

PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código : 20475805101

Fecha de envío : 06/03/2024

Nombre o Razón social : INNOVARE E-BUSINESS S.A.C.

Hora de envío : 23:49:48

Consulta: Nro. 1

Consulta/Observación:

Se indica que "Se aceptará como alternativa la contratación de suscripciones para la actual plataforma SIEM del BCRP (Trellix SIEM)". Nuestra solución es un NEXT-GEN SIEM que funciona 100% en la nube y no requiere de la instalación de equipos físicos en la red del cliente. Sino, sólo agentes recolectores que envían los datos para su análisis en la nube. Confirmar que aceptarán este tipo de plataformas actuales y modernas que han llegado para reemplazar a los SIEM tradicionales como Trellix.

Es importante indicar al BCRP que Trellix SIEM no está en el cuadrante mágico de SIEM y el producto que proponemos si se encuentra en ella por lo que es una solución de nueva generación de SIEM.

Acápites de las bases : Sección: General

Numeral: 3.1.2.2

Literal: a

Página: 22

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

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.

Según el numeral 3.1.4.4: ""La solución deberá ser implementada en modo On-Premise"". Sin embargo se precisa que la solución SIEM permitirá appliances virtuales para recolectar eventos de diversas fuentes del BCRP y plataformas en nube para realizar la correlación y analítica EN TIEMPO REAL.

Por lo que el numeral 3.1.4.4 quedara de la siguiente manera: ""La solución deberá ser implementada en modo On-Premise y/o híbrida""."

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

Se modificará el numeral 3.1.4.4 de la sección específica de las bases

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 2

Consulta/Observación:

Sírvase confirmar que aceptarán soluciones de nueva generación de SIEM que trabajan 100% en la nube y solo se requieren recolectores en la red del cliente. En este caso ya no se requeriría que el BCRP proporcione ninguna infraestructura.

Acápíte de las bases : Sección: General Numeral: 3.1.3 Literal: 3.1.3.1 Página: 23

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

Análisis respecto de la consulta u observación:

"No se confirma.
Según el numeral 3.1.4.4: ""La solución deberá ser implementada en modo On-Premise"". Sin embargo se precisa que la solución SIEM permitirá appliances virtuales para recolectar eventos de diversas fuentes del BCRP y plataformas en nube para realizar la correlación y analítica EN TIEMPO REAL.
Por lo que el numeral 3.1.4.4 quedara de la siguiente manera: ""La solución deberá ser implementada en modo On-Premise y/o híbrida"".
NOTA: No se aceptarán soluciones de nueva generación de SIEM que trabajan 100% en la nube."

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

"se incluirá la nota en el numeral 3.1.4.4 de la sección específica de las bases integradas.
"

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 3

Consulta/Observación:

Al ser nuestra plataforma 100% en la nube sírvase indicar que la se aceptarán soluciones de nueva generación de SIEM que incluyen de análisis de IA, UEBA, XDR, SOAR e ANALISIS de IDENTIDAD, sin dependen de hardware on-premise que muchas veces es limitado para las tareas de análisis del lago de datos que generan los equipos.

Acápite de las bases : **Sección:** General **Numeral:** 3.1.4 **Literal:** 3.1.4.4 **Página:** 24
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma. El numeral 3.1.4.4 quedara de la siguiente manera: ""La solución deberá ser implementada en modo On-Premise y/o hibrida"".
NOTA: No se aceptarán soluciones de nueva generación de SIEM que trabajan 100% en la nube."

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

Se modificará el numeral 3.1.4.4 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 4

Consulta/Observación:

Al proponer una solución 100% nube la alta disponibilidad se entrega por diseño, no por requerimiento. Sírvese confirmar que el BCRP con el fin de mejorar sus capacidades de analítica de datos y contar con una mejor solución que la actual permitirá este tipo de soluciones.

Acápite de las bases : Sección: General Numeral: 3.1.4 Literal: 3.1.4.5 Página: 24

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

Análisis respecto de la consulta u observación:

"No se confirma.
Las necesidades del Banco hacen que la solución deberá ser implementada en un esquema de alta disponibilidad por requerimiento.
NOTA: No se aceptarán soluciones de nueva generación de SIEM que trabajan 100% en la nube."

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

null

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 5

Consulta/Observación:

La data que generan nuestros recolectores son comprimidas y cifradas por lo que no se requiere realizar controles de uso de ancho de banda ya que se consume pocos megas. Sírvase confirmar que permitirán soluciones que compriman la información a enviar y/o permitir configurar controles de uso de ancho de banda.

Acápíte de las bases : Sección: General Numeral: 3.1.4 Literal: 3.1.4.18 Página: 25

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

Análisis respecto de la consulta u observación:

Los controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato será opcional, por lo que si el proveedor desea incluir soluciones que compriman la información a enviar y/o permitir configurar controles de uso de ancho de banda deberán de estar incluidos en el precio ofertado, precisando que no es obligatorio.

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

Se eliminará el numeral 3.1.4.18 de la sección específica de las bases integradas.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 6

Consulta/Observación:

Sírvase colocar el término ".. así como priorizar las transacciones críticas para su envío inmediato" como opcional ya que actualmente no hay transacciones críticas o no críticas puesto que se debe analizar todas las transacciones como se generen con el fin de anticipar o detectar un incidentes antes que llegue a materializarse. Este tipo de característica es obsoleta y hoy con el auge de la IA y los modelos de LLM los atacantes cada vez usan nuevas técnicas para evadir controles obsoletos como los usados por Trellix en el pasado.

Acápite de las bases : **Sección:** General **Numeral:** 3.1.4 **Literal:** 3.1.4.18 **Página:** 25
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
Los controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato será opcional, por lo que si el proveedor desea incluir soluciones que compriman la información a enviar y/o permitir configurar controles de uso de ancho de banda deberán de estar incluidos en el precio ofertado, precisando que no es obligatorio."

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

Se eliminará el numeral 3.1.4.18 de la sección específica de las bases integradas.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 7

Consulta/Observación:

Sírvase permitir que se pueda truncar o enmascarar la información sensible puesto que las soluciones modernas NEXT-GEN SIEM usan estas nuevas técnicas para no perder metadata necesaria para hacer correlación de eventos.

Acápíte de las bases : Sección: General Numeral: 3.1.4 Literal: 3.1.4.27 Página: 26

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

Análisis respecto de la consulta u observación:

"Se confirma.
En el numeral 3.1.4.27 se indica que la solución SIEM deberá permitir la capacidad de truncar la información sensible que es capturada en los eventos luego del proceso de parsing y normalización."

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 8

Consulta/Observación:

Sírvase colocar esta funcionalidad como opcional ya que las soluciones modernas que usan IA realizan ya esta tarea en forma autónoma sin depender de afinamientos manuales. Esto con el fin de permitir la participación de marcas más actuales que Trellix.

Acápite de las bases : **Sección:** General **Numeral:** 3.1.4 **Literal:** 3.1.4.34 **Página:** 26

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

Análisis respecto de la consulta u observación:

"No se confirma.
Las necesidades del Banco son que la solución SIEM permita probar reglas de correlación sobre eventos históricos con una ventana de tiempo configurable, que permitan afinar puntualmente las reglas de correlación previa a su despliegue en ambientes productivos,. Sean estas con tecnología legacy y/o con nuevas técnicas tales como IA y/o modelos LLM, u otra."

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

null

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20475805101	Fecha de envío :	06/03/2024
Nombre o Razón social :	INNOVARE E-BUSINESS S.A.C.	Hora de envío :	23:49:48

Consulta: Nro. 9

Consulta/Observación:

Este requerimiento de importar gráficas no es usual en soluciones de SIEM, menos en soluciones de NETX-GEN con Inteligencia Artificial que ya incluyen gráficas y panales que realizan la correlación de los eventos, análisis de causa raíz, uso de ID de Mittre y cientos de correlacionadores automatizados que ayudan a visualizar y hacer seguimiento a cualquier evento. Por ello sírvase colocar como opcional el término "deberá permitir la importación de gráficos" para permitir la participación de productos modernos que incluyen IA.

Acápite de las bases : Sección: General Numeral: 3.1.4 Literal: 3.1.4.48 Página: 27

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

Análisis respecto de la consulta u observación:

"Se corregirá el numeral 3.1.4.48 de la sección específica de las bases:

DICE: ""¿importación de gráficos¿""

DEBE DECIR: ""exportación de gráficos""

"

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

Se corregirá el numeral 3.1.4.48 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 10

Consulta/Observación:

DICE: Capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4500 EPS o superiores. Este requerimiento debe ser soportado por todos los componentes del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas).

CONSULTA: Se pide a la entidad confirmar que la cantidad de EPS para soportar los picos indicados hace referencia a la suma de las capacidades de los dos receivers que actualmente cuenta el BCRP según indicado en las bases ¿ Dos (02) appliances virtuales Event Receiver (ERC) del modelo McAfee ERC-VM-8 Cores + VM-4 Cores Add-On y . según documentación del fabricante.

Acápite de las bases : Sección: Especifico Numeral: 3.1.2.4 Literal: . Página: 22

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

Análisis respecto de la consulta u observación:

Se confirma que la cantidad de EPS para soportar los picos indicados hace referencia a la suma de las capacidades de los dos receivers que actualmente cuenta el BCRP.

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

null

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 11

Consulta/Observación:

DICE: Soportar los siguientes protocolos de recolección de datos: Syslog UDP, Syslog TCP, Secure-Syslog (y/o Syslog NG), RSYSLOG TCP RSYSLOG UDP, conexión por string JDBC (BD), SNMP, Cisco RDEP, SDEE, CheckPoint OPSEC, Checkpoint LEA, XML, archivos de texto y API.

CONSULTA: Debido a que la solución de SIEM de Trellix , antes McAfee se va actualizando y deja de soportar ciertas características que antes si habían sido soportadas tales como Secure-Syslog (y/o Syslog NG),conexión por string JDBC (BD),Cisco RDEPy SDEE ; se pide a la entidad por favor confirmar que el punto podrá quedar de la siguiente manera: " Soportar los siguientes protocolos de recolección de datos: Syslog UDP, Syslog TCP, RSYSLOG TCP, RSYSLOG UDP, SNMP, CheckPoint OPSEC, Checkpoint LEA, XML, archivos de texto y API"

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.1 Literal: .

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

Página: 23

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Las necesidades del Banco requieren que se soporte los protocolos de recolección de datos siguientes: Syslog UDP, Syslog TCP, RSYSLOG TCP, RSYSLOG UDP, archivos de texto y API. "

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

Los protocolos Secure-Syslog (y/o Syslog NG), SNMP, CheckPoint OPSEC, Checkpoint LEA, XML, conexión por string JDBC (BD), Cisco RDEP, SDEE, al ser opcionales, serán retirados del numeral 3.1.4.1 de la sección específica de las bases integradas.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 12

Consulta/Observación:

DICE: La solución debe ser implementada en un esquema de Alta Disponibilidad Activo-Activo para los core del appliance virtual.

CONSULTA: Se le pide a la entidad por favor confirmar que este punto hace referencia a una configuración en Alta Disponibilidad Activo-Activo para el componente de los receivers, ya que es la configuración soportada por Trellix

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.5 Literal: . Página: 24

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

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Se precisa que la solución SIEM para el esquema de alta disponibilidad activo-activo será únicamente para los receivers siendo esta de la misma marca u otra."

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Se incluirá la precisión el numeral 3.1.4.5 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 13

Consulta/Observación:

DICE: La solución debe ser implementada en un esquema de Alta Disponibilidad Activo-Activo para los core del appliance virtual.

CONSULTA: Se pide a entidad confirmar que esta configuración en alta disponibilidad se encuentra actualmente configurada y funcionando correctamente considerando que cuentan con dos ERC - Event Receiver.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.5 Literal: . Página: 24

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

Análisis respecto de la consulta u observación:

"Se confirma.

