

PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código : 20544303709

Fecha de envío : 21/02/2025

Nombre o Razón social : MICRO SOLUTIONS TI S.A.

Hora de envío : 17:37:00

Consulta: Nro. 1

Consulta/Observación:

Miembros del comité de selección sírvase precisar que se consideran como soluciones de seguridad la implementación de soluciones de respaldo y restauración de información para entornos físicos o virtualizados.

Una solución o plataforma de respaldo y restauración de información es considerado en el rubro tecnológico como una solución de seguridad, puesto que, permite proteger o salvaguardar los datos críticos al realizar copias de seguridad y permitir su recuperación en caso de pérdida.

Acápite de las bases : Sección: Especifico **Numeral:** 3.2 **Literal:** C **Página:** 42

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, las soluciones o plataformas de respaldo y restauración de información se consideran similares con el objeto de la convocatoria, puesto que hacen referencia a una solución de seguridad e incluirlos permitirá dar cumplimiento a los principios de libertad de concurrencia y competencia, ampliando de esa manera el universo de postores que pueden participar en el presente proceso de selección. En ese sentido se acepta la solicitud del participante y se incluirá el mencionado en los terminos de referencia. Asimismo, se precisa que se aceptaran servicios de soluciones y/o servicio de implementación de las soluciones consideradas como servicios similares.

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

"REQUISITOS DE CALIFICACIÓN

C. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

(...)

Se consideran servicios similares a los siguientes: servicios de soluciones y/o implementación de soluciones de seguridad y ciberseguridad (antivirus y/o antispam y/o XDR y/o EDR), soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática y/o soluciones de respaldo y restauración de información para entornos físicos o virtualizados y/o servicio de hackeo ético y/o servicio de ethical hacking y/o servicio de ejecución de ethical hacking y/o servicio para el análisis de vulnerabilidades y/o servicio de análisis de vulnerabilidades y/o servicio de pruebas de penetración y/o servicio para el análisis de ciberseguridad.

(Se incluyen ajustes en merito a la absolución de las consultas 3 y 38 incluidos)"

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20606052112	Fecha de envío :	21/02/2025
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	18:56:46

Observación: Nro. 2
Consulta/Observación:
9.2 Requisitos Del Personal Propuesto
Página 35

Se solicita en las bases administrativas que el jefe de proyectos cuente con la siguiente formación académica:

1. Ingeniero Titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Informática.
2. Certificación vigente en gestión de proyectos PMP o Scrum Máster Certified.
3. Certificación en ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC)
4. Participación en curso o taller Gestión De Ciber Crisis con un mínimo de ocho (08) horas.

El principio de libertad de concurrencia establece que en los procesos de contratación pública de bienes, servicios y obras se deben incluir regulaciones o disposiciones que fomenten la más amplia concurrencia o participación de postores. En virtud de este principio las reglas o disposiciones en el marco de un proceso de selección deben fomentar, estimular o garantizar la participación del mayor número de postores o posibles interesados en el proceso y para ello debe evitarse la existencia de exigencias costosas e innecesarias.

Si nos remitimos al perfil académico del jefe de proyecto observaremos una serie de certificados (04 en total) que limitan o restringen la participación de postores.

Se solicita en las bases administrativas que el jefe de proyectos cuente con la siguiente formación académica: Ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC). Existen en el campo académico una serie de certificados que no poseen el mismo nombre, pero si incluyen el mismo contenido curricular o incluso con un nivel superior. En ese sentido, SOLICITO que puedan considerar como similar o equivalente al certificado en Ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC), el Certified Cyber Security Management Professional ISO 27032.

Acápite de las bases : Sección: Especifico Numeral: 9.2 Literal: ----- Página: 35
Artículo y norma que se vulnera (En el caso de Observaciones):
Ley N°30225, artículo 2 literal a) y e)
Análisis respecto de la consulta u observación:

"En atención a la observación, Se precisa al participante que, los requisitos minimos exigidos al personal jefe de proyectos estan orientados al cumplimiento de las actividades que se le solicitan realizar ,ya que, se requiere que el personal cuente con dichos conocimiento para el optimo desarrollo de sus actividades, asimismo, estos requisitos son proporcionales al servicio que se requiere, por lo cual, no se está vulnerando el principio de libertad de concurrencia de la Ley de Contrataciones del Estado.

Sin perjuicio a ello, se acoge parcialmente la observación formulada, en razón a que permitirá dar cumplimiento a los principios de concurrencia y competencia, ampliando de esa manera el universo de postores que pueden participar en el presente proceso de selección. En ese sentido, se condierara como similar o equivalente al certificado en Ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC), el Certified Cyber Security Management Professional ISO 27032.

De igual manera, se le precisa al participante que, en merito a la absolución de la Observación N°10 y Consulta N°22, se ha aceptado que la Certificación en ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC),

Entidad convocante :	CONGRESO DE LA REPUBLICA
Nomenclatura :	CP-SM-2-2025-CR-1
Nro. de convocatoria :	1
Objeto de contratación :	Servicio
Descripción del objeto :	SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

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

Ley N°30225, artículo 2 literal a) y e)

Análisis respecto de la consulta u observación:

sea considerada de presentación opcional, por lo cual, el Certified Cyber Security Management Professional ISO 27032 contará con la misma condición."

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

9.2. Requisitos del Personal propuesto:

(...)

¿ Un (01) jefe de Proyectos.

Formación Académica, capacitación y otros:

- Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática. Con colegiatura vigente al realizar el servicio.
- Certificación vigente en gestión de proyectos PMP o Scrum Master Certified.
- Certificación en ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC) y/o Certified Cyber Security Management Professional ISO 27032. (La presentación de cualquiera de los certificados mencionados es opcional)
- Participación en curso o taller ¿Gestión de Ciber Crisis¿ con un mínimo de 08 horas lectivas.

Nota: se agregar ajustes realizado en merito a la absolución del consulta N° 10.

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20606052112	Fecha de envío :	21/02/2025
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	18:56:46

Consulta: Nro. 3

Consulta/Observación:

Sírvase confirmar que se consideran como soluciones de seguridad y/o ciberseguridad: antivirus y/o antispam y/o XDR y/o EDR y/o otros que tengan similar naturaleza.

Acápite de las bases : Sección: Especifico Numeral: 3.2 Literal: C Página: 42

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

Análisis respecto de la consulta u observación:

"Se acepta parcialmente la solicitado, debido a que el termino ""otros que tengan similar naturaleza"" es subjetivo, por lo tanto. se consideran como soluciones de seguridad y/o ciberseguridad: antivirus y/o antispam y/o XDR y/o EDR.

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

"REQUISITOS DE CALIFICACIÓN
C. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
(...)

Se consideran servicios similares a los siguientes: servicios de soluciones y/o implementación de soluciones de seguridad y ciberseguridad (antivirus y/o antispam y/o XDR y/o EDR), soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática y/o soluciones de respaldo y restauración de información para entornos físicos o virtualizados y/o servicio de hackeo ético y/o servicio de ethical hacking y/o servicio de ejecución de ethical hacking y/o servicio para el análisis de vulnerabilidades y/o servicio de análisis de vulnerabilidades y/o servicio de pruebas de penetración y/o servicio para el análisis de ciberseguridad.

(Se incluyen ajustes en merito a la absolución de las consultas 1 y 38 incluidos)

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20606052112	Fecha de envío :	21/02/2025
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	18:56:46

Consulta: Nro. 4

Consulta/Observación:

9.1 Requisitos Del Proveedor
Página 35

Se solicita en las bases administrativas que el postor deberá contar con al menos dos certificaciones de soluciones de ciberseguridad. Sírvase a precisar si la forma de acreditar esas dos certificaciones se podrá hacer mediante una carta del fabricante o representante local de las de soluciones de ciberseguridad en donde se acredite a la empresa como socio, partner o distribuidor autorizado.

