

# PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

Ruc/código : 20553935165

Nombre o Razón social : HYNET S.A.C.

Fecha de envío : 15/01/2025

Hora de envío : 17:18:14

## Observación: Nro. 1

### Consulta/Observación:

Con respecto al plazo de instalación y puesta en funcionamiento. En aras de cumplir con los plazos establecidos por la Entidad y no incurrir en penalidades, solicitamos a la Entidad tenga bien en considerar un plazo de cuarenta (40) días calendario. El presente concurso lleva componentes de hardware que deben ser importados desde el extranjero y esto puede tomar mas de 30 días.

Acápíte de las bases : Sección: Especifico Numeral: 1.8 Literal: - Página: 14

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

Principios que rigen las contrataciones del Estado

### Análisis respecto de la consulta u observación:

En atención a la observación formulada por el postor y con el ánimo de fomentar la mayor participación de postores, se acoge la observación de tal manera que el plazo de entrega de la licencia de suscripción se modificará de diez (10) días calendario a cuarenta (40) días calendario, contabilizado a partir del día siguiente de suscrito el contrato, ello con la finalidad de que los postores puedan cumplir con el requerimiento dentro de los plazos.

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

#### 6.1.1 PRESTACIÓN PRINCIPAL

El plazo total de la prestación principal es de cincuenta (50) días calendario, contados a partir del día siguiente de la firma del contrato, divididos de la siguiente manera:

#### Plazo de entrega de la licencia de suscripción

La entrega de la licencia de suscripción del servicio de gestión de eventos de seguridad en nube será realizado en un plazo no mayor a cuarenta (40) días calendario, contabilizado a partir del día siguiente de suscrito el contrato, y deberá ser remitido al correo electrónico [usrsegurinf@mtc.gob.pe](mailto:usrsegurinf@mtc.gob.pe), el mismo que es administrado por la Oficina de Infraestructura y Seguridad Informática de la Oficina General de Tecnología de la Información.

#### Plazo de instalación y puesta en funcionamiento

La instalación y puesta en funcionamiento de la solución ofertada, será en un plazo no mayor a diez (10) días calendarios, contados a partir del día siguiente de la entrega de la licencia de suscripción.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |              |                  |            |
|-------------------------|--------------|------------------|------------|
| Ruc/código :            | 20553935165  | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | HYNET S.A.C. | Hora de envío :  | 17:18:14   |

Consulta: Nro. 2

Consulta/Observación:

Con respecto a la acreditación de las especificaciones técnicas. solicitamos que las hojas de datos y/o datasheets y/o hojas técnicas y/o brochure que acrediten las características técnicas indicadas en el cuadro n° 01 puedan ser presentadas en idioma ingles o español. Esto en virtud de que se trata de información técnica complementaria por lo cual el postor es responsable de la exactitud y veracidad de dichos documentos.

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

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

Análisis respecto de la consulta u observación:

En atención a la consulta formulada por el postor, se aclara que tal cual como se indica en los términos de referencia: "cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado".

En cumplimiento con lo dispuesto en el art 59 del RLCE, es necesario que la documentacion solicitada en el literal b) del numeral 2.2.1.1 Documentos para la admisión de la oferta de las bases se encuentre en idioma español, puesto que es informacion que servirá como requisito de admisibilidad.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |              |                  |            |
|-------------------------|--------------|------------------|------------|
| Ruc/código :            | 20553935165  | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | HYNET S.A.C. | Hora de envío :  | 17:18:14   |

Consulta: Nro. 3

Consulta/Observación:

Favor de indicar el formato del Anexo 6, este no se encuentra presente en las bases.

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

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

Análisis respecto de la consulta u observación:

Se aclara la consulta y se incorporara el Anexo N° 6 en las Bases Integradas

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

Se adjunta:

(...)

Anexo N° 6

(¿)

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |              |                  |            |
|-------------------------|--------------|------------------|------------|
| Ruc/código :            | 20553935165  | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | HYNET S.A.C. | Hora de envío :  | 17:29:25   |

Observación: Nro. 4

Consulta/Observación:

Con respecto al documento de Términos de Referencia, en la sección de Aspectos Generales de la Prestación Principal se solicita un (01) colector del tipo appliance. Sin embargo, dado los plazo para la entrega de licencia e implementación tan cortos, imposibilitan el entregar el servicio en el plazo indicado, por lo que solicitamos a la Entidad tenga bien en aceptar propuesta que incluyan equipo colectores en formato de maquina virtual, para lo cual el proveedor deberá brindar los recursos de hardware necesario para su funcionamiento.

Acápite de las bases : Sección: Anexos Numeral: 5.2.1 Literal: - Página: 2

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

Principios que rigen las contrataciones

Análisis respecto de la consulta u observación:

En atención a la observación, y con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente y se aceptará colectores virtuales que cumplan como mínimo con las siguientes características:

- ¿ Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- ¿ Procesador de 8 núcleos mínimo.
- ¿ Memoria RAM de 16 GB mínimo.
- ¿ Espacio en disco de 3.5 TB mínimo.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 1 "Aspectos generales", literal h) de los Términos de Referencia lo siguiente:

h) Deberá incluir (01) un colector con las siguientes características mínimas:

¿ Deberá ser un hardware de propósito específico o virtualizado considerando incluir hardware de primer uso y el software licenciado necesario para el correcto funcionamiento de la solución.

En caso se trate de componente basado en hardware, este debe cumplir con las siguientes características mínimas:

- ¿ Contar mínimo con 04 interfaces RJ45 de 1GE.
- ¿ Capacidad mínima para 3.5 TB.

En caso se trate de colectores virtualizados, este debe cumplir con las siguientes características mínimas:

- ¿ Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- ¿ Procesador de 8 núcleos mínimo.
- ¿ Memoria RAM de 16 GB mínimo.
- ¿ Espacio en disco de 3.5 TB mínimo.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |              |                  |            |
|-------------------------|--------------|------------------|------------|
| Ruc/código :            | 20553935165  | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | HYNET S.A.C. | Hora de envío :  | 17:29:25   |

Consulta: Nro. 5

Consulta/Observación:  
Con respecto a la Formación Académica del Jefe de Proyectos, solicitamos que pueda aceptar personal de la carrera de Ingeniería Empresarial y de Sistemas

Acápíte de las bases : Sección: Especifico Numeral: 8.2.1 Literal: ii Página: 12

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

Análisis respecto de la consulta u observación:  
En atención a la consulta y con el ánimo de fomentar la mayor participación de postores, se aclara y se realizará la precisión en los TDR, de tal manera que el texto deberá indicar: Ingeniería Empresarial y de Sistemas.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:  
Se precisa en el literal a) del numeral 8.2.1 de los Términos de Referencia lo siguiente respecto al JEFE DE PROYECTO  
Experiencia:  
Profesional titulado en la carrera de Ingeniería de Sistemas, o Ingeniería Informática, o Ingeniería Electrónica, o Ingeniería de Telecomunicaciones, o Ingeniería de Redes, o Ingeniería de Seguridad y Auditoría Informática, o Ingeniería Empresarial y de Sistemas.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 6**

**Consulta/Observación:**

DICE:  
2.2.1.1. Documentos para la admisión de la oferta  
b) El postor deberá acreditar con hojas de datos y/o datasheets y/u hojas técnicas y/o brochure, el cumplimiento de las características indicadas en el Cuadro N° 01 de los Términos de Referencia, ¿Características técnicas para acreditar¿ en idioma español. Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado.

OBSERVACION:  
De acuerdo con lo establecido en el Decreto Legislativo N° 1017, Artículo 4, que regula los principios que rigen las contrataciones del Estado donde se debe incluir regularizaciones o tratamientos que fomenten la más amplia, objetiva e imparcial concurrencia, pluralidad y participación de postores. que establece la obligación de acreditar el cumplimiento de las características técnicas a través de hojas de datos, datasheets, hojas técnicas o brochures, ya que esta especificación parece estar dirigida a una sola marca fabricante, lo cual restringe la participación de postores y contraviene el principio de concurrencia, pluralidad e imparcialidad promovido por la ley.

Proponemos que se permita la inclusión de una carta del fabricante que garantice el cumplimiento de las características técnicas como parte de los documentos requeridos para la admisión de la oferta. Esta carta proporcionaría una validación adicional por parte del proveedor oficial del producto, lo que fortalecería la garantía de que los requisitos técnicos establecidos en los Términos de Referencia sean cumplidos, sin limitar la participación de otros postores que puedan ofrecer soluciones equivalentes o competitivas.

**Acápite de las bases : Sección: Especifico      Numeral: 2      Literal: 2.2.1      Página: 18**  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

Decreto Legislativo N° 1017, Artículo 4  
**Análisis respecto de la consulta u observación:**

No se acoge la observación, la carta de fabricante para sustentar los solicitado en el literal b) del numeral 2.2.1.1 Documentos para la admisión de la oferta, puesto que este documento no podrían presentarlo todos los postores. Cualquier solucion equivalente o competitiva deberia poder sustentar el cumplimiento de los requisitos tecnicos minimos con los documentos solicitados.

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

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Consulta: Nro. 7**

**Consulta/Observación:**  
DICE:  
Dos (02) Especialistas.  
Con experiencia mínima de cinco (05) años en implementación y/o soporte y/o mantenimiento de soluciones de gestión de eventos.

