

PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20552075341	Fecha de envío :	14/03/2023
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	18:09:34

Consulta: Nro. 1

Consulta/Observación:

Dice: "Colegiatura vigente y habilitada del personal clave, de acuerdo a lo señalado en el numeral 10 de los términos de referencia."

Consulta: Sírvase de confirmar que la colegiatura vigente y habilitada será requerida solo si el personal presentado es titulado profesional, en caso sea bachiller o técnico este requerimiento se considerara como opcional.

Acápite de las bases : **Sección:** Especifico **Numeral:** 2.3 **Literal:** J **Página:** 18

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se aclara que la colegiatura vigente y habilitada solo será necesaria para el personal clave "jefe de proyecto" el cual debe ser un ingeniero titulado.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20552075341	Fecha de envío :	14/03/2023
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	18:09:34

Consulta: Nro. 2

Consulta/Observación:

Dice: "Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática"

Consulta: Sirvase de confirmar que el especialista en seguridad puede ser Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática y/o Ingeniería de Seguridad y Auditoría Informática y/o Informática y Sistemas.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.2 **Literal:** A.1.1 **Página:** 44

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se acoge la consulta y se modificará el TDR.

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

En el numeral A.1 del literal A del numeral 10:

Dice:

Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática

Debe decir:

Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática y/o Ingeniería de Seguridad y Auditoría Informática y/o Informática y Sistemas.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20552075341	Fecha de envío :	14/03/2023
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	18:09:34

Consulta: Nro. 3

Consulta/Observación:

Dice: "Deberá contar con tres (3) años de experiencia en seguridad informática y/o en implementación y/o administración de la solución objeto de la convocatoria."

Consulta: Sírvase de confirmar que será aceptado que los especialista en seguridad pueden contar con un mínimo de dos (02) años de experiencia en seguridad informática y/o implementación y/o administración de la solución objeto de la convocatoria

Acápíte de las bases : Sección: Especifico Numeral: 3.2 Literal: A.2.1 Página: 46

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se acoge la consulta y se modificará el TDR.

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

En el numeral A.2 del literal A del numeral 10:

Dice:

Deberá contar con tres (3) años de experiencia en seguridad informática y/o en implementación y/o administración de la solución objeto de la convocatoria

Debe decir:

Deberá contar con dos (2) años de experiencia en seguridad informática y/o en implementación y/o administración de la solución objeto de la convocatoria.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20552075341	Fecha de envío :	14/03/2023
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	18:09:34

Consulta: Nro. 4

Consulta/Observación:

Dice: "Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática"

Consulta: Sírvase de confirmar que el especialista en seguridad puede ser Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática y/o Ingeniería de Seguridad y Auditoría Informática y/o Informática y Sistemas.

Acápite de las bases : Sección: Especifico Numeral: 3.2 Literal: A.2.2 Página: 46

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se acoge la consulta y se modificará el TDR.

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

En el numeral A.1 del literal A del numeral 10:

Dice:

Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática

Debe decir:

Titulado o Bachiller o Técnico en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónica y/o Redes y/o Comunicaciones y/o Computación y/o Computación e Informática y/o Ingeniería de Seguridad y Auditoría Informática y/o Informática y Sistemas.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20552075341	Fecha de envío :	14/03/2023
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	18:09:34

Consulta: Nro. 5

Consulta/Observación:

Dice: "Deberá contar con tres (3) años de experiencia en seguridad informática y/o en implementación y/o administración de la solución objeto de la convocatoria."

Consulta: Sírvase de confirmar que será aceptado que los especialista en seguridad pueden contar con un mínimo de dos (02) años de experiencia en seguridad informática y/o implementación y/o administración de la solución objeto de la convocatoria

Acápíte de las bases : Sección: Especifico Numeral: 3.2 Literal: A.1.2 Página: 45

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se acoge la consulta y se modificará el TDR.

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

En el numeral A.2 del literal A del numeral 10:

Dice:

Deberá contar con tres (3) años de experiencia en seguridad informática y/o en implementación y/o administración de la solución objeto de la convocatoria

Debe decir:

Deberá contar con dos (2) años de experiencia en seguridad informática y/o en implementación y/o administración de la solución objeto de la convocatoria.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608993909

Nombre o Razón social : IT ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 18:30:13

Consulta: Nro. 6

Consulta/Observación:

Dice: "La solución debe contar con la funcionalidad de detección y respuesta extendida (XDR) y la evaluación continua de vulnerabilidades de los endpoints para reducir el riesgo organizacional general, por lo menos en sistemas operativos Windows y Linux. Esta funcionalidad será opcional en el sistema operativo MacOS. La solución XDR debe combinar los conocimientos integrados de los datos de la red, la nube y los endpoints".

Consulta: A fin de permitir mayor pluralidad de postores y fabricantes, sírvase a la entidad de considerar este requerimiento como opcional.

Acápites de las bases : Sección: Especifico Numeral: 4.1.1 Literal: D **Página: 21**

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que el requerimiento indicado en el numeral 4.1.1.d de los TDR es mínimo para la Entidad.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608993909

Nombre o Razón social : IT ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 18:30:13

Consulta: Nro. 7

Consulta/Observación:

Dice: "En sistemas operativos Linux, debe soportar al menos las siguientes versiones:

- CentOS 7 y posteriores
- Red Hat Enterprise Linux 7 y posteriores
- Ubuntu 16 y posteriores"

Consulta: Sirvase a la entidad de confirmar que a fin de permitir mayor pluralidad de postores y fabricantes, la solución ofertada debe soportar al menos desde Ubuntu a partir de 18.04 y posteriores; o en su defecto, podrá proporcionar una solución diferente para satisfacer el requerimiento en dichos sistemas operativos.

Acápites de las bases : **Sección:** Especifico **Numeral:** 4.1.2 **Literal:** D **Página:** 21

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: De acuerdo a lo establecido en el literal e. del numeral 4.1.2, el requerimiento de la Entidad es Ubuntu 16 y posteriores. Cabe señalar, que para sistemas legacy el postor podrá utilizar una herramienta de terceros.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20608993909	Fecha de envío :	14/03/2023
Nombre o Razón social :	IT ONE S.A.C.	Hora de envío :	18:30:13

Consulta: Nro. 8

Consulta/Observación:

Dice: "El agente deberá contar con la funcionalidad de detección y respuesta extendida (XDR). Esta funcionalidad sera opcional en el sistema operativo MacOS."

Consulta: Sírvase de confirmar que a fin de permitir mayor pluralidad de postores, este requerimiento puede ser considerado como opcional para sistemas operativos Linux y MacOS.

Acápite de las bases : Sección: Especifico Numeral: 4.1.8 Literal: A Página: 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que el requerimiento indicado en el numeral 4.1.8.a de los TDR es mínimo para la Entidad.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608993909

Nombre o Razón social : IT ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 18:30:13

Consulta: Nro. 9

Consulta/Observación:

Dice: "Mínimo 100.000 eventos por segundo"

Consulta: Sírvase a la entidad de aclarar este requerimiento, ya que una solución de tipo SOAR no se mide, dimensiona o licencia por una métrica de eventos por segundos, en base a ello se le solicita a la entidad confirmar que este requerimiento puede ser considerado como opcional.

Acápites de las bases : Sección: Especifico Numeral: 4.2 Literal: N/A **Página:** 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que, con el fin de fomentar la pluralidad de postores, lo expresado en el numeral 4.2 de los TDR quedará de la siguiente forma: "Mínimo 50,000 eventos por segundo", tomando en cuenta la cantidad de dispositivos que conforman la arquitectura tecnológica de la Entidad actual y proyectada para 3 años.

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

En el numeral 4.2:

Dice:

Mínimo 100,000 eventos por segundo

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20608993909	Fecha de envío :	14/03/2023
Nombre o Razón social :	IT ONE S.A.C.	Hora de envío :	18:30:13

Consulta: Nro. 10

Consulta/Observación:

Dice: "Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el postor deberá entregar un portal web seguro con doble factor de autenticación para revisar las investigaciones, para por lo menos 20 usuarios de administración"

Consulta: Sírvase a la entidad de confirmar que el requerimiento será considerado para el ITEM 2 de forma similar a lo solicitado en el ITEM 1, es decir, un mínimo de 10 usuarios de administración.

Acápíte de las bases : Sección: Especifico Numeral: 5.1.2 Literal: R Página: 32

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que en el ítem 5.1.2.r se considerará un mínimo de 10 usuarios concurrentes.

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

En el literal r del numeral 5.1.1:

Debe decir:

Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el postor deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones, para por lo menos 10 usuarios concurrentes.

En el literal r del numeral 5.1.2:

Debe decir:

Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el postor deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones, para por lo menos 10 usuarios concurrentes.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608993909

Nombre o Razón social : IT ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 18:30:13

Consulta: Nro. 11

Consulta/Observación:

Dice: "Servicio de Solución de Respuesta, Automatización y Orquestación de la Seguridad (SOAR)."

Consulta: Sírvase a la entidad de confirmar que la cantidad de usuarios que deben acceder a la plataforma de SOAR será de un mínimo de 2 usuarios.

Acápites de las bases : Sección: Especifico Numeral: 4.2 Literal: N/A **Página:** 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20608993909	Fecha de envío :	14/03/2023
Nombre o Razón social :	IT ONE S.A.C.	Hora de envío :	18:30:13

Consulta: Nro. 12

Consulta/Observación:

Dice: "Servicio de Solución de Respuesta, Automatización y Orquestación de la Seguridad (SOAR)."