Al ser requerimiento del Banco la CONTRATACIÓN DEL SERVICIO DE SUSCRIPCIONES DE UN SIEM, es necesario que el postor que obtenga la buena pro, valide a conformidad del Banco durante la etapa de implementación la configuración de alta disponibilidad de la solución siguiendo los estándares y buenas prácticas de la marca. Este requerimiento es para todos los postores que opten por la opción de renovación según lo indicado en el numeral 3.1.2.2."

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

Se incluirá la precisión el numeral 3.1.4.5 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 14

Consulta/Observación:

DICE: Deberá ser integrable ¿fuera de la caja¿ (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes, mediante el uso de componentes denominados conectores/colectores. Como mínimo la solución deberá tener soporte nativo para los eventos provenientes de:

- .Cisco Email Security Appliance
- .McAfee/SkyHigh Security Web Gateway
- .Cisco Nexus
- .Palo Alto Next Generation Firewall
- .Radware Alteon/AppWall
- .RSA Authentication Manager
- .Citrix ADC
- .Kaspersky Endpoint Security
- .Microsoft Windows

CONSULTA: Se pide a la entidad confirmar que la solución deberá tener soporte nativo para las siguientes soluciones, siempre y cuando tengan las versiones detalladas a continuación:

- .Cisco Email Security Appliance 6x,7x
- .Cisco Nexus 4.x, 5.x
- .RSA Authentication Manager 7.x
- .Microsoft Windows XP, Windows 7,Windows 8,Windows 10

De no contar con estas versiones de sistemas operativos se pide a la entidad confirmar que aceptará la elaboración de parsers por parte del postor.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.8 **Literal:** . **Página:** 24
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

No se confirma.
Lo que se solicita es información confidencial y solo será proporcionada al contratista posterior a la firma de los acuerdos de confidencialidad.

En el numeral 3.1.4,8 de las bases se detalla la lista de marcas y plataformas mínimas admitidas para soporte de la solución SIEM.

Se indica en el numeral 3.1.10.7 que el objetivo de la implementación es tener en su totalidad los DataSources integrados. Los DataSources no homologados que requieran desarrollo de conectores/colectores para su integración serán en la etapa de soporte en coordinación con el Banco sin incurrir en costo alguno.

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

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 15

Consulta/Observación:

DICE: Deberá ser integrable ¿fuera de la caja¿ (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes, mediante el uso de componentes denominados conectores/colectores. Como mínimo la solución deberá tener soporte nativo para los eventos provenientes de:

- .Cisco Email Security Appliance
- .McAfee/SkyHigh Security Web Gateway
- .Cisco Nexus
- .Palo Alto Next Generation Firewall
- .Radware Alteon/AppWall
- .RSA Authentication Manager
- .Citrix ADC
- .Kaspersky Endpoint Security
- .Microsoft Windows

CONSULTA: Se pide a la entidad que por Citrix ADC, hace referencia a Citrix Netscaler

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.8 Literal: . Página: 24

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

Análisis respecto de la consulta u observación:

"Se confirma.
Citrix ADC hace referencia a Citrix Netscaler"

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 16

Consulta/Observación:

DICE: Deberá ser integrable ¿fuera de la caja¿ (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes, mediante el uso de componentes denominados conectores/colectores. Como mínimo la solución deberá tener soporte nativo para los eventos provenientes de:

- .Cisco Email Security Appliance
- .McAfee/SkyHigh Security Web Gateway
- .Cisco Nexus
- .Palo Alto Next Generation Firewall
- .Radware Alteon/AppWall
- .RSA Authentication Manager
- .Citrix ADC
- .Kaspersky Endpoint Security
- .Microsoft Windows

CONSULTA: Se pide a la entidad que por Kaspersky Endpoint Security hace referencia al Administration Kit - SQL Pull (Antivirus)

Acápites de las bases : **Sección:** Especifico **Numeral:** 3.1.4.8 **Literal:** . **Página:** 24

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

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que Kaspersky Endpoint Security hace referencia a la herramienta Kaspersky Security Center y no a Administración Kit - SQL Pull (Antivirus)."

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

null

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 17

Consulta/Observación:

DICE: Permitir configurar controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato.

CONSULTA: Debido a que la solución de SIEM de Trellix , antes McAfee se va actualizando y deja de soportar ciertas características que antes si habían sido soportadas se pide a la entidad confirmar que se podrá tomar este punto como opcional ya que actualmente no se encuentra soportado por el fabricante.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.18 Literal: . Página: 25

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

Análisis respecto de la consulta u observación:

Se precisa que los controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato será opcional, por lo que si el proveedor desea incluir soluciones que compriman la información a enviar y/o permitir configurar controles de uso de ancho de banda deberán de estar incluidos en el precio ofertado, precisando que no es obligatorio.

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

Se eliminará el numeral 3.1.4.18 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 18

Consulta/Observación:

DICE: Capacidad de ingestar identidades a partir de la conexión con Directorios LDAP, usado para realizar el análisis de comportamiento de los usuarios (capacidad UEBA).

CONSULTA: Se pide a la entidad confirmar que este punto es una característica y no un funcionalidad que se debe de implementar como parte del presente servicio solicitado.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.26 **Literal:** . **Página:** 26
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
La capacidad de ingestar identidades a partir de la conexión con Directorios LDAP, usado para realizar el análisis de comportamiento de los usuarios (capacidad UEBA) será una funcionalidad que se implementara como parte de la solución SIEM."

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 19

Consulta/Observación:

DICE: Capacidad de ingestar identidades a partir de la conexión con Directorios LDAP, usado para realizar el análisis de comportamiento de los usuarios (capacidad UEBA).

CONSULTA: Se pide a la entidad confirmar que por comportamiento de los usuarios (capacidad UEBA) hace en realidad referencia a la capacidad de UBA ya que UEBA también incluye entidades.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.26 **Literal:** . **Página:** 26
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que la capacidad de ingestar identidades a partir de la conexión con Directorios LDAP, usado para realizar el análisis de comportamiento de los usuarios y entidades será con capacidad UEBA."

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

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 20

Consulta/Observación:

DICE: Capacidad de ingestar identidades a partir de la conexión con Directorios LDAP, usado para realizar el análisis de comportamiento de los usuarios (capacidad UEBA).

CONSULTA: Se pide a la entidad confirmar que esta funcionalidad sea realizada integrando una solución adicional.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.26 Literal: . Página: 26

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

Análisis respecto de la consulta u observación:

Se confirma.

Se precisa que se requiere la funcionalidad mencionada independientemente de la forma en que lo oferte el postor.

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

Se incluirá la precisión en el numeral 3.1.4.26 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 21

Consulta/Observación:

DICE: Permitir la capacidad de truncar la información sensible que es capturada en los eventos luego del proceso de parsing y normalización.

CONSULTA: Se pide a la entidad confirmar que este punto hace referencia a que los usuarios administradores estarán basados en roles y puedan tener accesos específicos a logs de diferentes fuentes.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.27 Literal: . Página: 26

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

Análisis respecto de la consulta u observación:

"Se confirma
El numeral 3.1.4.27 hace referencia a que los usuarios administradores estarán basados en roles y puedan tener accesos específicos a logs de diferentes fuentes."

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

null

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 22

Consulta/Observación:

DICE: Permitir la correlación basada en reglas (rule-based) y mediante análisis estadístico (rule-less) ambas operando de manera concurrente.

CONSULTA: Debido a que la solución de SIEM de Trellix, antes McAfee se va actualizando y deja de soportar ciertas características que antes si habían sido soportadas se pide a la entidad confirmar que se podrá tomar este punto como opcional ya que actualmente no se encuentra soportado por el fabricante.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.29 Literal: . Página: 26

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

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
La solución SIEM deberá permitir la correlación basada en reglas (rule-based) y opcionalmente permitir la correlación mediante análisis estadístico (rule-less)."

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

Se incluirá la precisión en el numeral 3.1.4.29 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 23

Consulta/Observación:

DICE: Capacidad de abstraer datos a partir de los eventos base provenientes de los dispositivos, tales como realizar el cálculo de algún valor (por ejemplo, sumar o restar, redondear) o derivar algún dato particular (por ejemplo, día del mes, hora del día) que permita realizar un análisis de eventos basándose en el contexto (por ejemplo, generar una alerta si el evento se reporta en un horario no productivo a partir de la hora del evento reportado).

CONSULTA: Debido a que la solución de SIEM de Trellix, antes McAfee se va actualizando y deja de soportar ciertas características que antes si habían sido soportadas se pide a la entidad confirmar que se podrá tomar este punto como opcional ya que actualmente no se encuentra soportado por el fabricante.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.33 **Literal:** . **Página:** 26
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
Opcionalmente La solución SIEM deberá tener la capacidad de abstraer datos a partir de los eventos base provenientes de los dispositivos y/o aplicaciones.
Derivar algún dato particular (día del mes, hora del día) que permita realizar un análisis de eventos basándose en el contexto (por ejemplo, generar una alerta si el evento se reporta en un horario no productivo a partir de la hora del evento reportado)."

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 24

Consulta/Observación:

DICE: Contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:

- Importancia del evento
- Criticidad del activo
- Vulnerabilidades asociadas
- Antecedentes sobre el origen, destino o ambos

CONSULTA: Debido a que la solución de SIEM de Trellix , antes McAfee se va actualizando y deja de soportar ciertas características que antes si habían sido soportadas tales como la evaluación de riesgo utilizando antecedentes sobre el origen, destino o ambos ; se pide a la entidad por favor confirmar que el punto podrá quedar de la siguiente manera "Contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:

- Importancia del evento
- Criticidad del activo
- Vulnerabilidades asociadas"

Acápite de las bases : Sección: Específico Numeral: 3.1.4.35 Literal: . Página: 26

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

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Se precisa que las necesidades del Banco requieren capacidad de contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:
- Importancia del evento
- Criticidad del activo
- Vulnerabilidades asociadas
Opcionalmente, se aceptara que la solución SIEM podrá evaluar el nivel de riesgo considerando el siguiente factor:
- Antecedentes sobre el origen, destino o ambos."

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

Se incluirá la precisión en el numeral 3.1.4.35 de la sección específica de las bases.

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 25

Consulta/Observación:

DICE: La interface web de gestión deberá permitir la importación de gráficos a manera de diagramas que permitan asociar tableros gráficos visuales (dashboards) a una determinada porción o segmento del diagrama para proveer de una visualización lógica y estado situacional de la seguridad en determinada zona de la red o negocio.

CONSULTA: Se pide a la entidad confirmar que este punto hace referencia a la exportación de gráficos y no a la importación.

Acápite de las bases :Sección: EspecificoNumeral: 3.1.4.48Literal: .Página: 27

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

Análisis respecto de la consulta u observación:

"Se confirma.
Se precisa que por error de tipeo al momento de la transcripción se utilizo:
DICE: ""¿importación de gráficos¿"" DEBE DECIR: ""exportación de gráficos""
FE DE ERRATAS, corregir en el numeral 3.1.4.48"

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

Se modificará el numeral 3.1.4.48 de la sección específica de las bases.

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 26

Consulta/Observación:

DICE: Soportar la definición de listas de sesión en adición a las listas de observación. Las listas de sesión tendrán la capacidad de mantener un registro detallado de inicio y cierre que puedan ser utilizadas en la correlación de eventos y dispositivos orientados a sesión como VPN, DHCP y Active Directory.

CONSULTA: Debido a que la solución de SIEM de Trellix, antes McAfee se va actualizando y deja de soportar ciertas características que antes si habían sido soportadas se pide a la entidad confirmar que se podrá tomar este punto como opcional ya que actualmente no se encuentra soportado por el fabricante.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.59 Literal: .