Acápite de las bases : Sección: Especifico Numeral: 9.1 Literal: ----- Página: 35

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

Análisis respecto de la consulta u observación:

A fin de obtener mayor pluralidad de postores, se acepta la solicitud del participante. Se precisa en los terminos de referencia que el postor podrá acreditar el contar con al menos 2 certificaciones de soluciones de Ciberseguridad con: i) copias simples de los certificados oficiales emitidos por la entidad autorizada o documentos de designación formal o, ii) carta del fabricante o representante local de las de soluciones de ciberseguridad en donde se acredite al postor como socio, partner o distribuidor autorizado y se precise las certificaciones de soluciones de ciberseguridad con las que cuenta.

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

"9. REQUISITOS DEL PROVEEDOR Y SU PERSONAL
9.1. Requisitos del proveedor

(i)
¿ El postor deberá contar con al menos 2 certificaciones de soluciones de Ciberseguridad.
(...)

Acreditación centro de atención al cliente:

Para acreditar certificaciones de soluciones de ciberseguridad se aceptarán: i) copias simples de los certificados oficiales emitidos por la entidad autorizada o documentos de designación formal o, ii) carta del fabricante o representante local de las de soluciones de ciberseguridad en donde se acredite al postor como socio, partner o distribuidor autorizado y se precise las certificaciones de soluciones de ciberseguridad con las que cuenta."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20606052112	Fecha de envío :	21/02/2025
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	18:56:46

Consulta: Nro. 5

Consulta/Observación:

9.1 Requisitos Del Proveedor
Página 35

Se solicita en las bases administrativas que el postor adjudicado deberá ser distribuidor autorizado de la solución ofertada. Sírvase a precisar: 1) Dicha documentación en qué momento será presentada y 2) La carta o documento que acredita la condición de distribuidor autorizado podrá ser emitida por el representante local de la solución ofertada.

Acápite de las bases : Sección: Especifico Numeral: 9.1 Literal: ----- Página: 35

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

Análisis respecto de la consulta u observación:

A fin de obtener mayor pluralidad de postores, se acepta la solicitud del participante. Se precisa en los terminos de referencia que el postor deberá ser socio, partner o distribuidor autorizado por el fabricante o representante local de las soluciones de ciberseguridad ofertadas. Dicho requisito deberá ser acreditado para el perfeccionamiento del contrato con la presentación de carta del fabricante o representante local del fabricante de las de soluciones de ciberseguridad en donde se acredite al postor como socio, partner o distribuidor autorizado.

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

"9. REQUISITOS DEL PROVEEDOR Y SU PERSONAL

9.1. Requisitos del proveedor

(i)
¿ El postor adjudicado deberá ser socio, partner o distribuidor autorizado de la solución ofertada.
(...)

Acreditación centro de atención al cliente:

Para acreditar ser socio, partner o distribuidor autorizado por el fabricante, deberá presentar copia de carta del fabricante o representante local del fabricante de las de soluciones de ciberseguridad en donde se acredite al postor como socio, partner o distribuidor autorizado.

(...)
Estos documentos deberán ser presentados para el perfeccionamiento del contrato."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20606052112	Fecha de envío :	21/02/2025
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	18:56:46

Consulta: Nro. 6

Consulta/Observación:

9.1 Requisitos Del Proveedor
Página 35

Se solicita en las bases administrativas que el postor deberá: 1) Disponer de todos los equipos y herramientas de trabajo necesarios a ser utilizadas durante la prestación del servicio y 2) Contar con un sólido equipo de trabajo, el mismo que deberá garantizar el desarrollo del trabajo solicitado en el plazo y horarios establecidos.
Sírvasse a precisar si la forma de acreditar esas dos condiciones o requisitos se podrá hacer mediante una declaración jurada.

Acápíte de las bases : Sección: Especifico Numeral: 9.1 Literal: ----- Página: 35

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, los puntos en mención serán acreditados mediante la presentación de la declaración jurada de cumplimiento de los términos de referencia en su oferta (Anexo N°3), no siendo necesario presentar una declaración jurada adicional.

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

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20606052112	Fecha de envío :	21/02/2025
Nombre o Razón social :	CYBER SECURITY ENTERPRISE S.A.C.	Hora de envío :	18:56:46

Consulta: Nro. 7

Consulta/Observación:

Anexo N°6 ¿ Precio de la Oferta
Página 59

Se sirve a precisar si en el anexo N°6 solo se colocara el precio de la oferta, tal cual el formato brindado; o en su defecto, si se deberá detallar el precio en función a la forma de pago, para lo cual la Entidad brindará el formato.

Acápite de las bases : Sección: Especifico Numeral: Anexo 6 Literal: ----- Página: 59

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

Análisis respecto de la consulta u observación:

Se precisa al participante que, de acuerdo al numeral 22 de los terminos de referencia, la presente contratación se rige bajo el sistema de Suma Alzada, en ese sentido, el precio ofertado deberá ser por la suma total del servicio, incluido todos los impuestos de Ley. En ese sentido, se precisa que en el Anexo N°06 Precio de la Oferta, deberá consignar el monto total de su oferta, sin indicar ningún desglose de detalles de los precios, tal como se establece en el formato de las bases.

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

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20537328445	Fecha de envío :	21/02/2025
Nombre o Razón social :	IB TECHNOLOGY GROUP S.A.C.-IB TECH GROUP S.A.C.	Hora de envío :	21:43:15

Observación: Nro. 8

Consulta/Observación:

Estimados miembros del comité de selección en el numeral 3.2, literal C (experiencia del postor en la especialidad) se establece que se consideran como servicios similares a los siguientes: servicios de soluciones de seguridad y ciberseguridad, soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática. Dada la complejidad de las soluciones de seguridad y ciberseguridad la adquisición de estas lleva aparejada o incluye su implementación, soporte, capacitación, entre otros. Se observan las presentes bases y se solicita se acepte la venta de bienes y/o servicios de: soluciones de seguridad y/o soluciones de ciberseguridad y/o soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática.

Acápate de las bases : Sección: Especifico Numeral: 3.2 Literal: C Página: 42

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

Ley de Contrataciones del Estado, artículo 2

Análisis respecto de la consulta u observación:

"No se acoge la observación. El presente procedimiento de selección tiene como objeto la contratación de un servicio, la cual incluyen otras prestaciones menores como lo son su implementación, soporte y capacitación. Respecto a las prestaciones, se precisa que, de acuerdo a los términos de referencia, ninguna de estas involucra el suministro o adquisición de bienes.

Cabe precisar que, de acuerdo con lo establecido en el numeral 53.3 del artículo 53 del Reglamento de la Ley de Contrataciones de Estado, en el caso de contrataciones que involucren diversos tipos de prestaciones, el objeto se determina en función a la prestación que represente la mayor incidencia porcentual en el valor estimado de la contratación, siempre que no desvirtúe la naturaleza de la contratación. Considerando que las prestaciones que se incluyen también son servicios, se determina que objeto de la presente contratación es indefectiblemente un Servicio, por lo cual, correspondió a la Entidad utilizar las Bases Estándar para la contratación de servicios en general, aprobada mediante Directiva N°001-2019-CD/OSCE, para su convocatoria.

De acuerdo a dichas Bases Estandar, para el requisito de calificación: Experiencia del postor, se deben considerar servicios similares, para lo cual, las misma bases indican lo siguiente en dicho extremo referido: "[CONSIGNAR LOS SERVICIOS SIMILARES AL OBJETO CONVOCADO]"; por lo cual, experiencias cuyo objeto contractual este definido con la venta o adquisición de bienes, no puede ser aceptado como un servicio similar, ya que de hacerlo, se estaría contraviniendo lo establecido en las bases estándar."