Consulta: Sírvase a la entidad de confirmar que se debe proporcionar una herramienta de propósito específico de tipo SOAR para brindar el servicio solicitado.

Acápites de las bases : Sección: Especifico Numeral: 4.2 Literal: N/A Página: 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Se aclara que se requiere una solución SOAR de un solo fabricante, y no una integración de soluciones distintas que imiten una solución SOAR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20608993909	Fecha de envío :	14/03/2023
Nombre o Razón social :	IT ONE S.A.C.	Hora de envío :	18:30:13

Consulta: Nro. 13

Consulta/Observación:

Dice: "Servicio de Solución de Respuesta, Automatización y Orquestación de la Seguridad (SOAR)."

Consulta: Sírvase a la entidad de confirmar que no se aceptaran soluciones de propósito general o que tenga algún funcionalidad o características a través de un addon para realizar alguna tarea de orquestación y/o automatización.

Acápite de las bases : Sección: Especifico Numeral: 4.2 Literal: N/A Página: 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Se aclara que se requiere una solución SOAR de un solo fabricante, y no una integración de soluciones distintas que imiten una solución SOAR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 14

Consulta/Observación:

Dice:
05 hosts de virtualización Vmware ESXi 6.0 y vSphere 6 Enterprise Plus (300 servidores virtuales Windows y 90 servidores virtuales Linux)

Consulta:
Sírvasse aclarar que se está solicitando que la solución propuesta soporte servidores virtuales con sistema operativo Windows y Linux que se encuentren sobre Vmware ESXi 6.0 y vSphere 6 Enterprise Plus.

Acápíte de las bases : Sección: General Numeral: CAP III Literal: 4.1 Página: 20

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: La solución XDR debe brindar protección a los servidores (300 servidores virtuales Windows y 90 servidores virtuales Linux) contenidos en los 05 hosts de virtualización VMware ESXi 6.0 y vSphere 6 Enterprise Plus, y/o brindará protección a los 05 hosts de virtualización VMware ESXi 6.0 y vSphere 6 Enterprise Plus.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 15

Consulta/Observación:

Dice:
Debe permitir la sincronización con el directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección de dispositivos

Consulta:
Dado que los servidores suelen encontrarse dentro de un mismo grupo en el directorio activo y estos ejecutan servicios con una misma cuenta de administrador, en la práctica se utilizaría un solo grupo de AD a los que pertenecen, lo cual no permitiría diferenciar las políticas de seguridad. Este fin, es posible lograrlo también con un grupo local. Por ello, se solicita a la entidad confirmar que este requerimiento será opcional o que aceptarán soluciones que permitan crear grupos locales en la consola.

Acápite de las bases : Sección: General Numeral: CAP III Literal: 4.1.3.f Página: 22

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. En este caso, para la protección de dispositivos, el requerimiento está relacionado con la arquitectura tecnológica propia de la CGR, la cual utiliza la relación dinámica y de alta rotación de "grupo de usuarios - directorio activo", que es independiente y distinta a los despliegues de los agentes o los grupos locales.

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

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 16

Consulta/Observación:

Dice:
Debe permitir la sincronización con el directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección de dispositivos

Consulta:
La integración con active directory, permite utilizar el agrupamiento de dispositivos desde la plataforma de solución Endpoint, pero existe otros metodos de agilizar el agrupamiento de dispositivos, como por ejemplo el agrupamiento automático durante el despliegue del agente. Según lo expuesto, favor confirmar que se aceptará la sincronización con el directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección de dispositivos o permitir el agrupamiento automático durante el despliegue del agente

Acápite de las bases : Sección: General Numeral: CAP III Literal: 4.1.3.f Página: 22

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. En este caso, para la protección de dispositivos, el requerimiento está relacionado con la arquitectura tecnológica propia de la CGR, la cual utiliza la relación dinámica y de alta rotación de "grupo de usuarios - directorio activo", que es independiente y distinta a los despliegues de los agentes o los grupos locales.

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

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 17

Consulta/Observación:

Dice:
Debe proteger las funciones críticas en los navegadores de internet, incluida protección contra sitios web que realizan ataques de phishing y/o fingerprinting

Consulta:
Los ataques de phishing o de fingerprinting utilizan sitios web maliciosos para extraer credenciales y/o información de los usuarios, es decir se brinda mayor protección al prevenir la exfiltración de datos que utilizan sitios web malos al explotar las funciones críticas de los navegadores de internet. Por ello, sirvase a confirmar que se aceptarán soluciones que incluyan protección contra sitios web maliciosos o prevención de exfiltración de datos o phishing y/o fingerprinting.

Acápite de las bases : Sección: General Numeral: CAP III Literal: 4.1.4.s Página: 24

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

Análisis respecto de la consulta u observación:
El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 18

Consulta/Observación:

Dice:
Mínimo 100,000 eventos por segundo

Consulta:
Según la calculadora de almacenamiento de datos cierto fabricante (<https://apps.paloaltonetworks.com/cortex-sizing-estimator>), usualmente cada NGFW genera 10 evento por segundo (EPS) y tomando en cuenta que los NGFW generan mas evento que los equipos de comunicación, si realizamos una simulación de 700 equipos de comunicación y seguridad por 10 EPS obtenermos 7000 EPS (700 x 10 = 7000 EPS) y si le sumamos 1 EPS por cada agente XDR (6440 x 1 = 6440 EPS), resulta un total de 13440 EPS.

Realizando una simulación con otra fuente (https://siemsizecalculator.logpoint.com/?utm_source=optinmonster&utm_medium=popup&utm_campaign=sizing_calculator), se puede apreciar que 340 servidores (Windows Servers - HIGH EPS) pueden generar 2380 EPS, 100 servidores (Windows Servers - MED EPS (Event Log)) pueden generar 300 EPS, a nivel de correo 2000 Email Servers puede generar 4000 EPS, los equipos de comunicaciones considerando 50 Network Firewalls (Layer 7 Internal)) generan 12000 EPS, los 50 Network Firewalls (Layer 7 - DMZ) puede generar hasta 5000 EPS, considerando 200 Network Routers son 200 EPS y 400 Switchs son 800 EPS, una consola de antivirus genera 5 EPS y los 6000 endpoints generan 3 EPS.

Con esta estimaciones, se confirma que no se supera los 25000 EPS de acuerdo las características solicitas, incluso la recopilación de eventos es de las consolas, mas no de cada endpoint. Es por ello, sírvase confirmar que aceptarán como mínimo 25,000 eventos por segundo.

Acápíte de las bases : **Sección:** General **Numeral:** CAP III **Literal:** 4.2 **Página:** 26
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que, con el fin de fomentar la pluralidad de postores, lo expresado en el numeral 4.2 de los TDR quedará de la siguiente forma: "Mínimo 50,000 eventos por segundo", tomando en cuenta la cantidad de dispositivos que conforman la arquitectura tecnológica de la Entidad actual y proyectada para 3 años.

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

el numeral 4.2:
Dice:
Mínimo 100,000 eventos por segundo
Debe decir:
Mínimo 50,000 eventos por segundo

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 19

Consulta/Observación:

Dice:
Mínimo 100,000 eventos por segundo

Consulta:
Teniendo en cuenta que en la convocatoria anterior del Concurso Público N°007-2022-CGR dio como resultado desierto por superar el valor estimado de la contratación. Por ende, consideramos que requerir una solución que soporte como mínimo 100,000 eventos por segundo, solo encarece esta. Por ello, solicitamos que se pueda considerar que la solución como mínimo pueda soportar 25,000 eventos por segundo.

Acápite de las bases : Sección: General **Numeral:** CAP III **Literal:** 4.2 **Página:** 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que, con el fin de fomentar la pluralidad de postores, lo expresado en el numeral 4.2 de los TDR quedará de la siguiente forma:"Mínimo 50,000 eventos por segundo", tomando en cuenta la cantidad de dispositivos que conforman la arquitectura tecnológica de la Entidad actual y proyectada para 3 años.

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

En el numeral 4.2:
Dice:
Mínimo 100,000 eventos por segundo
Debe decir:
Mínimo 50,000 eventos por segundo

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 20

Consulta/Observación:

Dice:
Deben establecerse como minimo 6 zonas de recopilación de log, con la finalidad de optimizar el ancho de banda y evitar la perdida de la recopilación de datos

Consulta:
Confirmar que cuando se refiere a zona de recopilación es a la instalación de 6 colectores de evento en distinto punto definido dentro de la entidad

Acápite de las bases : Sección: General Numeral: CAP III Literal: 4.2.1.b Página: 27

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Las zonas de recopilación de logs se refiere a la instalación distribuida de distintos colectores de eventos.

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

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 21

Consulta/Observación:

Dice:
Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el postor deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones, para por lo menos 20 usuarios de administración

Consulta:
Permitir el acceso a 20 usuarios de administración concurrentes, encarece la solución. Se solicita a la entidad confirmar que se refiere a que la plataforma debe permitir crear al menos 20 usuarios de administración para el personal de la Contraloría, y que se le debe permitir el acceso concurrente al menos a dos usuarios.

Acápite de las bases : Sección: General Numeral: CAP III Literal: 5.1.2.r Página: 32

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que en el ítem 5.1.2.r se considerará un mínimo de 10 usuarios concurrentes.