**CONSULTA:**  
De acuerdo con el requerimiento actual que establece una experiencia mínima de cinco (05) años para el Jefe de Proyecto, solicitamos amablemente que dicho criterio sea reconsiderado y alineado conforme a las siguientes observaciones:

**Propuesta:**  
"Con experiencia mínima de dos (02) años en la implementación, soporte, mantenimiento de soluciones de gestión de eventos y/o operación de soluciones SIEM en la nube y/o plataformas de gestión de eventos de seguridad."

Esta modificación busca ampliar la participación de profesionales cualificados, manteniendo la calidad y experiencia necesaria para el desarrollo exitoso de la solución contratada.

**Acápite de las bases :    Sección: Especifico    Numeral: 3    Literal: 3.2    Página: 24**

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

**Análisis respecto de la consulta u observación:**  
En atención a la consulta formulada por el postor, se aclara que la entidad precisa que este requerimiento sea gerenciado con personal de basta experiencia en soluciones de esta naturaleza, dado de que se trata de servicios críticos. Por lo tanto, no se acoge la consulta.

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

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Consulta: Nro. 8**  
**Consulta/Observación:**  
DICE:  
a) Un (01) JEFE DE PROYECTO

Formación académica:  
Debe contar con certificación en ISO 20000 Gestión de Servicios de TI.

CONSULTA:  
Solicitamos considerar como opcional el requisito de certificación en ISO 20000 Gestión de Servicios de TI para el Jefe de Proyecto o, en su defecto, aceptar una Especialización avanzada en Gerencia de Proyectos y Calidad, quedando lo siguiente:

Propuesta:  
"Debe contar con certificación en ISO 20000 Gestión de Servicios de TI y/o Especialización avanzada en Gerencia de Proyectos y Calidad."

Esto permitiría valorar perfiles con competencias estratégicas y conocimientos aplicables a la gestión de proyectos tecnológicos, garantizando una conducción eficiente de la solución propuesta.

**Acápite de las bases :    Sección: Especifico    Numeral: 8    Literal: 8.2    Página: 12**  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

**Análisis respecto de la consulta u observación:**  
En atención a la consulta formulada por el postor, se aclara que no especifica como acreditará la especialización avanzada en Gerencia de Proyectos y Calidad. Por lo tanto, no se acoge la propuesta,  
**Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:**  
null



Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 9**

**Consulta/Observación:**

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

1. Aspectos Generales.
- h) Deberá incluir (01) un colector con las siguientes características mínimas:
- Deberá ser un hardware de propósito específico. No se aceptarán colectores virtualizados.
  - Capacidad mínima para 3.5 TB
  - Contar mínimo con 04 interfaces RJ45 de 1GE.

OBSERVACION:

El requerimiento de que el colector "Deberá ser un hardware de propósito específico. No se aceptarán colectores virtualizados" limita injustificadamente la participación de oferentes. Según lo especificado en el siguiente enlace: <https://www.fortinet.com/lat/products/siem/fortisiem> (FortiSIEM de Fortinet), esta es la única solución que cuenta con colectores en hardware de propósito específico, lo cual direcciona el proceso hacia una sola marca, contraviniendo el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la competencia y la igualdad de condiciones entre los postores.

Permitir colectores virtualizados con capacidades técnicas equivalentes no solo ampliaría la pluralidad de oferentes, sino que garantizaría una mayor flexibilidad y adaptabilidad de las soluciones propuestas.

Acápite de las bases : Sección: Especifico Numeral: 5 Literal: 5.2.1 Página: 2

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

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, y con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente ya que actualmente existen marcas que proveen el SIEM y sus colectores en hardware físico, no obstante, se aceptará que el colector pueda ser virtual. En caso de ofertar un colector virtual, el Postor debe incluir en su propuesta hardware de primer uso y el software licenciado necesario para el correcto funcionamiento de la solución que cumpla además con las siguientes características técnicas:

- ¿ Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- ¿ Procesador de 8 núcleos mínimo.
- ¿ Memoria RAM de 16 GB mínimo.
- ¿ Espacio en disco de 3.5 TB mínimo.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas - numeral 1 "Aspectos generales", literal h) de los Términos de Referencia lo siguiente:

h) Deberá incluir (01) un colector con las siguientes características mínimas:

- ¿ Deberá ser un hardware de propósito específico o virtualizado considerando incluir hardware de primer uso y el software licenciado necesario para el correcto funcionamiento de la solución.

En caso se trate de componente basado en hardware, este debe cumplir con las siguientes características mínimas:

- ¿ Contar mínimo con 04 interfaces RJ45 de 1GE.
- ¿ Capacidad mínima para 3.5 TB.

En caso se trate de colectores virtualizados, este debe cumplir con las siguientes características mínimas:

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

---

- ¿ Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- ¿ Procesador de 8 núcleos mínimo.
- ¿ Memoria RAM de 16 GB mínimo.
- ¿ Espacio en disco de 3.5 TB mínimo.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 10**

**Consulta/Observación:**

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

1. Aspectos Generales.

h) Deberá incluir (01) un colector con las siguientes características mínimas:

- Deberá ser un hardware de propósito específico. No se aceptarán colectores virtualizados.
- Capacidad mínima para 3.5 TB
- Contar mínimo con 04 interfaces RJ45 de 1GE.

**OBSERVACION:**

El requerimiento de que el colector "Deberá ser un hardware de propósito específico. No se aceptarán colectores virtualizados" limita injustificadamente la participación de oferentes. Según lo especificado en el siguiente enlace: <https://www.fortinet.com/lat/products/siem/fortisiem> (FortiSIEM de Fortinet), esta es la única solución que cuenta con colectores en hardware de propósito específico, lo cual direcciona el proceso hacia una sola marca, contraviniendo el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la competencia y la igualdad de condiciones entre los postores. Solicitamos reconsiderar el requisito y proponemos modificar el requisito para aceptar colectores virtualizados, con las siguientes especificaciones mínimas:

- Procesador de 4 núcleos mínimo.
- Memoria RAM de 8 GB mínimo.
- Espacio en disco de 512 GB mínimo.

Agradecemos la evaluación de esta solicitud para fomentar la competitividad y eficiencia en la implementación del sistema de gestión de información y eventos de seguridad.

**Acápite de las bases :**    **Sección:** Especifico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 2

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

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, y con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente la observación y se aceptará que en caso de incluir en su oferta un colector virtual, este debe poseer al menos las siguientes características:

- Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- Procesador de 8 núcleos mínimo.
- Memoria RAM de 16 GB mínimo.
- Espacio en disco de 3.5 TB mínimo.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas - numeral 1 "Aspectos generales", literal h) de los Términos de Referencia lo siguiente:

h) Deberá incluir (01) un colector con las siguientes características mínimas:

¿ Deberá ser un hardware de propósito específico o virtualizado considerando incluir hardware de primer uso y el software licenciado necesario para el correcto funcionamiento de la solución.

En caso se trate de componente basado en hardware, este debe cumplir con las siguientes características mínimas:

- ¿ Contar mínimo con 04 interfaces RJ45 de 1GE.
- ¿ Capacidad mínima para 3.5 TB.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

---

En caso se trate de colectores virtualizados, este debe cumplir con las siguientes características mínimas:

- ¿ Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- ¿ Procesador de 8 núcleos mínimo.
- ¿ Memoria RAM de 16 GB mínimo.
- ¿ Espacio en disco de 3.5 TB mínimo.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 11**  
**Consulta/Observación:**  
DICE:  
CARACTERISTICAS TÉCNICAS MÍNIMAS

1. Aspectos Generales.  
g) La solución estará licenciada con al menos cien (100) agentes avanzados para servers Linux/Windows y cincuenta (50) agentes UEBA.

OBSERVACION:  
Solicitamos la exclusion o reconsiderar el siguiente requisito técnico:

Observamos que la necesidad de agentes dedicados exclusivamente para UEBA puede resultar innecesaria, ya que diversas plataformas modernas de SIEM integran de manera nativa la funcionalidad de análisis de comportamiento sin requerir agentes adicionales. En estas soluciones, un único agente es capaz de soportar tanto las funciones del SIEM como las de UEBA, optimizando recursos y costos para la entidad.

Requerir agentes dedicados implica costos adicionales y complejidad operativa, lo que no necesariamente aporta valor agregado cuando existen tecnologías que suplen esta necesidad de manera eficiente.

**Acápite de las bases :**    **Sección:** Especifico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 2

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

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación, y con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente y se aceptará que la solución brinde UEBA como funcionalidad nativa o a través de licenciamiento con soporte de al menos cien (100) agentes avanzados para servers Linux/Windows y cincuenta (50) agentes UEBA.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas - numeral 1 "Aspectos generales", literal g) de los términos de referencia lo siguiente:

g) La solución debera brindar UEBA sea como funcionalidad nativa o a traves de licenciamiento con soporte de al menos cien (100) agentes avanzados para servers Linux/Windows y cincuenta (50) agentes UEBA.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 12**

**Consulta/Observación:**

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

2. Características

2.1 Análisis de seguridad en tiempo real

b) Realizar un descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad, manteniendo una base de datos de configuraciones (CMDB) siempre actualizada mediante redescubrimientos programados.

**OBSERVACION:**

El requerimiento de incluir usuarios en el proceso de descubrimiento y categorización podría no ser una práctica óptima, ya que puede generar problemas como el aprendizaje de cuentas de servicio, que corresponden a procesos automáticos y no a usuarios reales. Esto puede derivar en un incremento de falsos positivos y en una asignación poco fiable de identidades, afectando negativamente la precisión del análisis de seguridad y la detección de amenazas.