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

Página: 28

Análisis respecto de la consulta u observación:

"Se confirma.
La solución SIEM opcionalmente podrá soportar la definición de listas de sesión en adición a las listas de observación. Las listas de sesión tendrán la capacidad de mantener un registro detallado de inicio y cierre que puedan ser utilizadas en la correlación de eventos y dispositivos orientados a sesión como VPN, DHCP y Active Directory."

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

Se eliminará el numeral 3.1.4.59 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 27

Consulta/Observación:

DICE: Como parte de la implementación del servicio, se debe incluir lo siguiente:

- Configuración del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas) para la integración de los datasources del BCRP.
- En el caso de no contar con integración nativa con algún datasource en particular, deberá desarrollarse dicha integración sin costo adicional.
- Configuración de casos de uso y alertas iniciales, que sean apropiadas según buenas prácticas y experiencia del proveedor.
- Configuración de reportes periódicos.

CONSULTA: Del proveedor, de ir por la modalidad de renovación de su solución actual, se pide a la entidad confirmar que la configuración del SIEM así como los casos de uso no se cambiarán.

De no ser así se pide a la entidad especificar la cantidad de casos de uso adicionales que se deberá de elaborar. y especificar los equipos adicionales que requiere mandar logs al SIEM indicando descripción, cantidad y EPS que generan. Esto para poder validar si su solución SIEM actual soportará la ingesta de estos nuevos logs.

Acápite de las bases : **Sección:** Específico **Numeral:** 10.1.10.7 **Literal:** . **Página:** 32
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Se precisa que la configuración del SIEM, así como los casos de uso deberán ser revisados por el proveedor y, según sus buenas practicas, determinar agregar, mantener o eliminar los casos de uso pertinentes en la solución implementada.
Así mismo, se precisa que la solución debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente, tales como aplicaciones desarrolladas por la institución (in-house), según lo indicado en el numeral 3.1.4.11."

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

Dicha precisión se incluirá en las bases integradas numeral 3.1.10.7 de la sección específica de las bases

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 28

Consulta/Observación:

DICE: Como parte de la implementación del servicio, se debe incluir lo siguiente:

- Configuración del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas) para la integración de los datasources del BCRP.
- En el caso de no contar con integración nativa con algún datasource en particular, deberá desarrollarse dicha integración sin costo adicional.
- Configuración de casos de uso y alertas iniciales, que sean apropiadas según buenas prácticas y experiencia del proveedor.
- Configuración de reportes periódicos.

CONSULTA: Se pide a la entidad indicar la cantidad y periodicidad de los reportes periódicos.

Acápite de las bases : **Sección:** Especifico **Numeral:** 10.1.10.7 **Literal:** . **Página:** 32

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

Análisis respecto de la consulta u observación:

Se precisa que la periodicidad de los reportes generados desde la herramienta SIEM, mencionados en el numeral 3.1.10.7 serán de tipo semanal, quincenal, siendo el mensual reporte ejecutivo; adicionalmente estos reportes serán extraídos de la configuración del SIEM en formatos xls, csv, html u otro para integrarlos a nuestro dashboard de Microsoft Power BI.

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

Dicha precisión se incluirá en las bases integradas numeral 3.1.10.7 de la sección específica de las bases

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 29

Consulta/Observación:

DICE: Se cuenta con 35 fuentes de datos (datasources). Entre los datasources empleados tenemos: NGFW, AntiDDoS, WAF, Antispam, Antimalware, EDR, Web Proxy, Switches de Core, Wireless Controllers, VPN Gateway, Link Balancers, Microsoft Windows, Linux/Solaris y aplicaciones críticas, entre otros. La información detallada sobre los datasources es considerada confidencial por la Entidad.

CONSULTA: Se pide a la entidad confirmar si estas fuentes de datos se encuentran actualmente enviando logs al SIEM o si son nuevas fuentes de datos

Acápite de las bases : **Sección:** Especifico **Numeral:** 10.1.10.1 **Literal:** . **Página:** 32

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

Análisis respecto de la consulta u observación:

Se confirma parcialmente, se precisa que de las actuales fuentes de datos mencionadas en el numeral 3.1.10.1, estas se encuentran enviando logs al SIEM y por renovación de servicios, algunas requieren integrarse al SIEM las cuales serán de conocimiento del proveedor que obtenga la buena PRO.

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

Dicha precisión se incluirá en el numeral 3.1.10.1 de la sección específica de las bases

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 30

Consulta/Observación:

DICE: f) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.7 de la sección específica de las bases.
g) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.8 de la sección específica de las bases.
h) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.15 de la sección específica de las bases.
i) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.39 de la sección específica de las bases.
j) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.53 de la sección específica de las bases.

CONSULTA: De no contar el fabricante con documentación pública para sustentar estos puntos, se pide a la entidad confirmar que aceptará una carta de fabricante para su sustento y en su idioma original.

Acápite de las bases : Sección: Especifico **Numeral:** 2.2.1.1 **Literal:** . **Página:** 18

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

Análisis respecto de la consulta u observación:

Se precisa que, de no contar el fabricante con documentación pública para sustentar los numeral 3.1.4.7, 3.1.4.8, 3.1.4.15, 3.1.4.39, 3.1.4.53, se aceptará una carta de fabricante para su sustento en idioma original, si es en idioma distinto al español deberá estar acompañada por la correspondiente traducción, en la que se declare que se cumple con las capacidades solicitadas.

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

se incluirá dicha precisión en los numerales 3.1.4.7, 3.1.4.8, 3.1.4.15, 3.1.4.39, 3.1.4.53, de la sección específica de las bases integradas

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 31

Consulta/Observación:

DICE:
e) Autorización del fabricante o su representante, para comercializar la marca y brindar los servicios solicitados (numeral 3.1.2.8 de la sección específica de las bases).
CONSULTA:
Se solicita a la entidad se sirva confirmar que se podrá presentar carta del fabricante o filial o subsidiaria local o distribuidor, que acredite que el postor es partner autorizado en el Perú, para comercializar la marca y brindar los servicios solicitados (numeral 3.1.2.8 de la sección específica de las bases).

Acápite de las bases : **Sección:** Especifico **Numeral:** 2.2.1.1 **Literal:** . **Página:** 17
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se confirma que se podrá presentar carta del fabricante o filial o subsidiaria local o distribuidor siempre que acredite que el postor es partner autorizado en el Perú, para comercializar la marca y brindar los servicios solicitados (numeral 3.1.2.8 de la sección específica de las bases).

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

se incluirá dicha precisión en el numeral 2.2.1.1. de la sección específica de las bases integradas

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 32

Consulta/Observación:

DICE:
f) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.7 de la sección específica de las bases.
CONSULTA:
Se solicita a la entidad se sirva confirmar, que la documentación técnica y/o sustento que acredite la funcionalidad de lo requerido en el numeral 3.1.4.7 de la sección específica de las bases, se presente en idioma original.

Acápite de las bases : **Sección:** Especifico **Numeral:** 2.2.1.1 **Literal:** . **Página:** 18
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se confirma, se puede presentar en idioma original, si fuera distinta al idioma español, deberá contar con la correspondiente traducción.

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

se incluirá dicha precisión en los literales f, g, h, i, j, del numeral 2.2.1.1 de la sección específica de las bases integradas

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 33

Consulta/Observación:

DICE:

g) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.8 de la sección específica de las bases.

CONSULTA:

Se solicita a la entidad se sirva confirmar, que la documentación técnica y/o sustento que acredite la funcionalidad de lo requerido en el numeral 3.1.4.8 de la sección específica de las bases, se presente en idioma original.

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

Página: 18

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

Análisis respecto de la consulta u observación:

Se confirma, se puede presentar en idioma original, si fuera distinta al idioma español, deberá contar con la correspondiente traducción.

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

se incluirá dicha precisión en los literales f, g, h, i, j, del numeral 2.2.1.1 de la sección específica de las bases integradas

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFTE CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 34

Consulta/Observación:

DICE:
h) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.15 de la sección específica de las bases.
CONSULTA:
Se solicita a la entidad se sirva confirmar, que la documentación técnica y/o sustento que acredite la funcionalidad de lo requerido en el numeral 3.1.4.15 de la sección específica de las bases, se presente en idioma original.

Acápite de las bases : **Sección:** Especifico **Numeral:** 2.2.1.1 **Literal:** . **Página:** 18
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se confirma, se puede presentar en idioma original, si fuera distinta al idioma español, deberá contar con la correspondiente traducción.

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

se incluirá dicha precisión en los literales f, g, h, i, j, del numeral 2.2.1.1 de la sección específica de las bases integradas

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 35

Consulta/Observación:

DICE:
i) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.39 de la sección específica de las bases.
CONSULTA:
Se solicita a la entidad se sirva confirmar, que la documentación técnica y/o sustento que acredite la funcionalidad de lo requerido en el numeral 3.1.4.39 de la sección específica de las bases, se presente en idioma original.

Acápite de las bases : Sección: Especifico Numeral: 2.2.1.1 Literal: . Página: 18
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se confirma, se puede presentar en idioma original, si fuera distinta al idioma español, deberá contar con la correspondiente traducción.

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

se incluirá dicha precisión en los literales f, g, h, i, j, del numeral 2.2.1.1 de la sección específica de las bases integradas

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 36

Consulta/Observación:

DICE:
j) Documentación técnica que acredite la funcionalidad de lo requerido en el numeral 3.1.4.53 de la sección específica de las bases.
CONSULTA:
Se solicita a la entidad se sirva confirmar, que la documentación técnica y/o sustento que acredite la funcionalidad de lo requerido en el numeral 3.1.4.53 de la sección específica de las bases, se presente en idioma original.

Acápite de las bases : Sección: Especifico Numeral: 2.2.1.1 Literal: . Página: 18
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se confirma, se puede presentar en idioma original, si fuera distinta al idioma español, deberá contar con la correspondiente traducción.

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

se incluirá dicha precisión en los literales f, g, h, i, j, del numeral 2.2.1.1 de la sección específica de las bases integradas

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 37

Consulta/Observación:

DICE:

f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

CONSULTA:

Se solicita a la entidad, se sirva confirmar que también se podrá presentar copia de CARNÉ DE EXTRANJERÍA para el representante legal y/o apoderado legal.

Acápite de las bases : Sección: Especifico Numeral: 2.4 Literal: .

Página: 19

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

Análisis respecto de la consulta u observación:

Se confirma, se podrá presentar copia del carné de extranjería.

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 38

Consulta/Observación:

DICE:
Jefe de proyectos
Contar con un (01) especialista con una experiencia mínima de tres (03) años en la gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática. Dicho personal debe contar con certificación vigente en Gestión de Proyectos, siendo encargado de gestionar la implementación del servicio.
CONSULTA:
Sirvase confirmar a la entidad que también se aceptará presentar certificación vigente Project Management Professional (PMP), dado que dicha certificación aplica para la Gestión de Proyectos, pudiendo quedar el texto de la siguiente manera: Contar con un (01) especialista con una experiencia mínima de tres (03) años en la gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática. Dicho personal debe contar con certificación vigente en Gestión de Proyectos o Certificación Project Management Professional (PMP), siendo encargado de gestionar la implementación del servicio.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.8 **Literal:** . **Página:** 30
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
Se precisa contar con un (01) especialista con una experiencia mínima de tres (03) años en la gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática. Dicho personal debe contar con certificación vigente en Gestión de Proyectos y/o certificación vigente Project Management Professional (PMP) , siendo encargado de gestionar la implementación del servicio."

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

Se incluirá en el numeral 3.1.8.2 de la sección específica de las bases

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 39

Consulta/Observación:

DICE:
Requerimientos del personal clave
Se debe entregar al BCRP la nómina de personal clave y las actualizaciones que puedan efectuarse a la misma, durante la vigencia del contrato.