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

En el literal r del numeral 5.1.1:

Debe decir:
Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el postor deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones, para por lo menos 10 usuarios concurrentes

En el literal r del numeral 5.1.2:

Debe decir:
Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el postor deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones, para por lo menos 10 usuarios concurrentes.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:21:48

Consulta: Nro. 22

Consulta/Observación:

Dice:
Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes, CERT y Dark Web. La información de las fuentes de inteligencia de amenazas deberá ser enviada a la solución SOAR para correlacionar y generar detecciones. El postor deberá adjuntar a su propuesta técnica un listado de fuentes de inteligencia (mínimo 10) con las que operan.

Consulta:
Para mayor pluralidad de postores, solicitamos que se podrá aceptar Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes y CERT y/o Dark Web. La información de las fuentes de inteligencia de amenazas deberá ser enviada a la solución SOAR para correlacionar y generar detecciones.

Acápite de las bases : **Sección:** General **Numeral:** CAP III **Literal:** 5.1.2.r **Página:** 32

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que en el ítem 5.1.2.r, el requerimiento indicado quedará de la siguiente forma "Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes, CERT y/o Dark Web. La información de las fuentes de inteligencia de amenazas deberá ser enviada a la solución SOAR para correlacionar y generar detecciones. El postor deberá adjuntar a su propuesta técnica un listado de fuentes de inteligencia (mínimo 10) con las que operan".

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

En el literal r del numeral 5.1.2:

Dice:
Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes, CERT y Dark Web. La información de las fuentes de inteligencia de amenazas deberá ser enviada a la solución SOAR para correlacionar y generar detecciones. El postor deberá adjuntar a su propuesta técnica un listado de fuentes de inteligencia (mínimo 10) con las que operan

Debe decir:
Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes, CERT y/o Dark Web. La información de las fuentes de inteligencia de amenazas deberá ser enviada a la solución SOAR para correlacionar y generar detecciones. El postor deberá adjuntar a su propuesta técnica un listado de fuentes de inteligencia (mínimo 10) con las que operan.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:42:09

Observación: Nro. 23

Consulta/Observación:

Dice:

"Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico."

Observacion

Se observa que es posible automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de las soluciones XDR, brindando toda la información solicitada en el requerimiento. Por ello, se solicita a la entidad confirmar que se aceptará también el uso de la interfaz API para cubrir el requerimiento

Acápites de las bases : **Sección:** General **Numeral:** CAP III **Literal:** 4.1.3,q **Página:** 22

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

En caso no se acepte esta observación, se estaría vulnerando el inciso A y B del artículo 2 de la L

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, acoge la observación señalando lo siguiente: El numeral 4.1.3.q quedará de la siguiente forma: Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico. Los reportes podrán ser preparados manualmente por el ingeniero residente a pedido, excepto por los reportes que vienen por defecto. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

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

Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:42:09

Observación: Nro. 24

Consulta/Observación:

Dice: "Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico."
Observacion

El objetivo principal de la solución SOAR es de integrar diversas plataformas para optimizar los tiempos de análisis y respuesta, además el SOAR brinda capacidades de reportes automatizados con el enfoque de monitoreo de incidentes. En el ítem 2 - 4.2 Servicio de SOAR, se solicita una solución SOAR que puede cubrir el requerimiento actual. Por ello, a fin de adquirir una solución eficaz y eficiente y garantizar la pluralidad de postores, se solicita a la entidad confirmar que se aceptará también que se pueda cubrir el requerimiento con la solución SOAR del ítem 2.

Acápite de las bases : **Sección:** General **Numeral:** CAP III **Literal:** 4.1.3,q **Página:** 22

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

En caso no se acepte esta observación, se estaría vulnerando el inciso A, B y F del artículo 2 de la

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, no acoge la observación señalando lo siguiente: Se indica que el requerimiento indicado en el numeral 4.1.3.q, que corresponde al Servicio de Suscripción de Software de Detección y Respuesta Extendida (XDR) para la protección de endpoints, de los TDR es mínimo. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:42:09

Observación: Nro. 25

Consulta/Observación:

Dice: "Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado."

Se observa que es posible automatizar la generación de reportes con el uso de la interfaz API de las soluciones XDR, brindando toda la información solicitada en el requerimiento. Por ello, se solicita a la entidad confirmar que se aceptará también el uso de la interfaz API para cubrir el requerimiento

Acápites de las bases : **Sección:** General **Numeral:** CAP III **Literal:** 4.1.3- o **Página:** 22

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

En caso no se acepte esta observación, se estaría vulnerando el inciso A y B del artículo 2 de la Ley

Análisis respecto de la consulta u observación:

En el literal o del numeral 4.1.3:

Dice:
Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado

Debe decir:
Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado. Los reportes podrán ser preparados manualmente por el ingeniero residente a pedido, excepto por los reportes que vienen por defecto. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

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

El Comité de Selección, contando con opinión del Área Usuaria, acoge la observación señalando lo siguiente: El numeral 4.1.3.o quedará de la siguiente forma.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:42:09

Observación: Nro. 26

Consulta/Observación:

Dice: "Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado."

El objetivo principal de la solución SOAR es de integrar diversas plataformas para optimizar los tiempos de análisis y respuesta, además el SOAR brinda capacidades de reportes automatizados con el enfoque de monitoreo de incidentes. En el ítem 2 - 4.2 Servicio de SOAR, se solicita una solución SOAR que puede cubrir el requerimiento actual. Por ello, a fin de adquirir una solución eficaz y eficiente y garantizar la pluralidad de postores, se solicita a la entidad confirmar que se aceptará también que se pueda cubrir el requerimiento con la solución SOAR del ítem 2

Acápite de las bases : **Sección:** General **Numeral:** CAP III **Literal:** 4.1.3 - o **Página:** 22

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

Se esta observación, se estaría vulnerando el inciso A, B y F del artículo 2 de ley contrataciones

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, no acoge la observación señalando lo siguiente: Se indica que el requerimiento indicado en el numeral 4.1.3.q, que corresponde al Servicio de Suscripción de Software de Detección y Respuesta Extendida (XDR) para la protección de endpoints, de los TDR es mínimo. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:42:09

Observación: Nro. 27

Consulta/Observación:

Dice: "Debe poder generar excepciones ante falsos positivos."

Se observa que en la búsqueda de capacidades avanzadas de detección y respuesta, el generar excepciones a través de la recategorización de los incidentes es crucial y realizar de manera manual no es efectivo. Por ello, a fin de adquirir una solución eficaz y eficiente, se solicita a la entidad confirmar que se debe incluir la generación de excepciones de manera automática realizadas por la solución o a través de analistas del servicio Managed Detection and Response (MDR) del fabricante

Acápite de las bases : **Sección:** General **Numeral:** CAP III **Literal:** 4.1.5 -g **Página:** 25

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

Esta observación, se estaría vulnerando el inciso F del artículo 2 de la Ley de contrataciones

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, no acoge la observación señalando lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20602399991	Fecha de envío :	14/03/2023
Nombre o Razón social :	GURUTI SOCIEDAD ANONIMA CERRADA - GURUTI S.A.C.	Hora de envío :	19:42:09

Consulta: Nro. 28

Consulta/Observación:

Dice: "La solución debe tener la capacidad de realizar búsqueda de amenazas en los equipos de la red al menos por hash, dirección IP o URL."

Consulta

A fin de aclarar el requerimiento, se solicita a la entidad confirmar que se aceptará también que la solución permita agrupar los equipos de la red que se vieron afectados por la misma amenaza y que permita hacer la búsqueda al menos por un Indicador de Compromiso (IoC) entre hash o dirección IP o URL.

Acápíte de las bases : Sección: General Numeral: CAP III Literal: 4.1.8 -d Página: 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Se aclara que lo requerido en el numeral 4.8.1.d se refiere a que la solución debe tener la capacidad de realizar búsqueda de amenazas en los equipos de la red al menos por: hash y dirección IP o hash y URL .

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20545751811	Fecha de envío :	14/03/2023
Nombre o Razón social :	SMART GLOBAL SOCIEDAD ANONIMA CERRADA	Hora de envío :	21:16:45

Consulta: Nro. 29

Consulta/Observación:

Dice: "05 hosts de virtualización Vmware ESXi 6.0 y vSphere 6 Enterprise Plus (300 servidores virtuales Windows y 90 servidores virtuales Linux)"

Se solicita a la entidad confirmar que se está solicitando que la solución propuesta soporte servidores virtuales con sistema operativo Windows y Linux que se encuentren sobre Vmware ESXi 6.0 y vSphere 6 Enterprise Plus.

Acápites de las bases : Sección: Especifico Numeral: 4 Literal: 4.1 Página: 20

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: La solución XDR debe brindar protección a los servidores (300 servidores virtuales Windows y 90 servidores virtuales Linux) contenidos en los 05 hosts de virtualización VMware ESXi 6.0 y vSphere 6 Enterprise Plus, y/o brindará protección a los 05 hosts de virtualización VMware ESXi 6.0 y vSphere 6 Enterprise Plus.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20545751811	Fecha de envío :	14/03/2023
Nombre o Razón social :	SMART GLOBAL SOCIEDAD ANONIMA CERRADA	Hora de envío :	21:16:45

Observación: Nro. 30

Consulta/Observación:

Dice: "Debe permitir la sincronización con el directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección de dispositivos"

La integración con directorio activo (DA), permite utilizar el agrupamiento de dispositivos desde la plataforma de la solución Endpoint, sin embargo existen otros métodos de agilizar el agrupamiento de dispositivos, como por ejemplo el agrupamiento automático durante el despliegue del agente. Se observa que al solicitar un método específico de agrupamiento, el presente requerimiento restringe la pluralidad y participación de postores. Según lo expuesto, se solicita a la entidad confirmar que se aceptará la sincronización con el directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección de dispositivos o permitir el agrupamiento automático durante el despliegue del agente que permitirá los mismos resultados requeridos. En caso no se acepte esta observación, se estaría vulnerando el inciso A y B del artículo 2 de la Ley de Contrataciones del Estado.