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

null

Entidad convocante :	CONGRESO DE LA REPUBLICA
Nomenclatura :	CP-SM-2-2025-CR-1
Nro. de convocatoria :	1
Objeto de contratación :	Servicio
Descripción del objeto :	SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20537328445	Fecha de envío :	21/02/2025
Nombre o Razón social :	IB TECHNOLOGY GROUP S.A.C.-IB TECH GROUP S.A.C.	Hora de envío :	21:43:15

Observación: Nro. 9

Consulta/Observación:

Estimados miembros del comité de selección en el numeral 9.1 se establece lo siguiente: El postor adjudicado deberá ser distribuidor autorizado de la solución ofertada.

Teniendo en cuenta que las marcas de seguridad y ciberseguridad más representativas del mercado tecnológico, son de origen extranjero y que todas ellas para llegar al mayor número de países cuentan con un representante local, que se encarga representar a la marca en el territorio, la observación es la siguiente: Para permitir una mayor pluralidad de postores debe ser posible que la carta que acredite ser un distribuidor autorizado del producto ofertado pueda ser otorgada por el representante local de la marca o quien haga sus veces.

Permitir ello generaría una mayor pluralidad de postores y evitaría exigencias innecesarias, en concordación con el principio de concurrencia.

Acápíte de las bases : Sección: Específico **Numeral:** 9.1 **Literal:** NO TIENE **Página:** 35

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

Ley de Contrataciones del Estado articulo 2

Análisis respecto de la consulta u observación:

En atención a la observación, se acoge la observación formulada, estableciendo que los postores deberán acreditar su condición de distribuidores autorizados del producto ofertado, a través de un documento emitido por el fabricante y/o representante local de la marca ofertada.

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

null

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20537328445	Fecha de envío :	21/02/2025
Nombre o Razón social :	IB TECHNOLOGY GROUP S.A.C.-IB TECH GROUP S.A.C.	Hora de envío :	21:43:15

Observación: Nro. 10

Consulta/Observación:

Estimados miembros del comité de selección en el numeral 9.1 se establece que el jefe de proyectos cuente con la ¿Certificación en ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC)¿. La certificación en mención no brinda la opción de presentar un certificado de similar naturaleza como si lo hace la certificación vigente en gestión de proyectos PMP o Scrum Máster Certified.

Se observan las presentes bases y se solicita que la Certificación en ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC) sea declarada como opcional o en su defecto que puedan presentarse certificados de similar naturaleza.

Acápite de las bases : Sección: Especifico Numeral: 9.1 Literal: NO TIENE Página: 35

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

Ley de Contrataciones del Estado articulo 2

Análisis respecto de la consulta u observación:

"En atención a la observación, Se precisa al participante que, los requisitos mínimos exigidos al personal jefe de proyectos están orientados al cumplimiento de las actividades que se le solicitan realizar ,ya que, se requiere que el personal cuente con dichos conocimiento para el optimo desarrollo de sus actividades, asimismo, estos requisitos son proporcionales al servicio que se requiere, por lo cual, no se está vulnerando el principio de libertad de concurrencia de la Ley de Contrataciones del Estado.

Sin perjuicio a ellos, Se acoge parcialmente la observación formulada, en razón a que permitirá dar cumplimiento a los principios de concurrencia y competencia, ampliando de esa manera el espectro de postores que pueden participar en el presente proceso de selección. En ese sentido, el certificado de Ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC) será considerado como opcional."

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

"9.2. Requisitos del Personal propuesto:

(...)

¿ Un (01) jefe de Proyectos.

Formación Académica, capacitación y otros:

- Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática. Con colegiatura vigente al realizar el servicio.
- Certificación vigente en gestión de proyectos PMP o Scrum Master Certified.
- Certificación en ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC) y/o Certified Cyber Security Management Professional ISO 27032. (La presentación de cualquiera de los certificados mencionados es opcional).
- Participación en curso o taller ¿Gestión de Ciber Crisis¿ con un mínimo de 08 horas lectivas.

Nota: Se agregan ajustes realizado en merito a la absolución del consulta N° 02"

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20537328445	Fecha de envío :	21/02/2025
Nombre o Razón social :	IB TECHNOLOGY GROUP S.A.C.-IB TECH GROUP S.A.C.	Hora de envío :	21:43:15

Consulta: Nro. 11

Consulta/Observación:

Estimados miembros del comité de selección sírvanse a precisar si en el anexo N°4 se colocará el plazo de entrega acorde al formato brindado, y no se deberá incluir información adicional.

Acápite de las bases : Sección: Especifico Numeral: NO TIENE Literal: ANEXO N°4 Página: 56

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, el anexo N°4 deberá ser llenado de acuerdo a lo especificado en las bases administrativas, no será necesario incluir información adicional.

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

null

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Consulta: Nro. 12

Consulta/Observación:

Para una mayor pluralidad de postores sírvase confirmar que se aceptará carta de fabricante indicando como es el funcionamiento para aquellos puntos que no se encuentren en Catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento.

Acápite de las bases : Sección: Especifico Numeral: 2.2.1.1 Literal: e Página: 16

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, el servicio demanda alcances técnicos específicos que determinarán el éxito del proyecto, por lo que, el postor deberá adjuntar capturas de pantalla Catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales para acreditar las funcionalidades de las plataformas ofertadas que se describen en el numeral 7.5 de los términos de referencia. En ese sentido, no se aceptará carta del fabricante; no obstante, se hace la precisión en los terminos de referencia que, la presentación de dichos documentos es únicamente para acreditar las funcionalidades de la plataforma establecidas en el numeral 7.5 de los términos de referencia.

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

7.5. PRESENTACION OBLIGATORIA DENTRO DE LA PROPUESTA:

El Postor dentro de su propuesta, deberá acreditar mediante la presentación de catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento, el cumplimiento de los siguientes componentes:

Compatibilidad con sistemas operativos especificados, integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red), autenticación de dos factores (2FA), protocolos de comunicación segura, aislamiento del agente (sin conexiones entrantes ni control remoto), coadministración basada en roles (propietario, visualizador, resolutor de incidentes), capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK, reducción de la superficie de ataque mediante pruebas de penetración y (...)

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Consulta: Nro. 13

Consulta/Observación:

Para una mayor pluralidad de postores sírvase confirmar que se aceptará e) Catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales en idioma ingles y/o español

Acápíte de las bases : Sección: Especifico Numeral: 2.2.1.1 Literal: e Página: 16

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

Análisis respecto de la consulta u observación:

"De conformidad con el artículo 59 del Reglamento de la Ley de Contrataciones del Estado, se establece lo siguiente: ""Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, según corresponda, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que puede ser presentada en el idioma original.""", lo cual esta precisado en el numeral 1.7. del Capítulo I - Sección General de las bases del presente procedimiento de selección.

No obstante, la documentación referida se encuentra establecida como documento de presentación obligatoria para la admisión de la oferta (numeral 2.2.1.1 de la Sección Especifica de las bases), es decir, dichos documentos son esenciales en la oferta, de caracter obligatoria para acreditar componentes del servicio a prestar, por lo que no tendría la naturaleza de un documento complementario.

En ese sentido, en el caso que se presenten catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento, en idioma ingles, o cualquier otro idioma distinto al español, deberán estar acompañados de su respectiva traducción por traductor público juramentado o traductor colegiado certificado, según corresponda."

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

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Consulta: Nro. 14

Consulta/Observación:

SE DICE:

El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 3 para los productos de detección y respuesta ofertados.

SE CONSULTA:

Para una mayor pluralidad de postores sírvase confirmar que también se aceptará auditoría y/o certificación tipo SOC 2 y/o SOC 3

Acápito de las bases : Sección: Especifico **Numeral:** 3.1 **Literal:** 7.1 **Página:** 22

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

Análisis respecto de la consulta u observación:

"Se acepta lo solicitado de forma parcial:

Para garantizar mayor pluralidad y concurrencia, se modificará el requerimiento de la siguiente manera:

""El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 2 y SOC 3 para los productos de detección y respuesta ofertados.""

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

"7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA

(...)

El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 2 y SOC 3 para los productos de detección y respuesta ofertados"

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Consulta: Nro. 15

Consulta/Observación:

SE DICE:
La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con las normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0.