Según lo especificado en el siguiente enlace: <https://www.fortinet.com/lat/products/siem/fortisiem> (FortiSIEM de Fortinet), esta solución parece ser la única que aborda el descubrimiento y categorización de usuarios de la manera especificada en los términos del proceso. Esto direcciona el requerimiento hacia una marca específica, lo cual contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que establece la promoción de la libre competencia y la igualdad de condiciones entre postores.

**Acápite de las bases : Sección: Especifico      Numeral: 5      Literal: 5.2.1      Página: 2**

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

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente y se aclara que el descubrimiento y la categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad dentro de una base de datos de configuración (CMDB, Configuration Management Database) son características clave para una gestión centralizada de TI y la integración con herramientas de seguridad como un SIEM. Sin perjuicio de ello, y con el ánimo de fomentar la mayor participación de postores, se aceptará que el descubrimiento y categorización se realice mediante una herramienta complementaria al SIEM, que el postor deberá incluirlo como parte de su oferta.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 2. Características , numeral 2.1 Análisis de seguridad en tiempo real de los términos de referencia lo siguiente:

b) Realizar un descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad, manteniendo una base de datos de configuraciones (CMDB) directamente a través del SIEM o integrándose con sistemas CMDB siempre actualizada mediante redescubrimientos programados. Los sistemas CMDB deberán ser incluidos en la propuesta del postor.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 13**  
**Consulta/Observación:**  
DICE:  
CARACTERISTICAS TÉCNICAS MÍNIMAS

2. Características

2.1 Análisis de seguridad en tiempo real  
e) La solución debe integrarse a un asistente virtual con inteligencia artificial (IA) generativa (OpenAI) que permita guiar y potenciar las acciones de los analistas de seguridad durante la investigación de incidentes, búsqueda de amenazas, respuesta y otras opciones.

**OBSERVACION:**  
El requerimiento técnico que especifica a OpenAI como la única tecnología generativa de inteligencia artificial limita innecesariamente la pluralidad del proceso de licitación, restringiendo la participación de soluciones equivalentes en el mercado. Esto contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores.  
  
De acuerdo con la información disponible en el documento oficial de Fortinet: FortiSIEM Data Sheet, esta tecnología aborda funcionalidades avanzadas con capacidades similares o equivalentes a las especificadas, lo que sugiere que el requerimiento podría estar direccionado hacia una solución específica.

Proponemos que este requerimiento sea revisado para permitir el uso de cualquier tecnología generativa de inteligencia artificial que cumpla con las funciones descritas, como asistentes virtuales con IA generativa de diversas marcas o fabricantes.

**Acápite de las bases :    Sección: Especifico    Numeral: 5    Literal: 5.2.1    Página: 3**  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**  
En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge la propuesta y se aceptará que el postor incluya en su oferta la tecnología de inteligencia artificial generativa OpenAI o similar.

**Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:**  
Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 2. Características , numeral 2.1 Análisis de seguridad en tiempo real de los términos de referencia lo siguiente:  
e) La solución debe integrarse a un asistente virtual con inteligencia artificial (IA) generativa (OpenAI) o similar, que permita guiar y potenciar las acciones de los analistas de seguridad durante la investigación de incidentes, búsqueda de amenazas, respuesta y otras opciones.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 14**

**Consulta/Observación:**

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

## 2. Características

### 2.1 Análisis de seguridad en tiempo real

g) Correlación de eventos SOC/NOC, para disponer en un único punto de gestión de datos no sólo de eventos de seguridad, sino también de:

- o Rendimiento y disponibilidad
- o CPU, memoria y almacenamiento.
- o Detección de cambios de configuración.
- o Monitorización de transacciones sintéticas.
- o Cuadros de mando dinámicos.

#### OBSERVACION:

Solicitamos que el siguiente requisito sea considerado como opcional dentro de las características técnicas mínimas, ya que incluye elementos que no están directamente relacionados con el alcance principal de un sistema de gestión de información y eventos de seguridad (SIEM). La correlación de eventos SOC/NOC relacionada con aspectos como rendimiento, monitorización de transacciones sintéticas o cuadros de mando dinámicos no guarda un relacionamiento directo con la naturaleza principal del servicio requerido.

Este tipo de requisitos podría estar orientado a una solución específica, como lo describe el artículo de FortiSIEM en <https://fortixpert.blogspot.com/2021/10/fortisiem-metricas-de-rendimiento-en.html>. Si este requisito no se considera opcional, solicitamos que se suprima completamente, para permitir la participación de soluciones líderes del mercado que puedan ofrecer una mayor flexibilidad y competitividad, beneficiando a la Entidad y asegurando que el proceso de licitación sea inclusivo para diversas soluciones tecnológicas.

**Acápite de las bases :** Sección: Especifico      Numeral: 5      Literal: 5.2.1      Página: 3

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

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia

#### Análisis respecto de la consulta u observación:

En atención a la observación, se precisa que es importante que un SIEM correlacione eventos de seguridad y eventos de red para una gestión eficaz de la seguridad en cualquier infraestructura de TI. Esta capacidad permite identificar patrones, amenazas, y anomalías que serían difíciles de detectar si los eventos se analizarán de manera aislada.

Asimismo, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento, evidenciando en ese sentido que existe pluralidad de marcas de soluciones SIEM que permiten correlacionar datos de la red y eventos de seguridad. Por lo tanto, no se acoge la observación.

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

null



Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

Consulta: Nro. 15

Consulta/Observación:

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

2. Características

2.1 Análisis de seguridad en tiempo real

i) Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad.

CONSULTA:

Solicitamos amablemente que se considere como opcional el siguiente requisito. Es importante señalar que el análisis de rendimiento de aplicaciones y sistemas no siempre está directamente relacionado con la identificación de problemas de seguridad, ya que el enfoque principal de la solución es la detección y respuesta ante amenazas de seguridad. Por lo tanto, sugerimos que este análisis se considere opcional, ya que la inclusión de este requisito puede no ser esencial para todas las soluciones que cumplen con los requisitos principales de seguridad. Esto también permite una mayor flexibilidad en la oferta de soluciones.

Acápite de las bases :    Sección: Especifico    Numeral: 5    Literal: 5.2.1    Página: 3

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

Análisis respecto de la consulta u observación:

En atención a la consulta, se aclara que se requiere el análisis en tiempo real y rendimiento para detectar amenazas en tiempo oportuno y poder mitigarlas o corregirlas. Por lo tanto, no se acoge la consulta.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

Consulta: Nro. 16

Consulta/Observación:

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

2. Características

2.3 Informes de cumplimiento

a) Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls.

CONSULTA:

Solicitamos que se considere como opcional la inclusión de los SANS Critical Controls, específicamente en el punto relacionado.

Si bien los SANS Critical Controls son una herramienta para la mejora de la ciberseguridad, consideramos que su aplicación no es esencial. En este sentido, sugerimos que se permita a los proveedores ofrecer alternativas válidas y ajustadas a las normativas solicitadas (PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13) sin necesidad de integrar de manera obligatoria los controles específicos de SANS.

Acápite de las bases : Sección: Específico      Numeral: 5      Literal: 5.2.1      Página: 3

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

Análisis respecto de la consulta u observación:

En atención a la consulta formulada, se aclara que se requiere de una solución que posea controles SANS Critical Control para brindar los máximos beneficios y mejorar la postura frente a las amenazas.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 17**  
**Consulta/Observación:**  
DICE:  
CARACTERISTICAS TÉCNICAS MÍNIMAS

2. Características
- 2.4 Supervisión del rendimiento
- a) Monitor de métricas de sistema.
  - b) Estado del sistema a través de SNMP, WMI, PowerShell.
  - c) Estado de aplicaciones a través de JMX, WMI, PowerShell.
  - d) Monitoreo de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster.
  - e) Monitorización del rendimiento de aplicaciones a medida: Bases de datos - Oracle, MS SQL, MySQL a través de JDBC.
  - f) Análisis de flujo y rendimiento de la aplicación Netflow, SFlow, Cisco AVC e IPFIX.
  - g) Posibilidad de agregar métricas personalizadas.
  - h) Métricas de base y detección de desviaciones.

**OBSERVACION:**  
Solicitamos que los puntos mencionados sean considerados opcionales, el requisito relacionado con la "Supervisión del cambio de configuraciones en tiempo real" restringe la participación de soluciones equivalentes en el mercado al especificar características técnicas que parecen estar dirigidas a una sola marca incumbente, Tal como se detalla en el siguiente enlace <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf>. Este tipo de especificación contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores y fabricantes. La descripción del punto implica una orientación hacia productos específicos, lo que limita innecesariamente el acceso de otros proveedores que puedan ofrecer soluciones tecnológicamente equivalentes o superiores. Por tanto, solicitamos que el requerimiento sea considerado opcional o suprimido en su totalidad para permitir la participación de una gama más amplia de soluciones, promoviendo la competencia y garantizando que el proceso de contratación se mantenga dentro de los principios de igualdad de oportunidades.