Acápite de las bases : **Sección:** Especifico **Numeral:** 4.1.3 **Literal:** f **Página:** 22

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

inciso A y B del artículo 2

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, no acoge la observación señalando lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. En este caso, para la protección de dispositivos, el requerimiento está relacionado con la arquitectura tecnológica propia de la CGR, la cual utiliza la relación dinámica y de alta rotación de "grupo de usuarios - directorio activo", que es independiente y distinta a los despliegues de los agentes o los grupos locales.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20545751811	Fecha de envío :	14/03/2023
Nombre o Razón social :	SMART GLOBAL SOCIEDAD ANONIMA CERRADA	Hora de envío :	21:16:45

Consulta: Nro. 31

Consulta/Observación:

Dice: "La solución debe tener la capacidad de realizar búsqueda de amenazas en los equipos de la red al menos por hash, dirección IP o URL."

A fin de aclarar el requerimiento, se solicita a la entidad confirmar que se aceptará también que la solución permita agrupar los equipos de la red que se vieron afectados por la misma amenaza y que permita hacer la búsqueda al menos por un Indicador de Compromiso (IoC) entre hash o dirección IP o URL.

Acápites de las bases : Sección: Especifico Numeral: 4.1.8 Literal: d **Página:** 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Se aclara que lo requerido en el numeral 4.8.1.d se refiere a que la solución debe tener la capacidad de realizar búsqueda de amenazas en los equipos de la red al menos por: hash y dirección IP o hash y URL .

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20545751811	Fecha de envío :	14/03/2023
Nombre o Razón social :	SMART GLOBAL SOCIEDAD ANONIMA CERRADA	Hora de envío :	21:16:45

Observación: Nro. 32

Consulta/Observación:

Dice: "Mínimo 100,000 eventos por segundo."

Tomando en cuenta que la convocatoria previa del Concurso Público N°007-2022-CGR quedó desierta por superar el valor estimado de la contratación, consideramos que solicitar el soporte de mínimo 100,000 eventos por segundo, solo encarece la solución. Por ello, solicitamos confirmar que se aceptará como mínimo soportar 25,000 eventos por segundo. En caso no se acepte esta observación, se estaría vulnerando el inciso F del artículo 2 de la Ley de Contrataciones del Estado.

Acápite de las bases : Sección: Especifico Numeral: 4 Literal: 4.2 Página: 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, acoge parcialmente la observación señalando lo siguiente: Se indica que, con el fin de fomentar la pluralidad de postores, lo expresado en el numeral 4.2 de los TDR quedará de la siguiente forma:"Mínimo 50,000 eventos por segundo", tomando en cuenta la cantidad de dispositivos que conforman la arquitectura tecnológica de la Entidad actual y proyectada para 3 años.

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

En el numeral 4.2:

Dice:

Mínimo 100,000 eventos por segundo

Debe decir:

Mínimo 50,000 eventos por segundo

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20545751811	Fecha de envío :	14/03/2023
Nombre o Razón social :	SMART GLOBAL SOCIEDAD ANONIMA CERRADA	Hora de envío :	21:16:45

Consulta: Nro. 33

Consulta/Observación:

Se indica: b- El postor debe contar con un Centro de Operaciones de Seguridad (SOC) certificado con ISO27001 o deberá contar con personal que tenga certificado o curso ISO27001, para el servicio de soporte técnico...

Cabe mencionar que la certificación ISO27001 a nivel de empresa certifica procesos y procedimientos de la propia compañía que garantice la confidencialidad, integridad y disponibilidad de la información, sin embargo la certificación de personas en ISO27001 es basado en el conocimiento de la norma ISO27001 y no garantiza que el postor cuente con procesos certificados y auditados por una entidad certificadora, en ese sentido sírvase confirmar que se aceptará como mínimo la certificación ISO27001 del postor para el proceso de gestión de incidentes y cambios de su SOC y no de personal que puede rotar o salir de la empresa.

Acápites de las bases : Sección: Especifico Numeral: 5.1.1 Literal: b **Página:** 26

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Con el fin de garantizar la pluralidad de postores, se mantiene lo indicado en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20545751811	Fecha de envío :	14/03/2023
Nombre o Razón social :	SMART GLOBAL SOCIEDAD ANONIMA CERRADA	Hora de envío :	21:16:45

Consulta: Nro. 34

Consulta/Observación:

Se indica: b- El postor debe contar con un Centro de Operaciones de Seguridad (SOC) certificado con ISO27001 o deberá contar con personal que tenga certificado o curso ISO27001, para el servicio de soporte técnico...

Cabe mencionar que la certificación ISO27001 a nivel de empresa certifica procesos y procedimientos de la propia compañía que garantice la confidencialidad, integridad y disponibilidad de la información, sin embargo la certificación de personas en ISO27001 es basado en el conocimiento de la norma ISO27001 y no garantiza que el postor cuente con procesos certificados y auditados por una entidad certificadora, en ese sentido sírvase confirmar que se aceptará como mínimo la certificación ISO27001 del postor para el proceso de gestión de incidentes y cambios de su SOC y no de personal que puede rotar o salir de la empresa.

Acápites de las bases : Sección: Especifico Numeral: 5.1.2 Literal: b **Página:** 31

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Con el fin de garantizar la pluralidad de postores, se mantiene lo indicado en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20608991728	Fecha de envío :	14/03/2023
Nombre o Razón social :	GLOBAL LINK ONE S.A.C.	Hora de envío :	21:36:09

Consulta: Nro. 35

Consulta/Observación:

Dice: "Debe permitir la sincronización con el directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección de dispositivos"

Debido a que los servidores suelen encontrarse dentro de un mismo grupo en el directorio activo y estos ejecutan servicios con una misma cuenta de administrador, en la práctica se utilizaría un solo grupo de AD a los que pertenecen, para lo cual no se requiere diferentes políticas de seguridad. Este objetivo, es posible lograrlo también con un grupo local. Según lo expuesto, se solicita a la entidad confirmar que este requerimiento será opcional o que aceptarán soluciones que permitan crear grupos de manera local.

Acápites de las bases : Sección: Especifico Numeral: 4.1.3 Literal: f Página: 22

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. En este caso, para la protección de dispositivos, el requerimiento está relacionado con la arquitectura tecnológica propia de la CGR, la cual utiliza la relación dinámica y de alta rotación de "grupo de usuarios - directorio activo", que es independiente y distinta a los despliegues de los agentes o los grupos locales.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608991728

Nombre o Razón social : GLOBAL LINK ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 21:36:09

Observación: Nro. 36

Consulta/Observación:

Dice: "Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado."

Se observa que es posible automatizar la generación de reportes con el uso de la interfaz API de las soluciones XDR, brindando toda la información solicitada en el requerimiento. Por ello, se solicita a la entidad confirmar que se aceptará también el uso de la interfaz API para cubrir el requerimiento. En caso no se acepte esta observación, se estaría vulnerando la Ley de Contrataciones del Estado.

Acápite de las bases : **Sección:** Especifico **Numeral:** 4.1.3 **Literal:** 0 **Página:** 22

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

inciso A y B del artículo 2

Análisis respecto de la consulta u observación:

En el literal o del numeral 4.1.3:

Dice:

Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado

Debe decir:

Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado. Los reportes podrán ser preparados manualmente por el ingeniero residente a pedido, excepto por los reportes que vienen por defecto. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

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

El Comité de Selección, contando con opinión del Área Usuaria, acoge la observación señalando lo siguiente: El numeral 4.1.3.o quedará de la siguiente forma:

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608991728

Nombre o Razón social : GLOBAL LINK ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 21:36:09

Observación: Nro. 37

Consulta/Observación:

Dice: "Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado."

El objetivo principal de la solución SOAR es de integrar diversas plataformas para optimizar los tiempos de análisis y respuesta, además el SOAR brinda capacidades de reportes automatizados con el enfoque de monitoreo de incidentes. En el ítem 2 - 4.2 Servicio de SOAR, se solicita una solución SOAR que puede cubrir el requerimiento actual. Por ello, a fin de adquirir una solución eficaz y eficiente y garantizar la pluralidad de postores, se solicita a la entidad confirmar que se aceptará también que se pueda cubrir el requerimiento con la solución SOAR del ítem 2. En caso no se acepte esta observación, se estaría vulnerando la Ley de Contrataciones del Estado.

Acápite de las bases : Sección: Especifico **Numeral:** 4.1.3 **Literal:** 0 **Página:** 22

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

inciso A, B y F del artículo 2

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, no acoge la observación señalando lo siguiente: Se indica que el requerimiento indicado en el numeral 4.1.3.q, que corresponde al Servicio de Suscripción de Software de Detección y Respuesta Extendida (XDR) para la protección de endpoints, de los TDR es mínimo. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608991728

Nombre o Razón social : GLOBAL LINK ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 21:36:09

Observación: Nro. 38

Consulta/Observación:

Dice: "Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico."