SE CONSULTA:
Para una mayor pluralidad de postores sírvase confirmar que La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con al menos dos (02) de las siguientes normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0.

Acápite de las bases : Sección: Especifico Numeral: 3.1 Literal: 7.7 Página: 22

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

Análisis respecto de la consulta u observación:

Se acepta lo solicitado, por lo tanto se confirma que la plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con al menos dos (02) de las siguientes normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0.

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

"7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA
(...)
La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con al menos dos (02) de las siguientes normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Consulta: Nro. 16

Consulta/Observación:

SE DICE:
La plataforma debe proporcionar una capacidad segura, liviana y fácil de implementar para capturar la telemetría de seguridad desde los puntos finales a través de un agente ligero que no supere los ocho (08) MB de tamaño a fin de que el equipo de profesionales que trabaja en el SOC Data Center clasifique, correlacione y registre datos de forma eficiente y efectiva.

SE CONSULTA
Para una mayor pluralidad de postores sírvase confirmar que el agente no deberá superar los 80 MB de tamaño

Acápite de las bases : Sección: Especifico Numeral: 3.1 Literal: 7.1 Página: 23

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

Análisis respecto de la consulta u observación:

"En atención a la consulta se precisa que, lo señalado en ese punto es ocho(08)MB y no 80MB (como señala el participante). Ahora bien, con la finalidad de garantizar la mayor pluralidad de postores se retira el requerimiento el tamaño máximo del agente."

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

"7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA
(...)

La plataforma debe proporcionar una capacidad segura, liviana y fácil de implementar para capturar la telemetría de seguridad desde los puntos finales a través de un agente ligero, a fin de que el equipo de profesionales que trabaja en el SOC Data Center clasifique, correlacione y registre datos de forma eficiente y efectiva."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Consulta: Nro. 17

Consulta/Observación:

SE DICE:
La plataforma debe contar con una aplicación que brinde la posibilidad de recopilar y analizar eventos en CEF (formato de evento común) y LEEF (formato extendido de evento de registro) a través de Syslog.

SE CONSULTA
para una mayor pluralidad de postores sÍrvase confirmar que se podrÁ analizar eventos en CEF y/o LEEF

Acápite de las bases : Sección: Especifico Numeral: 3.1 Literal: 7.1 Página: 23

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, el registro y análisis de eventos CEF y LEEF es absolutamente necesario a fin de garantizar la compatibilidad e integración con el mayor número de componentes de red e infraestructura, por lo cual, no se acepta su solicitud.

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

null

Entidad convocante :CONGRESO DE LA REPUBLICA

Nomenclatura :CP-SM-2-2025-CR-1

Nro. de convocatoria :1

Objeto de contratación :Servicio

Descripción del objeto :SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Consulta: Nro. 18

Consulta/Observación:

SE DICE:

La plataforma de Cyber SOC deberá estar diseñada específicamente para buscar TTP sobre el dispositivo local Windows, Mac y Linux en varias categorías, incluidas mínimamente descubrimiento, persistencia, evasión de defensa, ejecución, acceso a credenciales, escalada de privilegios y movimiento lateral.

SE CONSULTA

Sírvase confirmar que son servidores windows y/o linux

Acápite de las bases : Sección: Especifico Numeral: 3.1 Literal: 7.1 Página: 24

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, el alcance debe cubrir un entorno de red multiplataforma a fin de no dejar puntos ciegos en la gestión, por lo que la plataforma deberá estar diseñada para buscar TTP sobre dispositivos con Sistema Operativo Windows, Mac y Linux.

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

null

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	22:55:52

Observación: Nro. 19

Consulta/Observación:

SE DICE:

La plataforma de Cyber SOC deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas considerando mínimamente las siguientes metodologías de prueba de búsqueda de amenazas como Browser visit, DNS Cache Entry, Driver File Hash, Driver File Name, File Hash, File Name, Event in log source, Event in log category, Event ID in log, Event type in log, Service state, User Account, Network connection, Process Hash, Process Name, Registry Key y YARA rules.

OBSERVACIÓN:

Solicitamos que el punto técnico sea considerado opcional, se observa claramente que el punto técnico SOLO ES CUMPLIDO POR UN FABRICANTE como se demuestra en la siguiente página web del Fabricante ROCKETCYBER, de igual manera el contratista está cerrando este punto técnico ya que menciona "CONSIDERANDO MÍNIMAMENTE" por lo que indica que todas las características que menciona deben ser cumplidas.

<https://www.rocketcyber.com/faqs/>

luego expandir la siguiente pregunta número 2: "2. What threat-hunting capabilities does RocketCyber have?" y verán que todas las características que solicitan son iguales.

ante lo antes mencionado no sabemos si los demás puntos son exclusivamente de este Fabricante.

Este tipo de especificación contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores y fabricantes. La descripción del punto implica una orientación hacia productos específicos, lo que limita innecesariamente el acceso de otros proveedores que puedan ofrecer soluciones tecnológicamente equivalentes o superiores. Por tanto, solicitamos que el requerimiento sea considerado opcional o suprimido en su totalidad para permitir la participación de una gama más amplia de soluciones, promoviendo la competencia y garantizando que el proceso de contratación se mantenga dentro de los principios de igualdad de oportunidades.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1 **Literal:** 7.1 **Página:** 24

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

Análisis respecto de la consulta u observación:

"Se acoge la observación formulada parcialmente, en razón a que las funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas constituyen un estándar en la industria y soluciones como la de IBM QRadar SIEM, Splunk Enterprise Security y otros cumplen y extienden capacidades con respecto a lo requerido; por lo que los principios que inspiran la contratación pública no se ven vulnerados.

Sin perjuicio a ellos, el requerimiento sera modificado con el siguiente texto: ""La plataforma de Cyber SOC deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizada"

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

"7.2. CAPACIDADES DE DETECCION Y RESPUESTA DE CIBERATAQUES

(...)

La plataforma de Cyber SOC deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	23:04:21

Observación: Nro. 20

Consulta/Observación:

SE DICE:
La plataforma debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2 permitiendo solo los siguientes conjuntos de cifrado fuertes:
o TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_GCM_SHA384

OBSERVACIÓN:
se observa claramente que el punto técnico SOLO ES CUMPLIDO POR UN FABRICANTE como se demuestra en la siguiente página web del Fabricante ROCKETCYBER, de igual manera el contratista está cerrando este punto técnico ya que menciona "PERMITIENDO SOLO LOS SIGUIENTES CONJUNTOS DE CIFRADOS FUERTES" por lo que indica que todas las características que menciona deben ser cumplidas.
página web: <https://help.rocketcyber.kaseya.com/help/Content/general/rocketcyber-managed-soc-agent-architecture-and-capabilities.htm>
y verán que todas las características que solicitan son iguales.
ante lo antes mencionado no sabemos si los demás puntos son exclusivamente de este Fabricante (consulta número 8 también es del fabricante rocketcyber).

Este tipo de especificación contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores y fabricantes. La descripción del punto implica una orientación hacia productos específicos, lo que limita innecesariamente el acceso de otros proveedores que puedan ofrecer soluciones tecnológicamente equivalentes o superiores. Por tanto, solicitamos que el requerimiento sea considerado opcional o suprimido en su totalidad para permitir la participación de una gama más amplia de soluciones, promoviendo la competencia y garantizando que el proceso de contratación se mantenga dentro de los principios de igualdad de oportunidades.

