas que espera del soc? INDICAR SI / NO u Opcional

SIEM :

SOAR :

UEBA :

Análisis de vulnerabilidades :

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: VII Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Lo esperado como mínimo para el servicio ha sido establecido en los TDR, y como se precisa "El contratista proveerá todo el hardware (servidor de recolección, servidor de monitoreo, u otros componentes) y software necesario para la prestación óptima del servicio".

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 10

Consulta/Observación:

Parrafo:

El alcance del servido comprende la gestión de eventos e incidentes de seguridad de los siguientes activos:

- ¿ 08 Servidores de aplicaciones IIS
- ¿ 02 Active Directory
- ¿ 03 Servidores ORACLE
- ¿ 02 servidor Microsoft SQL

Consulta:

Por favor indicar el número total de servidores que tiene la entidad (formen o no formen parte del alcance de este TDR o que estiman tener por crecimiento), para tener como referencia el porcentaje de servidores que están incluidos como fuente a monitorear

Acápite de las bases : Sección: Especifico Numeral: VII Literal: VII Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se cuenta con 125 servidores entre físicos y virtuales

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Se agregara en las bases lo siguiente:

- (...)
- VII. DESCRIPCIÓN DEL SERVICIO
- (...)

El monitoreo de los activos debe soportar como mínimo protocolo SYSLOG y/o SNMP y/o WMI y/o API's; si durante la implementación se ve la necesidad de cambiar alguno de los activos críticos por otro, esto deberá ser soportado por el proveedor considerando que la comunicación será por los protocolos antes mencionados.

Se cuenta con 125 servidores entre físicos y virtuales.

(...)

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 11

Consulta/Observación:

Parrafo: "Serán labores realizadas por los analistas expertos, que permitirán descubrir amenazas avanzadas que no son detectadas por los controles de seguridad automatizados de prevención-detección. Esta labor representará prácticas muy avanzadas en seguridad de cara a identificar de forma proactiva amenazas persistentes y ocultas."

Consulta:

Confirmar que la ejecución de ejercicios está acotada a dos ejercicios en un año , caso contrario indicar cuantos ejercicios de Threat Hunting se deben tener en un año , teniendo en cuenta que cada ejercicio puede tomar tiempos por encima de 60 horas

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: D Página: 23

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

El componente de THREAT HUNTING es constante e ininterrumpido durante toda la prestación del servicio.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 12

Consulta/Observación:

Parrafo: "Serán labores realizadas por los analistas expertos, que permitirán descubrir amenazas avanzadas que no son detectadas por los controles de seguridad automatizados de prevención-detección. Esta labor representará prácticas muy avanzadas en seguridad de cara a identificar de forma proactiva amenazas persistentes y ocultas."

COnsulta:

Confirmar que los ejercicios de Threat Hunting se ejecutaran en horario de oficina.

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: D Página: 23

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

El componente de THREAT HUNTING es constante e ininterrumpido durante toda la prestación del servicio.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 13

Consulta/Observación:

Parrafo: "Serán labores realizadas por los analistas expertos, que permitirán descubrir amenazas avanzadas que no son detectadas por los controles de seguridad automatizados de prevención-detección. Esta labor representará prácticas muy avanzadas en seguridad de cara a identificar de forma proactiva amenazas persistentes y ocultas."

CONSULTA :

Confirmar que el alcance del servicio de Threat hunting solo corresponde a la comunicación de las recomendaciones sobre lo encontrado , la ejecución será por parte del equipo tecnico del cliente o de sus proveedores de sus tecnologias implementadas.

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: D Página: 23

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Como se indica en el TDR, el contratista es quien ejecuta o realiza las labores de THREAT HUNTING.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 14

Consulta/Observación:

Parrafo: El alcance del servido comprende la gestión de eventos e incidentes de seguridad de los siguientes activos:

COnsulta:Confirmar si el listado de fuentes no cambiará durante el contrato , y no forma parte del alcance el reemplazo/adición/modificación de las fuentes de logs , de indicar lo contrario , sirvase de proporcionar el crecimiento en número/tipo de fuentes .

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: VII Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Como se indica en el TDR, "...si durante la implementación se ve la necesidad de cambiar alguno de los activos críticos por otro, esto deberá ser soportado por el proveedor¿", además no se ha solicitado que consideren el crecimiento del número de activos a monitorear

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 15

Consulta/Observación:

Parrafo: El contratista proveerá de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) que ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad, el equipo deberá estar inscrito como miembro del FIRST (Forum of Incident Response and Security Teams).