Se observa que es posible automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de las soluciones XDR, brindando toda la información solicitada en el requerimiento. Por ello, se solicita a la entidad confirmar que se aceptará también el uso de la interfaz API para cubrir el requerimiento y considerando que se obtendría el mismo resultado. En caso no se acepte esta observación, se estaría vulnerando la Ley de Contrataciones del Estado.

Acápites de las bases : Sección: Especifico Numeral: 4.1.3 Literal: q **Página: 22**

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

inciso A y B del artículo 2

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, acoge la observación señalando lo siguiente: El numeral 4.1.3.q quedará de la siguiente forma: Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico. Los reportes podrán ser preparados manualmente por el ingeniero residente a pedido, excepto por los reportes que vienen por defecto. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

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

Debe decir:

Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608991728

Nombre o Razón social : GLOBAL LINK ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 21:36:09

Observación: Nro. 39

Consulta/Observación:

Dice: "Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico."

El objetivo principal de la solución SOAR es de integrar diversas plataformas para optimizar los tiempos de análisis y respuesta, además el SOAR brinda capacidades de reportes automatizados con el enfoque de monitoreo de incidentes. En el ítem 2 - 4.2 Servicio de SOAR, se solicita una solución SOAR que puede cubrir el requerimiento actual. Por ello, a fin de adquirir una solución eficaz y eficiente y garantizar la pluralidad de postores, se solicita a la entidad confirmar que se aceptará también que se pueda cubrir el requerimiento con la solución SOAR del ítem 2. En caso no se acepte esta observación, se estaría vulnerando la Ley de Contrataciones del Estado.

Acápite de las bases : Sección: Especifico **Numeral:** 4.1.3 **Literal:** q **Página:** 22

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

inciso A, B y F del artículo 2

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, no acoge la observación señalando lo siguiente: Se indica que el requerimiento indicado en el numeral 4.1.3.q, que corresponde al Servicio de Suscripción de Software de Detección y Respuesta Extendida (XDR) para la protección de endpoints, de los TDR es mínimo. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608991728

Nombre o Razón social : GLOBAL LINK ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 21:36:09

Observación: Nro. 40

Consulta/Observación:

Dice: "Debe proteger las funciones críticas en los navegadores de internet, incluida protección contra sitios web que realizan ataques de phishing y/o fingerprinting"

Se observa que los ataques de phishing o de fingerprinting utilizan sitios web maliciosos para extraer credenciales y/o información de los usuarios, es decir se brinda mayor protección al prevenir la exfiltración de datos que utilizan sitios web maliciosos al explotar las funciones críticas de los navegadores de internet. Por ello, a fin de adquirir una solución eficaz y eficiente, se solicita a la entidad confirmar que se aceptarán soluciones que incluyan protección contra sitios web maliciosos o prevención de exfiltración de datos o phishing y/o fingerprinting. En caso no se acepte esta observación, se estaría vulnerando la Ley de Contrataciones del Estado.

Acápite de las bases : **Sección:** Especifico **Numeral:** 4.1.4 **Literal:** s **Página:** 24

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

inciso F del artículo 2

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, no acoge la observación señalando lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20608991728	Fecha de envío :	14/03/2023
Nombre o Razón social :	GLOBAL LINK ONE S.A.C.	Hora de envío :	21:36:09

Observación: Nro. 41

Consulta/Observación:

Dice: "Debe poder generar excepciones ante falsos positivos."

Se observa que en la búsqueda de capacidades avanzadas de detección y respuesta, el generar excepciones a través de la recategorización de los incidentes es crucial y realizar de manera manual no es efectivo. Por ello, a fin de adquirir una solución eficaz y eficiente, se solicita a la entidad confirmar que se debe incluir la generación de excepciones de manera automática realizadas por la solución o a través de analistas del servicio Managed Detection and Response (MDR) del fabricante. En caso no se acepte esta observación, se estaría vulnerando la Ley de Contrataciones del Estado.

Acápite de las bases : **Sección:** Especifico **Numeral:** 4.1.5 **Literal:** g **Página:** 25

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

inciso F del artículo 2

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, no acoge la observación señalando lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608991728

Nombre o Razón social : GLOBAL LINK ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 21:36:09

Observación: Nro. 42

Consulta/Observación:

Dice: "Mínimo 100,000 eventos por segundo."

Según la calculadora de almacenamiento de datos del fabricante Palo Alto Networks (<https://apps.paloaltonetworks.com/cortex-sizing-estimator>), usualmente cada NGFW genera 10 evento por segundo (EPS) y tomando en cuenta que los NGFW generan mas evento que los equipos de comunicación, si realizamos una simulación de 700 equipos de comunicación y seguridad por 10 EPS obtenermos 7000 EPS (700 x 10 = 7000 EPS) y si le sumamos 1 EPS por cada agente XDR (6440 x 1 = 6440 EPS), resulta un total de 13440 EPS.

Realizando una simulación con otra fuente (https://siemsizecalculator.logpoint.com/?utm_source=optinmonster&utm_medium=popup&utm_campaign=sizing_calculator), se puede apreciar que 340 servidores (Windows Servers - HIGH EPS) pueden generar 2380 EPS, 100 servidores (Windows Servers - MED EPS (Event Log)) pueden generar 300 EPS, a nivel de correo 2000 Email Servers puede generar 4000 EPS, los equipos de comunicaciones considerando 50 Network Firewalls (Layer 7 Internal)) generan 12000 EPS, los 50 Network Firewalls (Layer 7 - DMZ) puede generar hasta 5000 EPS, considerando 200 Network Routers son 200 EPS y 400 Switchs son 800 EPS, una consola de antivirus genera 5 EPS y los 6000 endpoints generan 3 EPS.

Se observa que con esta estimaciones no se supera los 25,000 EPS de acuerdo a las características solicitas. Por ello, a fin de adquirir una solución eficaz y eficiente, sírvase confirmar que aceptarán como mínimo 25,000 eventos por segundo. En caso no se acepte esta observación, se estaría vulnerando la Ley de Contrataciones del Estado.

Acápíte de las bases : Sección: Especifico Numeral: 4 Literal: 4.2 **Página: 26**

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

inciso F del artículo 2

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, acoge parcialmente la observación señalando lo siguiente: Se indica que, con el fin de fomentar la pluralidad de postores, lo expresado en el numeral 4.2 de los TDR quedará de la siguiente forma: "Mínimo 50,000 eventos por segundo", tomando en cuenta la cantidad de dispositivos que conforman la arquitectura tecnológica de la Entidad actual y proyectada para 3 años.

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

En el numeral 4.2:

Dice:

Mínimo 100,000 eventos por segundo

Debe decir:

Mínimo 50,000 eventos por segundo

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20608991728

Nombre o Razón social : GLOBAL LINK ONE S.A.C.

Fecha de envío : 14/03/2023

Hora de envío : 21:36:09

Consulta: Nro. 43

Consulta/Observación:
CONFIDENCIALIDAD

Considerando que se debe mantener la confidencialidad de los datos e información que la Contraloría entregue al contratista durante el servicios lo cual se garantiza con una adecuada gestión de los procesos sobre la información, agradeceremos a la entidad confirmar que se debe incluir dentro de la documentación para la presentación de la oferta la certificación de Sistema de Gestión de Seguridad de la Información ISO 27001 orientado a procesos o gestión o servicios en cumplimiento de lo indicado en el requerimiento.

Acápites de las bases : Sección: Especifico **Numeral:** 17 **Literal:** - **Página:** 43

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Con el fin de garantizar la pluralidad de postores, se mantiene lo indicado en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 44

Consulta/Observación:

Consulta:

Teniendo en cuenta que el numeral 2.2.1. de las Bases Estándar para la contratación de servicios en general, aprobada mediante Directiva N° 001-2019-OSCE/CD, dispone que: "El órgano encargado de las contrataciones o comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites ¿Documentos para la admisión de la oferta¿.

Solicitamos a la Entidad confirmar que los documentos señalados en el numeral 2.2.1, serán los únicos necesarios para la admisión de las ofertas los postores.

Acápite de las bases : Sección: Especifico **Numeral:** 2.1.1 **Literal:** - **Página:** 16

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

Análisis respecto de la consulta u observación:

El Comité de Selección, en atención a la consulta formulada, aclara que: la documentación señalada en el numeral 2.2.1 del Capítulo II de la Sección Específica de las Bases, será la documentación que deberán presentar los postores para la admisión de su oferta.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 45

Consulta/Observación:

Solicitamos confirmar que cuando indican "en pago parcial" se refieren a pagos mensuales.