Acápíte de las bases : Sección: Especifico Numeral: 3.1 Literal: 7.1 Página: 23

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

Análisis respecto de la consulta u observación:
Se acoge la observación formulada parcialmente, por lo tanto el requerimiento sera modificado con el siguiente texto: "La plataforma debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2"

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
"7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCION Y RESPUESTA
(...)
La plataforma debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	23:12:25

Observación: Nro. 21

Consulta/Observación:

SE DICE:

La plataforma debe permitir la coadministración efectiva por parte del Congreso de la Republica a través de la integración de un sistema de acceso basado en roles considerando mínimamente:

o Rol de propietario, habilitando control total sobre la plataforma

o Rol visualizador, habilitando funciones de seguimiento y generación de informes sobre todos los eventos generados y procesados

o Rol resolutor de incidentes, habilitando funciones de seguimiento, generación de informes, aislamiento y liberación de host afectados.

OBSERVACIÓN:

se observa claramente que el punto técnico SOLO ES CUMPLIDO POR UN FABRICANTE como se demuestra en la siguiente página web del Fabricante ROCKETCYBER, de igual manera el contratista utiliza los MISMOS NOMBRES DE ROLES que el fabricante ROCKETCYBER utiliza por lo que se observa una clara inclinación hacia ese fabricante

página web:<https://help.rocketcyber.kaseya.com/help/Content/general/roles-and-access-permissions-in-rocketcyber.html?Highlight=profile>

y verán que todas las características que solicitan están en inglés pero cuya traducción es lo solicitado por la entidad:

Provider Owner = propietario

Viewer= visualizador

Incident Responder = resolutor de incidentes

ante lo antes mencionado no sabemos si los demás puntos son exclusivamente de este Fabricante (consulta número 8 y 9 también es del fabricante rocketcyber).

Este tipo de especificación contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores y fabricantes. La descripción del punto implica una orientación hacia productos específicos, lo que limita innecesariamente el acceso de otros proveedores que puedan ofrecer soluciones tecnológicamente equivalentes o superiores. Por tanto, solicitamos que el proceso sea considerado no válido

Acápite de las bases : Sección: Especifico Numeral: 3.1 Literal: 7.1 Página: 23
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se acoge la observación, a fin de contar con mayor pluralidad de postores, se modificará el texto indicado lo siguientes:

""La plataforma debe permitir la coadministración efectiva por parte del Congreso de la Republica a través de la integración de un sistema de acceso basado en roles, considerando como mínimo roles de administración y visualización"

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

"7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCION Y RESPUESTA

(...)

La plataforma debe permitir la coadministración efectiva por parte del Congreso de la Republica a través de la

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

integración de un sistema de acceso basado en roles, considerando como mínimo roles de administración y visualización."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	23:47:09

Consulta: Nro. 22

Consulta/Observación:

SE DICE:

Un (01) jefe de Proyectos.

Formación Académica, capacitación y otros:

o Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática. Con colegiatura vigente al realizar el servicio.

o Certificación vigente en gestión de proyectos PMP o Scrum Master Certified.

o Certificación en Ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC).

o Participación en curso o taller ¿Gestión de Ciber Crisis¿ con un mínimo de 08 horas lectivas.

SE CONSULTA:

Solicitamos considerar como opcional el requisito de certificación en Ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC). para el Jefe de Proyecto, ya que la función principal del Jefe de Proyectos es de garantizar la conducción adecuada del proyecto Esto permitiría valorar perfiles con competencias estratégicas y conocimientos aplicables a la gestión de proyectos. Dicho punto vulnera la libre participación de postores ya que se están especificando certificaciones y cursos que son más aptos para los operadores.

Acápite de las bases : Sección: Especifico **Numeral:** 3.1 **Literal:** 9.2 **Página:** 36

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

Análisis respecto de la consulta u observación:

"En atención a la observación, Se precisa al participante que, los requisitos minimos exigidos al personal jefe de proyectos estan orientados al cumplimiento de las actividades que se le solicitan realizar ,ya que, se requiere que el personal cuente con dichos conocimiento para el optimo desarrollo de sus actividades, asimismo, estos requisitos son proporcionales al servicio que se requiere, por lo cual, no se está vulnerando el principio de libertad de concurrencia de la Ley de Contrataciones del Estado.

Sin perjuicio a ellos, Se acepta parcialmente lo solicitado, en razón a que permitirá dar cumplimiento a los principios de concurrencia y competencia, ampliando de esa manera el espectro de postores que pueden participar en el presente proceso de selección. En ese sentido, el certificado de Ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC) será considerado como opcional"

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

"9.2. Requisitos del Personal propuesto:

(...)

¿ Un (01) jefe de Proyectos.

Formación Académica, capacitación y otros:

- Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática. Con colegiatura vigente al realizar el servicio.
- Certificación vigente en gestión de proyectos PMP o Scrum Master Certified.
- Certificación en ciberseguridad Lead Cybersecurity Profesional Certificate (LCSPC) y/o Certified Cyber Security Management Professional ISO 27032. (La presentación de cualquiera de los certificados mencionados es opcional)
- Participación en curso o taller ¿Gestión de Ciber Crisis¿ con un mínimo de 08 horas lectivas.

Nota: Se agregan ajustes realizado en merito a la absolución del consulta N° 02"

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	23:51:41

Consulta: Nro. 23

Consulta/Observación:

se dice:

Un (01) Operador de Servicio

Formación Académica, capacitación y otros:

o Técnico profesional en redes y comunicaciones y/o telecomunicaciones.

o Certificación técnica vigente en CEH V12 - Certified Ethical Hacker

o Participación en curso o taller ¿Gestión de Ciber Crisis¿ con un mínimo de 08 horas lectivas

SE CONSULTA:

Para una mayor pluralidad de postores sírvase confirmar que el Operador de Servicio tenga Certificación técnica vigente en CEH V12 - Certified Ethical Hacker y/o ISO 27032 y/o Ethical Hacking Professional Certification (CEHPC)

Acápite de las bases : **Sección:** Específico **Numeral:** 3.1 **Literal:** 9.2 **Página:** 37

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

Análisis respecto de la consulta u observación:

"En atención a la consulta se precisa que la certificación internacional vigente CEH V12 - Certified Ethical Hacker constituye la base de los procedimientos que se desarrollaran con el servicio, por lo que, se deberá evidenciar la habilitación de esta certificación.

Sin perjuicio a ellos, Se acepta parcialmente lo solicitado, en razón a que permitirá dar cumplimiento a los principios de concurrencia y competencia, ampliando de esa manera el universo de postores que pueden participar en el presente proceso de selección. En ese sentido, el certificado Ethical Hacking Professional Certification (CEHPC) será considerado como equivalente.

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

"9.2. Requisitos del Personal propuesto:

(¿)

¿ Un (01) Operador de Servicio

(¿)

Certificación técnica vigente en CEH V12 - Certified Ethical Hacker y/o Ethical Hacking Professional Certification (CEHPC)."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20601252989	Fecha de envío :	21/02/2025
Nombre o Razón social :	ALLSAFE CORPORATION EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA - ALLSAFE CORP E.I.R.L.	Hora de envío :	23:53:46

Consulta: Nro. 24

Consulta/Observación:

se dice:
Un (01) Operador de Servicio
Formación Académica, capacitación y otros:
o Técnico profesional en redes y comunicaciones y/o telecomunicaciones.
o Certificación técnica vigente en CEH V12 - Certified Ethical Hacker
o Participación en curso o taller ¿Gestión de Ciber Crisis¿ con un mínimo de 08 horas lectivas

SE CONSULTA:
Para una mayor pluralidad de postores sírvase confirmar que el Operador de Servicio podrá ser ingeniero titulado y/o bachiller y/o técnico titulado y/o técnico profesional en redes y comunicaciones y/o telecomunicaciones y/o sistemas e informática y/o electrónica y/o informática y/o carreras afines.

Acápite de las bases : Sección: Específico **Numeral:** 3.1 **Literal:** 9.2 **Página:** 37

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

Análisis respecto de la consulta u observación:

"A fin de obtener mayor pluralidad de postores, se acepta parcialmente su solicitud. Se precisa que el personal requerido: operador del servicio, deberá contar con el grado de Profesional Técnico Titulado y/o Titulo o Bachiller profesional en ingeniería en redes y comunicaciones y/o telecomunicaciones y/o sistemas y/o informática.
No se acepta electronica, debio a que no se encuentra directamente vinculado con las actividades a realizar por el Operador de Servicio."