CONSULTA:
Se solicita a la entidad se sirva confirmar que también se podrá presentar el Registro de Información Laboral T-Registro de Sunat, pudiendo quedar el texto de la siguiente manera:
Se debe entregar al BCRP la nómina o el Registro de Información Laboral T-Registro de Sunat de personal clave y las actualizaciones que puedan efectuarse a la misma, durante la vigencia del contrato.

Acápite de las bases : Sección: Especifico Numeral: 3.1.8 Literal: .

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

Página: 30

Análisis respecto de la consulta u observación:

El BCRP no considera necesario que presenten el Registro de Información Laboral T-Registro de Sunat.

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	21:39:19

Consulta: Nro. 40

Consulta/Observación:

DICE:
EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
Se consideran servicios similares a los siguientes Venta de equipos, licencias y/o renovación de licencias, servicios y/o suscripciones y/o servicios gestionados, de soluciones SIM (Security Information Management), SEM (Security Event Management), SIEM (Security Information and Event Management), NG SIEM (Next Generation SIEM), así como los servicios de implementación, mantenimiento, capacitación/entrenamiento y soporte técnico correspondientes.
CONSULTA:
A fin de permitir mayor apertura de postores por libre competencia, se solicita a la entidad se sirva confirmar que también se aceptarán como similares los siguientes servicios:
- ADQUISICIÓN DE CORRELACIÓN DE EVENTOS PLATAFORMA SIEM
- SERVICIO DE INSTALACIÓN SIEM
- RENOVACIÓN DE SOPORTE DE SECURITY ANALYTICS - SIEM
- IMPLEMENTACIÓN EQUIPO SIEM
- SERVICIO DE SEGURIDAD PARA CORRELACION DE EVENTOS SIEM
- SERVICIO INTERNO DE IMPLEMENTACIÓN DE LA SOLUCIÓN SIEM
- RENOVACIÓN SIEM
- LICENCIAMIENTO SIEM
- ADQUISICIÓN DE UNA SOLUCION DE CORRELACIONADOR DE EVENTOS SIEM
- RENOVACIÓN LICENCIAMIENTO SIEM
- SERVICIO INTERNO DE IMPLEMENTACIÓN DE LA SOLUCIÓN SIEM
- SERVICIOS DE INSTALACION DE EQUIPO SIEM
- RENOVACION DE SERVICIOS DE LA SOLUCION DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD INFORMATICA SIEM

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.2 **Literal:** B **Página:** 35
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Se considerara adicionalmente a los otros descritos en el numeral 3.2 literal B como servicios similares los siguientes: ADQUISICIÓN DE CORRELACIÓN DE EVENTOS PLATAFORMA SIEM, SERVICIO DE INSTALACIÓN SIEM, RENOVACION DE SERVICIOS DE LA SOLUCION DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD INFORMATICA SIEM.
Cabe señalar que el resto solicitado por el participante se encuentra dentro de lo que se esta aceptando como servicios similares."

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

Se incluirá lo señalado en el numeral 3.2 de la sección específica de la bases, literal B.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 41

Consulta/Observación:

Dice: "Recolectar eventos desde diversas fuentes (datasources)"

Consulta: Con la finalidad de garantizar que las soluciones propuestas puedan integrarse correctamente con las fuentes de seguridad del cliente, se solicita a la Entidad confirmar la lista de fuentes a integrar, de manera que el postor pueda validar correctamente el cumplimiento del mismo.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.2.1 **Literal:** a **Página:** 22
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se precisa que según numeral 3.1.10.1 indica que la información detallada sobre los datasources es considerada confidencial por la Entidad; por lo que la lista de detalle de Datasources se facilitara después de la firma de los acuerdos de confidencialidad.

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

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 42

Consulta/Observación:

Dice: "La solución estará conformada por appliances virtuales y/o appliances físicos de un mismo fabricante."

Consulta: Se solicita a la Entidad confirmar que se aceptarán arquitecturas mixtas, que impliquen appliances virtuales para recolectar eventos de diversas fuentes onpremise del BCRP, y plataformas en nube para realizar la correlación y analítica.

Acápite de las bases : Sección: Especifico Numeral: 3.1.2.1 Literal: a Página: 22

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

Análisis respecto de la consulta u observación:

"Se confirma.
Según el numeral 3.1.4.4: ""La solución deberá ser implementada en modo On-Premise"". Sin embargo se precisa que la solución SIEM permitirá appliances virtuales para recolectar eventos de diversas fuentes del BCRP y plataformas en nube para realizar la correlación y analítica EN TIEMPO REAL.
Por lo que el numeral 3.1.4.4 quedara de la siguiente manera: ""La solución deberá ser implementada en modo On-Premise y/o híbrida"".

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

Se incluirá la precisión en el numeral 3.1.2.1 y se modificará el numeral 3.1.4.4 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 43

Consulta/Observación:

Dice: " Se aceptará como alternativa la contratación de suscripciones para la actual plataforma SIEM del BCRP (Trellix SIEM) "

Consulta: Con la finalidad de garantizar la igualdad de participación de los postores, se solicita al cliente considerar que los recursos de hardware serán provistos por el postor con la respectiva migración de la plataforma actual.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.2.2 **Literal:** a **Página:** 22
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Se precisa:
Para el caso en que el proveedor presente una arquitectura mixta como alternativa donde entregara appliances virtuales para recolectar eventos de diversas fuentes del BCRP y plataformas en nube para realizar la correlación y analítica, al tratarse de una solución nueva, es responsable de las suscripciones de la solución nueva y migración de la plataforma actual en coordinación con el Banco por los casos de uso.
El proveedor deberá garantizar todo lo necesario para que funcione tan igual como la actual plataforma SIEM sin degradación del servicio, teniendo en cuenta los indicado en los numerales 3.1.2 y 3.1.3."

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

Se modificará el numeral 3.1.2 de la sección específica de las bases

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 44

Consulta/Observación:

Dice: "Capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4500 EPS o superiores..."

Consulta: Con la finalidad de garantizar la igualdad de participación de los postores, considerando que entre las diferentes marcas existe diferentes tipos de licenciamiento, donde la cantidad de EPS puede ser un factor determinante en los costos, se solicita a la Entidad confirmar que la solución ofertada debe de soportar o estar licenciada mínimamente para soportar 4500 EPS.

Acápite de las bases : Sección: Especifico **Numeral:** 3.1.2.4 **Literal:** a **Página:** 22

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

Análisis respecto de la consulta u observación:

"No se confirma.

Se precisa que, con la finalidad de permitir mayor participación de postores, la solución SIEM deberá tener capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4000 EPS, pudiendo variar en algunas ocasiones hasta 4500 EPS. Este requerimiento debe ser soportado por todos los componentes del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas)."

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 45

Consulta/Observación:

Dice: "La solución debe incluir dentro de las fuentes de información a un servicio de reputación del fabricante para detección proactiva de amenazas."

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad considerar como opcional el presente requerimiento.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.2.5 **Literal:** a **Página:** 22
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Las necesidades del Banco requieren que la solución deba incluir dentro de las fuentes de información un servicio de reputación para detección proactiva de amenazas, precisando que no necesariamente sea de la misma marca."

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
se incluirá la precisión en el numeral 3.1.2.5 de la sección específica de las bases integradas.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 46

Consulta/Observación:

Dice: Condiciones de infraestructura y componentes complementarios."

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad confirmar que se considerará soluciones basadas en nube, siempre y cuando dichas soluciones provea las características técnicas requeridas en las bases.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.3 **Literal:** a **Página:** 23
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
Según el numeral 3.1.4.4: ""La solución deberá ser implementada en modo On-Premise"". Sin embargo se precisa que la solución SIEM permitirá appliances virtuales para recolectar eventos de diversas fuentes del BCRP y plataformas en nube para realizar la correlación y analítica EN TIEMPO REAL.
Por lo que el numeral 3.1.4.4 quedara de la siguiente manera: ""La solución deberá ser implementada en modo On-Premise y/o híbrida"".
NOTA: No se aceptarán soluciones de nueva generación de SIEM que trabajan 100% en la nube."

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

"se incluirá la nota en el numeral 3.1.4.4 de la sección específica de las bases integradas.
"

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 47

Consulta/Observación:

Dice: "Soportar los siguientes protocolos de recolección de datos: Syslog UDP, Syslog TCP, Secure-Syslog (y/o Syslog NG), RSYSLOG TCP RSYSLOG UDP, conexión por string JDBC (BD), SNMP, Cisco RDEP, SDEE, CheckPoint OPSEC, Checkpoint LEA, XML, archivos de texto y API."

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad considerar como opcional SNMP, Cisco RDEP, SDEE, Checkpoint OPSEC, LEA, XML.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.1 **Literal:** a **Página:** 23

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

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Las necesidades del Banco requieren que se soporte los protocolos de recolección de datos siguientes: Syslog UDP, Syslog TCP, RSYSLOG TCP, RSYSLOG UDP, archivos de texto y API. "

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

Los protocolos Secure-Syslog (y/o Syslog NG), SNMP, CheckPoint OPSEC, Checkpoint LEA, XML, conexión por string JDBC (BD), Cisco RDEP, SDEE, al ser opcionales, serán retirados del numeral 3.1.4.1 de la sección específica de las bases integradas.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 48
Consulta/Observación:
Dice: "La solución deberá ser implementada en modo On-Premise"

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad confirmar que se aceptaran colectores de logs onpremise, pero consola de gestión en nube.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.4 **Literal:** a **Página:** 23

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

Análisis respecto de la consulta u observación:

"Se confirma.

Según el numeral 3.1.4.4: ""La solución deberá ser implementada en modo On-Premise"". Sin embargo se precisa que la solución SIEM permitirá appliances virtuales para recolectar eventos de diversas fuentes del BCRP y plataformas en nube para realizar la correlación y analítica EN TIEMPO REAL.

Por lo que el numeral 3.1.4.4 quedara de la siguiente manera: ""La solución deberá ser implementada en modo On-Premise y/o hibrida"".

"

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

Se actualizara el numeral 3.1.4.4 de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 49

Consulta/Observación:

Dice: "La solución debe ser implementada en un esquema de Alta Disponibilidad Activo-Activo para los core del appliance virtual"

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad confirmar que se aceptaran que los colectores podran estar en Activo-Pasivo

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.5 **Literal:** a **Página:** 24
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
La actual arquitectura de la solución SIEM del Banco esta implementada en un esquema de Alta Disponibilidad Activo-Activo para los core del appliance virtual, como se indica en el numeral 3.1.4.5 de la sección especifica de las bases. Por lo que cualquier arquitectura on-premise y/o hibrida propuesta por el postor deberá cumplir con este requerimiento del Banco."

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:17:03

Consulta: Nro. 50

Consulta/Observación:

Dice: "Deberá ser integrable ¿fuera de la caja¿ (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes, mediante el uso de componentes denominados conectores/colectores."

Consulta: Con la finalidad de garantizar el correcto dimensionamiento del requerimiento, se solicita a la Entidad confirmar la relación de marcas y dispositivos a integrar, toda vez que la cantidad de dispositivos y marcas ofertadas pueden no ser las necesarias para la cubrir la necesidad de la Entidad.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.8 **Literal:** a **Página:** 24
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se precisa que en el numeral 3.1.4.8 de las bases se detalla la lista de marcas y plataformas mínimas admitidas para soporte de la solución SIEM. La lista de detalle de Datasources se facilitará después de la firma de los acuerdos de confidencialidad.

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

Se incluirá la precisión en el numeral 3.1.4.8 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	22:38:23

Consulta: Nro. 51

Consulta/Observación:

DICE: Capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4500 EPS o superiores. Este requerimiento debe ser soportado por todos los componentes del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas).

CONSULTA: Se pide poder actualizar este punto de 4500 EPS a 4000 debido a que con su licenciamiento actual, Event Receiver (ERC) del modelo McAfee ERC-VM-8 Cores + VM-4 Cores Add. pueden soportar hasta 4000 EPS.

