PRONUNCIAMIENTO N° 087-2025/OSCE-DGR

Entidad : Seguro Social de Salud

Referencia : Concurso Público N° 11-2024-ESSALUD/GCL-1, convocado para la "Contratación del servicio de una malla de seguridad informática e implementación del sistema de gestión de seguridad de información - SGSI"

---

1. ANTECEDENTES

Mediante el formulario de solicitud de emisión de pronunciamiento, recibido el 6[1] de enero de 2025 y subsanado en fecha 21[2] de enero de 2025, el presidente del comité de selección a cargo del procedimiento de selección de la referencia remitió al Organismo Supervisor de las Contrataciones del Estado (OSCE) la solicitud de elevación de cuestionamientos al pliego absolutorio de consultas y observaciones e integración de bases presentada por el participante **DANAE CONTRATISTAS GENERALES EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA,** en cumplimiento de lo dispuesto por el artículo 21 de la Ley de Contrataciones del Estado, aprobada mediante la Ley N° 30225, en adelante la "Ley", y el artículo 72 de su Reglamento, aprobado por el Decreto Supremo Nº 344-2018-EF, en adelante el "Reglamento".

Firmado digitalmente por LAURA SILVA Anthony David FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 06.02.2025 17:32:31 -05:00

Asimismo, cabe precisar que en la emisión del presente pronunciamiento se utilizó el orden establecido por el comité de selección en el pliego absolutorio y los temas materia de cuestionamientos de los mencionados participantes, conforme al siguiente detalle:

Firmado digitalmente por CHAMOCHUMBI CHERRE Carlos Ernesto FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 06.02.2025 17:27:58 -05:00

- **Cuestionamiento Único** : Respecto a la absolución de la consulta y/u observación N° 29, referida a los **"Equipos de seguridad de cortafuegos y control de navegación web tipo I y II"**

Firmado digitalmente por VARGAS PEREZ Wilberth FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 06.02.2025 17:23:17 -05:00

2. CUESTIONAMIENTOS

De manera previa, cabe señalar que el OSCE no ostenta la calidad de perito técnico dirimente respecto a las posiciones de determinados aspectos del requerimiento (especificaciones técnicas, términos de referencia y expediente técnico de obra, según corresponda); sin embargo, puede requerir a la Entidad informes que contengan la posición técnica al respecto[3], considerando que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

---

[1] Mediante Trámite Documentario N° 2025-002355.
[2] Mediante Trámite Documentario N° 2025-0010124.
[3] Ver el Comunicado N° 011-2013-OSCE/PRE.

<u>Cuestionamiento Único</u>: **Respecto a los "Equipos de seguridad de cortafuegos y control de navegación web tipo I y II"**

El participante **DANAE CONTRATISTAS GENERALES EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA**, respecto a los equipos de seguridad de cortafuegos y control de navegación web tipo I y II, cuestionó la absolución de la consulta y/u observación N° 29, alegando que la Entidad ha manifestado la existencia de pluralidad de marcas, determinando, entre otros, las marcas: Palo Alto y Hillstone; no obstante, las referidas marcas no cumplirían con las especificaciones solicitadas e incluso afirmarían que no tienen conocimiento de su participación en el estudio de mercado. Por lo tanto, la afirmación de pluralidad de marcas realizada por la Entidad podría no ser válida, por lo que se estaría vulnerando diversos principios de la Ley, como la Libertad de Concurrencia, Igualdad de Trato y Competencia.

Por lo que, el recurrente **<u>solicitó que la Entidad efectúe las modificaciones al requerimiento, a fin de que las marcas "Palo Alto" y "Hillstone" cumplan con el mismo.</u>**

Pronunciamiento

Al respecto, de la revisión de los literales A y B, del acápite 5.1.1, referido a los "Equipos de seguridad de cortafuegos y control de navegación web tipo I y II", establecidos en el contenido del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

*"**CAPÍTULO III***
3.1 ESPECIFICACIONES TÉCNICAS
(…)
5.1. Del equipamiento mínimo requerido para el Servicio de una Malla de Seguridad Informática e implementación del Sistema de Gestión de Seguridad de Información – SGSI

5.1.1. Equipamiento y funcionalidades del servicio requerido.
El presente servicio debe contemplar mínimamente los siguiente equipos y componentes.

A. ***EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO I***

EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO I	
Cantidad	***02 UNIDADES DE TIPO CORTAFUEGOS (01 CLÚSTER EN HA)***
RENDIMIENTO MÍNIMO (POR CADA EQUIPO)	
(…)	*(…)*
Sesiones Concurrentes	*11'000,000 conexiones o sesiones concurrentes;* ***<u>o 4'000,000 sesiones concurrentes como mínimo medidos en HTTP.</u>***
Conexiones por segundo	*745,000 conexiones o sesiones por segundo****<u>; o 300,000 sesiones por segundo como mínimo medidos en HTTP.</u>***
(…)	*(…)*
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
Consideraciones Generales	***<u>● El fabricante de la solución de seguridad debe estar presente en los últimos seis 06 reportes de Gartner (Magic Cuadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.</u>***
(…)	*(…)*

B. ***EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO II***

EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO II	
Cantidad	***02 UNIDADES DE TIPO CORTAFUEGOS (01 CLÚSTER EN HA)***
RENDIMIENTO MÍNIMO (POR CADA EQUIPO)	
(...)	*(...)*
Sesiones Concurrentes	*22'000,000 conexiones o sesiones concurrentes;* ***o 10'000,000 sesiones concurrentes como mínimo medidos en HTTP.***
Conexiones por segundo	*950,000 conexiones o sesiones por segundo; o* ***450,000 sesiones por segundo como mínimo medidos en HTTP.***
(...)	*(...)*
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
Consideraciones Generales	***● El fabricante de la solución de seguridad debe estar presente en los últimos seis 06 reportes de Gartner (Magic Cuadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.***
(...)	*(...)*

(…)"

(El subrayado y resaltado es agregado)

Mediante la consulta y/u observación N° 29 del pliego, el participante **JAPAN COMPUTER SERVICE S.A.C.** solicitó reducir de los requisitos en los equipos de seguridad de los Corta fuegos y control de navegación web, estableciendo un mínimo de 3,000,000 de sesiones concurrentes y 240,000 conexiones por segundo para los equipos tipo I, y un mínimo de 5,000,000 de sesiones concurrentes y 260,000 conexiones por segundo para los equipos tipo II. Además, se ha requerido que ambos tipos de equipos sean capaces de identificar o bloquear la transmisión de aplicaciones maliciosas a través de túneles SSH, utilizando los protocolos SCP y SFTP, y opcionalmente, que cuenten con una protección que permita modificar archivos durante descargas HTTP/HTTPS, eliminando componentes riesgosos como código o enlaces maliciosos.

Por otro lado, ha requerido que, en caso de no acoger lo anterior, solicita que confirme que validó la pluralidad de marcas durante el estudio de mercado e indique las marcas que fueron validadas.

Ante lo cual, la Entidad dispuso acoger parcialmente lo solicitado, precisando que las especificaciones solicitadas por el participante para los Corta fuegos Tipo I y Tipo II no son óptimas, ya que los requisitos de sesiones concurrentes y conexiones por segundo, superan las capacidades requeridas, que son de más de 4,000,000 y 10,000,000, respectivamente. Además, en relación con los protocolos SCP y SFTP, aclara que se mantendrá la necesidad de bloquear la transmisión de virus, ya que, de permitirse sólo la identificación, no se fortalecería la seguridad. En cuanto a los protocolos HTTP/HTTPS, se aclara que son universales, y la solución debe poder modificar archivos para eliminar componentes riesgosos, lo que no limita la participación de proveedores. También, se ha decidido eliminar el requisito de que los equipos provengan de fabricantes en el cuadrante mágico de Gartner, y de esa forma se reafirma la existencia de pluralidad de marcas y proveedores, como Fortinet, Palo Alto y Hillstone.