Consulta:

Frente a lo indicado en el ítem donde se menciona que : "ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad". Confirmar que lo requerido es acompañamiento/recomendaciones y no ejecución ya que entendemos que la ejecución será por parte del equipo técnico del cliente o de sus proveedores de sus tecnologías implementadas.

Acápites de las bases : Sección: Específico Numeral: VII Literal: C Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

El objetivo del equipo CSIRT ante un incidente es ayudar a OSIPTEL a mitigar, contener y dar solución, esto implica de ser necesario ejecutar acciones previa coordinación y autorización del OSIPTEL.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Se agregará en las bases lo siguiente:

- (...)
- C. RESPUESTA ANTE INCIDENTES DE SEGURIDAD
- (...)

El contratista proveerá de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) que ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad, esto implica de ser necesario ejecutar acciones previa coordinación y autorización del OSIPTEL, el equipo deberá estar inscrito como miembro del FIRST (Forum of Incident Response and Security Teams).

(...)

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 16

Consulta/Observación:

Parrafo:
El contratista proveerá de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) que ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad, el equipo deberá estar inscrito como miembro del FIRST (Forum of Incident Response and Security Teams).
Consulta:
Frente a lo indicado en el ítem donde se menciona que : "ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad". Confirmar que lo requerido es acompañamiento/recomendaciones y no ejecución ya que entendemos que la ejecución será por parte del equipo técnico del cliente o de sus proveedores de sus tecnologías implementadas.

Acápite de las bases : Sección: Especifico Numeral: VII Literal: C Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

El objetivo del equipo CSIRT ante un incidente es ayudar a OSIPTEL a mitigar, contener y dar solución, esto implica de ser necesario ejecutar acciones previa coordinación y autorización del OSIPTEL.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Se agregara en las bases lo siguiente:
(...)
C. RESPUESTA ANTE INCIDENTES DE SEGURIDAD
(...)
El contratista proveera de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) que ayudara al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad, esto implica de ser necesario ejecutar acciones previa coordinacion y autorizacion del OSIPTEL, el equipo debera estar inscrito como miembro del FIRST (Forum of Incident Response and Securirty Teams).
(...)

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 17

Consulta/Observación:

Parrafo: El contratista proveerá de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) que ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad, el equipo deberá estar inscrito como miembro del FIRST (Forum of Incident Response and Security Teams).

Consulta:

Confirmar que este acompañamiento es de manera remota

Acápite de las bases : Sección: Especifico Numeral: VII Literal: C Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Como se indica en el TDR, sección Lugar de prestación del servicio, el servicio es ejecutado principalmente de manera remota, de ser necesaria visitas físicas se realiza previa coordinación del OSIPTEL.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 18

Consulta/Observación:

Parrafo:
El contratista proveerá de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) que ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad, el equipo deberá estar inscrito como miembro del FIRST (Forum of Incident Response and Security Teams).

Consulta:
Confirmar que cuando se refiere que el equipo debe estar inscrito en el FIRST , se refiere al equipo del SOC , o al SOC propiamente dicho

Acápite de las bases : Sección: Especifico Numeral: VII Literal: C Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Como se indica en el TDR, sección documentos para la admisión de la propuesta, el registro del CSIRT en el FIRST debe ser a nombre del postor.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 19

Consulta/Observación:

Parrafo:El contratista proveerá de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) que ayudará al OSIPTEL a mitigar, contener y dar solución ante un incidente de seguridad, el equipo deberá estar inscrito como miembro del FIRST (Forum of Incident Response and Security Teams).

Consulta:

Cual es el promedio de incidentes de ciberseguridad que ha tenido OPSITEL en estos últimos dos años

Acápite de las bases : Sección: Especifico Numeral: VII Literal: C Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

El OSIPTEL define incidente como aquel evento que ha comprometido su seguridad con un impacto negativo. Si bien el OSIPTEL no ha tenido en los 2 últimos años incidentes de ciberseguridad, esto no es un factor determinante para el postor ya que el OSIPTEL es una entidad del sector público y este sector viene siendo atacado continuamente por ciberdelicuentes y/o hacktivistas.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 20

Consulta/Observación:

parrafo:
"El grado de bachiller o título profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <http://www.titulosinstitutos.pe/>, según corresponda. En caso el grado de bachiller o título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida."