Acápite de las bases : Sección: Especifico **Numeral:** 3.1.2.4 **Literal:** . **Página:** 22

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

Análisis respecto de la consulta u observación:

No se confirma.
Se precisa que, con la finalidad de permitir mayor participación de postores, la solución SIEM deberá tener capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4000 EPS, pudiendo variar en algunas ocasiones hasta 4500 EPS. Este requerimiento debe ser soportado por todos los componentes del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas).

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

Se actualizara el numeral 3.1.2.4 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	22:38:23

Consulta: Nro. 52

Consulta/Observación:

DICE: Capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4500 EPS o superiores. Este requerimiento debe ser soportado por todos los componentes del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas).

CONSULTA: De mantenerse el requerimiento de 4500 EPS, se pide a la entidad confirmar que aceptará que no podrá ser considerado renovar el componente Event Receiver (ERC) y se deberá considerar como licenciamiento nuevo para soportar el nuevo requerimiento de 4500 EPS esto significando una implementación nueva para este componente

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.2.4 **Literal:** . **Página:** 22
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que, con la finalidad de permitir mayor participación de postores, la solución SIEM deberá tener capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4000 EPS, pudiendo variar en algunas ocasiones hasta 4500 EPS. Este requerimiento debe ser soportado por todos los componentes del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas)."

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

Se actualizara el numeral 3.1.2.4 de las bases.

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20601317461	Fecha de envío :	07/03/2024
Nombre o Razón social :	SECURESOFT CORPORATION S.A.C	Hora de envío :	22:38:23

Consulta: Nro. 53

Consulta/Observación:

DICE: Capacidad de ingestar identidades a partir de la conexión con Directorios LDAP, usado para realizar el análisis de comportamiento de los usuarios (capacidad UEBA).

CONSULTA: Se pide a la entidad, indicar la cantidad de usuarios que se requeriría para esta capacidad

Acápíte de las bases : Sección: Especifico Numeral: 3.1.4.26 Literal: . Página: 26

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

Análisis respecto de la consulta u observación:

Se precisa que la cantidad de usuarios requeridos para esta capacidad será de 1250 usuarios.

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

Se incluirá la precisión en el numeral 3.1.4.26 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 54

Consulta/Observación:

Dice: "Deberá ser integrable ¿fuera de la caja¿ (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes, mediante el uso de componentes denominados conectores/colectores."

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad confirmar que como parte de la propuesta del Postor, se podran personalizar conectores mínimamente para Cisco Email Security, McAfee Security Web Gateway, Cisco Nexus, Radware Alteon, RSA Auth Manager, Citrix ADC, Kaspersky Endpoint Security.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.8 **Literal:** a **Página:** 24
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
En el numeral 3.1.4.8 de las bases se precisa que las necesidades del Banco requieren que la solución SIEM sea integrable ¿fuera de la caja¿ (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes. Teniendo en consideración el esquema actual de infraestructura el cual contempla la siguiente lista de marcas y plataformas mínimas admitidas para soporte de la solución SIEM:
¿ Cisco Email Security Appliance
¿ McAfee/SkyHigh Security Web Gateway
¿ Cisco Nexus
¿ Palo Alto Next Generation Firewall
¿ Radware Alteon/AppWall
¿ RSA Authentication Manager
¿ Citrix ADC
¿ Kaspersky Endpoint Security
¿ Microsoft Windows "

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 55

Consulta/Observación:

Dice: " La solución debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente, tales como aplicaciones desarrolladas por la institución (in-house) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes"

Consulta: El presente requerimiento puede resultar ambiguo, considerando que la integración de una fuente no soportada en la actualidad puede representar costos adicionales, tiempos no determinados para los mismos, u otros, por lo cual se solicita a la Entidad considerar como opcional el presente requerimiento u en su defecto, considerar soluciones que soporten la integración de fuentes a traves de algunos de los tipos listados: Archivos de registro (logs) con campos delimitados, Archivos de registro (logs) de longitud variable (no delimitados), Traps SNMP, Eventos enviados mediante Syslog, Archivos con formato XM/JSON.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.11 **Literal:** a **Página:** 24

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

Análisis respecto de la consulta u observación:

"No se confirma.
La solución debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente, tales como aplicaciones desarrolladas por la institución (in-house) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes:

- Archivos de registro (logs) con campos delimitados.
- Archivos de registro (logs) de longitud variable (no delimitados).
- Traps SNMP.
- Eventos enviados mediante Syslog.
- Archivos con formato XM/JSON.

Se precisa que la integración de estas fuentes no homologadas sean realizadas por el proveedor durante la etapa de soporte, sin incurrir en costo alguno según lo indicado en el numeral 3.1.10.7"

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

null

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 56

Consulta/Observación:

Dice: " Capacidad de preservar, bajo demanda, el evento en su formato original (raw) en adición al evento previamente normalizado"

Consulta: Se solicita confirmar que se aceptaran plataformas que permitan elegir si la data recolectada permanece en bien en formato original (raw) o bien en formato normalizado.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.14 Literal: a Página: 25

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

Análisis respecto de la consulta u observación:

"No se confirma.

Se precisa que la solución SIEM cuente con la capacidad de preservar ambas características: Formato original (raw) y Formato Normalizado."

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 57

Consulta/Observación:

Dice: " Capacidad de generar una firma o huella digital sobre los eventos en su formato original (raw) mediante el uso de algoritmos criptográficos de una sola vía, así mismo los conectores deberán tener la capacidad de validar la integridad de estos eventos"

Consulta: Se solicita confirmar que de manera alternativa a este requerimiento se aceptará que la plataforma envíe los eventos hacia el servidor de analítica y gestión en un protocolo encriptado, para asegurar la confidencialidad en la transferencia de los eventos.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.16 **Literal:** a **Página:** 25
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
Se precisa que la solución SIEM de manera alternativa enviara los eventos hacia el servidor de analítica y gestión en un protocolo encriptado, para asegurar la confidencialidad en la transferencia de los eventos."

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

Se actualizara el numeral 3.1.4.16 de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 58

Consulta/Observación:

Dice: " Permitir configurar controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato"

Consulta: Se solicita confirmar que el control de consumo de ancho de banda para el envío de los eventos recolectados, desde el colector onpremise hacia el servidor central en la nube podrá ser realizado por el firewall perimetral del BCRP. Respecto a la transacciones críticas, se solicita confirmar que se aceptarán soluciones que siempre envíen en línea cualquier eventos recolectado, de tal manera que no haya necesidad de priorizar puesto que todos los eventos son enviados a la consola en nube ni bien se reciban.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.18 Literal: a Página: 25
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se precisa que los controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato será opcional, por lo que si el proveedor desea incluir soluciones que compriman la información a enviar y/o permitir configurar controles de uso de ancho de banda deberán de estar incluidos en el precio ofertado, precisando que no es obligatorio.

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

Se eliminará el numeral 3.1.4.18 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 59

Consulta/Observación:

Dice: " Permitir configurar el retraso voluntario en el envío de eventos a la solución de almacenamiento y administración de eventos basado en horarios, de tal forma que el colector de eventos guarde en su cache los eventos y envíe eventos con prioridad alta durante el horario configurado. Una vez finalizado el horario, se enviarán los eventos de más baja prioridad"

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad considerar como opcional el presente requerimiento.

Acápite de las bases : Sección: Especifico **Numeral:** 3.1.4.19 **Literal:** a **Página:** 25
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
La solución SIEM opcionalmente deberá permitir configurar el retraso voluntario en el envío de eventos a la solución de almacenamiento y administración de eventos basado en horarios, de tal forma que el colector de eventos guarde en su cache los eventos y envíe eventos con prioridad alta durante el horario configurado. Una vez finalizado el horario, se enviarán los eventos de más baja prioridad"

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

Se eliminará el numeral 3.1.4.19 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 60

Consulta/Observación:

Dice: "Contar con múltiples perfiles de configuración, los cuales entrarán en funcionamiento en función de horarios preestablecidos"

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad considerar como opcional el presente requerimiento.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.20 **Literal:** a **Página:** 25
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que los perfiles de configuración se refieren a perfiles propios de la solución SIEM tales como monitoreo, administrador, superadmin, entre otros según cada fabricante y/o marca lo identifique."

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

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 61

Consulta/Observación:

Dice: " Permitir definir ubicaciones físicas o lógicas internas, a las cuales se les podrán asignar coordenadas (latitud, longitud) que permitan identificar la ubicación geoespacial de origen y destino de los eventos aún y cuando se encuentren bajo segmentos privados de direcciones IP"

Consulta: Se solicita confirmar que de manera alternativa a este requerimiento se aceptará plataformas que brinden información de una IP pública, con detalles tales como país, ASN, organización, fecha de registro, incidentes relacionados.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.32 Literal: a Página: 26

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

Análisis respecto de la consulta u observación:

"Se confirma.
Se precisa que el servicio de geolocalización es parte de un complemento que puede ser fuente externa y será consultado a través de la plataformas que brinden información de una IP pública, con detalles tales como país, ASN, organización, fecha de registro, incidentes relacionados, entre otros."

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 62

Consulta/Observación:

Dice: " Contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:

- Importancia del evento
- Criticidad del activo
- Vulnerabilidades asociadas
- Antecedentes sobre el origen, destino o ambos."

Consulta: Se solicitar confirmar que se aceptarán plataformas que cuenten con un módulo de scoring integrado, que permitan dar una valoración cuantitativa de las alertas en base a diferentes atributos de la alerta, tales como equipo afectado y su criticidad (la cual podrá ser configurable), importancia, tipo de ataque, origen y/o destino del ataque, técnica o táctica de MITRE, entre otros.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.35 **Literal:** a **Página:** 26

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

Análisis respecto de la consulta u observación:

"Se confirma.

Se aceptaran plataformas que cuenten con módulo de scoring integrado, que permitan dar una valoración cuantitativa de las alertas en base a diferentes atributos de la alerta, tales como equipo afectado y su criticidad (la cual podrá ser configurable), importancia, tipo de ataque, técnica o táctica de MITRE, entre otros que podrán considerarse los siguientes factores:

- Importancia del evento
- Criticidad del activo
- Vulnerabilidades asociadas

Opcionalmente, se aceptara que la solución SIEM podrá evaluar el nivel de riesgo considerando el siguiente factor:

- Antecedentes sobre el origen, destino o ambos."

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

Se incluirá la precisión el numeral 3.1.4.35 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 63

Consulta/Observación:

- Dice: "
- 4.39. Contar con un flujo de trabajo (workflow) nativo, automatizado y con el manejo de niveles de escalamiento parametrizable para el manejo de incidentes de seguridad.
- 4.40. Permitir crear grupos de notificación, cada grupo deberá podrá contener uno o más niveles de escalamiento y por cada nivel de escalamiento deberá contar con un destinatario para la notificación.
- 4.41. Permitir definir por cada destinatario de notificación lo siguiente: El tipo de notificación que recibirá (por ejemplo: consola, correo electrónico), así como el horario bajo el cual se podrán entregar notificaciones.
- 4.42. Permitir definir en función de la severidad de las alertas generadas el tiempo máximo de espera previo a que la notificación sea escalada al nivel inmediato superior soportando el proceso de respuesta a incidentes y flujo de trabajo. "

Consulta: Se solicita confirmar que se aceptarán plataformas que permitan establecer acciones automáticas respecto al manejo de los incidentes, tales como cada una de las siguientes acciones de manera individual o una combinación de ellas: asignar el incidente a uno o más analistas; enviar correos electrónicos a una o más personas; modificar la criticidad del incidente; enviar un mensaje por Slack. Las cuales se podrán activar ante alguna condiciones del incidente de seguridad como activo afectado, tipo de ataque, TTP acorde a MITRE ATT&CK, IP origen/destino, fuente del log, entre otros.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.39 **Literal:** a **Página:** 27
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.