En consecuencia, tras la integración de las Bases, de la revisión de los literales A y B, del acápite 5.1.1, referido a los "Equipos de seguridad de cortafuegos y control de

navegación web tipo I y II", establecidos en el contenido del numeral 3.1 del Capítulo III pertenecientes a la Sección Específica de las Bases Integradas no definitivas, se aprecia lo siguiente:

*"**CAPÍTULO III***
3.1 ESPECIFICACIONES TÉCNICAS
(…)
5.1. Del equipamiento mínimo requerido para el Servicio de una Malla de Seguridad Informática e implementación del Sistema de Gestión de Seguridad de Información – SGSI

5.1.1. Equipamiento y funcionalidades del servicio requerido.
El presente servicio debe contemplar mínimamente los siguiente equipos y componentes.

A. ***EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO I***

EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO I	
Cantidad	***02 UNIDADES DE TIPO CORTAFUEGOS (01 CLÚSTER EN HA)***
RENDIMIENTO MÍNIMO (POR CADA EQUIPO)	
(…)	*(…)*
Sesiones Concurrentes	*11'000,000 conexiones o sesiones concurrentes; o 4'000,000 sesiones concurrentes como mínimo medidos en HTTP.*
Conexiones por segundo	*745,000 conexiones o sesiones por segundo; o 300,000 sesiones por segundo como mínimo medidos en HTTP.*
(…)	*(…)*
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
~~***Consideraciones Generales***~~	• ~~*El fabricante de la solución de seguridad debe estar presente en los últimos seis 06 reportes de Gartner (Magic Cuadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.*~~
(…)	*(…)*

B. ***EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO II***

EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO II	
Cantidad	***02 UNIDADES DE TIPO CORTAFUEGOS (01 CLÚSTER EN HA)***
RENDIMIENTO MÍNIMO (POR CADA EQUIPO)	
(…)	*(…)*
Sesiones Concurrentes	*22'000,000 conexiones o sesiones concurrentes; o 10'000,000 sesiones concurrentes como mínimo medidos en HTTP.*
Conexiones por segundo	*950,000 conexiones o sesiones por segundo; o 450,000 sesiones por segundo como mínimo medidos en HTTP.*
(…)	*(…)*
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
~~***Consideraciones Generales***~~	• ~~*El fabricante de la solución de seguridad debe estar presente en los últimos seis 06 reportes de Gartner (Magic Cuadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.*~~
(…)	*(…)*

(…)"

En ese contexto, mediante el Informe N° 040-OSI-GCTIC-ESSALUD-2024[4], el área usuaria de la Entidad precisó lo siguiente:

"De acuerdo con lo señalado en el punto 1.1 y 1.2, a continuación, se presenta evidencia del cumplimiento de múltiples marcas.

[4] Mediante Trámite Documentario N° 2025-08868, de fecha 17 de enero de 2025.

a) SOBRE LO REQUERIDO PARA EL CORTAFUEGOS TIPO I:

Sesiones Concurrentes:

- *11´000,000 conexiones o sesiones concurrentes; o 4´000,000 sesiones concurrentes como mínimo medidos en HTTP.*

Conexiones por segundo:

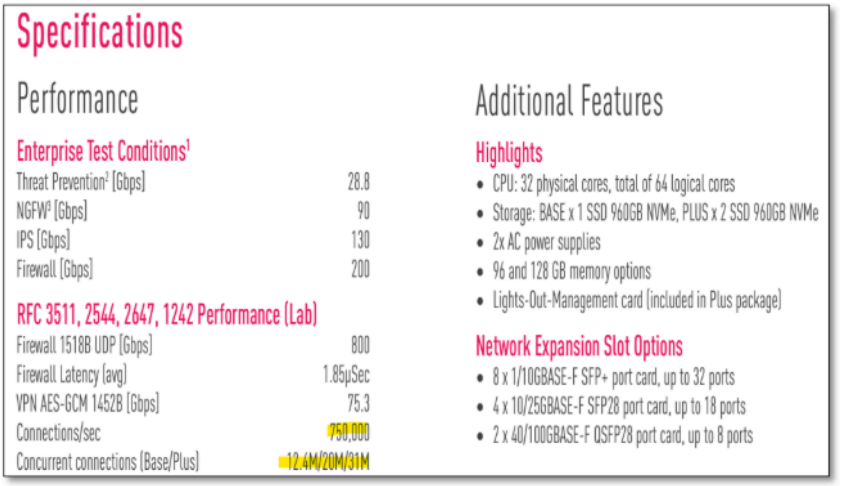
- *745,000 conexiones o sesiones por segundo; o 300,000 sesiones por segundo como mínimos medidos en HTTP.*

a.1 Cumplimiento de diferentes marcas:

De acuerdo con lo solicitado, se adjunta evidencia de cumplimiento de múltiples marcas:

I Check Point:

https://www.checkpoint.com/downloads/products/quantum-force-19100- datasheet.pdf



Specifications

Performance

Enterprise Test Conditions[1]

Threat Prevention[2] [Gbps]	28.8
NGFW[3] [Gbps]	90
IPS [Gbps]	130
Firewall [Gbps]	200

RFC 3511, 2544, 2647, 1242 Performance (Lab)

Firewall 1518B UDP [Gbps]	800
Firewall Latency (avg)	1.85µSec
VPN AES-GCM 1452B [Gbps]	75.3
Connections/sec	750,000
Concurrent connections (Base/Plus)	12.4M/20M/31M

Additional Features

Highlights

- CPU: 32 physical cores, total of 64 logical cores
- Storage: BASE x 1 SSD 960GB NVMe, PLUS x 2 SSD 960GB NVMe
- 2x AC power supplies
- 96 and 128 GB memory options
- Lights-Out-Management card (included in Plus package)

Network Expansion Slot Options

- 8 x 1/10GBASE-F SFP+ port card, up to 32 ports
- 4 x 10/25GBASE-F SFP28 port card, up to 18 ports
- 2 x 40/100GBASE-F QSFP28 port card, up to 8 ports

II Palo Alto:
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-5400-series

Table 1: PA-5400 Series Performance and Capacities					
	PA-5410	PA-5420	PA-5430	PA-5440	PA-5445
Firewall throughput (appmix)*	52 Gbps	70 Gbps	80 Gbps	85 Gbps	90 Gbps
Threat Prevention throughput (appmix)†	35 Gbps	50 Gbps	60 Gbps	70 Gbps	76 Gbps
IPsec VPN throughput‡	20 Gbps	28 Gbps	42 Gbps	58 Gbps	64 Gbps
Max concurrent sessions§	5M	7M	9M	20M	48M
New sessions per second‖	270,000	370,000	380,000	390,000	449,000
Virtual systems (base/max)#	10/20	15/65	25/125	25/225	25/225

III. Fortinet:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf

	FG-1000F	FG-1800F
Firewall Throughput (1518/512/64 byte UDP)	198 / 196 / 134 Gbps	198 / 197 / 140 Gbps
IPsec VPN Throughput (512 byte) [1]	55 Gbps	55 Gbps
IPS Throughput (Enterprise Mix) [2]	19 Gbps	22 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	15 Gbps	17 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	13 Gbps	15 Gbps
Firewall Latency	3.45 µs	3.22 µs
Concurrent Sessions	7.5 Million	12 Million / 40 Million [6]
New Sessions/Sec	650 000	750 000 / 2 Million [6]

IV. HILLSTONE

Firewall Hillstone Serie-A de Próxima Generación

Hillstone NETWORKS

Especificaiones del Producto (Continuación)

	SG-6000-A5200	SG-6000-A5500	SG-6000-A5600	SG-6000-A5800
[redacted]				
Firewall Throughput [2]	32/65 Gbps	40/80 Gbps	60/85 Gbps	80/95 Gbps
NGFW Throughput [3]	15.84 Gbps	17.12 Gbps	30.84 Gbps	31.94 Gbps
Threat Protection Throughput [4]	11.37 Gbps	10.43 Gbps	19.13 Gbps	18.43 Gbps
Maximum Concurrent Sessions [5]	12,000,000	12,000,000	20,000,000	24,000,000
New Sessions/s [6]	400,000	500,000	800,000	930,000
IPS Throughput [7]	20/35 Gbps	25/40 Gbps	35/60 Gbps	45/75 Gbps

b) SOBRE LO REQUERIDO PARA CORTAFUEGOS TIPO II:

Sesiones Concurrentes:

- *22´000,000 conexiones o sesiones concurrentes; o 10´000,000 sesiones concurrentes como mínimo medidos en HTTP.*

Conexiones por segundo:

- *950,000 conexiones o sesiones por segundo; o 450,000 sesiones por segundo como mínimos medidos en HTTP.*

b.1 Cumplimiento de diferentes marcas:

I Check Point:
https://www.checkpoint.com/downloads/products/quantum-force-29100-datasheet.pdf

Specifications

Performance

Enterprise Test Conditions[1]

Threat Prevention[2] [Gbps]	47.4
NGFW[3] [Gbps]	130
IPS [Gbps]	175
Firewall [Gbps]	365

RFC 3511, 2544, 2647, 1242 Performance (Lab)

Firewall 1518B UDP [Gbps]	1,400
Firewall Latency (avg)	1.85µSec
VPN AES-GCM 1452B [Gbps]	103
Connections/sec	1,250,000
Concurrent connections (Base/Plus/Max)	30M/48M/67M

Additional Features

Highlights

- CPU: 56 physical cores, total of 112 logical cores
- Storage: BASE x 1 SSD 960GB NVMe, PLUS x 2 SSD 960GB NVMe
- 2x AC power supplies
- 128, 192 and 256 GB memory options
- Lights-Out-Management card (included in Plus package)

Network Expansion Slot Options

- 8 x 1/10GBASE-F SFP+ port card, up to 56 ports
- 4 x 10/25GBASE-F SFP28 port card, up to 30 ports
- 2 x 40/100GBASE-F QSFP28 port card, up to 14 ports

II Palo Alto:
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-5400-series

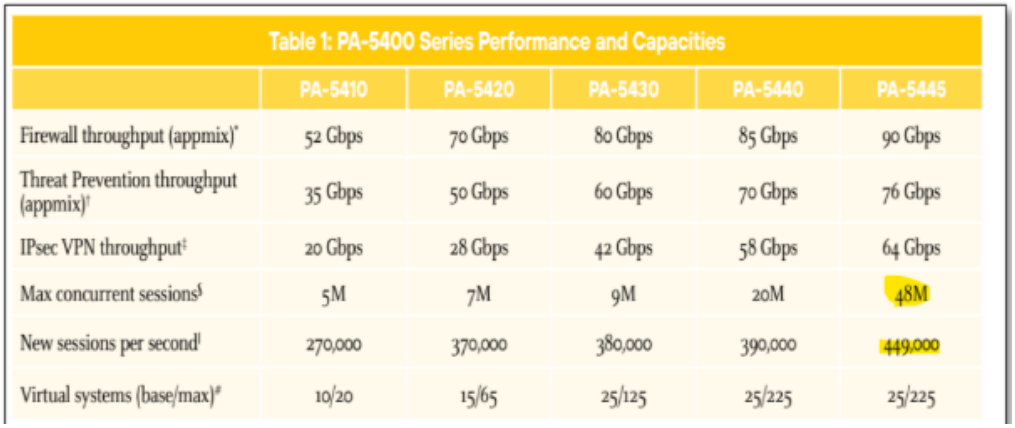


Table 1: PA-5400 Series Performance and Capacities

	PA-5410	PA-5420	PA-5430	PA-5440	PA-5445
Firewall throughput (appmix)*	52 Gbps	70 Gbps	80 Gbps	85 Gbps	90 Gbps
Threat Prevention throughput (appmix)†	35 Gbps	50 Gbps	60 Gbps	70 Gbps	76 Gbps
IPsec VPN throughput‡	20 Gbps	28 Gbps	42 Gbps	58 Gbps	64 Gbps
Max concurrent sessions§	5M	7M	9M	20M	48M
New sessions per second‖	270,000	370,000	380,000	390,000	449,000
Virtual systems (base/max)¶	10/20	15/65	25/125	25/225	25/225

III. Fortinet:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet Product_Matrix.pdf

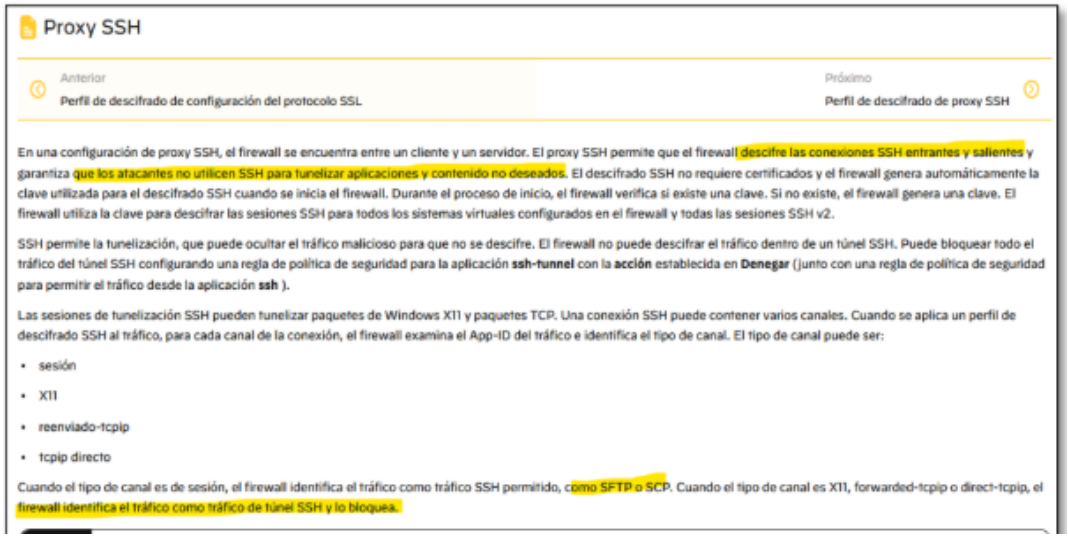
	FG-1000F	FG-1800F	FG-2600F
Firewall Throughput (1518/512/64 byte UDP)	198 / 196 / 134 Gbps	198 / 197 / 140 Gbps	198 / 196 / 140 Gbps
IPsec VPN Throughput (512 byte) [1]	55 Gbps	55 Gbps	55 Gbps
IPS Throughput (Enterprise Mix) [2]	19 Gbps	22 Gbps	31 Gbps
NGFW Throughput (Enterprise Mix) [2,4]	15 Gbps	17 Gbps	27 Gbps
Threat Protection Throughput (Ent. Mix) [2,5]	13 Gbps	15 Gbps	25 Gbps
Firewall Latency	3.45 µs	3.22 µs	3.41 µs
Concurrent Sessions	7.5 Million	12 Million / 40 Million [6]	24 Million / 40 Million [6]
New Sessions/Sec	650 000	750 000 / 2 Million [6]	1 Million / 2 Million [6]

c) CON RESPECTO AL 1.2 DE LA CARTA S/N Y REFERIDO AL SCP Y SFTP INDICA QUE:
"referente al SCP Y SFTP El requerimiento del contratista apertura una posible reducción en el alcance de lo solicitado por el área usuaria, es decir, de solo identificar la aplicación maliciosa y no bloquearla, acción que no coadyuva a fortalecer la protección integral de la información de la entidad. En tal sentido, el requerimiento queda tal cual se ha indicado en las bases del Servicio "Bloquea la transmisión de virus a través de los protocolos SCP y SFTP". con respecto al HTTP/HTTPS.
Se indica al participante que los protocolos http/https, son universales y no particulares de una sola marca, dicho esto, la Entidad requiere necesariamente que la solución requerida pueda soportar modificar archivos, eliminando componentes riesgosos. En cuanto a la terminología, se informa al participante que este es utilizado por más de un fabricante de la solución requerida; Por consiguiente, no se limita la participación de otros proveedores. (...)
Sobre la pluralidad se mantienen los aspectos de pluralidad, dado que el resultado de la indagación de mercado se obtuvo pluralidad de proveedores y de marcas, tales como: Fortinet, Palo alto y Hillstone. *(Subrayado es nuestro)"*
Sobre lo indicado en la observación descrita precedentemente, EsSalud requiere que la solución:

- ***Deber tener la capacidad de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:***
- ***Bloquea la transmisión de virus a través de protocolos SCP y SFTP***

c.1 Cumplimiento de diferentes marcas:
I. Palo Alto:

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/decryption-concepts/ssh-proxy#id2053e5f5-25e0-4543-b372-b2e027316753



Proxy SSH

Anterior
Perfil de descifrado de configuración del protocolo SSL

Próximo
Perfil de descifrado de proxy SSH

En una configuración de proxy SSH, el firewall se encuentra entre un cliente y un servidor. El proxy SSH permite que el firewall descifre las conexiones SSH entrantes y salientes y garantiza que los atacantes no utilicen SSH para tunelizar aplicaciones y contenido no deseados. El descifrado SSH no requiere certificados y el firewall genera automáticamente la clave utilizada para el descifrado SSH cuando se inicia el firewall. Durante el proceso de inicio, el firewall verifica si existe una clave. Si no existe, el firewall genera una clave. El firewall utiliza la clave para descifrar las sesiones SSH para todos los sistemas virtuales configurados en el firewall y todas las sesiones SSH v2.