Acápite de las bases : Sección: Especifico **Numeral:** 2.5 **Literal:** - **Página:** 20

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

Análisis respecto de la consulta u observación:

El Comité de Selección, en atención a la consulta formulada, aclara que: los pagos de la prestación se efectuarán de acuerdo a lo señalado en el numeral 2.5 del Capítulo II de la Sección Específica de la Bases y el numeral 12 de los términos de referencia.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20428698569	Fecha de envío :	14/03/2023
Nombre o Razón social :	AMERICATEL PERU S.A.	Hora de envío :	21:47:55

Consulta: Nro. 46

Consulta/Observación:
EXPERIENCIA DEL PERSONAL CLAVE
Un (1) Jefe de Proyecto:

Deberá contar con cuatro (4) años de experiencia en supervisión de servicios de despliegue y/o implementación y/o administración de la solución objeto de la convocatoria y/o proyectos en general relacionados con TI y/o gestión de proyectos de servicios de TI y/o Ciberseguridad y/o Proyectos informáticos de infraestructura tecnológica y/o Seguridad informática u otros proyectos asociados a como gestor o coordinador o jefe de proyectos (ciberseguridad y/o proyectos informáticos y/o proyectos de seguridad informática).

Solicitamos se sirva confirmar que para el jefe de proyectos, se evaluarán el cumplimiento de las funciones, ello independiente del cargo que se señale en las constancias, por lo cual, se podrá presentar un personal que haya sido: Analista y/o Supervisor y/o Jefe y/o Coordinador; siempre y cuando sus funciones habrían sido Gestión y/o supervisión y/o implementación de proyectos de tecnología de la información (TI) como Hosting y/o Housing.

Acápito de las bases : Sección: Especifico Numeral: 3.2.A.1.2 Literal: - Página: 45

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

Análisis respecto de la consulta u observación:
El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente:
Se precisa que se mantiene la experiencia del Jefe de Proyecto solicitada indicada en el TDR.
Adicionalmente, se aclara que la experiencia indicada en la consulta (Hosting y/o Housing) no es parte del objeto del proceso. Además, se precisa que la experiencia mínima solicitada es la indicada en el TDR, independientemente del nombre del cargo.

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

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20428698569	Fecha de envío :	14/03/2023
Nombre o Razón social :	AMERICATEL PERU S.A.	Hora de envío :	21:47:55

Consulta: Nro. 47

Consulta/Observación:

EXPERIENCIA DEL PERSONAL CLAVE

Dos (2) Esp. en Seguridad

Deberá contar con tres (3) años de experiencia en seguridad informática y/o en implementación y/o administración de la solución objeto de la convocatoria.

Agradeceremos confirmar que se aceptará como válido la experiencia en el cargo como Jefe de la Seguridad de la Información y/o Gerente de proyectos de la Seguridad de la Información y/o team Leader Analista NSOC (Network Security Operation Center) y/o Jefe de equipo Analista NSOC.

Acápíte de las bases : Sección: Especifico Numeral: 3.2.A.1.2 Literal: - Página: 45

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se precisa que la experiencia mínima solicitada es la indicada en el TDR, independientemente del nombre del cargo.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 48

Consulta/Observación:

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD - ITEM 1

Servicio de instalación y configuración y/o implementación de soluciones antivirus, y/o servicio de instalación y configuración y/o implementación de soluciones de sistemas de control o detección o protección, y seguridad de puntos finales o endpoints, y/o servicio de instalación y configuración y/o implementación y/o soporte y/o servicio gestionado de soluciones de ciberseguridad y/o antimalware avanzado y/o seguridad perimetral (FW, NGFW, Antispam, Filtro-Web, Firewall de Aplicaciones Web, IPS, Anti-DDoS y sus consolas de gestión) y/o protección contra amenazas, y/o servicio de instalación y configuración y/o implementación y/o soporte de soluciones EDR y/o implementación y/o reconfiguración de soluciones basadas en Firewalls y/o solución en hardware y/o software de Protección contra Amenazas Avanzadas y/o solución en hardware y/o software de Defensa contra Amenazas Avanzadas.

Siendo que las denominaciones de los servicios pueden no coincidir literalmente entre los diversos operadores, sírvase confirmar que el servicio de seguridad gestionada se admitirá como equivalente al servicio gestionado de soluciones de ciberseguridad.

Acápites de las bases : Sección: Específico Numeral: 3.2.B Literal: - **Página:** 47

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se precisa que la experiencia mínima solicitada es la indicada en el TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 49

Consulta/Observación:

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD - ACREDITACION

Respecto de la acreditación de la experiencia del postor, las Bases señalan en el Requisito de Calificación B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD que ¿En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; (¿)¿

Con relación a la vinculación de facturas como una sola contratación, la Dirección Técnica Normativa del OSCE en su Opinión N° 149-2018/DTN señaló lo siguiente: ¿Ahora bien, los medios para acreditar dicha vinculación pueden ser diversos siempre que permitan demostrar fehacientemente que todos los comprobantes de pago corresponden a un mismo contrato. Entre los medios podemos mencionar la indicación expresa en los mismos comprobantes de pago que estos corresponden a un mismo contrato, la copia de las conformidades, constancia de prestación o cualquier otro documento emitido por el receptor de la prestación que indique que tales comprobantes de pago responden a un mismo contrato, entre otros mecanismos. Sin embargo, cabe precisar que la acreditación mencionada no es posible, únicamente, mediante la presentación de una declaración jurada donde el emisor de los comprobantes de pago indique que éstos corresponden a una misma relación contractual."

En atención al criterio señalado por el OSCE, y considerando que la normativa de contrataciones permite la acreditación tanto de contrataciones públicas como privadas, siendo que estas últimas no guardan una formalidad similar a las contrataciones públicas, sírvase confirmar que será admisible como elementos de vinculación para la agrupación de comprobantes de pago como una sola contratación, la indicación de ¿un mismo número de negocio¿, ¿un mismo código¿, ¿un mismo objeto social¿ y ¿sucesión correlativa¿ consignada en los comprobantes de pago que acreditan dicho servicio.

Acápite de las bases : Sección: Especifico **Numeral:** 3.2.B **Literal:** - **Página:** 47

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

Análisis respecto de la consulta u observación:

El comité de selección, en atención a la consulta formulada, señala que: la experiencia del postor deberá ser acreditada conforme a lo señalado en el literal B del numeral 3.2 de la sección específica de la Bases.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 50

Consulta/Observación:

FORMA DE PAGO

Agradeceremos confirmar si la factura debe tener una glosa específica o debe ser detallada.

Acápito de las bases : Sección: Especifico Numeral: 2.5

Literal: -

Página: 19

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

Análisis respecto de la consulta u observación:

El comité de selección, en atención a la consulta formulada, señala que: la factura deberá contener el objeto de la contratación y el pago al que corresponde (ítem, prestación principal o accesorio, etc.).

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20428698569	Fecha de envío :	14/03/2023
Nombre o Razón social :	AMERICATEL PERU S.A.	Hora de envío :	21:47:55

Consulta: Nro. 51

Consulta/Observación:

FORMA DE PAGO

Agradeceremos confirmar si la facturación será enviada de forma física y/o electrónica, en caso de ser electrónica, ¿estos se ingresan a una mesa de partes especial?

Acápite de las bases : Sección: Especifico Numeral: 2.5 Literal: - Página: 19

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

Análisis respecto de la consulta u observación:

El comité de selección, en atención a la consulta formulada, señala que: la documentación deberá ser presentada de acuerdo a lo indicado en el numeral 2.5 del Capítulo II de la Sección Específica de las Bases.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20428698569	Fecha de envío :	14/03/2023
Nombre o Razón social :	AMERICATEL PERU S.A.	Hora de envío :	21:47:55

Consulta: Nro. 52

Consulta/Observación:

FORMA DE PAGO

Agradeceremos confirmar si existe algún plazo para la presentación de la facturación.

Acápíte de las bases : Sección: Especifico Numeral: 2.5 Literal: - Página: 19

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

Análisis respecto de la consulta u observación:

El comité de selección, en atención a la consulta formulada, señala que: la documentación deberá ser presentada de acuerdo a lo indicado en el numeral 2.5 del Capítulo II de la Sección Específica de las Bases.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 53

Consulta/Observación:
FORMA DE PAGO

Sirvanse confirmar si el documento de facturación (recibo/factura) debe contener alguna información que el cliente considere imprescindible?.

Acápite de las bases : Sección: Especifico Numeral: 2.5 Literal: - **Página:** 19

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

Análisis respecto de la consulta u observación:

El comité de selección, en atención a la consulta formulada, señala que: la factura deberá contener el objeto de la contratación y el pago al que corresponde (ítem, prestación principal o accesorio, etc.).

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 54

Consulta/Observación:

En las bases se indica:

"Para sistemas operativos no vigentes o legacy y para sistemas operativos no compatibles con la solución ofertada, se deberá considerar el uso de parches virtuales o protección de vulnerabilidades o similar, que permita la protección de vulnerabilidades en los equipos de la entidad con estos sistemas operativos; pudiendo el postor para cumplir con este requerimiento ofrecer una herramienta adicional a la solución propuesta, la cual podrá ser de distinto fabricante. Se precisa que la entidad cuenta con aproximadamente con 120 servidores con sistemas operativos no vigentes o legacy (Windows Server 2003, Windows Server 2008, Red Hat Enterprise Linux 5.8, Red Hat Enterprise Linux 5.10, Debian) y con aproximadamente 360 equipos con Windows 7."