En el numeral 3.1.4.39 la solución SIEM deberá contar con un flujo de trabajo (workflow), automatizado y con el manejo de niveles de escalamiento parametrizable para el manejo de incidentes de seguridad. Siendo estas configuraciones de playbooks automatizados de la misma marca u otra plataforma.

Para los numerales 3.1.4.40, 3.1.4.41 y 3.1.4.42 el proveedor podrá opcionalmente entregar plataformas que permitan establecer acciones automáticas respecto al manejo de los incidentes, tales como cada una de las siguientes acciones de manera individual o una combinación de ellas: asignar el incidente a uno o más analistas; enviar correos electrónicos a una o más personas; modificar la criticidad del incidente; enviar mensajes. Las cuales se podrán activar ante alguna condiciones del incidente de seguridad como activo afectado, tipo de ataque, TTP acorde a MITRE ATT&CK, IP origen/destino, fuente del log, entre otros.

"

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

Se incluirá la precisión en los numerales 3.1.4.40; 3.1.4.41 y 3.1.4.42 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 64

Consulta/Observación:

Dice: " La interface web de gestión deberá tener la capacidad de realizar búsquedas sobre los eventos almacenados ya sea a través de palabras clave (keywords), campos específicos o bien una combinación de ambas. Estas búsquedas podrán ser ingresadas en formato libre a través de un cuadro de texto. "

Consulta: Confirmar que las busquedas podrán ser realizadas a partir de un formato de la plataforma, sencillo y basado en expresiones regulares.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.44 **Literal:** a **Página:** 27

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

Análisis respecto de la consulta u observación:

"Se confirma.
Las búsquedas podrán ser realizadas por un formato según la plataforma SIEM propuesta.
"

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 65

Consulta/Observación:

Dice: " Capacidad de enviar alertas vía email, traps SNMPv2 y SNMPv3, así como notificaciones directas a la consola de gestión. "

Consulta: Se solicita confirmar que SNMP será opcional para las ofertas que consideren consolas de gestión en nube, ya que la consola de gestión es tipo SaaS, con un SLA de uptime mensual de 99.9%.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.54 **Literal:** a **Página:** 28
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
La solución SIEM deberá tener capacidad de enviar alertas vía email. Opcionalmente enviara alertas vía traps y/o SNMPv2 y/o SNMPv3, así como notificaciones directas a la consola de gestión."

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

Se actualizara el numeral 3.1.4.54 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 66

Consulta/Observación:

Dice: " Capacidad de crear casos de forma automatizada e incluso de alimentar casos (tickets) ya existentes como mecanismos de acción de las reglas de correlación. "

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad considerar como opcional el presente requerimiento.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.55 **Literal:** a **Página:** 28
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
La solución SIEM opcionalmente tendrá la capacidad de crear casos de forma automatizada e incluso de alimentar casos (tickets) ya existentes como mecanismos de acción de las reglas de correlación."

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

Se eliminará el numeral 3.1.4.55 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 67

Consulta/Observación:

Dice: " Permitir el monitoreo de los componentes de la solución, incluyendo estadísticas de uso de CPU, memoria, disco duro, estado de los servicios y estado de las conexiones. "

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad considerar como opcional el presente requerimiento para propuestas SaaS.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.63 **Literal:** a **Página:** 28
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
El proveedor deberá garantizar que su solución SIEM propuesta permita sea monitoreada en sus componentes on premise, incluyendo estadísticas de uso de CPU, memoria, disco duro, estado de los servicios y estado de las conexiones, con plataformas de monitoreo propias de la institución."

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

Se actualizara el numeral 3.1.4.63 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 68

Consulta/Observación:

Dice: " La solución de correlación de eventos deberá contar con funcionalidades integradas en la interfaz de administración gráfica para la definición, ejecución, calendarización y entrega automatizada de reportes ejecutivos y detallados en los siguientes formatos: PDF, CSV y HTML. "

Consulta: Con la finalidad de garantizar la pluralidad de marcas y de postores, se solicita a la Entidad considerar el formato HTML como opcional.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.66 **Literal:** a **Página:** 29

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

Análisis respecto de la consulta u observación:

"Se confirma.
La solución SIEM deberá contar con funcionalidades integradas en la interfaz de administración gráfica para la definición, ejecución, calendarización y entrega automatizada de reportes ejecutivos y detallados en los siguientes formatos: PDF, CSV y opcionalmente HTML."

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

Se actualizara el numeral 3.1.4.66 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 69

Consulta/Observación:

Dice: " La solución deberá permitir políticas de retención de eventos basadas ya sea en tamaño (GB) y/o tiempo (días), las cuales aplicarán de forma independiente a cada grupo de almacenamiento de eventos, lo que permitirá contar con un almacenamiento de eventos inteligente y auto administrado. "

Consulta: Se solicita confirmar que se aceptarán plataformas que almacenen todos los logs, eventos y alertas recibidas durante 30 días; y respecto a las alertas e incidentes de seguridad durante 180 días.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.69 **Literal:** a **Página:** 29

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

Análisis respecto de la consulta u observación:

"No se confirma.
La solución deberá permitir políticas de retención de eventos basadas ya sea en tamaño (GB) y/o tiempo (días), las cuales aplicarán de forma independiente a cada grupo de almacenamiento de eventos, lo que permitirá contar con un almacenamiento de eventos inteligente y auto administrado.
Se precisa que la actual solución SIEM del Banco permite almacenar logs, eventos y alertas durante 6 meses y alertas e incidentes de seguridad durante 270 días, por lo que el proveedor deberá permitir este almacenamiento en ese tiempo definido en la plataforma propuesta.
"

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

Se actualizara el numeral 3.1.4.69 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	22:46:59

Consulta: Nro. 70

Consulta/Observación:

Dice: "

4.77. Permitir generar reportes de cumplimiento de las regulaciones ISO 27001 y/o ISO 27002.

4.78. Contar con más de 350 reportes predefinidos y listos para ejecutarse en los rubros de cumplimiento, red, host, seguridad, almacenamiento "

Consulta: Confirmar si este tipo de reportes podrán ser personalizados durante la etapa de despliegue e instalación.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.77 Literal: a Página: 29

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

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.

Este tipo de reportes podrán ser personalizados durante la etapa de despliegue e instalación, como también en toda la ejecución de la etapa de soporte."

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20552075341	Fecha de envío :	07/03/2024
Nombre o Razón social :	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	Hora de envío :	23:22:56

Consulta: Nro. 71

Consulta/Observación:

Dice: "Se consideran servicios similares a los siguientes Venta de equipos, licencias y/o renovación de licencias, servicios y/o suscripciones y/o servicios gestionados, de soluciones SIM (Security Information Management), SEM (Security Event Management), SIEM (Security Information and Event Management), NG SIEM (Next Generation SIEM), así como los servicios de implementación, mantenimiento, capacitación/entrenamiento y soporte técnico correspondientes."

Consulta: Se solicita a la Entidad considerar como servicios similares a los siguientes: Venta de equipos, licencias y/o renovación de licencias, servicios y/o suscripciones y/o servicios gestionados, de soluciones de Software de Gestión de seguridad de la información y/o gestión de eventos; y/o Soluciones de Ciberseguridad y/o correlacionador de eventos; por ser afines a la experiencia requerida.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.2 **Literal:** B **Página:** 35
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente
Se considerara adicionalmente a los otros descritos en el numeral 3.2 literal B. como servicio similar a ""gestión de eventos y/o correlacionador de eventos"".
No se aceptan el resto sugerido por el participante en vista que se trata de servicios que no guardan relación con el objeto de esta contratación."

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

Se incluirá lo señalado en el numeral 3,2 de la sección específica de la bases, literal B.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 72

Consulta/Observación:

Dice: Implementación del SIEM

Consulta: ¿Las actas seran entregadas de manera virtual en algun portal o de manera fisica a mesa de partes?

Acápíte de las bases : Sección: Especifico **Numeral:** 1.7 **Literal:** 1.7 **Página:** 14

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

Análisis respecto de la consulta u observación:

Se precisa que las actas serán entregadas de manera virtual a la dirección electrónica mesadeparteshvirtual@bcrp.gob.pe y deberán ser dirigidos al Departamento de Ciberdefensa.

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

Dicha precisión se incluirá en las bases integradas numerales 1.7 y 3.1.1 de la sección específica de las bases

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 73
Consulta/Observación:
Dice: Suscripciones del SIEM
Consulta 1: Indicar si la suscripción puede ser entregada con un acta

Consulta 2: ¿Confirmar que el inicio de los 2 años es con fecha del acta de conformidad de la implementación? O ¿con fecha de aceptación de dicha acta?

Acápites de las bases : **Sección:** Especifico **Numeral:** 1.7 **Literal:** 1.7 **Página:** 14
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:
"1. Se precisa que las suscripciones del SIEM, deberán ser entregadas a través de carta del proveedor con las vigencias indicadas según el numeral 1.7. a través de mesadeparteshvirtual@bcrp.gob.pe.
2. Se confirma que el inicio de las suscripciones será de 2 años a partir de la fecha de aceptación del acta de conformidad de implementación"

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Dicha precisión se incluirá en las bases integradas numerales 1.7 y 3.1.1 de la sección específica de las bases

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 74

Consulta/Observación:

Dice: El 50% a la culminación del último servicio de mantenimiento preventivo.

Consulta: según los ítem 1.7 y 3.1.1. El mantenimiento forma parte de la prestación accesorio por lo que no debe ser un entregable para la facturación de la prestación principal

Acápite de las bases : **Sección:** Especifico **Numeral:** 2.6 **Literal:** 2.6 **Página:** 20

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

Análisis respecto de la consulta u observación:

"Se modificará la forma de pago de la prestación principal:

DICE: :

- El 50% a la conformidad de implementación del servicio.
- El 50% a la culminación del último servicio de mantenimiento preventivo.

DEBE DECIR:

- El 50% a la entrega de las suscripciones según carta del proveedor indicando su vigencia
- El 50% a la conformidad de implementación del servicio. "

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

se modificará la forma de pago para la prestación principal en las bases integradas.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 75

Consulta/Observación:

Dice: El 8% a la conformidad de realización de la capacitación.

Consulta: lo indicado en el punto 3.1.11 de la pagina 33 se indica que el curso puede ser a demanda, lo que implica que no controlamos cuando terminen en capacitarse los usuarios. Por lo que esta opcion de capacitacion deberia ser sustentada con la entrega de los cursos y no con la realización del mismo.

Acápite de las bases : **Sección:** Especifico **Numeral:** 2.6 **Literal:** 2.6 **Página:** 20

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

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que la capacitación será precedida de un ""plan de capacitación"" propuesta por el proveedor y en donde se estipularan las fechas tentativas de inicio y fin del mismo, las cuales deberán ser tomadas en 2 grupos de forma online sincrona, es decir, en el mismo momento tanto asistentes como instructor."

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

Se incluirá dicha precisión en el numeral 3.1.11 CAPACITACIÓN.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 76

Consulta/Observación:

Dice: Capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4500 EPS o superiores.

Consulta: Cuando se indica que debe soportar picos superiores a 4500 EPS, indicar por un espacio de tiempo para este pico y cual seria el estimado a los referido como superior a 4500 EPS

Acápite de las bases : Sección: Especifico **Numeral:** 3.1.2.4 **Literal:** 3.1.2.4 **Página:** 22

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

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Se precisa que, con la finalidad de permitir mayor participación de postores, la solución SIEM deberá tener capacidad de soportar un uso promedio diario de 3500 eventos por segundo (EPS), soportando picos de 4000 EPS, pudiendo variar en algunas ocasiones hasta 4500 EPS. Este requerimiento debe ser soportado por todos los componentes del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas Avanzadas).
El espacio de tiempo para los picos percibidos es de un lapso entre 10min a 30min."

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

Se actualizara el numeral 3.1.2.4 de las bases.