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

"9.2. Requisitos del Personal propuesto:
(¿)
¿ Un (01) Operador de Servicio
(¿)
Técnico profesional Titulado y/o Titulo o Bachiller profesional en ingeniería en redes y comunicaciones y/o telecomunicaciones y/o sistemas y/o informática."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 25

Consulta/Observación:

Dice:
sobre un total de 100 SERVIDORES (Físicos y Virtuales), integrando las fuentes necesarias (antivirus, antispam, correo, firewalls y/o componentes de red) para mejorar la tasa de detección y respuesta.

Consultas

1. Se entiende que el servicio se realizará sobre 100 servidores, por favor indicar la cantidad de equipos físicos y virtuales.
2. Para aumentar las capacidades de detección se sugiere que la telemetría también debe ser obtenida de todos los endpoints; es decir servidores, equipos de cómputo de usuario final (laptop, workstation); o dicho de otro modo, cualquier equipo que cuente con un Sistema Operativo de tipo Windows, Linux o Mac. Por favor indicar si los equipos informaticos de los usuarios finales (endpoints) deben monitorearse. Indicar la cantidad de estos equipos.
3. Indicar el fabricante y versiones de antivirus, antispam, correo, firewalls y/o componentes de red
4. Indicar la cantidad de EPS que debe soportar la plataforma
5. Indicar si los endpoints tienen salida directa a internet para capturar la telemetría. De no ser así compartir una arquitectura de colección y si el Congreso de la Republica proveerá la infraestructura para el/los colectores (indicar si es Nube Privada, fabricante y versión de Hypervisor)

Acápíte de las bases : Sección: Especifico Numeral: 7 Literal: General Página: 2

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

Análisis respecto de la consulta u observación:

- "En atención a la consulta, se precisa que:
1. Las capacidades de prevención, detección y respuesta activa se ejecutarán sobre 100 host (físicos o virtuales).
 2. Las capacidades de correlación, detección y respuesta deberán cubrir la totalidad de endpoints a través de la integración con el directorio activo.
 3. La integración de las fuentes antivirus, firewalls, correo y demás deberán realizarse de acuerdo a estándares de la industria comprendiendo todo lo relevante para la gestión.
 4. El procesamiento de los registros no deberá tener límites para el desarrollo del servicio.
 5. No es posible brindar el detalle de la información solicitada por seguridad, sin embargo esta información será entregada al contratista previa firma del acuerdo de confidencialidad.
- Para todos lo numerales de la consulta, no es posible brindar todo el detalle de la información solicitada por seguridad, sin embargo esta información será entregada al contratista previa firma del acuerdo de confidencialidad."

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

null

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 26

Consulta/Observación:

Dice:
El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 3 para los productos de detección y respuesta ofertados.

Consulta:
La auditoría SOC 3 es una extensión del SOC 2. Por otro lado, en la página 7 se menciona: ¿La plataforma deberá evaluar el cumplimiento normativo mínimamente de NIST CSF, ISO, STIG y SOC-2¿. Considerando el alcance del servicio por favor confirmar que el cumplimiento normativo debe ser como mínimo SOC 2.

Acápite de las bases : Sección: Especifico Numeral: 7 Literal: 7.1 Página: 2

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

Análisis respecto de la consulta u observación:
"Se acepta la consulta presentada y para garantizar mayor pluralidad y concurrencia, se modificará el requerimiento de la siguiente manera:

""El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC-2 y SOC-3 para los productos de detección y respuesta ofertados.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
"7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA
(...)
El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 2 y SOC 3 para los productos de detección y respuesta ofertados"

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 27

Consulta/Observación:

Dice:

¿La plataforma debe proporcionar una capacidad segura, liviana y fácil de implementar para capturar la telemetría de seguridad desde los puntos finales a través de un agente ligero que no supere los ocho (08) MB de tamaño¿, y en el punto 7.3.3 (página 7) dice:

¿La plataforma deberá ser de tipo SaaS con una arquitectura basada en agente ligero el cual no supere los 20 MB de tamaño para su optimo desempeño.¿

Consulta:

El desempeño de un agente o facilidad de implementar (incluso de cualquier software) no tiene relación con el tamaño del instalador o del espacio utilizado luego de ser instalado. Lo importante, y que está alineado con el alcance del servicio, es la telemetría que el agente es capaz de obtener del endpoint. Sugerimos quitar esta limitación.

Sí, en su defecto, se desea limitar el tamaño, indicar a que se refiere el tamaño en Megabytes (MB) indicado: al instalador, al espacio luego de instalado o el aspecto que hayan considerado.

Acápíte de las bases : Sección: Especifico Numeral: 7 Literal: 7.1 Página: 3

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, con la finalidad de garantizar la mayor pluralidad de postores se retira el requerimiento el tamaño máximo del agente.

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

"7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA (...)

La plataforma debe proporcionar una capacidad segura, liviana y fácil de implementar para capturar la telemetría de seguridad desde los puntos finales a través de un agente ligero, a fin de que el equipo de profesionales que trabaja en el SOC Data Center clasifique, correlacione y registre datos de forma eficiente y efectiva."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código : 20600050738

Fecha de envío : 21/02/2025

Nombre o Razón social : 3G IT CONSULTING S.A.C.

Hora de envío : 23:54:38

Consulta: Nro. 28

Consulta/Observación:

Dice:

La plataforma debe tener una arquitectura multitenant que le permita crear instancias de gobierno independiente asignadas a usuarios clave dentro de la organización.

Consulta:

Una arquitectura multitenant permite, con una sola instancia, servir a muchos clientes. El texto es confuso porque se solicita que la plataforma tenga una arquitectura multitenant para crear instancias. Se entiende que el Congreso de la Republica es el único cliente y debe tener una instancia de un solo tenant para el servicio. Es posible que se esté confundiendo con la capacidad de dar permisos de visualización en la plataforma a los usuarios de la organización (dependiendo de su rol en la organización), algo que se puede manejar con capacidades de roles y permisos. Por favor quitar o aclarar la capacidad que se requiere en este punto.

Acápate de las bases : Sección: Especifico

Numeral: 7

Literal: 7.1

Página: 3

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, el requerimiento de multitenant refiere a que los servidores serán gobernados sobre diferentes criterios y diferentes profesionales responsables y lo que se quiere es que se tenga la posibilidad de crear una cuenta maestra que audite las instancias de gobierno anidadadas.

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

null

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código : 20600050738

Nombre o Razón social : 3G IT CONSULTING S.A.C.

Fecha de envío : 21/02/2025

Hora de envío : 23:54:38

Consulta: Nro. 29

Consulta/Observación:

Dice:

La plataforma debe contar con la capacidad de detectar archivos maliciosos a través de su propio motor de detección de malware desarrollado como parte de la solución integrada, escaneando archivos escritos en el disco o ejecutados en busca de atributos maliciosos para proporcionar redundancia sobre la solución antimalware con la que ya cuenta la institución.

Consulta:

Las reglas YARA identifican ataques direccionados a través de la detección de patrones malware. Confirmar que lo enunciado debe realizarse o potenciarse con la aplicación de las reglas YARA.

Acápite de las bases : Sección: Especifico **Numeral:** 7 **Literal:** 7.2 **Página:** 4

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

Análisis respecto de la consulta u observación:

Se aclara que no se está solicitando el uso específico de reglas YARA para la detección de archivos maliciosos, sin embargo se aceptará que el motor de detección de malware integre y/o use reglas YARA como mecanismo adicional de detección.

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

null

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código : 20600050738

Nombre o Razón social : 3G IT CONSULTING S.A.C.