SSH permite la tunelización, que puede ocultar el tráfico malicioso para que no se descifre. El firewall no puede descifrar el tráfico dentro de un túnel SSH. Puede bloquear todo el tráfico del túnel SSH configurando una regla de política de seguridad para la aplicación **ssh-tunnel** con la **acción** establecida en **Denegar** (junto con una regla de política de seguridad para permitir el tráfico desde la aplicación **ssh**).

Las sesiones de tunelización SSH pueden tunelizar paquetes de Windows X11 y paquetes TCP. Una conexión SSH puede contener varios canales. Cuando se aplica un perfil de descifrado SSH al tráfico, para cada canal de la conexión, el firewall examina el App-ID del tráfico e identifica el tipo de canal. El tipo de canal puede ser:

- sesión
- X11
- reenviado-tcpip
- tcpip directo

Cuando el tipo de canal es de sesión, el firewall identifica el tráfico como tráfico SSH permitido, como SFTP o SCP. Cuando el tipo de canal es X11, forwarded-tcpip o direct-tcpip, el firewall identifica el tráfico como tráfico de túnel SSH y lo bloquea.

II. Check Point:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ Threat Prevention_AdminGuide/Topics-TPG/Using-SSH-Inspection.htm

Inspección profunda de paquetes SSH

Puede utilizar la función de inspección profunda de paquetes SSH ("SSH DPI") para descifrar y cifrar el tráfico SSH y dejar que la solución de prevención de amenazas lo proteja contra amenazas avanzadas, bots y otro malware.

Motivación y objetivos clave para SSH DPI

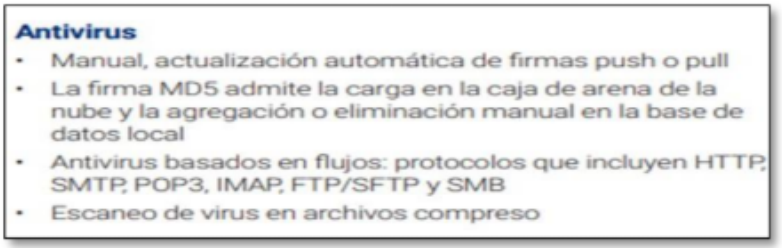
Arquitectura DPI de SSH

De manera similar a la inspección HTTPS, SSH DPI funciona como un intermediario.

```
SSH_CLIENT <=> Security Gateway <=> SSH_SERVER
```

Nota : Todo el tráfico TCP debe pasar a través del Security Gateway.

III. Hillstone:
https://www.hillstonenet.lat/wp-content/uploads/Hillstone_E-Series_V5.5R9_SP_0125.pdf



Antivirus

- Manual, actualización automática de firmas push o pull
- La firma MD5 admite la carga en la caja de arena de la nube y la agregación o eliminación manual en la base de datos local
- Antivirus basados en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP y SMB
- Escaneo de virus en archivos compreso

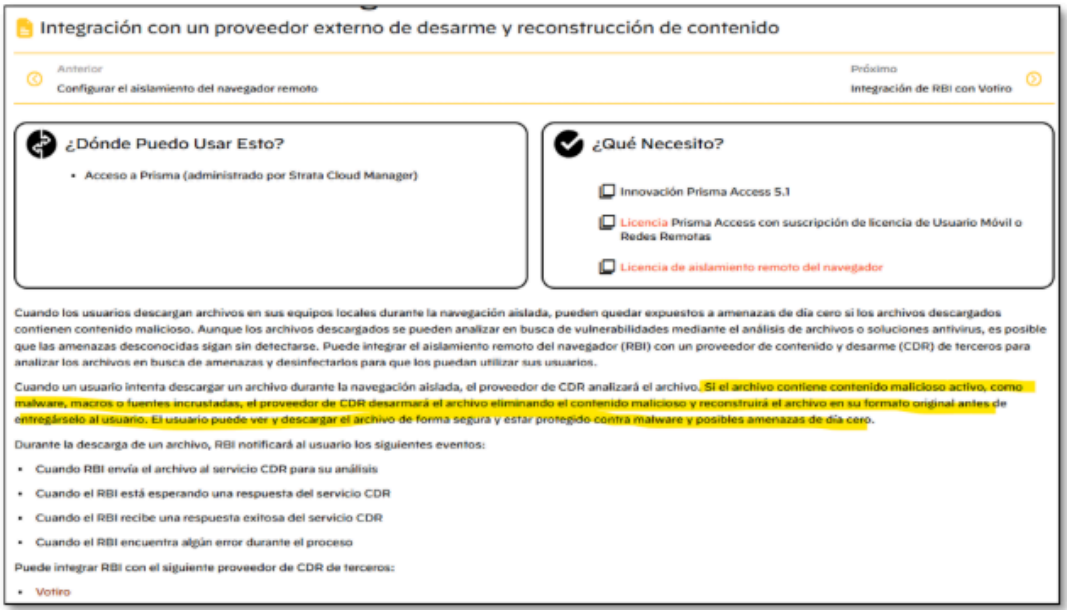
d) ***De mismo modo, se brinda sustento de dos marcas líderes, sobre el siguiente punto observado:***

** Tener habilitado la protección que al hacer una descarga por http/https, debe soportar modificar archivos (reconstruido durante su análisis) eliminados componentes riesgosos (código, link).*

I. PALO ALTO

Aquí podemos evidenciar que la marca Palo Alto también cumpliría con el requerimiento con la integración de un tercero. Las bases no limitan que el postor pueda complementar con herramientas de terceros a fin de cumplir con lo requerido.

https://docs.paloaltonetworks.com/remote-browser-isolation/administration/integrate-rbi-with-a-third-party-cdr- rovider



Integración con un proveedor externo de desarme y reconstrucción de contenido

Anterior: Configurar el aislamiento del navegador remoto

Próximo: Integración de RBI con Votiro

¿Dónde Puedo Usar Esto?

- Acceso a Prisma (administrado por Strata Cloud Manager)

¿Qué Necesito?

- Innovación Prisma Access 5.1
- Licencia Prisma Access con suscripción de licencia de Usuario Móvil o Redes Remotas
- Licencia de aislamiento remoto del navegador

Cuando los usuarios descargan archivos en sus equipos locales durante la navegación aislada, pueden quedar expuestos a amenazas de día cero si los archivos descargados contienen contenido malicioso. Aunque los archivos descargados se pueden analizar en busca de vulnerabilidades mediante el análisis de archivos o soluciones antivirus, es posible que las amenazas desconocidas sigan sin detectarse. Puede integrar el aislamiento remoto del navegador (RBI) con un proveedor de contenido y desarme (CDR) de terceros para analizar los archivos en busca de amenazas y desinfectarlos para que los puedan utilizar sus usuarios.

Cuando un usuario intenta descargar un archivo durante la navegación aislada, el proveedor de CDR analizará el archivo. Si el archivo contiene contenido malicioso activo, como malware, macros o fuentes incrustadas, el proveedor de CDR desarmará el archivo eliminando el contenido malicioso y reconstruirá el archivo en su formato original antes de entregárselo al usuario. El usuario puede ver y descargar el archivo de forma segura y estar protegido contra malware y posibles amenazas de día cero.