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 77

Consulta/Observación:

Dice:
¿ Datacenter Principal: 40 vCPUs, 96 GB RAM, 1000 GB de disco.
¿ Datacenter de contingencia: 28 vCPUs, 64 GB RAM, 1000 GB de disco.

Consulta: Confirmar si los discos proporcionados por la entidad pueden ser SSD (Discos Solidos)

Acápite de las bases : Sección: Especifico Numeral: 3.1.3.1 Literal: 3.1.3.1 Página: 23

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

Análisis respecto de la consulta u observación:

"No se confirma.
La infraestructura actual no dispone de discos SSD."

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 78

Consulta/Observación:

Dice: Soportar los siguientes protocolos de recolección de datos: Syslog UDP, Syslog TCP, Secure-Syslog (y/o Syslog NG), RSYSLOG TCP RSYSLOG UDP, conexión por string JDBC (BD), SNMP, Cisco RDEP, SDEE, CheckPoint OPSEC, Checkpoint LEA, XML, archivos de texto y API.

Consulta:
Este requerimiento o cada protocolo debe ser opcional ya que si un Datasource no cuenta con un conector nativo, seria desarrollado como parte del soporte.

Acápíte de las bases : Sección: Especifico **Numeral:** 3.1.4.1 **Literal:** 3.1.4.1 **Página:** 23
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
Las necesidades del Banco requieren que se soporte los protocolos de recolección de datos siguientes: Syslog UDP, Syslog TCP, RSYSLOG TCP, RSYSLOG UDP, archivos de texto y API. "

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

Los protocolos Secure-Syslog (y/o Syslog NG), SNMP, CheckPoint OPSEC, Checkpoint LEA, XML, conexión por string JDBC (BD), Cisco RDEP, SDEE, al ser opcionales, serán retirados del numeral 3.1.4.1de la sección especifica de las bases integradas.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 79

Consulta/Observación:

Dice: Capacidad de integrarse con soluciones o módulos SOAR y/o permita ejecutar script para respuestas automáticas.

Consulta: Confirmar que en lo requerido debe formar parte una capa o licencia de SOAR.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.7 Literal: 3.1.4.7 Página: 24

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

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que lo descrito en el numeral 3.1.4.7 es referido a que la solución SIEM permita integrarse, cuando se requiera, a soluciones SOAR."

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 80

Consulta/Observación:

Dice: Deberá ser integrable ¿fuera de la caja¿ (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes, mediante el uso de componentes denominados conectores/colectores.

Consulta:

Aclarar que las métricas de dimensionamiento son:

- 1.- los 3500 EPS con picos de 4500 EPS o
- 2.- la integracion de los 300 dispositivos sin tener en cuenta la cantidad de EPS generados.

Acápíte de las bases : **Sección:** Especifico **Numeral:** 3.1.4.8 **Literal:** 3.1.4.8 **Página:** 24

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

Análisis respecto de la consulta u observación:

Se precisa que los 300 dispositivos mencionados en el numeral 3.1.4.8 esta referido a la capacidad de integración por defecto de la solución SIEM, sin necesidad de incurrir en desarrollo de integración. Esto no esta referido al numero de Data Sources a integrar que se realizara durante la etapa de implementación en la cual se indicara una lista con los 35 Data Sources de manera referencial para este propósito, pudiendo modificarse durante la etapa de soporte sin que esto afecte a la cantidad de EPS indicados en el numeral 3.1.2.4

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

Se actualizara el numeral 3.1.4.8 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 81

Consulta/Observación:

Dice: Debe de permitir la modificación de los line-filter de las integraciones out-of- the-box, esto con el fin de poder normalizar otros parámetros de los eventos recibidos.

Nota: La mencionada funcionalidad deberá sustentarse mediante la presentación de documentación técnica del fabricante, durante la presentación de ofertas.

Consulta:
Teniendo en cuenta que como parte del servicio es requerido el soporte de fabrica, los requerimientos integracion para fuentes no homologadas debe formar parte del servicio de soporte y realizada por el fabricante para evitar errores con estas integraciones. Por lo que se solicita que se modifique este requerimiento en donde solo se indique la necesidad de integrar fuentes nuevas no homologadas.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.8 **Literal:** 3.1.4.8 **Página:** 24

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

Análisis respecto de la consulta u observación:

"No se confirma.
Las integraciones out of the box deben ser realizadas durante la etapa de implementación y durante la etapa de soporte, según se requiera."

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

null

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 82

Consulta/Observación:

Dice: La solución debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente, tales como aplicaciones desarrolladas por la institución (in-house) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes:

- ¿ Archivos de registro (logs) con campos delimitados.
- ¿ Archivos de registro (logs) de longitud variable (no delimitados).
- ¿ Traps SNMP.
- ¿ Eventos enviados mediante Syslog.
- ¿ Archivos con formato XM/JSON.

Consulta:

Teniendo en cuenta que como parte del servicio es requerido el soporte de fabrica, los requerimientos integracion para fuentes no homologadas debe formar parte del servicio de soporte y realizada por el fabricante para evitar errores con estas integraciones. Por lo que se solicita que se modifique este requerimiento en donde solo se indique la necesidad de integrar fuentes nuevas no homologadas.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.11 **Literal:** 3.1.4.11 **Página:** 24
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma parcialmente.
La solución debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente, tales como aplicaciones desarrolladas por la institución (in-house) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes:

- Archivos de registro (logs) con campos delimitados.
- Archivos de registro (logs) de longitud variable (no delimitados).
- Traps SNMP.
- Eventos enviados mediante Syslog.
- Archivos con formato XM/JSON.

Se precisa que el objetivo de la implementación es tener en su totalidad los DataSources integrados, los DataSources no homologados que requieran desarrollo de conectores/colectores para su integración serán en la etapa de soporte en coordinación con el Banco sin incurrir en costo alguno según lo indicado en el numeral 3.1.10.7

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Se incluirá dicha precisión en el numeral 3.1.10.7 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 83

Consulta/Observación:

Dice: El conjunto de herramientas para definir la lógica para extraer, obtener, normalizar y categorizar los eventos no deberá utilizar ningún lenguaje de programación, JavaScript ni XML, para definir la lógica de recolección de eventos. Únicamente se permitirá el uso de expresiones regulares o REGEX para definir patrones de búsqueda de cadenas de texto.

Consulta:
Teniendo en cuenta que como parte del servicio es requerido el soporte de fabrica, los requerimientos integracion para fuentes no homologadas debe formar parte del servicio de soporte y realizada por el fabricante para evitar errores con estas integraciones. Por lo que se solicita que se modifique este requerimiento en donde solo se indique la necesidad de integrar fuentes nuevas no homologadas.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.12 **Literal:** 3.1.4.12 **Página:** 24
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

No se confirma.
La solución deberá proveer el conjunto de herramientas para definir la lógica para extraer, obtener, normalizar y categorizar los eventos y no deberá utilizar ningún lenguaje de programación, JavaScript ni XML, para definir la lógica de recolección de eventos. Únicamente se permitirá el uso de expresiones regulares o REGEX para definir patrones de búsqueda de cadenas de texto.

Precisando que el uso de estas herramientas será para todos los Data Sources homologados y no homologados.

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

Se incluirá la precisión en el numeral 3.1.4.12 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 84

Consulta/Observación:

Dice:
Soportar la recolección de eventos en modo agent-less, permitiendo la recolección de múltiples dispositivos desde un único componente de captura.

Consulta:
Confirmar que se refiere al colector del SIEM

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.13 Literal: 3.1.4.13 Página: 25

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

Análisis respecto de la consulta u observación:

"Se confirma.
El único componente de captura indicado en el numeral 3.1.4.13 es referido al colector del SIEM."

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 85

Consulta/Observación:

Dice:
Permitir configurar controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato.

Consulta:
Teniendo en cuenta que los eventos que están en el colector y no han pasado por los motores de correlación. El colector no debería establecer si un evento es de prioridad alta o baja ya que un evento de prioridad baja puede formar parte de un ataque silencioso. Por lo que se solicita poner como opcional este punto.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.18 **Literal:** 3.1.4.18 **Página:** 25

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

Análisis respecto de la consulta u observación:

Se precisa que los controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato será opcional, por lo que si el proveedor desea incluir soluciones que compriman la información a enviar y/o permitir configurar controles de uso de ancho de banda deberán de estar incluidos en el precio ofertado, precisando que no es obligatorio.

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

Se eliminará el numeral 3.1.4.18 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 86

Consulta/Observación:

Dice:
Permitir configurar el retraso voluntario en el envío de eventos a la solución de almacenamiento y administración de eventos basado en horarios, de tal forma que el colector de eventos guarde en su cache los eventos y envíe eventos con prioridad alta durante el horario configurado. Una vez finalizado el horario, se enviarán los eventos de más baja prioridad.

Consulta:
Teniendo en cuenta que los eventos que están en el colector y no han pasado por los motores de correlación. El colector no debería establecer si un evento es de prioridad alta o baja ya que un evento de prioridad baja puede formar parte de un ataque silencioso. Por lo que se solicita poner como opcional este punto.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.19 **Literal:** 3.1.4.19 **Página:** 25
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
La solución SIEM opcionalmente deberá permitir configurar el retraso voluntario en el envío de eventos a la solución de almacenamiento y administración de eventos basado en horarios, de tal forma que el colector de eventos guarde en su cache los eventos y envíe eventos con prioridad alta durante el horario configurado. Una vez finalizado el horario, se enviarán los eventos de más baja prioridad"

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Se eliminará el numeral 3.1.4.19 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 87

Consulta/Observación:

Dice:
Contar con múltiples perfiles de configuración , los cuales entrarán en funcionamiento en función de horarios preestablecidos.

Consulta:
Indicar que espera de estos perfiles y a que componentes deben ser implementados.

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.20 Literal: 3.1.4.20 Página: 25

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

Análisis respecto de la consulta u observación:

"Los perfiles de configuración se refieren a perfiles propios de la solución SIEM tales como monitoreo, administrador, superadmin, entre otros según cada fabricante y/o marca lo identifique.
Estos deben estar implementados con la consola de administración como componente principal."

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

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 88

Consulta/Observación:
Dice: Soportar un mecanismo de autenticación nativo además de soportar mecanismos alternativos como Microsoft Active Directory, LDAP y SAML .

Consulta:
Siendo mecanismos alternativos confirmar que el requerimiento es Microsoft Active Directory y/o LDAP y/o SAML

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.22 Literal: 3.1.4.22 Página: 25

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

Análisis respecto de la consulta u observación:
"No se confirma.
La solución SIEM deberá Soportar un mecanismo de autenticación nativo además de soportar mecanismos alternativos como Microsoft Active Directory, LDAP y SAML"

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

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 89

Consulta/Observación:

Dice:

Capacidad de ingestar identidades a partir de la conexión con Directorios LDAP, usado para realizar el análisis de comportamiento de los usuarios (capacidad UEBA).

Consulta:

Confirmar que es requerido como parte del servicio una licencia o funcionalidad de UEBA

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.26 Literal: 3.1.4.26 Página: 26

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

Análisis respecto de la consulta u observación:

"Se confirma.

El proveedor deberá proveer esta funcionalidad y/o licencia UEBA como parte de la solución SIEM."

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

Se incluirá la precisión en el numeral 3.1.4.26 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 90

Consulta/Observación:

Dice: Capacidad de abstraer datos a partir de los eventos base provenientes de los dispositivos, tales como realizar el cálculo de algún valor (por ejemplo, sumar o restar, redondear) o derivar algún dato particular (por ejemplo, día del mes, hora del día) que permita realizar un análisis de eventos basándose en el contexto (por ejemplo, generar una alerta si el evento se reporta en un horario no productivo a partir de la hora del evento reportado).