Fecha de envío : 21/02/2025

Hora de envío : 23:54:38

Consulta: Nro. 30

Consulta/Observación:

Dice:

La reducción de la superficie de ataque se hará efectiva a través de la ejecución de ejercicios de hacking ético, pentesting y la priorización de vulnerabilidades, configuraciones débiles y anomalías.

Consultas:

1. Por favor indicar cuantos ejercicios de cada tipo deben realizarse por año.
2. Por favor indicar si los ejercicios de hacking ético deben ser realizados de forma continua o en una cierta cantidad de veces por año.

Acápite de las bases : Sección: Específico **Numeral:** 7.3 **Literal:** 7.3.1 **Página:** 5

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

Análisis respecto de la consulta u observación:

"En atención a su consulta sobre ejercicios de reducción de superficie de ataque, se informa:

Cantidad de Ejercicios solicitados anualmente:

Hacking Ético: 2 ejercicios completos por año
Pentesting: 2 ejercicios completos por año
Priorización de Vulnerabilidades: 4 evaluaciones (una cada trimestre)

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

"7.3.1. GESTION COLABORATIVA Y PRESENTACION DE RESULTADOS DE POSTURA DE SEGURIDAD EN EL TIEMPO

(...)

La reducción de la superficie de ataque se hará efectiva a través de la ejecución de ejercicios de hacking ético, pentesting y la priorización de vulnerabilidades, configuraciones débiles y anomalías, la cantidad de ejercicios solicitados anualmente son: Hacking Ético: 2 ejercicios completos por año, Pentesting: 2 ejercicios completos por año y priorización de

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 31

Consulta/Observación:

Dice:
La plataforma deberá permitir documentar la actividad sobre cada vulnerabilidad y/o riesgo cibernético identificado, permitiendo ingresar y actualizar información referida a la descripción, solución, tipo de vulnerabilidad, nivel de severidad, información adicional, relación con el activo específico afectado, relación con otras vulnerabilidades, actividades realizadas, usuarios responsables de cada actividad, captura de pantalla y/o evidencia de remediación aplicada y cierre o mitigación formal de riesgo.

Consulta:
Para una mejor valoración de la amenaza y/o vulnerabilidad; y que contribuye a la identificación de falsos positivos, la plataforma, además del nivel de severidad, debería determinar la gravedad de la amenaza o vulnerabilidad. Por favor indicar si la plataforma debe ofrecer, además del nivel de la severidad, una puntuación que permita identificar la gravedad de la amenaza y/o vulnerabilidad.

Acápite de las bases : Sección: Especifico Numeral: 7.3 Literal: 7.3.1 Página: 6

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

Análisis respecto de la consulta u observación:
Se precisa que no se ha solicitado la generación de puntuación de gravedad de amenazas, sin embargo se aceptarán soluciones que así lo hagan.

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

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 32

Consulta/Observación:

Dice:
La plataforma deberá evaluar el cumplimiento normativo mínimamente de NIST CSF, ISO, STIG y SOC-2 a través de la validación que realice el agente instalado sobre los servidores y/o estaciones seleccionadas.

Consulta:
El cumplimiento normativo mínimo indicado es muy amplio, para una mayor pluralidad de postores indicar que se puede cumplir: ¿NIST CSF, ISO, STIG o SOC-2¿

Acápite de las bases : Sección: Especifico Numeral: 7.3 Literal: 7.3.3 Página: 7

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

Análisis respecto de la consulta u observación:

"En atención a la consulta se precisa que, con la finalidad de garantizar la mayor pluralidad de postores se modifica el texto de la siguiente manera:

""La plataforma deberá evaluar el cumplimiento normativo mínimamente de NIST CSF, ISO, STIG y/o SOC-2 a través de la validación que realice el agente instalado sobre los servidores y/o estaciones seleccionadas."

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

"7.3.3. MONITOREO Y REDUCCION CONTINUA DEL NIVEL DE EXPOSICION AL RIESGO INTERNO (...)

La plataforma deberá evaluar el cumplimiento normativo mínimamente de NIST CSF, ISO, STIG y/o SOC-2 a través de la validación que realice el agente instalado sobre los servidores y/o estaciones seleccionadas."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 33

Consulta/Observación:

Dice:
El servicio ofertado deberá incluir el acceso, administración y reportes a una plataforma de Cyber Threat Intelligence capaz de poder implementar capacidades de predictibilidad de ataques cibernéticos dirigidos y no dirigidos a través del monitoreo continuo de dark web y diversos canales utilizados por hackers y ciberdelincuentes.

Consulta:
Para ampliar las capacidades de Cyber Threat Intelligence indicar si la plataforma incluida en el servicio ofertado debe tener la capacidad de añadir nuevas fuentes de inteligencia con conceptos como ¿Bring Your Own Threat Intelligence¿

Acápíte de las bases : Sección: Específico Numeral: 7 Literal: 7.4 Página: 9

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

Análisis respecto de la consulta u observación:

En atención a la consulta se precisa que, la plataforma Cyber Threat Intelligence deberá ser capaz de poder implementar capacidades de predictibilidad de ataques cibernéticos dirigidos y no dirigidos a través del monitoreo continuo de dark web y diversos canales utilizados por hackers y ciberdelincuentes. Se aclara que, no se solicita que el servicio ofertado debe tener la capacidad de añadir nuevas fuentes de inteligencia con conceptos como Bring Your Own Threat Intelligence; sin embargo, se aceptarán soluciones que la contemplen como una característica adicional a las solicitadas. La característica adicional no generara un costo adicional a la entidad

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

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código : 20600050738

Nombre o Razón social : 3G IT CONSULTING S.A.C.

Fecha de envío : 21/02/2025

Hora de envío : 23:54:38

Consulta: Nro. 34

Consulta/Observación:

Dice:

La plataforma deberá documentar más de 10 años de datos históricos sobre amenazas.

Consulta:

No se entiende este requerimiento. Por favor indicar a que se refiere la capacidad mencionada.

Acápite de las bases : **Sección:** Especifico **Numeral:** 7 **Literal:** 7.4 **Página:** 10

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

Análisis respecto de la consulta u observación:

Se acepta la consulta presentada y para garantizar mayor pluralidad y concurrencia se retirará ese punto.

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

"Se elimina parrafo:

7.4. CAPACIDADES DE PREDICTIBILIDAD DE ATAQUES

(...)

La plataforma deberá documentar más de 10 años de datos históricos sobre amenazas. (se elimina parrafo)."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 35

Consulta/Observación:

Dice:
El Postor dentro de su propuesta, deberá acreditar fehacientemente el cumplimiento de las especificaciones técnicas solicitadas numeral 7. ESPECIFICACIONES TÉCNICAS MÍNIMAS (7.1, 7.2, 7.3, 7.4), catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento.

Consulta:
Dado que el fabricante de la plataforma es extranjero. ¿Se puede entregar catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla en idioma inglés?

Acápite de las bases : Sección: Especifico Numeral: 7 Literal: 7.5 Página: 10

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

Análisis respecto de la consulta u observación:

"De conformidad con el artículo 59 del Reglamento de la Ley de Contrataciones del Estado, se establece lo siguiente:
""Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, según corresponda, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que puede ser presentada en el idioma original"", lo cual esta precisado en el numeral 1.7. del Capítulo I - Sección General de las bases del presente procedimiento de selección.

No obstante, la documentación referida se encuentra establecida como documento de presentación obligatoria para la admisión de la oferta (numeral 2.2.1.1 de la Sección Especifica de las bases), es decir, dichos documentos son esenciales en la oferta, de carácter obligatoria para acreditar componentes del servicio a prestar, por lo que no tendría la naturaleza de un documento complementario.

En ese sentido, en el caso que se presenten catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento, en idioma ingles, o cualquier otro idioma distinto al español, deberán estar acompañados de su respectiva traducción por traductor público juramentado o traductor colegiado certificado, según corresponda."