Durante la descarga de un archivo, RBI notificará al usuario los siguientes eventos:

- Cuando RBI envía el archivo al servicio CDR para su análisis
- Cuando el RBI está esperando una respuesta del servicio CDR
- Cuando el RBI recibe una respuesta exitosa del servicio CDR
- Cuando el RBI encuentra algún error durante el proceso

Puede integrar RBI con el siguiente proveedor de CDR de terceros:

- Votiro

II. Check Point

Dejamos evidencia que otra marca también cumple con este requerimiento: ***https://www.checkpoint.com/es/infinity/zero-day-protection/threat-extraction/***

CHECK POINT

Soluciones | ES LA PREVENCIÓN | Soporte técnico y Servicios | Socios | Más

Extracción de amenazas

Desarme y reconstrucción de contenido (CDR)

La extracción de amenazas elimina las características de riesgo de los archivos, como macros, objetos incrustados, etc., en lugar de determinar su carácter malicioso. Limpiando el archivo antes de que entre en la organización. La extracción de amenazas previene tanto las amenazas conocidas como las desconocidas, proporcionando una mejor protección contra los ataques de día cero.

e) ***En el párrafo 1.3 de la Carta señala que las marcas Palo Alto y Hillstone no cumplen con el requerimiento solicitado y tampoco tienen conocimiento que hayan***

participado en el estudio de mercado.

"1.3. No obstante, como se puede verificar en el Análisis de la observación, la entidad señala que en la etapa que en estudio de mercado participaron la marca Fortinet, Palo Alto y Hillstone, por lo que supuestamente existiría pluralidad de marcas ya que esta cumplirían con lo requerido en las especificaciones, sin embargo al momento de hacer la consulta a la marca Palo Alto y Hillstone estas mencionan que no cumplen con el requerimiento solicitado y tampoco tienen conocimiento que hayan participado en el estudio de mercado, por lo que en ese sentido se estaría vulnerando claramente el articulo 02 e inciso e) del Reglamento de la Ley de Contrataciones con el Estado, por lo que se solicita que se revise dicho requerimiento"

Respuesta de la Oficina de Seguridad Informática

Esta Oficina debe informar que, de acuerdo con la indagación de mercado realizado como actos preparatorios, se adjunta en el ítem de Anexos los documentos presentados por las empresas que participaron con sus propuestas de estudio de mercado.

2. CONCLUSIONES Y RECOMENDACIONES:

En base a lo revisado y analizado en el capítulo 2 del presente documento, se sugiere continuar con las gestiones correspondientes para proseguir con la convocatoria del Concurso Público N° 11-2024- ESSLAUD/GCL-1 "Contratación del Servicio de una Malla de Seguridad Informática e Implementación del Sistema de Gestión de Seguridad de Información-SGSI".

(...)"

(El subrayado y resaltado es agregado)

Adicionalmente, mediante memorando N° 08-OSI-GCTIC-ESSALUD-2025[5], el área usuaria de la Entidad complementó lo siguiente:

"(...)

2.2.1. Sustento técnico de los motivos de no haber acogido la observación N°29

Motivo de no haber acogido la observación:

Se informa que actualmente la Oficina de Seguridad Informática cuenta con una solución de Firewall, el cual, mediante las herramientas de monitoreo, muestran un registro de sesiones concurrentes a nivel Institucional para los siguientes equipos de corta fuegos:

TIPO DE FIREWALL	***MUESTRA DE FIREWALL INSTITUCIONAL***	***FIREWALL REQUERIDO***	***RIESGOS DE CONTAR CON FIREWALL DE MENOR CAPACIDAD***

[5] Mediante Trámite Documentario N° 2025-08868, de fecha 17 de enero de 2025.

CORTAFUEGOS TIPO I:	*Se ha obtenido hasta 4'000,000 sesiones concurrentes medidos en HTTP en el Firewall de la Institución.*	*Como mínimo debe soportar 4'000,000 sesiones concurrentes medidos en HTTP*	● ***Riesgo operativo tecnológico**, por la sobre carga de una solución tecnológica que no soporte los umbrales requeridos, ocasionando lentitud en los servicios que brinda la Institución; comprometiendo la funcionalidad y operatividad de los sistemas informáticos de la institución.* ● ***Riesgo de imagen Institucional**, comprometiendo la percepción y confianza por parte de los asegurados y ciudadanos en general, al no brinda adecuada continuidad operativa tecnológica Institucionalmente. Institucionalmente.*

TIPO DE FIREWALL	***MUESTRA DE FIREWALL INSTITUCIONAL***	***FIREWALL REQUERIDO***	***RIESGOS DE CONTAR CON FIREWALL DE MENOR CAPACIDAD***
			● ***Riesgo operativo de negocio,** la indisponibilidad o lentitud de los sistemas informáticos comprometería la continuidad operativa asistencial y administrativa de EsSalud.*
	Se ha obtenido hasta 300,000 registros de sesiones por segundo en el Firewall de la Institución.	*Como mínimo debe soportar 300,000 registros de sesiones por segundo.*	● ***Riesgo operativo tecnológico**, por la sobre carga de una solución tecnológica que no soporte los umbrales requeridos, ocasionando lentitud en los servicios que brinda la Institución; comprometiendo la funcionalidad y operatividad de los sistemas informáticos de la institución.* ● ***Riesgo de imagen Institucional**, Comprometiendo la percepción y confianza por parte de los asegurados y ciudadanos en general, al no brindar adecuada continuidad operativa tecnológica institucionalmente.* ● ***Riesgo operativo de negocio,** la indisponibilidad o lentitud de los sistemas informáticos comprometería la continuidad operativa asistencial y administrativa de EsSalud.*

CORTAFUEGOS TIPO II:	*Se ha obtenido hasta 10'000,000 sesiones concurrentes medidos en HTTP en el Firewall de la Institución.*	*Como mínimo debe soportar 10'000,000 Sesiones concurrentes medidos en HTTP.*	● ***Riesgo operativo tecnológico****, por la sobre carga de una solución tecnológica que no soporte los umbrales requeridos, ocasionando lentitud en los servicios que brinda la Institución; comprometiendo la funcionalidad y operatividad de los sistemas informáticos de la institución.* ● ***Riesgo de imagen Institucional****, comprometiendo la percepción y confianza por parte de los asegurados y ciudadanos en general, al no brindar adecuada continuidad operativa tecnológica Institucionalmente.* *tecnológica Institucionalmente.*

TIPO DE FIREWALL	***MUESTRA DE FIREWALL INSTITUCIONAL***	***FIREWALL REQUERIDO***	***RIESGOS DE CONTAR CON FIREWALL DE MENOR CAPACIDAD***
			● ***Riesgo operativo de negocio,*** *la indisponibilidad o lentitud de los sistemas informáticos comprometería la continuidad operativa asistencial y administrativa de EsSalud.*
	Se ha obtenido hasta 450,000 registros de sesiones por segundo en el Firewall de la Institución.	*Como mínimo debe soportar 450,000 registros de sesiones por segundo.*	● ***Riesgo operativo tecnológico****, por la sobre carga de una solución tecnológica que no soporte los umbrales requeridos, ocasionando lentitud en los servicios que brinda la Institución; comprometiendo la funcionalidad y operatividad de los sistemas informáticos de la institución.* ● ***Riesgo de imagen Institucional****, comprometiendo la percepción y confianza por parte de los asegurados y ciudadanos en general, al no brinda adecuada continuidad operativa tecnológica Institucionalmente.* ● ***Riesgo operativo de negocio,*** *la indisponibilidad o lentitud de los sistemas informáticos comprometería la continuidad operativa asistencial y administrativa de EsSalud.*

Por lo expuesto precedentemente, ***esta Oficina no acoge la consulta y/u observación. Asimismo, informa que las especificaciones técnicas del equipamiento (Corta Fuegos Tipo I y Tipo II) no limitan la participación de proveedores, siendo que, resultan necesarios para la lo requerido por EsSalud.***
(...)"

(El subrayado y resaltado es agregado)

Por su parte, mediante la Nota N° 070-2025-SGPyA-GA-GCL/ESSALUD[6], con respecto al estudio de mercado, el Órgano Encargado de las Contrataciones de la Entidad, precisó lo siguiente:

"(...)
Se remite INFORME N° 13-2024-LEYH, de fecha 23 de octubre de 2024, en el cual, la especialista a cargo de la indagación de mercado remitió el informe de indagación de

[6] Mediante Trámite Documentario N° 2025-08868, de fecha 17 de enero de 2025.

mercado complementario para la "Contratación de servicio de una malla de seguridad informática e implementación del sistema de gestión de seguridad de información - SGSI", el mismo que obra en el expediente de contratación. ***Al respecto es necesario precisar que las marcas Fortinet, Palo Alto y Hillstone no participaron de la indagación como empresas, sin embargo, los proveedores que remitieron sus cotizaciones adjuntaron las fichas, catálogos o brochure de estas marcas para verificar el cumplimiento de los bienes solicitados como parte de la prestación del servicio.***
(...)"