Consulta:Teniendo en cuenta que lo requerido son casos de usos específicos. Se solicita colocar como opcional la forma o métodos que el SIEM use para que pueda determinar la ofensa

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.33 Literal: 3.1.4.33 Página: 26

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

Análisis respecto de la consulta u observación:

"Se confirma.
Opcionalmente La solución SIEM deberá tener la capacidad de abstraer datos a partir de los eventos base provenientes de los dispositivos y/o aplicaciones.
Derivar algún dato particular (día del mes, hora del día) que permita realizar un análisis de eventos basándose en el contexto (por ejemplo, generar una alerta si el evento se reporta en un horario no productivo a partir de la hora del evento reportado)."

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Se eliminará el numeral 3.1.4.33 de la sección específica de las bases integradas, al ser opcional.

Entidad convocante :BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura :AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria :2

Objeto de contratación :Servicio

Descripción del objeto :Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 91

Consulta/Observación:

Dice:Permitir probar reglas de correlación sobre eventos históricos con una ventana de tiempo configurable, que permitan afinar puntualmente las reglas de correlación previa a su despliegue en ambientes productivos.

Consulta:
Teniendo en cuenta que el afinamiento o adaptabilidad del caso de uso se puede hacer con Machine Learning o Inteligencia artificial. Indicar si este item sea opcional

Acápite de las bases :Sección: Especifico Numeral: 3.1.4.34 Literal: 3.1.4.34 Página: 26

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

Análisis respecto de la consulta u observación:

"No se confirma.
La solución SIEM debe permitir probar reglas de correlación sobre eventos históricos con una ventana de tiempo configurable, que permitan afinar puntualmente las reglas de correlación previa a su despliegue en ambiente productivo sin que se vea afectada la continuidad operativa. "

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 92

Consulta/Observación:

Dice: Contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:

- ¿ Importancia del evento
- ¿ Criticidad del activo
- ¿ Vulnerabilidades asociadas
- ¿ Antecedentes sobre el origen, destino o ambos.

Consulta:
Teniendo en cuenta que los SIEM evalúan el riesgo con Machine learning e Inteligencia artificial, contextualizando el entorno del cliente. Se solicita que este ítem sea opcional.

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.35 **Literal:** 3.1.4.35 **Página:** 26

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

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que las necesidades del Banco requieren capacidad de contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:
- Importancia del evento
- Criticidad del activo
- Vulnerabilidades asociadas
Opcionalmente, se aceptara que la solución SIEM podrá evaluar el nivel de riesgo considerando el siguiente factor:
- Antecedentes sobre el origen, destino o ambos."

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

"No se confirma.
Se precisa que las necesidades del Banco requieren capacidad de contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:
- Importancia del evento
- Criticidad del activo
- Vulnerabilidades asociadas
Opcionalmente, se aceptara que la solución SIEM podrá evaluar el nivel de riesgo considerando el siguiente factor:
- Antecedentes sobre el origen, destino o ambos."

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 93

Consulta/Observación:

Dice: Proporcionar un módulo integrado para la gestión de casos (tickets) de seguridad permitiendo asociar eventos a acciones tales como enviar una notificación al equipo de operadores, abrir y asignar un caso a un usuario para su investigación a partir de la identificación de un incidente de seguridad.

Consulta:
Cuantos usuarios son requeridos

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.38 Literal: 3.1.4.38 Página: 26

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

Análisis respecto de la consulta u observación:

Se precisa que el numeral 3.1.4.38 tenga capacidad de permitir acceso mínimo a 8 usuarios para la característica descrita.

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

Se incluirá la precisión en el numeral 3.1.4.38 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 94

Consulta/Observación:

Dice: Contar con un flujo de trabajo (workflow) nativo, automatizado y con el manejo de niveles de escalamiento parametrizable para el manejo de incidentes de seguridad.

Consulta: Confirmar que lo requerido es la configuracion de PlayBooks

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.39 **Literal:** 3.1.4.39 **Página:** 27
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"Se confirma.
El numeral 3.1.4.39 deberá contar con un flujo de trabajo (workflow), automatizado y con el manejo de niveles de escalamiento parametrizable para el manejo de incidentes de seguridad. Siendo estas configuraciones de playbooks automatizados en la solución SIEM ya sea de la misma marca u otra plataforma."

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

Se incluirá la precisión en el numeral 3.1.4.39 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 95

Consulta/Observación:

Dice: Capacidad de enviar alertas vía email, traps SNMPv2 y SNMPv3, así como notificaciones directas a la consola de gestión.

Consulta:Considerar este punto como: Capacidad de enviar alertas vía emaily/o traps y/o SNMPv2 y/o SNMPv3, así como notificaciones directas a la consola de gestión

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.54 Literal: 3.1.4.54 Página: 28

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

Análisis respecto de la consulta u observación:

"Se confirma.
La solución SIEM deberá tener capacidad de enviar alertas vía email. Opcionalmente enviara alertas vía traps y/o SNMPv2 y/o SNMPv3, así como notificaciones directas a la consola de gestión."

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

Se actualizara el numeral 3.1.4.54 de la sección específica de las bases.

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 96

Consulta/Observación:

Dice: Permitir el monitoreo de los componentes de la solución, incluyendo estadísticas de uso de CPU, memoria, disco duro, estado de los servicios y estado de las conexiones.

Consulta: Confirmar que puede usarse una herramienta de un tercero para realizar esta actividad

Acápite de las bases : Sección: Especifico Numeral: 3.1.4.63 Literal: 3.1.4.63 Página: 28

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

Análisis respecto de la consulta u observación:

"No se confirma.

El proveedor deberá garantizar que su solución SIEM propuesta permita sea monitoreada en sus componentes on premise, incluyendo estadísticas de uso de CPU, memoria, disco duro, estado de los servicios y estado de las conexiones, con plataformas de monitoreo propias de la institución."

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

Se actualizara el numeral 3.1.4.63 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 97

Consulta/Observación:

Dice:
La solución de correlación de eventos deberá contar con funcionalidades integradas en la interfaz de administración gráfica para la definición, ejecución, calendarización y entrega automatizada de reportes ejecutivos y detallados en los siguientes formatos: PDF, CSV y HTML.

Consulta: Confirmar quepuede ser PDF y/o CSV y/o HTML

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.66 **Literal:** 3.1.4.66 **Página:** 29
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
La solución SIEM deberá contar con funcionalidades integradas en la interfaz de administración gráfica para la definición, ejecución, calendarización y entrega automatizada de reportes ejecutivos y detallados en los siguientes formatos: PDF, CSV y opcionalmente HTML."

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

Se actualizara el numeral 3.1.4.66 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 98

Consulta/Observación:

dice: La solución de correlación de eventos deberá contar con un mecanismo que optimice la generación de reportes sobre periodos largos de tiempo.

Consulta:
Por favor, definir "largos tiempos"

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.67 **Literal:** 3.1.4.67 **Página:** 29
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

Se precisa que la solución SIEM deberá contar con un mecanismo que optimice la generación de reportes sobre periodos largos de tiempo. Siendo estos periodos a considerar con una extensión mínima de 6 meses y personalizable según se requiera.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:
Se actualizara el numeral 3.1.4.67 de la sección específica de las bases.

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 99

Consulta/Observación:

Dice:
Contar con más de 350 reportes predefinidos y listos para ejecutarse en los rubros de cumplimiento, red, host, seguridad, almacenamiento.

Consulta:
Teniendo en cuenta que los reportes son consecuencia de los casos de usos. Confirmar que estos 350 reportes predeterminados sean opcional. Ya que si la entidad requiere reportes especificos y/o detallados en funcion a los casos de uso se pueden realizar acorde a la necesidad

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.4.78 **Literal:** 3.1.4.78 **Página:** 29

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

Análisis respecto de la consulta u observación:

"No se confirma.
Los reportes predefinidos no son referidos únicamente a casos de uso, también deberán ser en base a los eventos recibidos de todas las plataformas de seguridad integradas al SIEM."

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 100

Consulta/Observación:

Dice:
Se cuenta con 35 fuentes de datos (datasources)

Consulta: Confirmar que lo requerido es integrar solo los 35 data source o los 300 dispositivos sin tener en cuenta la cantidad de EPS generados. Indicado en el 3.1.4.8

Acápite de las bases : **Sección:** Especifico **Numeral:** 3.1.10 **Literal:** 3.1.10 **Página:** 32
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
Se precisa que los 300 dispositivos mencionados en el numeral 3.1.4.8 esta referido a la capacidad de integración por defecto de la solución SIEM, sin necesidad de incurrir en desarrollo de integración.
Esto no esta referido al numero de Data Sources a integrar durante la etapa de implementación en la cual se indicara una lista con los 35 Data Sources de manera referencial para este propósito, pudiéndose modificar durante la etapa de soporte sin que esto afecte a la cantidad de EPS indicados en el numeral 3.1.2.4"

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

Entidad convocante :	BANCO CENTRAL DE RESERVA DEL PERÚ
Nomenclatura :	AS-SM-10-2024-BCRPLIM-2
Nro. de convocatoria :	2
Objeto de contratación :	Servicio
Descripción del objeto :	Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 101

Consulta/Observación:

Dice: Las configuraciones requeridas en los datasources para su integración con el componente colector, serán responsabilidad del BCRP.

Consulta: Confirmar que la integracion de los datasource no es un entregable de la etapa de implementación y si de la etapa de soporte

Acápite de las bases : **Sección:** Especifico **Numeral:** 10.1.10.4 **Literal:** 10.1.10.4 **Página:** 32
Artículo y norma que se vulnera (En el caso de Observaciones):

Análisis respecto de la consulta u observación:

"No se confirma.
Lo indicado en el numeral 3.1.10.6 es una necesidad de continuidad operativa.
El objetivo al culminar la implementación es tener en su totalidad los DataSources indicados en el numeral 3.1.10.1, Los nuevos Data Sources durante el periodo del servicio, se integraran en la etapa de soporte en coordinación con el Banco."

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

null

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 102

Consulta/Observación:

Dice:
Configuración del SIEM (Sistema de Gestión de Correlación de Eventos para la Detección, Investigación y Respuesta frente a Amenazas
Cosulta:
Confirmar que la configuracion de casos de uso personalizados no forma parte del entregable de la etapa de implementacion.

Acápite de las bases : Sección: Especifico Numeral: 10.1.10.7 Literal: 10.1.10.7 Página: 32

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

Análisis respecto de la consulta u observación:

Se confirma.
La configuración de casos de uso personalizados no forma parte de la etapa de implementación. Sin embargo serán entregables en la etapa de soporte.

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

Dicha precisión se incluirá en las bases integradas numeral 3.1.10.7 de la sección específica de las bases

Entidad convocante : BANCO CENTRAL DE RESERVA DEL PERÚ

Nomenclatura : AS-SM-10-2024-BCRPLIM-2

Nro. de convocatoria : 2

Objeto de contratación : Servicio

Descripción del objeto : Contratación del servicio de suscripciones de un SIEM (Sistema de gestión de correlación de eventos para la detección, investigación y respuesta frente a amenazas avanzadas)

Ruc/código :	20477830626	Fecha de envío :	07/03/2024
Nombre o Razón social :	ETEK INTERNATIONAL CORPORATION SUCURSAL PERU	Hora de envío :	23:52:15

Consulta: Nro. 103

Consulta/Observación:

Confirmar que el desarrollo de conectores para la integracion de datasource formaría parte de la etapa de soporte y no de la etapa de implementacion

Acápite de las bases : Sección: Especifico Numeral: 10.1.10.7 Literal: 10.1.10.7 Página: 32

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

Análisis respecto de la consulta u observación:

"Se confirma.
El objetivo de la implementación es tener en su totalidad los DataSources integrados, los nuevos DataSources que requieran desarrollo de conectores/colectores para su integración serán durante la etapa de soporte en coordinación con el Banco."

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

Dicha precisión se incluirá en las bases integradas numeral 3.1.10.7 de la sección específica de las bases