**Acápite de las bases :**    **Sección:** Especifico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 4

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

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente la observación, ya que es fundamental que un SIEM monitoree el estado de los equipos, rendimiento y la disponibilidad de los servicios porque esto contribuye directamente a la seguridad, el rendimiento, y la continuidad operativa de la infraestructura de TI. Por lo tanto, se aceptarán soluciones que supervisen a menos cinco (05) de las características listadas en los términos de referencia.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 2. Características, numeral 2.4 Supervisión del rendimiento de los términos de referencia lo siguiente:  
Debe soportar al menos cinco (05) de las supervisiones solicitadas a continuación:

- a) Monitor de métricas de sistema.
- b) Estado del sistema a través de SNMP, WMI, PowerShell.
- c) Estado de aplicaciones a través de JMX, WMI, PowerShell.
- d) Monitoreo de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster.
- e) Monitorización del rendimiento de aplicaciones a medida: Bases de datos - Oracle, MS SQL, MySQL a través de JDBC.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

---

- f) Análisis de flujo y rendimiento de la aplicación Netflow, SFlow, Cisco AVC e IPFIX.
- g) Posibilidad de agregar métricas personalizadas.
- h) Métricas de base y detección de desviaciones.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 18**

**Consulta/Observación:**

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

2. Características

- 2.5 Supervisión del cambio de configuraciones en tiempo real
- a) Recopilar archivos de configuración de red, almacenados en un repositorio versionado.
  - b) Recopilar las versiones de software instaladas, almacenadas en un repositorio versionado.
  - c) Detección automatizada de cambios en la configuración de la red y el software instalado.
  - d) Detección automatizada de cambios de archivos y carpetas -Windows y Linux con detalles técnicos.
  - e) Detección automatizada de cambios desde un archivo de configuración.
  - f) Posibilidad de detección automatizada de cambios en el registro de Windows a través de agente.

**OBSERVACION:**

Solicitamos que los puntos mencionados sean considerados opcionales, el requisito relacionado con la "Supervisión del cambio de configuraciones en tiempo real" restringe la participación de soluciones equivalentes en el mercado al especificar características técnicas que parecen estar dirigidas a una sola marca incumbente, Tal como se detalla en el siguiente enlace <https://fortixpert.blogspot.com/2021/10/fortisiem-metricas-de-rendimiento-en.html>. Este tipo de especificación contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores y fabricantes. La descripción del punto implica una orientación hacia productos específicos, lo que limita innecesariamente el acceso de otros proveedores que puedan ofrecer soluciones tecnológicamente equivalentes o superiores. Por tanto, solicitamos que el requerimiento sea considerado opcional o suprimido en su totalidad para permitir la participación de una gama más amplia de soluciones, promoviendo la competencia y garantizando que el proceso de contratación se mantenga dentro de los principios de igualdad de oportunidades.

**Acápite de las bases : Sección: Especifico      Numeral: 5      Literal: 5.2.1      Página: 4**

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

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación se menciona que es importante que un SIEM supervise los cambios en la configuración de los equipos monitoreados, ya que dichos cambios pueden ser indicadores de actividades maliciosas o no autorizadas, como ataques internos, compromisos de cuentas privilegiadas, o errores administrativos que pueden comprometer la seguridad de una red. La supervisión del cambio de configuraciones permite detectar eventos que podrían ser indicativos de ataques en curso o futuras vulnerabilidades, además de facilitar el cumplimiento normativo al documentar las configuraciones de los sistemas.

Asimismo, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento, también precisar que actualmente existen diversas marcas de soluciones SIEM que permiten monitorear cambios en las configuraciones de sus equipos monitoreados. Por lo tanto, no se acoge la observación.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

Consulta: Nro. 19

Consulta/Observación:

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

3 Contexto del dispositivo y de la aplicación.

c) Servidores, incluyendo Windows, Linux, AIX, HP UX.

CONSULTA:

Solicitamos amablemente que se considere como opcional la inclusión de HP UX, específicamente en el punto relacionado con los servidores soportados (Windows, Linux, AIX, HP UX).

Aunque HP UX es una plataforma válida, sugerimos que se considere su uso de manera opcional, esto permitiría una mayor flexibilidad y eficiencia en la implementación, además de reducir la necesidad de agentes adicionales, que no soporta HP UX.

Acápite de las bases : Sección: Especifico Numeral: 5 Literal: 5.2.1 Página: 4

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

Análisis respecto de la consulta u observación:

En atención a la consulta formulada y con el ánimo de fomentar la mayor cantidad de postores se aclara que se aceptará como opcional el tipo de servidor HP UX.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 3. Contexto del dispositivo y de la aplicación , literal c) de los términos de referencia lo siguiente:

c) Servidores, incluyendo Windows, Linux, AIX. Opcionalmente HP UX.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

Consulta: Nro. 20

Consulta/Observación:

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

4 Recolección de log.

d) La solución debe soportar agentes de Windows, que puedan proporcionar una colección de eventos altamente escalable y rica, incluida la supervisión de integridad de archivos, los cambios de software instalados y la supervisión de cambios en el registro.

CONSULTA:

Solicitamos amablemente que se considere como opcional el punto relacionado con la recolección de logs. Si bien entendemos que los agentes de Windows pueden ser útiles para la recolección de eventos, sugerimos que se permita flexibilidad en la implementación, permitiendo el uso de alternativas tecnológicas o enfoques de integración que no necesariamente requieran agentes dedicados, especialmente en entornos donde la solución ya pueda integrarse de manera eficiente sin la necesidad de estos. Esto podría reducir la carga operativa y mejorar la escalabilidad de la solución en ciertos contextos.

Acápite de las bases : Sección: Especifico      Numeral: 5      Literal: 5.2.1      Página: 5

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

Análisis respecto de la consulta u observación:

En atención a la consulta formulada, se aclara que se requiere de agentes de Windows en caso que los eventos no puedan ser recolectados por otros mecanismos.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

Consulta: Nro. 21

Consulta/Observación:

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

4 Recolección de log.

g) Creación de nuevos analizadores (plantillas XML) a través del entorno de desarrollo integrado y capacidad para compartir a través de la función de exportación / importación.

CONSULTA:

Solicitamos amablemente que se considere como opcional el punto relacionado con la recolección de logs. A fin de obtener mayor claridad sobre el alcance de este requerimiento, solicitamos que se especifique con mayor detalle a qué hacen referencia los "analizadores" en este contexto. Esto nos permitirá entender mejor el proceso y evaluar si es una función esencial para todas las soluciones o si, en determinados casos, existen alternativas viables para cumplir con los requisitos sin necesidad de creación y gestión de plantillas XML de manera obligatoria.

Acápite de las bases : Sección: Especifico      Numeral: 5      Literal: 5.2.1      Página: 5

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

Análisis respecto de la consulta u observación:

En atención a la consulta formulada, se aclara que esta funcionalidad hace referencia a analizadores de registros o log parser que traducen los archivos de registro estructurados o no estructurados para que el sistema de gestión de registros pueda leer, indexar y almacenar sus datos. De esta manera, puede filtrar, analizar y manipular fácilmente la información de clave-valor.

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

null



Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

Consulta: Nro. 22

Consulta/Observación:

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

5 Notificación y gestión de incidentes.

b) Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico.

CONSULTA:

Solicitamos amablemente una mayor clarificación sobre el punto relacionado con la notificación y gestión de incidentes, No queda claro qué tipo de comandos de corrección se requieren ni cómo se ejecutarán esos comandos. Por lo tanto, solicitamos que se proporcione un detalle adicional sobre los tipos de incidentes que activarían dichos comandos y si existen especificaciones técnicas sobre cómo deben ser configurados o gestionados dentro de la solución.

Acápite de las bases :    Sección: Especifico    Numeral: 5    Literal: 5.2.1    Página: 5

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

Análisis respecto de la consulta u observación:

En atención a la consulta formulada, se aclara que una secuencia de comandos de corrección o respuesta, hace referencia a la ejecucion de un script o comandos que servirán para solucionar un incidente de seguridad.

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

null

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 23**  
**Consulta/Observación:**  
DICE:  
CARACTERISTICAS TÉCNICAS MÍNIMAS

6 Analítica y escalabilidad  
j) Análisis escalable mediante la adición de nodos worker en caliente.

OBSERVACION:  
Solicitamos amablemente que se considere la opción de no incluir el requisito, este punto esta orientado a soluciones que solo cumplen con los estándares de una única marca, como Fortinet, lo que podría restringir la pluralidad de opciones dentro del proceso. Consideramos que es más adecuado permitir flexibilidad en cuanto a la escalabilidad de la solución, sin requerir una implementación específica que limite la opción de diferentes proveedores.

**Acápite de las bases :**    **Sección:** Especifico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 5  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**  
En atención a la observación formulada y con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente la observacion y se aceptará que la solución sea escalable mediante la adición de nodos o equivalente.

**Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:**  
Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 6. Analítica y escalabilidad, literal j) de los términos de referencia lo siguiente:  
j) Análisis escalable mediante la adición de nodos o equivalente.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

Consulta: Nro. 24

Consulta/Observación:

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

7 Integración de tecnología externa

e) Soporte de Kafka para la integración con informes mejorados de análisis, como ELK, Tableau y Hadoop.

CONSULTA:

Solicitamos amablemente que se considere la opción de no hacer obligatoria la integración mediante Kafka, consideramos que también es posible realizar estas integraciones de manera eficiente a través de la API, lo cual podría ser una alternativa más sencilla y flexible para lograr la conexión con las plataformas mencionadas. Esto permitiría una mayor pluralidad en la implementación, sin limitar a los proveedores a utilizar una tecnología específica como Kafka.

Acápite de las bases : Sección: Especifico Numeral: 5 Literal: 5.2.1 Página: 6

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

Análisis respecto de la consulta u observación:

En atención a la consulta formulada y con el ánimo de fomentar la mayor participación de postores, se aclara la consulta y este requerimiento será considerado opcional.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 7. Integración de tecnología externa, literal e) de los términos de referencia lo siguiente:

e) Opcionalmente debe ofrecer soporte de Kafka para la integración con informes mejorados de análisis, como ELK, Tableau y Hadoop.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 25**  
**Consulta/Observación:**  
DICE:  
CARACTERISTICAS TÉCNICAS MÍNIMAS

- 7 Integración de tecnología externa.  
f) API para una fácil integración con sistemas de aprovisionamiento.  
g) API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.  
h) API para integrar inteligencia externa de amenazas - Dominios de malware, IPs, URL, hashes, nodos Tor.