(El subrayado y resaltado es agregado)

Es así que, de la revisión del Informe N° 13-2024-LEYH[7], con respecto al estudio de mercado, el Órgano Encargado de las Contrataciones de la Entidad, precisó lo siguiente:

"(...)
Tercera indagación de mercado

- *Mediante correo electrónico de fecha 16 de octubre de 2024,* ***reinicie la indagación de mercado solicitando a los proveedores dedicados al objeto de la contratación (anexo 3), que envíen su respectiva cotización, adjuntando los términos de referencia (versión 10) y requisitos de calificación, indicando como fecha máxima para presentar las cotizaciones el 17 de octubre de 2024.***
- ***Dentro del plazo otorgado se recibió las siguientes cotizaciones:***

Mediante correo electrónico: manuel@bigsecure.net, de fecha 17 de octubre de 2024, la empresa BIGSECURE SAC, envió su cotización (...) y asimismo remitió consultas.
Mediante correo electrónico: agallardo@gurutiperu.com, de fecha 17 de octubre de 2024, la empresa GURUTI SAC, envió su cotización (...).

- *Mediante Nota N° 1855-2024-SGPA-GA-GCL/ESSALUD, de fecha 18 de octubre de 2024, la Sub Gerencia de Programación y Almacenamiento remitió a la Gerencia Central de Tecnologías de Información y Comunicación las cotizaciones para su revisión y evaluación.*
- *Mediante Memorando N° 2708-2024-GCTIC/ESSALUD, de fecha 21 de octubre de 2024,* ***el área usuaria valido las cotizaciones, siendo estos los siguientes:***

Cotizaciones

N°	*Proveedores*	*RNP*	*P. Total S/.*	*Fecha de Cotización*	*Estado*
1	*BIGSECURE SAC*	*SI*	*(...)*	*17/10/2024*	*Cumple*
2	*GURUTI SAC*	*SI*	*(...)*	*17/10/2024*	*Cumple*

(...)"

Al respecto, cabe señalar que en el artículo 16 de la Ley y el artículo 29 del Reglamento, se establece que el área usuaria es la responsable de la elaboración del requerimiento, debiendo éste contener la descripción objetiva y precisa de las características y/o requisitos funcionales relevantes para cumplir la finalidad pública de la contratación y las condiciones en las que debe ejecutarse la contratación, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

Por otro lado, cabe señalar que los Principios de Libertad de Concurrencia y Competencia, consignados en los literales a) y e) del artículo 2 de la Ley, establecen que los procesos de contratación deben establecer condiciones de competencia

[7] Mediante Trámite Documentario N° 2025-08868, de fecha 17 de enero de 2025.

efectiva, promoviendo el libre acceso y participación de proveedores, de tal modo que se obtenga la propuesta más ventajosa para satisfacer el interés público. Encontrándose prohibida la adopción de prácticas que restrinjan o afecten o limiten la competencia.

Ahora bien, en atención al aspecto cuestionado por el recurrente, se aprecia que la Entidad, mediante su informe técnico y en atención al mejor conocimiento de las necesidades que desea satisfacer, ha ratificado lo absuelto, precisando lo siguiente:

- Se ha señalado el cumplimiento de múltiples marcas en relación con los requisitos establecidos para el Corta Fuegos Tipo I, destacando la capacidad de manejar un mínimo de 4,000,000 sesiones concurrentes y 300,000 conexiones por segundo, con marcas que pueden alcanzar hasta 11,000,000 y 745,000, respectivamente. Esta información sugiere que existen diversas opciones en el mercado que pueden satisfacer las necesidades de la Entidad, lo cual se respalda mediante la información publicada en los links de las páginas web de las empresas "Check point", "Palo alto", "Fortinet" y "Hillstone", con la cual se demuestra la existencia de pluralidad de postores y marcas con capacidad de cumplir los términos de referencia.

- Asimismo, ha señalado el cumplimiento de múltiples marcas en relación con los requisitos establecidos para el Corta Fuegos Tipo II, destacando la capacidad de manejar un mínimo de 10,000,000 sesiones concurrentes y 450,000 conexiones por segundo, con marcas que pueden alcanzar hasta 22,000,000 y 950,000, respectivamente. Esta información sugiere que existen diversas opciones en el mercado que pueden satisfacer las necesidades de la Entidad, lo cual se respalda mediante la información publicada en los links de las páginas web de las empresas "Check point", "Palo alto" y "Fortinet", con la cual se demuestra la existencia de pluralidad de postores y marcas con capacidad de cumplir los términos de referencia.

- Por otro lado, señala que el requerimiento para los protocolos SCP y SFTP se mantendrán en su forma original, exigiendo no sólo la identificación de aplicaciones maliciosas, sino también su bloqueo, para asegurar una protección integral de la información de la Entidad. Además, se aclara que los protocolos HTTP/HTTPS son universales y que la solución debe ser capaz de modificar archivos para eliminar componentes riesgosos, lo que no restringe la participación de otros proveedores en el proceso de contratación, lo cual respalda mediante la información publicada en los links de las páginas web de las empresas "Palo alto", "Check point" y "Hillstone".

- Además, se ha aclarado que, aunque las marcas Fortinet, Palo Alto y Hillstone no participaron de forma directa en la indagación de mercado, sus productos fueron evaluados mediante las fichas, catálogos y brochures presentados por los proveedores BIGSECURE SAC y GURUTI SAC, quienes sí enviaron cotizaciones a la Entidad. Esto indica que, a pesar de la ausencia de participación directa de las marcas, el cumplimiento de las mismas, respecto de los requisitos de seguridad informática, ha sido verificado a través de la documentación de otros participantes. Destacando

además que, el estudio de mercado fue validado por el área usuaria, como se detalla en el Informe N° 0127-2024-OSI-GCTIC/ESSALUD, en el cual concluye que se demostró la pluralidad de postores con la participación de BIGSECURE SAC y GURUTI SAC. Así, dicha conclusión se respalda en la información consignada en el cuadro comparativo, que forma parte integral del estudio de mercado y evidencia la competencia entre los proveedores analizados.

En consecuencia, se ha evidenciado el cumplimiento de múltiples marcas para los Corta Fuegos Tipo I y II, que satisfacen requisitos de alto rendimiento en sesiones concurrentes y conexiones por segundo, respaldado por la información publicada por empresas como Check Point, Palo Alto, Fortinet y Hillstone. Además, se ha decidido mantener el requerimiento para los protocolos SCP y SFTP, exigiendo tanto la identificación como el bloqueo de aplicaciones maliciosas, y se aclara que los protocolos HTTP/HTTPS son universales, permitiendo así la participación de diversos proveedores. Por último, aclara que, aunque algunas marcas no participaron directamente en la indagación de mercado, ello no es óbice para que sus productos no fueran evaluados a través de la documentación presentada por otros proveedores, asegurando así el cumplimiento de los requisitos de seguridad informática, demostrando de ese modo, la pluralidad de marcas y postores con capacidad de cumplir los términos de referencia.

En ese sentido, considerando lo señalado en los párrafos precedentes, y en la medida que la pretensión del recurrente se encuentra orientada a que la Entidad efectúe las modificaciones al requerimiento, a fin de que las marcas “Palo Alto” y “Hillstone” cumplan con el mismo, y en tanto que la Entidad, mediante su informe técnico, se ha ratificado en el contenido del requerimiento, aclarando el cumplimiento de varias marcas para los Corta Fuegos Tipo I y II, este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento, por lo que considerando lo indicado en el informe técnico remitido por la Entidad, se dispone implementar las siguientes disposiciones:

- **Se deberá tener en cuenta**[8] lo precisado en el Informe N° 040-OSI-GCTIC-ESSALUD-2024, así como la Nota N° 070-2025-SGPyA-GA-GCL/ESSALUD, el Informe N° 13-2024-LEYH y el Memorando N° 08-OSI-GCTIC-ESSALUD-2025, a fin de complementar el sustento técnico de lo absuelto en la consulta y/u observación N° 29 del Pliego.