Consulta:

Sírvase confirmar que los sistemas operativos Red Hat Enterprise Linux 5.8 y 5.10 serán actualizados por la Entidad a mínimamente la versión 6.7 a fin de permitir una mayor pluralidad de postores, quedando el enunciado de la siguiente manera: "Para sistemas operativos no vigentes o legacy y para sistemas operativos no compatibles con la solución ofertada, se deberá considerar el uso de parches virtuales o protección de vulnerabilidades o similar, que permita la protección de vulnerabilidades en los equipos de la entidad con estos sistemas operativos; pudiendo el postor para cumplir con este requerimiento ofrecer una herramienta adicional a la solución propuesta, la cual podrá ser de distinto fabricante. Se precisa que la entidad cuenta con aproximadamente con 120 servidores con sistemas operativos no vigentes o legacy (Windows Server 2003, Windows Server 2008, Red Hat Enterprise Linux 6.7, Debian) y con aproximadamente 360 equipos con Windows 7."

Acápite de las bases : Sección: Especifico **Numeral:** 3.1 **Literal:** 4.1.2 **Página:** 21

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se aclara que el requerimiento citado es una necesidad de la Entidad. Cabe señalar que en el numeral 4.1.2 literal e. se indica lo siguiente: "...el postor para cumplir con este requerimiento ofrecer una herramienta adicional a la solución propuesta, la cual podrá ser de distinto fabricante...".

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Consulta: Nro. 55

Consulta/Observación:

En las bases se indica:

"Para sistemas operativos no vigentes o legacy y para sistemas operativos no compatibles con la solución ofertada, se deberá considerar el uso de parches virtuales o protección de vulnerabilidades o similar, que permita la protección de vulnerabilidades en los equipos de la entidad con estos sistemas operativos; pudiendo el postor para cumplir con este requerimiento ofrecer una herramienta adicional a la solución propuesta, la cual podrá ser de distinto fabricante. Se precisa que la entidad cuenta con aproximadamente con 120 servidores con sistemas operativos no vigentes o legacy (Windows Server 2003, Windows Server 2008, Red Hat Enterprise Linux 5.8, Red Hat Enterprise Linux 5.10, Debian) y con aproximadamente 360 equipos con Windows 7."

Consulta:

Sírvase confirmar que los sistemas operativos Red Hat Enterprise Linux 5.8 y 5.10 podrán ser opcionales a fin de permitir una mayor pluralidad de postores.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1 **Literal:** 4.1.2 **Página:** 21

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se aclara que el requerimiento citado es una necesidad de la Entidad. Cabe señalar que en el numeral 4.1.2 literal e. se indica lo siguiente: "...el postor para cumplir con este requerimiento ofrecer una herramienta adicional a la solución propuesta, la cual podrá ser de distinto fabricante...".

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20428698569	Fecha de envío :	14/03/2023
Nombre o Razón social :	AMERICATEL PERU S.A.	Hora de envío :	21:47:55

Consulta: Nro. 56

Consulta/Observación:

En las bases se indica:
"Para sistemas operativos no vigentes o legacy y para sistemas operativos no compatibles con la solución ofertada, se deberá considerar el uso de parches virtuales o protección de vulnerabilidades o similar, que permita la protección de vulnerabilidades en los equipos de la entidad con estos sistemas operativos; pudiendo el postor para cumplir con este requerimiento ofrecer una herramienta adicional a la solución propuesta, la cual podrá ser de distinto fabricante. Se precisa que la entidad cuenta con aproximadamente con 120 servidores con sistemas operativos no vigentes o legacy (Windows Server 2003, Windows Server 2008, Red Hat Enterprise Linux 5.8, Red Hat Enterprise Linux 5.10, Debian) y con aproximadamente 360 equipos con Windows 7."

Consulta:
Sírvase indicar la versión y build (kb) exacto de cada sistema operativo a fin de comprobar la compatibilidad exacta de cada sistema operativo no vigente o legacy.

Acápite de las bases : Sección: Especifico Numeral: 3.1 Literal: 4.1.2 Página: 21

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Se precisa que todos los sistemas operativos legacy mencionados en el TDR deben ser protegidos independientemente de su build o versión específica.

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

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20428698569

Nombre o Razón social : AMERICATEL PERU S.A.

Fecha de envío : 14/03/2023

Hora de envío : 21:47:55

Observación: Nro. 57

Consulta/Observación:

En las bases se indica:

"r. El servicio de soporte técnico incluirá un servicio de monitoreo y gestión de incidencias sobre la plataforma XDR a través del SOC solicitado, por parte del contratista, el cual deberá cumplir con lo siguiente:..."

Observación:

Considerando que lo solicitado se superpone con lo solicitado en el numeral 3.1, literal 5.1.2.r, página 32, correspondiente al ítem 2, y que, además, los requisitos mencionados corresponden a un servicio de SOAR (tal cual lo solicitado en el ítem 2), al haber distintos postores por cada ítem podría haber una incongruencia de servicios puesto que no se sabría qué proveedor tendría que habilitar el servicio solicitado, sírvase confirmar que lo solicitado en el numeral 3.1, literal 5.1.1.r, página 30 será suprimido del requerimiento o trasladado al ítem que verdaderamente corresponde.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1 **Literal:** 5.1.1 **Página:** 30

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

TEXTO ÚNICO ORDENADO LEY Nº 30225, LCE, Artículo 2. Principio de transparencia.

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, no acoge la observación señalando lo siguiente: Los servicios requeridos en los numerales 5.1.1.r y 5.1.2.r son distintos y cada postor debe asegurar el cumplimiento de los mismos, de acuerdo al ítem que corresponda al servicio por brindar.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20428698569	Fecha de envío :	14/03/2023
Nombre o Razón social :	AMERICATEL PERU S.A.	Hora de envío :	21:47:55

Observación: Nro. 58

Consulta/Observación:

En las bases se indica:
"r. El servicio de soporte técnico incluirá un servicio de monitoreo y gestión de incidencias sobre la plataforma XDR a través del SOC solicitado, por parte del contratista, el cual deberá cumplir con lo siguiente:"

Observación:
Considerando que el principio de economía menciona que en toda contratación se aplicarán los criterios de simplicidad, austeridad, concentración y ahorro en el uso de los recursos, en las etapas de los procesos de selección y en los acuerdos y resoluciones recaídos sobre ellos, debiéndose evitar exigencias y formalidades costosas e innecesarias en las Bases y en los contratos; y, adicionalmente, el principio de eficiencia menciona que las contrataciones deben efectuarse bajo las mejores condiciones de calidad, precio y plazos de ejecución y entrega y con el mejor uso de los recursos materiales y humanos disponibles (las contrataciones deben observar criterios de celeridad, economía y eficacia), lo solicitado genera un sobre costo para la Entidad al superponerse con lo solicitado en el numeral 3.1, literal 5.1.2.r, página 32, correspondiente al ítem 2, pues están solicitando las mismas funcionalidades. Por tal motivo y ante todo lo mencionado, se solicita a la Entidad confirmar que lo solicitado (numeral 3.1, literal 5.1.1.r, página 30) será suprimido del requerimiento o trasladado al ítem que corresponde.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1 **Literal:** 5.1.1 **Página:** 30

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

TEXTO ÚNICO ORDENADO LEY N° 30225, LCE, Artículo 2. Principio de transparencia.

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, no acoge la observación señalando lo siguiente: En caso sea un mismo proveedor para ambos Ítems, el SOC solicitado podrá ser uno solo para satisfacer lo requerido en los numerales 5.1.1.r y 5.1.2.r.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20503795079

Nombre o Razón social : DESYSWEB SAC

Fecha de envío : 14/03/2023

Hora de envío : 22:48:17

Consulta: Nro. 59

Consulta/Observación:

ÍTEM 1: Servicio de instalación y configuración y/o implementación de soluciones antivirus, y/o servicio de instalación y configuración y/o implementación de soluciones de sistemas de control o detección o protección, y seguridad de puntos finales o endpoints, y/o servicio de instalación y configuración y/o implementación y/o soporte y/o servicio gestionado de soluciones de ciberseguridad y/o antimalware avanzado y/o seguridad perimetral (FW, NGFW, Antispam, Filtro-Web, Firewall de Aplicaciones Web, IPS, Anti-DDoS y sus consolas de gestión) y/o protección contra amenazas, y/o servicio de instalación y configuración y/o implementación y/o soporte de soluciones EDR y/o implementación y/o reconfiguración de soluciones basadas en Firewalls y/o solución en hardware y/o software de Protección contra Amenazas Avanzadas y/o solución en hardware y/o software de Defensa contra Amenazas Avanzadas

Considerando que las herramientas de monitoreo y los equipos de comunicaciones son parte de las soluciones XDR, sírvase confirmar que también se aceptará implementación y/o puesta en servicio de herramientas de monitoreo y equipos de comunicaciones.

Acápite de las bases : Sección: Especifico **Numeral:** 3.2 **Literal:** B **Página:** 47

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se precisa que se mantiene la experiencia del postor solicitada indicada en el TDR, debido a que la experiencia indicada en la consulta no es parte del objeto del proceso.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20503795079	Fecha de envío :	14/03/2023
Nombre o Razón social :	DESYSWEB SAC	Hora de envío :	22:48:17

Consulta: Nro. 60

Consulta/Observación:

ÍTEM 1: Servicio de instalación y configuración y/o implementación de soluciones antivirus, y/o servicio de instalación y configuración y/o implementación de soluciones de sistemas de control o detección o protección, y seguridad de puntos finales o endpoints, y/o servicio de instalación y configuración y/o implementación y/o soporte y/o servicio gestionado de soluciones de ciberseguridad y/o antimalware avanzado y/o seguridad perimetral (FW, NGFW, Antispam, Filtro-Web, Firewall de Aplicaciones Web, IPS, Anti-DDoS y sus consolas de gestión) y/o protección contra amenazas, y/o servicio de instalación y configuración y/o implementación y/o soporte de soluciones EDR y/o implementación y/o reconfiguración de soluciones basadas en Firewalls y/o solución en hardware y/o software de Protección contra Amenazas Avanzadas y/o solución en hardware y/o software de Defensa contra Amenazas Avanzadas

Sírvase confirmar que se aceptará como servicios similares el mantenimiento preventivo y/o correctivo de equipos de comunicaciones y/o seguridad.