**OBSERVACION:**  
Solicitamos amablemente que no se considere el requisito relacionado o se considere como opcional con la integración de tecnología externa, específicamente en los puntos f), g) y h) mencionados, Si bien entendemos la importancia de contar con capacidades de integración mediante API, sugerimos que se permita una mayor pluralidad y flexibilidad, de modo que los proveedores puedan integrar sus soluciones con diferentes tecnologías y plataformas de manera abierta, sin depender de un único fabricante o producto específico.

**Acápite de las bases :**    **Sección:** Específico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 6  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación y con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente la observación, de tal manera que se requiere que el SIEM tenga integracion con tecnología externa, por la cual se permite que pueda ser integrado mediante API y/o otra tecnología similar.

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

- Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 7. Integración de tecnología externa, literales f), g) y h) de los términos de referencia lo siguiente:  
f) API o tecnología similar para una fácil integración con sistemas de aprovisionamiento.  
g) API o tecnología similar para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.  
h) API o tecnología similar para integrar inteligencia externa de amenazas - Dominios de malware, IPs, URL, hashes, nodos Tor.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 26**

**Consulta/Observación:**

DICE:

CARACTERISTICAS TÉCNICAS MÍNIMAS

8 Administración

g) Archivado basado en políticas.

OBSERVACION:

Solicitamos amablemente que no se considere el requisito o sea considerado como opcional dado que el archivado basado en políticas puede afectar negativamente el rendimiento de los servicios.

En el contexto de soluciones basadas en Big Data Lake, este tipo de archivado no es necesario, ya que las plataformas de esta naturaleza están diseñadas para manejar grandes volúmenes de datos sin recurrir a políticas de archivado que puedan impactar la eficiencia del sistema. Recomendamos considerar una solución que optimice el rendimiento y la escalabilidad sin imponer restricciones adicionales por medio de archivado.

**Acápite de las bases :**    **Sección:** Especifico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 6

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

Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación y con el ánimo de fomentar la mayor participación de postores, se acoge la observacion y se tomará como opcional el punto mencionado.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 8 Administración, literal g) de los términos de referencia lo siguiente:

g) Opcional archivado basado en políticas.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:49:43   |

**Observación: Nro. 27**  
**Consulta/Observación:**  
DICE:  
CARACTERISTICAS TÉCNICAS MÍNIMAS

- 9 Supervisión
- a) Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento.
  - b) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.
  - c) Monitorización del hardware y del entorno.

**OBSERVACION:**  
Solicitamos que los puntos mencionados sean considerados opcionales, el requisito relacionado con la "Supervisión del cambio de configuraciones en tiempo real" restringe la participación de soluciones equivalentes en el mercado al especificar características técnicas que parecen estar dirigidas a una sola marca incumbente, Tal como se detalla en el siguiente enlace <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf>. Este tipo de especificación contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores y fabricantes. La descripción del punto implica una orientación hacia productos específicos, lo que limita innecesariamente el acceso de otros proveedores que puedan ofrecer soluciones tecnológicamente equivalentes o superiores. Por tanto, solicitamos que el requerimiento sea considerado opcional o suprimido en su totalidad para permitir la participación de una gama más amplia de soluciones, promoviendo la competencia y garantizando que el proceso de contratación se mantenga dentro de los principios de igualdad de oportunidades.

**Acápite de las bases : Sección: Especifico      Numeral: 5      Literal: 5.2.1      Página: 6**  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado,

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente, de tal manera que en los términos de referencia se indicará lo siguiente:

- a) Sistema de monitorización de estado a través de Ping, SNMP, WMI, Uptime Analysis. Opcionalmente:interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento..
- b) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.
- c) Monitorización del hardware y del entorno.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 9. Supervisión, literales a), b), y c) de los términos de referencia lo siguiente:

- a) Sistema de monitorización de estado a través de Ping, SNMP, WMI, Uptime Analysis. Opcionalmente:interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento.
- b) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

---

c) Monitorización del hardware y del entorno.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Observación: Nro. 28**

**Consulta/Observación:**

En las bases se indica:

"2.2.1.1. Documentos para la admisión de la oferta

b) El postor deberá acreditar con hojas de datos y/o datasheets y/u hojas técnicas y/o brochure, el cumplimiento de las características indicadas en el Cuadro N° 01 de los Términos de Referencia, ¿Características técnicas para acreditar¿ en idioma español. Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado"

Se consulta:

"observamos que el requisito de presentar hojas de datos, datasheets, hojas técnicas o brochures en idioma español, o con traducción certificada por traductor público juramentado o colegiado, podría limitar innecesariamente la participación de postores.

Sugerimos que este requisito se reconsidere y se aplique como parte del perfeccionamiento del contrato, en lugar de ser un requisito para la admisión de la oferta. Esta modificación permitiría un proceso más inclusivo y competitivo, asegurando que se mantenga la calidad y transparencia sin restringir el acceso a una mayor diversidad de soluciones en el mercado. De acuerdo con lo establecido en el Decreto Legislativo N° 1017, Artículo 4, que regula los principios de las contrataciones del Estado y fomenta la concurrencia, pluralidad y participación objetiva de postores se puede determinar que el cumplimiento del Cuadro N° 01 de los Términos de Referencia, ¿Características técnicas para acreditar¿ esta haciendo referencia a puntos claves de una sola marca."

**Acápite de las bases : Sección: Especifico Numeral: 2.2.1 Literal: - Página: 18**

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

Artículo 4, que regula los principios de las contrataciones del Estado

**Análisis respecto de la consulta u observación:**

No se acoge la observación, se aclara que para los casos que la documentacion no se encuentre en idioma español se deberá adjuntar la traducción conforme a lo indicado en los términos de referencia. Por otro lado, las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento.

Se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento.

En cumplimiento con lo dispuesto en el art 59 del RLCE, es necesario que la documentacion solicitada en el literal b) del numeral 2.2.1.1 Documentos para la admisión de la oferta de las bases se encuentre en idioma español, puesto que es informacion que servirá como requisito de admisibilidad.

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

null



|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Consulta:** Nro. 29

**Consulta/Observación:**

En las bases se indica:

**C) EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**

Se consideran similares a los siguientes: servicio de licenciamiento para el sistema de seguridad informática, o servicio de renovación de licenciamiento de software de la plataforma de seguridad, o servicio de renovación de licencia antimalware, o licenciamiento y soporte firewall, o renovación de soporte o mantenimiento de equipos de seguridad informática, o renovación de licencias de soluciones de seguridad informática.

Se consulta:

-SERVICIO DE DETACCION DE AMENAZAS DE PUNTOS FINALES EN GENERAL

SERVICIO DE CIBERSEGURIDAD

¿ SERVICIO DE SEGURIDAD INFORMATICA EN LA NUBE PARA APLICACIONES WEB

¿ SERVICIO DE SOFTWARE DE PROTECCION, DETECCION Y RESPUESTA EXTENDIDA (XDR)

¿ SERVICIO DE SOPORTE DE FIREWALL DE BASE DE DATOS

¿ CONTRATACION DE LA SOLUCION PARA EL DESCUBRIMIENTO PREDICTIVO DE AMENAZAS AVANZADAS

¿ SERVICIO DE PROTECCION AVANZADA ANTIMALWARE

¿ SERVICIO DE SUSCRIPCION DE ANTIMALWARE

**Acápite de las bases :** Sección: Específico      **Numeral:** 3.2      **Literal:** -      **Página:** 24

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

**Análisis respecto de la consulta u observación:**

En atención a la consulta formulada y con el ánimo de fomentar la mayor cantidad de postores se aclara que se aceptará como similar lo siguiente:

-SERVICIO DE SOFTWARE DE PROTECCION, DETECCION Y RESPUESTA EXTENDIDA (XDR)

-SERVICIO DE SOPORTE DE FIREWALL DE BASE DE DATOS

-SERVICIO DE PROTECCION AVANZADA ANTIMALWARE

-SERVICIO DE SUSCRIPCION DE ANTIMALWARE,

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

Se precisa en el literal C. Experiencia del Postor en la Especialidad, lo siguiente respecto a similares a lo solicitado en los términos de referencia:

Se consideran similares a los siguientes: servicio de licenciamiento para el sistema de seguridad informática, o servicio de renovación de licenciamiento de software de la plataforma de seguridad, o servicio de renovación de licencia antimalware, o licenciamiento y soporte firewall, o renovación de soporte o mantenimiento de equipos de seguridad informática, o renovación de licencias de soluciones de seguridad informática, o servicio de protección, detección y respuesta extendida (XDR), o servicio de soporte de firewall de base de datos, o servicio de protección avanzada antimalware, o servicio de suscripción antimalware.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Consulta: Nro. 30**

**Consulta/Observación:**

En las bases se indica: "Un (01) Jefe de proyecto.  
Con experiencia mínima de cinco (05) años como Jefe o Supervisor o Gerente en la gestión de proyectos de soluciones de infraestructura tecnológica y/o seguridad informática."

Se consulta: "De acuerdo con el requerimiento actual que establece una experiencia mínima de cinco (05) años para el Jefe de Proyecto, solicitamos amablemente que dicho criterio sea reconsiderado y alineado conforme a las siguientes observaciones:

Propuesta:  
""Con experiencia mínima de tres (03) años como Jefe, Supervisor o Gerente en la gestión de proyectos de soluciones de infraestructura tecnológica, seguridad informática y/o coordinación de Proyectos de TI.""