Finalmente, cabe precisar que de conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y el **informe técnico**, así como la atención de los pedidos de información requeridos, en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, son responsables de la información que obra en los actuados para la adecuada realización de la contratación.

[8] La presente disposición deberá ser tenida en cuenta en la etapa pertinente del procedimiento, por lo que no resulta necesaria su implementación en las Bases Integradas definitivas.

3. ASPECTOS REVISADOS DE OFICIO

Si bien el procesamiento de la solicitud de pronunciamiento, por norma, versa sobre los supuestos cuestionamientos derivados de la absolución de consultas y/u observaciones, y no representa la convalidación de ningún extremo de las bases, este Organismo Técnico Especializado ha visto por conveniente hacer indicaciones puntuales a partir de la revisión de oficio, según el siguiente detalle:

3.1. Respecto al plazo de prestación del servicio

De la revisión conjunta del numeral 1.8 del Capítulo I y el acápite 5.12.2 del numeral 3.1 del Capítulo III, ambos pertenecientes a la Sección Específica de las Bases Integradas no definitivas, se aprecia que la Entidad consignó lo siguiente:

> ***"CAPÍTULO I***
> *(...)*
> ***1.8. PLAZO DE PRESTACIÓN DEL SERVICIO***
> *Los servicios materia de la presente convocatoria se prestarán en el plazo de un mil noventa y cinco (1,095) días calendario, los cuales serán contabilizados* ***a partir del día siguiente de firmada el Acta de Conformidad de Puesta en producción de los componentes implementados****,* ***en concordancia con lo establecido en el expediente de contratación.***
> *(...)*
> ***CAPÍTULO III***
> *(...)*
> ***5.12.2 Plazo de ejecución del servicio***
> *El plazo de ejecución del servicio será de un mil noventa y cinco (1,095) días calendario, los cuales serán contabilizados* ***a partir del día siguiente de firmada el Acta de Conformidad de Puesta en producción de los componentes implementados****.*
> *(...)"*

(El subrayado y resaltado es agregado)

De la revisión del numeral 1.8, del Capítulo I, de la Sección Específica de las Bases objeto del presente procedimiento de selección, se aprecia lo siguiente:

> *" **1.8 PLAZO DE PRESTACIÓN DEL SERVICIO***
> *Los servicios materia de la presente convocatoria se prestarán en el plazo de [CONSIGNAR EL PLAZO DE PRESTACIÓN DEL SERVICIO] en concordancia con lo establecido en el expediente de contratación."*

Al respecto, de la revisión de los extremos citados de las Bases, se aprecia que, el plazo planteado no se condice con los alcances de las Bases estándar objeto del presente procedimiento de selección, ya que conforme al requerimiento establecido por el área usuaria, la Entidad ha determinado que el servicio se realizará en 1,095 días calendario, los cuales serán contabilizados a partir del día siguiente de firmada el Acta de Conformidad de Puesta en producción de los componentes implementados. Asimismo, en el numeral 1.8 de las mismas Bases se ha previsto el término *"en concordancia con lo establecido en el expediente de contratación"*. De lo cual, se colige que ambos extremos resultan disímiles entre sí, lo cual podría

confundir a los participantes, vulnerando lo establecido por el Principio de Transparencia.

En ese contexto, mediante el documento Nota N° 07-2025-CP-SM-11-2024-ESSALUD/GCL-1[9], el área usuaria de la Entidad precisó lo siguiente:

> *"(...)*
> *Como se puede apreciar dichas bases estándar solicitan se complete,* ***consignando el plazo de prestación de servicio, el mismo que, se extrae de los términos de referencia, señalando el hito desde el cual se contabiliza dicho plazo, adicionando la frase "en concordancia con lo establecido en el expediente de contratación", frase que garantiza que no exista contradicción entre lo señalado en las bases*** *y en los TDR(...)"*

(El subrayado y resaltado es agregado)

En ese sentido, considerando lo declarado en el informe técnico de la Entidad y con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se adecuará** el contenido del numeral 5.12.2 del Capítulo III de la Sección Específica de las Bases Integradas Definitivas, según el siguiente detalle:

> ***"****(...)*
> ***CAPÍTULO III***
> *(...)*
> ***5.12.2 Plazo de prestación ~~ejecución~~ del servicio***
> *El plazo de prestación ~~ejecución~~ del servicio será de un mil noventa y cinco (1,095) días calendario, los cuales serán contabilizados a partir del día siguiente de firmada el Acta de Conformidad de Puesta en producción de los componentes implementados, en concordancia con lo establecido en el expediente de contratación.*
> *(...)"*

- **Se dejará sin efecto y/o ajustará** todo extremo del pliego absolutorio, las Bases o Informe Técnico que se oponga a las disposiciones previstas en los párrafos anteriores.

3.2. Respecto al costo de reproducción y entrega de las bases

Al respecto, de la revisión del numeral 1.9 del Capítulo I de la sección específica de las Bases Estándar objeto de la presente contratación, se aprecia lo siguiente:

> *"**1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES***
> *Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar [CONSIGNAR EL COSTO DE REPRODUCCIÓN DE*

[9] Mediante Trámite Documentario N° 2025-008868, de fecha 17 de enero de 2025.

LAS BASES] en [CONSIGNAR LA FORMA Y LUGAR PARA REALIZAR EL PAGO Y RECABAR LAS BASES].”

Ahora bien, de la revisión del numeral 1.9 del Capítulo I de la Sección Específica de las Bases Integradas no definitivas, se aprecia lo siguiente:

“(...)
CAPÍTULO I
(...)
1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES
Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/. 5.00 (cinco con 00/100 Soles), costo que incluye el costo de reproducción de las bases y cuya cancelación se realizará en la Caja de la Entidad, situada en Jr. Domingo Cueto Nro. 120 – Jesús María”.

De lo expuesto, se advierte que, si bien la Entidad determinó que los participantes pueden recabar un ejemplar de las Bases, la forma y lugar de pago, sin embargo, la Entidad omitió consignar la forma y lugar para recabar las referidas Bases, conforme a lo requerido en las Bases estándar aplicables.

En ese contexto, mediante el documento Nota N° 07-2025-CP-SM-11-2024-ESSALUD/GCL-1[10], el área usuaria de la Entidad precisó lo siguiente:

“(...)
En ese sentido se adecuará el contenido del numeral 1.9 “Costo de Reproducción y Entrega de Bases”, del Capítulo I de la Sección Específica de las Bases Integradas Definitivas, conforme a lo siguiente:

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES
Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/. 5.00 (cinco con 00/100 Soles), costo que incluye el costo de reproducción de las bases y cuya cancelación se realizará en la Caja Central de la Gerencia de Tesorería de la Gerencia Central de Gestión Financiera de Essalud, sito Jr. Domingo Cueto Nro. 120 – Jesús María, en el horario de 08:00 a 17:00 horas.

Una vez efectuado el pago por el costo de reproducción de bases, este se recaba en la Gerencia de Tesorería de la Gerencia Central de Gestión Financiera de Essalud, sito en el Segundo Piso de la Sede Central de EsSalud (ubicado en el Jr. Domingo Cueto Nro. 120 – Jesús María), en el horario de 08:00 a 17:00 horas”.

(El subrayado y resaltado es agregado)

En ese sentido, considerando lo declarado en el informe técnico de la Entidad y con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

[10] Mediante Trámite Documentario N° 2025-008868, de fecha 17 de enero de 2025.

- **<u>Se adecuará</u>** el numeral 1.9 del Capítulo I de la Sección Específica de las Bases Integradas Definitivas, según el siguiente detalle:

> *"(...)*
> ***CAPÍTULO I***
> *(...)*
> ***1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES***
> *Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/. 5.00 (cinco con 00/100 Soles), costo que incluye el costo de reproducción de las bases y cuya cancelación se realizará en la Caja Central de la Gerencia de Tesorería de la Gerencia Central de Gestión Financiera de Essalud, ~~de la Entidad, situada~~ sito en Jr. Domingo Cueto Nro. 120 – Jesús María, en el horario de 08:00 a 17:00 horas.*
>
> *Una vez efectuado el pago por el costo de reproducción de bases, este se recaba en la Gerencia de Tesorería de la Gerencia Central de Gestión Financiera de Essalud, sito en el Segundo Piso de la Sede Central de EsSalud (ubicado en el Jr. Domingo Cueto Nro. 120 – Jesús María), en el horario de 08:00 a 17:00 horas.*

- **<u>Se dejará sin efecto y/o ajustará</u>** todo extremo del pliego absolutorio, las Bases o Informe Técnico que se oponga a las disposiciones previstas en los párrafos anteriores.