Consulta:
Del personal clave , confirmar que es posible presentar perfiles extranjeros y que estos no tengan que estar registrados en SUNEDU (se compartirá copia del diploma oficial)

Acápíte de las bases : Sección: Especifico Numeral: XX Literal: XX Página: 28

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se precisa que es posible presentar personal con estudios en el extranjero, cabe resaltar que los grados y títulos obtenidos en el extranjero obtienen validez en el Perú cuando estos están otorgada por la autoridad competente (SUNEDU), a través de los procedimientos de ¿revalidación¿ o ¿reconocimiento¿ regulados en la normativa especial de la materia; por lo que resulta razonable concluir que, a fin de determinar si los postores cuentan con las capacidades necesarias para ejecutar las prestaciones que son objeto del contrato-, se acredita que los profesionales extranjeros que integran el personal profesional clave, cumplen con la ¿formación académica¿ válida en el Perú, para cuyo efecto, deberá presentarse copia simple del documento de la revalidación o del reconocimiento, del grado académico o título profesional otorgados en el extranjero, según corresponda.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 21

Consulta/Observación:

Parrafo:"Cada CyberSOC así como los procesos que soportan el servicio de CyberSOC ofertado, deben de contar con certificación vigente en el estándar internacional de Seguridad de la Información ISO/IEC 27001:2013;"

Consulta:

Teniendo en cuenta que las infraestructuras de SOC están en HA geografica. Confirmar que se aceptarán propuestas donde uno de ellos se encuentra certificado en ISO/IEC 27001

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: i Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Como se indica en el TDR "Cada CyberSOC así como los procesos que soportan el servicio de CyberSOC ofertado, deben de contar con certificación vigente en el estándar internacional de Seguridad de la Información ISO/IEC 27001:2013"

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 22

Consulta/Observación:

Parrafo:
"El postor deberá de contar con procedimientos para el manejo de diversos tipos de incidentes tales como phishing, infecciones de malware, alteración no autorizada del sitio web y ataques de negación de servicio (DoS), ransomware."

Consulta:
Confirmar que los mencionados procedimientos serán los desarrollados para su entorno y arquitectura

Acápíte de las bases : Sección: Especifico Numeral: VII Literal: C Página: 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:
El postor que proveerá al CSIRT debe contar previamente a la contratación del servicio con los procedimientos establecidos, los mismos que son solicitados como documentos para la admisión de la propuesta.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 23

Consulta/Observación:

parrafo: "El servicio debe ser brindado a través de dos (02) Cyber Security Operation Center (CyberSOC) estado activo-activo"

Consulta:
Confirmar si el servicio puede ser ofrecido con infraestructura que esté en sedes como activo - pasivo , no obstante cumpliendo con el 99.9% de disponibilidad requerida.

Acápite de las bases : Sección: Especifico Numeral: VII Literal: i Página: 24

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Como se indica en el TDR "El servicio debe ser brindado a través de dos (02) Cyber Security Operation Center (CyberSOC) estado activo-activo" para garantizar la continuidad del servicio.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:55:27

Consulta: Nro. 24

Consulta/Observación:

parrafo:
"El análisis de Ciberriesgo brindará un reporte mensual de seguridad sobre la postura de riesgo del OSIPTEL. Este análisis se logrará recopilando continuamente los datos de inteligencia de seguridad y calificará a OSIPTEL numéricamente en categorías de seguridad cruciales."
Consulta:
Confirmar que lo mencionado hace parte de un servicio de Cyber threat intelligence que te permita evaluar activos en dark web, deppweb , fuga de contraseñas , evaluación de terceros. De requerir un CTI por favor indicar el número de dominios , palabras claves y takedowns. Por favor limitar el alcance de estos servicios .

Acápite de las bases : Sección: Especifico Numeral: VII Literal: F Página: 23

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Como se indica en el TDR, el análisis de Ciberriesgo brindará un reporte mensual de seguridad sobre la postura de riesgo del OSIPTEL, pero para este análisis no es un requerimiento que existan evaluaciones específicas de activos en dark web, deppweb , fuga de contraseñas, evaluación de terceros como parte de un servicio de Cyber THREAT INTELLIGENCE.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna

Entidad convocante : ORGANISMO SUPERVISOR DE INVERSION PRIVADA EN TELECOMUNICACIONES

Nomenclatura : AS-SM-6-2024-OSIPTEL-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : Servicio de Gestión de Eventos e Incidentes de Seguridad Digital

Ruc/código :	20477830626	Fecha de envío :	09/05/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:57:33

Consulta: Nro. 25

Consulta/Observación:

Teniendo en cuenta que es requerido hardware, y estos tienen un tiempo de llegada de 40 o 45 días.

COnsulta:

Confirmar que el entregable n2 puede ser hasta 60 días

Acápíte de las bases : Sección: Especifico Numeral: X Literal: entregable Página: 25

Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

La necesidad del OSIPTEL es contar con el servicio implementado a los 30 días calendario, ya que el servicio es de suma importancia para garantizar la seguridad de los activos críticos del OSIPTEL.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Ninguna