Acápite de las bases : Sección: Especifico Numeral: 3.2 Literal: b Página: 47

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se precisa que se mantiene la experiencia del postor solicitada indicada en el TDR, debido a que la experiencia indicada en la consulta no es parte del objeto del proceso.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20503795079

Nombre o Razón social : DESYSWEB SAC

Fecha de envío : 14/03/2023

Hora de envío : 22:48:17

Consulta: Nro. 61

Consulta/Observación:

ÍTEM 2: Servicio de instalación y configuración y/o implementación de soluciones de sistemas automatizados de seguridad de puntos finales o endpoints, y/o servicio de instalación y configuración y/o implementación y/o soporte y/o servicio gestionado de soluciones de recolección de eventos de seguridad de endpoints y equipos de comunicación y seguridad perimetral y/o recolección de eventos contra amenazas, y/o servicio de instalación y configuración y/o implementación y/o soporte de soluciones SIEM.

Sírvase confirmar que se aceptará como servicios similares servicio de instalación y/o configuración y/o implementación y/o puesta en servicio y/o mantenimiento preventivo y/o reconfiguración de soluciones basadas en Firewalls y/o Seguridad Perimetral y/o equipos de comunicaciones y/o software de monitoreo y/o software de Protección contra Amenazas Avanzadas y/o solución en hardware y/o software de Defensa contra Amenazas Avanzadas

Acápite de las bases : Sección: Especifico **Numeral:** 3.2 **Literal:** B **Página:** 47

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

Análisis respecto de la consulta u observación:

En el literal B del numeral 10:

Dice:

ÍTEM 2: Servicio de instalación y configuración y/o implementación de soluciones de sistemas automatizados de seguridad de puntos finales o endpoints, y/o servicio de instalación y configuración y/o implementación y/o soporte y/o servicio gestionado de soluciones de recolección de eventos de seguridad de endpoints y equipos de comunicación y seguridad perimetral y/o recolección de eventos contra amenazas, y/o servicio de instalación y configuración y/o implementación y/o soporte de soluciones SIEM.

Debe decir:

ÍTEM 2: Servicio de instalación y configuración y/o implementación de soluciones de sistemas automatizados de seguridad de puntos finales o endpoints, y/o servicio de instalación y configuración y/o implementación y/o soporte y/o servicio gestionado de soluciones de recolección de eventos de seguridad de endpoints y equipos de comunicación y seguridad perimetral y/o recolección de eventos contra amenazas, y/o servicio de instalación y configuración y/o implementación y/o soporte de soluciones SIEM y/o servicio de instalación y/o configuración y/o implementación y/o puesta en servicio y/o mantenimiento preventivo y/o reconfiguración de soluciones basadas en Firewalls y/o Seguridad Perimetral y/o equipos de comunicaciones y/o software de monitoreo y/o software de Protección contra Amenazas Avanzadas y/o solución en hardware y/o software de Defensa contra Amenazas Avanzadas.

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

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se acoge la consulta y se modificará el TDR.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20503795079

Nombre o Razón social : DESYSWEB SAC

Fecha de envío : 14/03/2023

Hora de envío : 22:48:17

Consulta: Nro. 62

Consulta/Observación:

"Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado."

Sírvase confirmar que estos reportes automáticos pueden ser preparados manualmente por el personal residente dedicado o el SOC del contratista como parte del soporte técnico los cuales podrán ser solicitados a demanda o pueda realizarse a través del uso de la integración de una interfaz API.

Acápite de las bases : Sección: Especifico **Numeral:** 4.1.3 **Literal:** 0 **Página:** 22

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

Análisis respecto de la consulta u observación:

En el literal o del numeral 4.1.3:

Dice:

Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado

Debe decir:

Debe permitir la generación de reportes de la actividad maliciosa en toda la red. Estos reportes deben poder generarse o exportarse a pedido y de manera automática programada. La generación automática de reportes debe poder realizarse como mínimo para los reportes que vienen por defecto. Deberá tener la posibilidad de mostrar información como nombre de la máquina, versión de los componentes de la solución, sistema operativo, dirección IP, fecha de la actualización, fecha de la última verificación, eventos recientes y estado. Los reportes podrán ser preparados manualmente por el ingeniero residente a pedido, excepto por los reportes que vienen por defecto. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

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

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: El numeral 4.1.3.o quedará de la siguiente forma.

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20503795079

Nombre o Razón social : DESYSWEB SAC

Fecha de envío : 14/03/2023

Hora de envío : 22:48:17

Consulta: Nro. 63

Consulta/Observación:

"Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico."

Sírvase confirmar que estos reportes programados pueden ser preparados manualmente por el personal residente dedicado o el SOC del contratista como parte del soporte técnico los cuales podrán ser solicitados a demanda o pueda realizarse a través del uso de la integración de una interfaz API.

Acápites de las bases : Sección: Especifico Numeral: 4.1.3 Literal: q Página: 22

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: El numeral 4.1.3.q quedará de la siguiente forma: Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico. Los reportes podrán ser preparados manualmente por el ingeniero residente a pedido, excepto por los reportes que vienen por defecto. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado.

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

En el literal q del numeral 4.1.3:

Los reportes cuya ejecución sea programada, deben poder ser enviados por correo electrónico. Opcionalmente, se puede automatizar la generación de reportes y el envío por correo con el uso de la interfaz API de la solución XDR, con las siguientes condiciones:

- La información incluida en los reportes gestionados a través de la interfaz API será como mínimo la misma que ofrezca la solución XDR.
- No requiera instalación en los servidores de la Entidad.
- No se utilizará software de desarrolladores desconocidos.
- No se vulnerará la seguridad de la solución requerida ni de la información de la Entidad.
- Los niveles de disponibilidad no serán menores a la solución XDR SaaS.
- No implicará costos adicionales para la Entidad.
- No requerirá recursos adicionales a la Entidad.
- Si se requiriera de algún tipo de licenciamiento, este estará a nombre de la Entidad y no supondrá costos adicionales y estará disponible por lo menos durante el periodo contratado

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20503795079	Fecha de envío :	14/03/2023
Nombre o Razón social :	DESYSWEB SAC	Hora de envío :	22:48:17

Consulta: Nro. 64

Consulta/Observación:

"Debe permitir la sincronización con el directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección de dispositivos"

Considerando que se cuentan con diversos Enpoint y Servidores y siendo la Consola de Administración la encargada del despliegue, monitoreo y administración de las políticas de protección de los dispositivos no siendo necesario una integración con el directorio activo, más aún siendo las consolas en nube, sírvase confirmar que este requerimiento será opcional o se permitirá soluciones que puedan crear grupos de manera local.

Acápite de las bases : Sección: Especifico Numeral: 4.1.3 Literal: f Página: 22

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaría, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. En este caso, para la protección de dispositivos, el requerimiento está relacionado con la arquitectura tecnológica propia de la CGR, la cual utiliza la relación dinámica y de alta rotación de "grupo de usuarios - directorio activo", que es independiente y distinta a los despliegues de los agentes o los grupos locales.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código : 20503795079

Nombre o Razón social : DESYSWEB SAC

Fecha de envío : 14/03/2023

Hora de envío : 22:48:17

Consulta: Nro. 65

Consulta/Observación:

"Debe proteger las funciones críticas en los navegadores de internet, incluída protección contra sitios web que realizan ataques de phishing y/o fingerprinting"

Considerando que los ataques de phishing y/o de fingerprinting se basan en el uso de sitios web maliciosos para extraer credenciales y/o información de los usuarios de la entidad, sírvase confirmar que se aceptarán soluciones que incluyan protección contra sitios web maliciosos y/o prevención de exfiltración de datos y/o phishing y/o fingerprinting.

Acápite de las bases : Sección: Especifico Numeral: 4.1.4 Literal: s **Página:** 24

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null

Entidad convocante : CONTRALORIA GENERAL DE LA REPUBLICA

Nomenclatura : AS-SM-2-2023-C.G.R.-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CGR

Ruc/código :	20503795079	Fecha de envío :	14/03/2023
Nombre o Razón social :	DESYSWEB SAC	Hora de envío :	22:48:17

Consulta: Nro. 66

Consulta/Observación:

"Debe poder generar excepciones ante falsos positivos."

Sírvase confirmar que se podrá generar excepciones ante falsos positivos ya sea manual o automáticamente a través de la solución propuesta o especialistas del fabricante evitando así algún error involuntario por la manipulación del personal.

Acápite de las bases : Sección: Especifico Numeral: 4.1.5 Literal: g Página: 25

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

Análisis respecto de la consulta u observación:

El Comité de Selección, contando con opinión del Área Usuaria, señala lo siguiente: Se indica que los requerimientos indicados en los TDR son mínimos. Funcionalidades adicionales serán aceptadas siempre que no afecten el cumplimiento de lo requerido en los TDR.

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

null