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

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 36

Consulta/Observación:

Dice:

El servicio de seguridad gestionada deberá destinar un recurso (Especialista) local en las instalaciones del Congreso que se comunicará por correo electrónico y otros medios para coordinar las siguientes actividades:

- Consolidar y presentar los resultados obtenidos de la plataforma tipo SOAR (Cyber SOC) para brindar capacidades de detección y respuesta ante ataques cibernéticos, mostrando evidencia del correlacionamiento de eventos de múltiples fuentes, alertas sobre servicios o aplicaciones sospechosas, conexiones con redes ciberterroristas e infracciones de seguridad revisadas en el tiempo con su respectiva telemetría.
- Consolidar y presentar los resultados obtenidos de la plataforma y/o tecnología utilizada para las capacidades de prevención con respecto al hacking, pentesting y reducción de superficie de ataque interna y externa, adjuntando información sobre la gestión de riesgos basado en vulnerabilidades, configuraciones débiles y anomalías.
- Absolución de consultas técnicas y soporte a incidentes reportados en la institución.

Consultas:

1. El requerimiento indica que el especialista debe estar en las instalaciones del Congreso de la República y también indica que la comunicación se realizará por correo electrónica. Siendo así, y en consideración de que la plataforma se entrega SaaS y de las actividades mencionadas, la ubicación del especialista no es importante para la ejecución del servicio y dichas actividades. Por esta razón, se solicita que el recurso asignado al servicio pueda ejecutar las actividades de forma remota.
2. Si el especialista debe estar remoto por favor indicar que facilidades se entregarán al especialista: equipo de cómputo, acceso a la red interna, escritorio, otros.
3. Por favor indicar si el especialista solicitado se refiere al Operador de Servicio incluido en el Personal Clave mencionado en el punto 9.2 de las páginas 16 y 17.

Acápite de las bases : Sección: Especifico **Numeral:** 7 **Literal:** 7.6 **Página:** 11

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

Análisis respecto de la consulta u observación:

"En atención a la consulta se precisa que, el especialista u operador del servicio podrá desarrollar su trabajo de forma virtual o presencial según demande la actividad relacionada. Para el desarrollo de sus actividades del especialista u operador deberá contar con un equipo de cómputo el cual deberá ser proporcionado por el postor que lo presente como integrante del personal clave propuesto, mientras que por parte de la Entidad, se le proporcionarán todas las facilidades para que pueda desarrollar su servicio. Se precisa que el especialista solicitado se refiere al Operador de Servicio incluido en el Personal Clave mencionado en el punto 9.2 de las páginas 16 y 17, en ese sentido, se reemplazará la denominación como operador de servicio.

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

"7.6. CARACTERISITICAS DE LA SEGURIDAD GESTIONADA

(...)

El servicio de seguridad gestionada deberá destinar un recurso (Operador de servicio) local en las instalaciones del Congreso o remota, que se comunicará por correo electrónico y otros medios para coordinar las siguientes actividades:

(...)

- Para el desarrollo de sus actividades del especialista u operador deberá contar con un equipo de cómputo el cual deberá ser proporcionado por el postor que lo presente como integrante del personal clave propuesto."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 37

Consulta/Observación:

Dice:
Elaboración e implementación de directivas y estrategias de concienciación en ciberseguridad a través de webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la institución.

Consultas:
1. Las actividades mencionadas pueden ser ejecutadas remotamente por especialistas que realizarán el monitoreo 24x7. Por favor indicar que estas actividades pueden ser ejecutadas remotamente.
2. Se solicita que se cuantifiquen los webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la organización.

Acápite de las bases : Sección: Específico Numeral: 7 Literal: 7.6 Página: 11

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

Análisis respecto de la consulta u observación:

"En atención a la consulta se precisa que:
1.Las actividades tales como la simulación de phishing y formación pueden ser ejecutadas remotamente por especialistas propuestos como personal clave que realizarán el monitoreo 24x7.
2.La cantidad de los webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la organización deberán ser mínimo tres (03) veces al año.

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

"7.6. CAPACIDADES DE SEGURIDAD GESTIONADA
(...)
Elaboración e implementación de directivas y estrategias de concienciación en ciberseguridad a través de webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la institución, la cantidad de los webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la organización deberán ser mínimo tres (03) veces al año."

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 38

Consulta/Observación:

Dice:
Se consideran servicios similares a los siguientes: servicios de soluciones de seguridad y ciberseguridad, soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática.

Consulta:
Para mayor pluralidad de postores incluir como servicios similares:

- Servicio de hackeo ético
- Servicio de ethical hacking
- Servicio de ejecución de ethical hacking
- Servicio para el análisis de vulnerabilidades
- Servicio de análisis de vulnerabilidades
- Servicio de pruebas de penetración
- Servicio para el análisis de ciberseguridad

Acápites de las bases : Sección: Especifico Numeral: C Literal: C Página: 23

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

Análisis respecto de la consulta u observación:
En atención a la consulta y para permitir una mayor cantidad de postores se precisa que, se incluirá como servicios similares: Servicio de hackeo ético y/o Servicio de ethical hacking y/o Servicio de ejecución de ethical hacking y/o Servicio para el análisis de vulnerabilidades y/o Servicio de análisis de vulnerabilidades y/o Servicio de pruebas de penetración y/o Servicio para el análisis de ciberseguridad.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
"REQUISITOS DE CALIFICACIÓN
C. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
(...)

Se consideran servicios similares a los siguientes: servicios de soluciones y/o implementación de soluciones de seguridad y ciberseguridad (antivirus y/o antispam y/o XDR y/o EDR), soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática y/o soluciones de respaldo y restauración de información para entornos físicos o virtualizados y/o servicio de hackeo ético y/o servicio de ethical hacking y/o servicio de ejecución de ethical hacking y/o servicio para el análisis de vulnerabilidades y/o servicio de análisis de vulnerabilidades y/o servicio de pruebas de penetración y/o servicio para el análisis de ciberseguridad.

(Se incluyen ajustes en mérito a la absolución de las consultas 1 y 3)

Entidad convocante : CONGRESO DE LA REPUBLICA

Nomenclatura : CP-SM-2-2025-CR-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA

Ruc/código :	20600050738	Fecha de envío :	21/02/2025
Nombre o Razón social :	3G IT CONSULTING S.A.C.	Hora de envío :	23:54:38

Consulta: Nro. 39

Consulta/Observación:

Dice:
La plataforma deberá cubrir la seguridad, correlacionamiento de eventos de seguridad, detección y respuesta ante incidentes tipo SOAR para la totalidad de los servidores de misión crítica y determinados activos estratégicos

Consulta:
1. Un servicio CyberSOC debe incluir remediación para mejorar la postura de seguridad. Por favor indicar si la remediación debe ser incluida en el servicio ofertado.
2. Un servicio CyberSOC debe incluir respuesta ante incidentes. Por favor indicar si la asistencia de respuesta ante incidentes debe ser incluida en el servicio ofertado.

Acápite de las bases : Sección: Específico Numeral: 7 Literal: General Página: 2

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

Análisis respecto de la consulta u observación:

"En atención a la consulta se precisa que:
1. Se deberá incluir para el servicio de CyberSOC la remediación y mitigación de amenazas que deriven de las vulnerabilidades, configuraciones débiles, anomalías y uso de software no permitido para mejorar la postura de seguridad en la institución, asumiendo descarga, distribución y aplicación de parches sobre los hosts protegidos.
2. Se deberá incluir para el servicio de CyberSOC la contención efectiva de cualquier tipo de ciberataque mediante el agente y la asistencia de respuesta ante incidentes a través de una plataforma de gestión de incidencias integrada al SOAR propuesto.
Respecto de las dos (2) consultas, deben estar incluidas en el precio del servicio ofertado."

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

"7. CARACTERISTICAS DEL SERVICIO A REALIZAR
(...)
La plataforma deberá cubrir la seguridad, correlacionamiento de eventos de seguridad, detección, respuesta ante incidentes y remediación tipo SOAR para la totalidad de los servidores de misión crítica y determinados activos estratégicos, (...)."