Esta modificación busca ampliar la participación de profesionales cualificados, manteniendo estándares adecuados para la correcta ejecución del proyecto, y permitiendo incluir perfiles con una gestión adicional relevante que enriquezca el desarrollo de la solución."

**Acápite de las bases :    Sección: Especifico    Numeral: 3.2    Literal: -    Página: 23**  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

**Análisis respecto de la consulta u observación:**

En atención a la consulta formulada se aclara que el presente requerimiento corresponde a un servicio especializado por lo que se requiere que el jefe de proyecto cuente con la experiencia solicitada en los términos de referencia.

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

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Consulta:** Nro. 31

**Consulta/Observación:**

En las bases se indica: "Dos (02) Especialistas.  
Con experiencia mínima de cinco (05) años en implementación y/o soporte y/o mantenimiento de soluciones de gestión de eventos."

Se consulta: "De acuerdo con el requerimiento actual que establece una experiencia mínima de cinco (05) años para el Jefe de Proyecto, solicitamos amablemente que dicho criterio sea reconsiderado y alineado conforme a las siguientes observaciones:

Propuesta:  
""Con experiencia mínima de tres (03) años en la implementación, soporte, mantenimiento de soluciones de gestión de eventos y/o operación de soluciones SIEM en la nube y/o plataformas de gestión de eventos de seguridad.""

Esta modificación busca ampliar la participación de profesionales cualificados, manteniendo la calidad y experiencia necesaria para el desarrollo exitoso de la solución contratada."

**Acápite de las bases :**    **Sección:** Específico    **Numeral:** 3.2    **Literal:** -    **Página:** 24  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

**Análisis respecto de la consulta u observación:**

En atención a la consulta formulada se aclara que el presente requerimiento corresponde a un servicio especializado por lo que se requiere que los especialistas cuenten con la experiencia solicitada en los términos de referencia.

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

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Consulta:** Nro. 32  
**Consulta/Observación:**  
En las bases se indica: "b) DOS (02) ESPECIALISTAS

Formación académica:  
Adicionalmente deberá contar con al menos tres (03) de las siguientes certificaciones:  
o Deben contar con certificación en ISO 20000 Gestión de Servicios de TI.  
o Deben contar con certificación o constancia oficial en Ethical Hacking.  
o Deben contar con certificación en Ciberseguridad.  
o Al menos un especialista deberá contar con Certificación oficial vigente en ITIL 4 fundamentos otorgado por una institución acreditada.  
"

Se consulta: "De acuerdo con lo establecido en el Decreto Legislativo N° 1017, Artículo 4, que regula los principios de las contrataciones del Estado y fomenta la concurrencia, pluralidad y participación objetiva de postores, solicitamos que los siguientes requisitos de formación académica para los especialistas sean reconsiderados y no exigidos de manera obligatoria:

Certificación en ISO 20000 Gestión de Servicios de TI.  
Certificación o constancia oficial en Ethical Hacking.  
Certificación en Ciberseguridad.  
Certificación oficial vigente en ITIL 4 fundamentos.  
Consideramos que estos requisitos podrían limitar la participación de profesionales altamente calificados con experiencia práctica y conocimientos relevantes, los cuales pueden aportar un valor significativo al proyecto sin necesidad de contar con todas las certificaciones mencionadas. Modificar esta exigencia ampliaría la participación y garantizaría una evaluación más inclusiva y competitiva, favoreciendo soluciones que maximicen los beneficios del proyecto."

**Acápite de las bases :** Sección: Especifico      **Numeral:** 8.2      **Literal:** -      **Página:** 12  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

**Análisis respecto de la consulta u observación:**  
En atención a la consulta formulada, se aclara que al tratarse de un servicio especializado, es necesario que el personal clave relacionado a los dos (02) especialistas cuenten con las certificaciones indicadas en los términos de referencia. Se precisa que durante la etapa de estudio de mercado se presentaron diferentes empresas que cumplen con este requerimiento mínimo.  
**Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:**  
null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Observación: Nro. 33**

**Consulta/Observación:**

En las bases indica: "1. Aspectos Generales.

h) Deberá incluir (01) un colector con las siguientes características mínimas:

- Deberá ser un hardware de propósito específico. No se aceptarán colectores virtualizados.
- Capacidad mínima para 3.5 TB
- Contar mínimo con 04 interfaces RJ45 de 1GE."

Observacion: "Solicitamos reconsiderar el requisito que establece:

""Deberá ser un hardware de propósito específico. No se aceptarán colectores virtualizados.""

Esta especificación limita innecesariamente la participación de oferentes al cerrar el proceso a soluciones específicas de la marca Fortinet, como se menciona en el enlace de su producto FortiSIEM, que es la única solución que exige colectores en hardware de propósito específico. Esto contraviene el artículo 4° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la competencia y la igualdad de condiciones entre los postores.

Recomendamos evaluar la aceptación de alternativas que no se limiten exclusivamente a hardware de propósito específico o suprimir dicho requerimiento, para permitir la participación de soluciones líderes del mercado que benefician a la Entidad."

**Acápíte de las bases : Sección: Especifico Numeral: 5.2.1 Literal: - Página: 2**

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

artículo 4° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la competencia y la i

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento, Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente ya que actualmente existen marcas que proveen el SIEM y sus colectores en hardware físico, no obstante, se aceptará que el colector pueda ser virtual.

En caso de ofertar un colector virtual, el Postor debe incluir en su propuesta el hardware de primer uso y el software licenciado necesario para el correcto funcionamiento de la solución que cumpla además con las siguientes características técnicas:

- ¿ Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- ¿ Procesador de 8 núcleos mínimo.
- ¿ Memoria RAM de 16 GB mínimo.
- ¿ Espacio en disco de 3.5 TB mínimo.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas - numeral 1 "Aspectos generales", literal h) de los Términos de Referencia lo siguiente:

h) Deberá incluir (01) un colector con las siguientes características mínimas:

- ¿ Deberá ser un hardware de propósito específico o virtualizado considerando incluir hardware de primer uso y el software licenciado necesario para el correcto funcionamiento de la solución.

En caso se trate de componente basado en hardware, este debe cumplir con las siguientes características mínimas:

- ¿ Contar mínimo con 04 interfaces RJ45 de 1GE.
- ¿ Capacidad mínima para 3.5 TB.

En caso se trate de colectores virtualizados, este debe cumplir con las siguientes características mínimas:

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

---

- ¿ Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V
- ¿ Procesador de 8 núcleos mínimo.
- ¿ Memoria RAM de 16 GB mínimo.
- ¿ Espacio en disco de 3.5 TB mínimo.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Consulta:** Nro. 34  
**Consulta/Observación:**  
En las bases se indica: "2. Características

2.1 Análisis de seguridad en tiempo real  
e) La solución debe integrarse a un asistente virtual con inteligencia artificial (IA) generativa (OpenAI) que permita guiar y potenciar las acciones de los analistas de seguridad durante la investigación de incidentes, búsqueda de amenazas, respuesta y otras opciones."

Se consulta: Solicitamos reconsiderar el siguiente requerimiento técnico en el proceso. El especificar OpenAI como la única tecnología generativa de inteligencia artificial limita innecesariamente la pluralidad del proceso de licitación, ya que existen otras soluciones competentes en el mercado que cumplen con estos requisitos. Por esta razón, solicitamos que este requerimiento sea revisado para permitir el uso de cualquier asistente virtual con IA generativa que cumpla las funciones descritas, garantizando que no se cierre el acceso a opciones tecnológicas igualmente efectivas.

**Acápite de las bases :** Sección: Especifico      **Numeral:** 5.2.1      **Literal:** -      **Página:** 2  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

**Análisis respecto de la consulta u observación:**  
En atención a la consulta y con el ánimo de fomentar la mayor participación de postores, se aclara que se aceptará que el postor incluya en su oferta la tecnología de inteligencia antificial generativa OpenAI o similar.

**Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:**  
Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas,numeral 2. Características, numeral 2.1 Análisis de seguridad en tiempo real, literal e) de los términos de referencia lo siguiente:  
e) La solución debe integrarse a un asistente virtual con inteligencia artificial (IA) generativa (OpenAI) o similar, que permita guiar y potenciar las acciones de los analistas de seguridad durante la investigación de incidentes, búsqueda de amenazas, respuesta y otras opciones.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

Ruc/código : 20608981412

Nombre o Razón social : ENEBRO INGENIERIA S.A.C.

Fecha de envío : 15/01/2025

Hora de envío : 23:52:50

**Observación: Nro. 35**

**Consulta/Observación:**

En las bases se indica: "

## 2. Características

### 2.1 Análisis de seguridad en tiempo real

g) Correlación de eventos SOC/NOC, para disponer en un único punto de gestión de datos no sólo de eventos de seguridad, sino también de:

- o Rendimiento y disponibilidad
- o CPU, memoria y almacenamiento.
- o Detección de cambios de configuración.
- o Monitorización de transacciones sintéticas.
- o Cuadros de mando dinámicos."

Observacion: "Solicitamos que se consideren como opcionales los siguientes puntos mencionados este tipo de requisito esta orientado a una solución específica de FortiSIEM en <https://fortixpert.blogspot.com/2021/10/fortisiem-metricas-de-rendimiento-en.html>. Si este requisito no se considera opcional, solicitamos que se suprima completamente, específicamente en el apartado g) Correlación de eventos SOC/NOC:

- CPU, memoria y almacenamiento
- Monitorización de transacciones sintéticas
- Cuadros de mando dinámicos

Si bien estos elementos pueden aportar valor en ciertos escenarios, no siempre son esenciales para el cumplimiento de los objetivos principales de correlación de eventos SOC/NOC relacionados al proceso solicitado. Dado que su implementación puede variar dependiendo de las necesidades y capacidades específicas de cada proveedor, consideramos que hacerlos opcionales permitirá mayor flexibilidad para que los postulantes presenten soluciones ajustadas a las necesidades del cliente sin comprometer la funcionalidad básica requerida o integrar soluciones terceras para el cumplimiento del mismo. Esto contraviene el artículo 4° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la competencia y la igualdad de condiciones entre los postores y fabricantes."

**Acápite de las bases :** Sección: Especifico Numeral: 5.2.1

**Literal:** -

**Página:** 2

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

artículo 4° de la Ley N° 30225, Ley de Contrataciones del Estado

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento, también se precisa que es importante que un SIEM correlacione eventos de seguridad y eventos de red para una gestión eficaz de la seguridad en cualquier infraestructura de TI. Esta capacidad permite identificar patrones, amenazas, y anomalías que serían difíciles de detectar si los eventos se analizaran de manera aislada.

En ese sentido, actualmente existen diversas marcas de soluciones SIEM que permiten correlacionar datos de la red y eventos de seguridad. Por lo tanto, no se acoge la observación.

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

null



|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Consulta:** Nro. 36

**Consulta/Observación:**

En las bases se indica: "

1. Aspectos Generales.

b) Se requiere de un SIEM en nube modalidad SaaS administrable desde una consola que brinde visibilidad sobre el rendimiento de los sistemas, servicios y los eventos de seguridad."

Se consulta:

Se solicita a la Entidad considerar como opcional el requerimiento de brindar desde la consola del SIEM la visibilidad del rendimiento de los sistemas, ya que estás acciones no corresponden a funcionalidades de un SIEM, las soluciones pueden brindar alertas o estados de conexión de las fuentes integradas más no monitorear sus performance, si se desea controlar dichos parametros la fuente debe enviarlo al SIEM a través de log.

**Acápite de las bases :**    **Sección:** Especifico    **Numeral:** 5.2.1    **Literal:** -    **Página:** 2

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

**Análisis respecto de la consulta u observación:**

En atención a la consulta formulada, se aclara que es fundamental que un SIEM monitoree el estado de los equipos, rendimiento y la disponibilidad de los servicios porque esto contribuye directamente a la seguridad, el rendimiento y la continuidad operativa de la infraestructura de TI. Por lo tanto, no se acoge la consulta.

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

null

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:52:50   |

**Consulta:** Nro. 37

**Consulta/Observación:**

En las bases se indica: "

1. Aspectos Generales.

c) El fabricante ofertante deberá disponer de un método de licenciamiento escalable tanto por número de dispositivos como por EPS asociados."

Se consulta: Se solicita a la Entidad confirmar que como parte de la escalabilidad requerida, la solución ofertada podrá utilizar la consola de gestión de algunas de las herramientas de seguridad que cuenta la entidad, extendiendo a esta las capacidades de SIEM de acuerdo a lo requerido en bases.

**Acápite de las bases :** Sección: Especifico      **Numeral:** 5.2.1      **Literal:** -      **Página:** 2

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

**Análisis respecto de la consulta u observación:**

En atención a la consulta formulada, se aclara que el servicio debe incluir todos los componentes de hardware y software necesarios para el correcto funcionamiento del servicio. Por lo tanto, no se acoge la propuesta.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

Ruc/código : 20608981412

Nombre o Razón social : ENEBRO INGENIERIA S.A.C.

Fecha de envío : 15/01/2025

Hora de envío : 23:52:50

**Consulta: Nro. 38**

**Consulta/Observación:**

En las bases indica: "

2. Características

2.4 Supervisión del rendimiento

- a) Monitor de métricas de sistema.
- b) Estado del sistema a través de SNMP, WMI, PowerShell.
- c) Estado de aplicaciones a través de JMX, WMI, PowerShell.
- d) Monitoreo de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster.
- e) Monitorización del rendimiento de aplicaciones a medida: Bases de datos - Oracle, MS SQL, MySQL a través de JDBC.
- f) Análisis de flujo y rendimiento de la aplicación Netflow, SFlow, Cisco AVC e IPFIX.
- g) Posibilidad de agregar métricas personalizadas.
- h) Métricas de base y detección de desviaciones."

Se consulta: "Solicitamos reconsiderar el alcance de los requerimientos especificados en los puntos mencionados sean considerados como opcionales, dado este tipo de requisitos podría estar orientado a una solución específica, como lo describe FortiSIEM en <https://fortixpert.blogspot.com/2021/10/fortisiem-metricas-de-rendimiento-en.html>. Si este requisito no se considera opcional, solicitamos que se suprima completamente.

La naturaleza de un servicio de SIEM se centra principalmente en la recolección, análisis y correlación de eventos de seguridad para la detección y respuesta a incidentes. Por lo tanto, funcionalidades relacionadas con la supervisión del rendimiento del sistema, métricas personalizadas y monitoreo de virtualización o bases de datos no constituyen requisitos fundamentales para el objetivo de esta contratación.

Al considerar estos puntos como opcionales, se permitirá una mayor flexibilidad y enfoque en los elementos clave del servicio, optimizando el proceso de adquisición y la competitividad de las soluciones propuestas."

**Acápite de las bases : Sección: Especifico Numeral: 5.2.1 Literal: - Página: 4**

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

**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente la observación, ya que es fundamental que un SIEM monitoree el estado de los equipos, rendimiento y la disponibilidad de los servicios porque esto contribuye directamente a la seguridad, el rendimiento, y la continuidad operativa de la infraestructura de TI. Por lo tanto, se aceptarán soluciones que supervisen a menos cinco (05) de las características listadas en los términos de referencia.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 2. Características, numeral 2.4 Supervisión del rendimiento de los términos de referencia lo siguiente:

Debe soportar al menos cinco (05) de las supervisiones solicitadas:

- a) Monitor de métricas de sistema.
- b) Estado del sistema a través de SNMP, WMI, PowerShell.
- c) Estado de aplicaciones a través de JMX, WMI, PowerShell.
- d) Monitoreo de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster.

**Entidad convocante :** MINISTERIO DE TRANSPORTES Y COMUNICACIONES

**Nomenclatura :** CP-SM-17-2024-MTC/10-1

**Nro. de convocatoria :** 1

**Objeto de contratación :** Servicio

**Descripción del objeto :** CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

---

- e) Monitorización del rendimiento de aplicaciones a medida: Bases de datos - Oracle, MS SQL, MySQL a través de JDBC.
- f) Análisis de flujo y rendimiento de la aplicación Netflow, SFlow, Cisco AVC e IPFIX.
- g) Posibilidad de agregar métricas personalizadas.
- h) Métricas de base y detección de desviaciones.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:53:54   |

**Observación: Nro. 39**

**Consulta/Observación:**

DICE:  
4 Recolección de log.

b) Debe contar con una amplia gama de métodos de recopilación de datos basados en agentes y sin agentes para recopilar registros de una variedad de dispositivos y aplicaciones, que incluyen: SNMP, Syslog, Windows Management Instrumentation (WMI) and Open Management Infrastructure (OMI), Cisco SDEE, Checkpoint LEA, JDBC, VMware SDK, JMX, Telnet, SSH, NetFlow, HTTPS, IMAP, POP, entre otros.

**OBSERVACION:**  
Solicitamos reconsiderar el alcance del requisito descritos: Considerando los métodos especificados (SNMP, WMI, OMI, Cisco SDEE, VMware SDK, JMX, Telnet, SSH, HTTPS, IMAP, POP) sean considerados como opcionales. Esto permitiría a los proveedores proponer soluciones flexibles que se adapten a las necesidades específicas del cliente, sin limitar la competitividad ni la pluralidad de opciones en el proceso de selección. el requisito relacionado restringe la participación de soluciones equivalentes en el mercado al especificar características técnicas que parecen estar dirigidas a una sola marca incumbente se detalla en el siguiente enlace <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf>. Este tipo de especificación contraviene el artículo 3° de la Ley N° 30225, Ley de Contrataciones del Estado, que promueve la libre competencia y la igualdad de condiciones entre los postores y fabricantes.

**Acápite de las bases :**    **Sección:** Específico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 2  
**Artículo y norma que se vulnera (En el caso de Observaciones):**

artículo 3° de la Ley N° 30225  
**Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento. Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente la observación y se aceptarán soluciones que soporten al menos dos de las siguientes tecnologías: SNMP, Syslog (obligatorio), Windows Management Instrumentation (WMI) and Open Management Infrastructure (OMI), Cisco SDEE, Checkpoint LEA, JDBC, VMware SDK, JMX, Telnet, SSH, NetFlow, HTTPS, IMAP, POP, entre otros.

**Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:**  
Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 4. Recolección de log, literal b) de los términos de referencia lo siguiente:  
b) Debe contar con una amplia gama de métodos de recopilación de datos basados en agentes y sin agentes para recopilar registros de una variedad de dispositivos y aplicaciones, que incluyen al menos dos de las siguientes tecnologías: SNMP, Syslog (obligatorio), Windows Management Instrumentation (WMI) and Open Management Infrastructure (OMI), Cisco SDEE, Checkpoint LEA, JDBC, VMware SDK, JMX, Telnet, SSH, NetFlow, HTTPS, IMAP, POP, entre otros.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:53:54   |

**Observación: Nro. 40**

**Consulta/Observación:**

DICE:  
7 Integración de tecnología externa.  
f) API para una fácil integración con sistemas de aprovisionamiento.  
g) API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.  
h) API para integrar inteligencia externa de amenazas - Dominios de malware, IPs, URL, hashes, nodos Tor.

**OBSERVACION**  
Solicitamos amablemente que no se considere el requisito relacionado o se considere como opcional con la integración de tecnología externa, específicamente en los puntos f), g) y h) mencionados, Si bien entendemos la importancia de contar con capacidades de integración mediante API, sugerimos que se permita una mayor pluralidad y flexibilidad, de modo que los proveedores puedan integrar sus soluciones con diferentes tecnologías y plataformas de manera abierta, sin depender de un único fabricante o producto específico.

**Acápite de las bases : Sección:** Especifico      **Numeral:** 5      **Literal:** 5.2.1      **Página:** 6

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

artículo 3° de la Ley N° 30225

**Análisis respecto de la consulta u observación:**

En atención a la observación y con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente la observacion, de tal manera que se requiere que el SIEM tenga integracion con tecnologia externa, por la cual se permite que pueda ser integrado mediante API y/o otra tecnologia similar.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 7. Integración de tecnología externa, literales f), g) y h) de los términos de referencia lo siguiente:  
f) API o tecnologia similar para una fácil integración con sistemas de aprovisionamiento.  
g) API o tecnologia similar para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.  
h) API o tecnologia similar para integrar inteligencia externa de amenazas - Dominios de malware, IPs, URL, hashes, nodos Tor.

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                               |                  |            |
|-------------------------|-------------------------------|------------------|------------|
| Ruc/código :            | 20392869981                   | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | AB SOLUCIONES GLOBALES S.R.L. | Hora de envío :  | 23:53:54   |

**Observación: Nro. 41**

**Consulta/Observación:**

DICE:

#### 9 Supervisión

- a) Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento.
- b) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.
- c) Monitorización del hardware y del entorno.

#### OBSERVACION:

Solicitamos reconsiderar el alcance de los requerimientos especificados en los puntos mencionados sean considerados como opcionales, dado este tipo de requisitos podría estar orientado a una solución específica, como lo describe FortiSIEM en <https://fortixpert.blogspot.com/2021/10/fortisiem-metricas-de-rendimiento-en.html>. Si este requisito no se considera opcional, solicitamos que se suprima completamente.

El objetivo de un servicio SIEM se enfoca principalmente en la recolección, análisis y correlación de eventos de seguridad. Si bien la supervisión de la infraestructura y disponibilidad es importante en otros contextos, la inclusión de estos requisitos no impacta directamente en el rendimiento y efectividad de la solución SIEM, que se centra en los eventos de seguridad y la gestión de incidentes.

Al considerar estos puntos como opcionales, se fomentaría la flexibilidad en la oferta de soluciones, sin desviar el enfoque principal hacia áreas que no son cruciales para el servicio solicitado.

**Acápite de las bases :**    **Sección:** Especifico    **Numeral:** 5    **Literal:** 5.2.1    **Página:** 6

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

Ley N° 30225, Ley de Contrataciones del Estado,

#### **Análisis respecto de la consulta u observación:**

En atención a la observación, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento, Sin embargo, con el ánimo de fomentar la mayor participación de postores, se acoge parcialmente, de tal manera que en los términos de referencia se indicará lo siguiente:

- a) Sistema de monitorización de estado a través de Ping, SNMP, WMI, Uptime Analysis. Opcionalmente:interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento..
- b) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.
- c) Monitorización del hardware y del entorno.

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 9. Supervisión, literales a), b), y c) de los términos de referencia lo siguiente:

- a) Sistema de monitorización de estado a través de Ping, SNMP, WMI, Uptime Analysis. Opcionalmente:interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento.
- b) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.

|                          |  |
|--------------------------|--|
| Entidad convocante :     | MINISTERIO DE TRANSPORTES Y COMUNICACIONES   |
| Nomenclatura :           | CP-SM-17-2024-MTC/10-1   |
| Nro. de convocatoria :   | 1  |
| Objeto de contratación : | Servicio   |
| Descripción del objeto : | CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE |

---

c) Monitorización del hardware y del entorno.



Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

Ruc/código : 20608981412

Nombre o Razón social : ENEBRO INGENIERIA S.A.C.

Fecha de envío : 15/01/2025

Hora de envío : 23:54:53

**Consulta:** Nro. 42

**Consulta/Observación:**

En las bases indica\_:

"

## 2. Características

### 2.5 Supervisión del cambio de configuraciones en tiempo real

- Recopilar archivos de configuración de red, almacenados en un repositorio versionado.
- Recopilar las versiones de software instaladas, almacenadas en un repositorio versionado.
- Detección automatizada de cambios en la configuración de la red y el software instalado.
- Detección automatizada de cambios de archivos y carpetas -Windows y Linux con detalles técnicos.
- Detección automatizada de cambios desde un archivo de configuración.
- Posibilidad de detección automatizada de cambios en el registro de Windows a través de agente."

Se consulta: "Solicitamos reconsiderar el alcance de los requerimientos especificados en los puntos mencionados sean considerados como opcionales, dado este tipo de requisitos podría estar orientado a una solución específica, como lo describe FortiSIEM en <https://fortixpert.blogspot.com/2021/10/fortisiem-metricas-de-rendimiento-en.html>. Si este requisito no se considera opcional, solicitamos que se suprima completamente.

El enfoque principal de un servicio SIEM es la recolección, análisis y correlación de eventos de seguridad para la detección y respuesta a incidentes. La supervisión de cambios en configuraciones, archivos y registros, aunque relevante en otros contextos, no es fundamental para el objetivo principal de un SIEM, que se centra en la seguridad de eventos y la mitigación de amenazas.

Al considerar estos puntos como opcionales, se permitirá una mayor flexibilidad y enfoque en los elementos clave del servicio, optimizando el proceso de adquisición y la competitividad de las soluciones propuestas."

**Acápite de las bases :** Sección: Especifico      **Numeral:** 5.2.1      **Literal:** -      **Página:** 4

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

### **Análisis respecto de la consulta u observación:**

En atención a la consulta, se menciona que es importante que un SIEM supervise los cambios en la configuración de los equipos monitoreados, ya que dichos cambios pueden ser indicadores de actividades maliciosas o accesos no autorizados, como ataques internos, compromisos de cuentas privilegiadas, o errores administrativos que pueden comprometer la seguridad de una red. La supervisión del cambio de configuraciones permite detectar eventos que podrían ser indicativos de ataques en curso o futuras vulnerabilidades, además de facilitar el cumplimiento normativo al documentar las configuraciones de los sistemas.

Asimismo, se aclara que las características técnicas fueron validadas durante la etapa de estudio de mercado donde varios proveedores indicaron su cumplimiento ya que actualmente existen diversas marcas de soluciones SIEM que permiten monitorear cambios en las configuraciones de sus equipos monitoreados. Por lo tanto, no se acoge la consulta.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:54:53   |

Consulta: Nro. 43

Consulta/Observación:

En las bases indica: "

1. Aspectos Generales.
- e) El SIEM debe estar licenciado para soportar al menos 6600 EPS de dispositivos de red y soluciones de seguridad como Firewalls, switches, routers y servidores entre otros."

Se consulta: Se solicita a la entidad confirmar que se aceptará que la solución ofertada soporte al menos 6600 EPS o su equivalente en GB por día.

Acápite de las bases : Sección: Especifico Numeral: 5.2.1 Literal: - Página: 2

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

Análisis respecto de la consulta u observación:

En atención a la consulta se aclara que en el mercado actual existen muchas marcas de soluciones SIEM que dimensionan sus soluciones en funcion de eventos procesados, medidos en EPS (Event per second) ya que es un parametro clave para evaluar la capacidad del sistema. Por lo tanto, no se acepta.

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

null

Entidad convocante : MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Nomenclatura : CP-SM-17-2024-MTC/10-1

Nro. de convocatoria : 1

Objeto de contratación : Servicio

Descripción del objeto : CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE UN SISTEMA DE GESTION DE INFORMACION Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

|                         |                          |                  |            |
|-------------------------|--------------------------|------------------|------------|
| Ruc/código :            | 20608981412              | Fecha de envío : | 15/01/2025 |
| Nombre o Razón social : | ENEBRO INGENIERIA S.A.C. | Hora de envío :  | 23:54:53   |

Consulta: Nro. 44

Consulta/Observación:

En las bases indica: "

4 Recolección de log.

a) Recopilación, análisis, normalización, indexación y almacenamiento de logs de seguridad a velocidades muy altas."

Se consulta: Para evitar con ambigüedades en el requerimiento, se solicita retirar el requerimiento de "velocidades muy altas", ya que esto puede ser interpretado de diferentes formas.

Acápite de las bases : Sección: Especifico      Numeral: 5.2.1      Literal: -      Página: 4

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

**Análisis respecto de la consulta u observación:**

En atencón a la consulta formulada y con el ánimo de fomenar la mayor participación de postores, se aclara la consulta por lo que se retirará la condición de"velocidades muy altas" y será reemplazado por "velocidades que permitan una óptima operación de la solución".

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

Se precisa en el numeral 5.2.1. Prestación Principal - Características técnicas mínimas, numeral 4 Recolección de log, literal a) de los términos de referencia lo siguiente:  
a) Recopilación, análisis, normalización, indexación y almacenamiento de logs de seguridad a velocidades que permitan una optima operación de la solución.