3.3. Respecto a los requisitos para perfeccionar el contrato

De la revisión de los literales b), j), k), l), m), n) o), y p) del numeral 2.3, del Capítulo II, de la Sección Específica de las Bases Integradas no definitivas, se aprecia lo siguiente:

> *"**2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO***
> *El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:*
> *(...)*
> *b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.*
>
> *(...)*
>
> *j) Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete[11].*
> *k) Deberá presentar como requisito para la suscripción del contrato los documentos que acrediten que todo el personal que realizará los trabajos cuenta con "Seguro Complementario de Trabajo de Riesgo (SCTR)" vigente, con cobertura de salud y pensiones por accidente de trabajo y enfermedad profesional.*
> *l) Deberán presentarse en copia de las certificaciones del jefe de proyecto como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.*
> *m) Deberán presentarse en copia de las certificaciones del jefe del Proyecto para el Sistema de Gestión de Seguridad de la información como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y*

[11] Incluir solo en caso de contrataciones por paquete.

serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.
n) Deberán presentarse en copia de las certificaciones del especialista en Normatividad de Seguridad de la Información como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.
o) Deberán presentarse en copia de las certificaciones del ingeniero Especialista como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.
p) Deberán presentarse en copia de las certificaciones del Residente de Operación como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.
(...)"

Al respecto, de la revisión de los citados documentos para perfeccionar el contrato, se aprecia que, la Entidad habría determinado la presentación de diversos documentos, conforme a lo descrito, de lo cual se advierte lo siguiente:

- Respecto a los documentos solicitados en los literales b) y j), correspondiente a la "Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso" y "Detalle del precio de la oferta de cada uno de los bienes que conforman el paquete", se advierte que conforme a la ficha del SEACE del procedimiento, esta no contempla prestaciones accesorias, ni la contratación por "paquete".

- Respecto a los documentos solicitados, en los literales k), l), m), n), o), y p), se aprecia que los extremos requeridos no resultan claros, debiendo aclarar cada requisito conforme al Principio de Transparencia, consignado en el literal c) del artículo 2 de la Ley, que establece que la Entidad debe proporcionar información clara y coherente con el fin de que ésta sea comprendida por todos los potenciales proveedores.

En ese contexto, mediante el documento Nota N° 07-2025-CP-SM-11-2024-ESSALUD/GCL-1[12], el área usuaria de la Entidad precisó lo siguiente:

"(...)
Respuesta:

En ese sentido, considerando lo señalado en los documentos solicitados en los literales b) y j), correspondientes a la "Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso" y "Detalle del precio de la oferta de cada uno de los bienes que conforman el paquete", ***se suprimirá ya que este procedimiento no contempla prestaciones accesorias y no determina paquete.***

Así mismo, se dejará sin efecto todo extremo de las Bases o el Pliego que contravenga a la presente disposición.

[12] Mediante Trámite Documentario N° 2025-008868, de fecha 17 de enero de 2025.

(...)

De acuerdo a lo expuesto en los literales k), l), m), n), o), y p), del numeral 2.3, del Capítulo II de la Sección Especifica de las Bases Integradas definitivas, se realizará la corrección, de la siguiente manera:

k) El postor ganador de la buena pro, deberá presentar el Seguro Complementario de Trabajo de Riesgo (SCTR) vigente con cobertura de salud y pensiones por accidente de trabajo y enfermedad profesional de todo el personal que realizará los trabajos.
l) Copia de las certificaciones del jefe de Proyecto para la malla de seguridad (Personal Clave), las mismas que deberán estar vigentes durante la ejecución de la prestación.
m) Copia de las certificaciones del jefe de Proyecto para el Sistema de Gestión de la Seguridad de Información (Personal Clave), las mismas que deberán estar vigente durante la ejecución de la prestación.
n) Copia de las certificaciones del especialista en Normativa de Seguridad de la Información (Personal Clave), las mismas que deberán estar vigentes durante la ejecución de la prestación.
o) Copia de las certificaciones del ingeniero especialista (Personal Clave), las mismas que deberán estar vigentes durante la ejecución de la prestación.
p) Copia de las certificaciones (facultativo) del residente de operación (personal clave), las mismas que deberán estar vigente durante la ejecución de la prestación."

(El subrayado y resaltado es agregado)

En ese sentido, considerando lo declarado en el informe técnico de la Entidad y con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se suprimirán** los literales b) y j) del numeral 2.3 del Capítulo II de la Sección Específica de las Bases Integradas definitivas.

- **Se adecuarán** los literales k), l), m), n), o), y p), del numeral 2.3 del Capítulo II de la Sección Específica de las Bases Integradas definitivas, según el siguiente detalle:

*"**2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO***
El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:
(...)
k) Deberá presentar ~~como requisito para la suscripción del contrato los documentos que acrediten que todo el personal que realizará los trabajos cuenta con~~ "Seguro Complementario de Trabajo de Riesgo (SCTR)" vigente, con cobertura de salud y pensiones por accidente de trabajo y enfermedad profesional de todo el personal que realizará los trabajos.
l) ~~Deberán presentarse en~~ Copia de las certificaciones del jefe de proyecto para la malla de seguridad (Personal Clave), ~~como requisito para la suscripción del contrato~~, las mismas que deberán estar vigentes durante la ejecución de la prestación ~~y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.~~
m) ~~Deberán presentarse en~~ Copia de las certificaciones del jefe del Proyecto para el Sistema de Gestión de la Seguridad de ~~la~~ Información (Personal Clave), ~~como requisito para la suscripción del contrato,~~ las mismas que deberán estar vigentes durante la ejecución de la prestación. ~~y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y~~

~~*Comunicaciones.*~~
n) ~~*Deberán presentarse en*~~ *Copia de las certificaciones del especialista en Normativa* ~~*idad*~~ *de Seguridad de la Información (Personal Clave),* ~~*como requisito para la suscripción del contrato,*~~ *las mismas que deberán estar vigentes durante la ejecución de la prestación.* ~~*y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.*~~
o) ~~*Deberán presentarse en*~~ *Copia de las certificaciones del ingeniero Especialista (Personal Clave),* ~~*como requisito para la suscripción del contrato,*~~ *las mismas que deberán estar vigentes durante la ejecución de la prestación.* ~~*y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.*~~
p) ~~*Deberán presentarse en*~~ *Copia de las certificaciones (facultativo) del Residente de Operación (personal clave),* ~~*como requisito para la suscripción del contrato,*~~ *las mismas que deberán estar vigentes durante la ejecución de la prestación.* ~~*y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.*~~
(...)"

- **<u>Se dejará sin efecto y/o ajustará</u>** todo extremo del pliego absolutorio, las Bases o Informe Técnico que se oponga a las disposiciones previstas en los párrafos anteriores.

3.4. Respecto a la forma de pago

De la revisión conjunta del numeral 2.5 del Capítulo II y el acápite 5.23 del numeral 3.1 del Capítulo III, ambos pertenecientes a la Sección Específica de las Bases Integradas no definitivas, se aprecia que la Entidad consignó lo siguiente:

*"**CAPÍTULO II***
(...)
2.5. FORMA DE PAGO
La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS PARCIALES.
PRIMER ENTREGABLE
Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:
- *Informe del funcionario responsable de la Gerencia Central de Tecnología de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada previo informe de la Oficina de Seguridad Informática.*
- *Comprobante de pago.*
- *Acta de conformidad de puesta en producción*

Dicha documentación se debe presentar en en la Sub Gerencia de Adquisiciones de la Gerencia de Abastecimiento de la Gerencia Central de Logística, sitio en Av. Arenales N° 1402- Jesus Maria – 5 Piso, en horario de 08:00 horas a 16:00 p.m.

A PARTIR DEL SEGUNDO ENTREGABLE
Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:
- *Informe del funcionario responsable de la Gerencia Central de Tecnología de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada*

previo informe de la Oficina de Seguridad Informática.
- *Comprobante de pago.*
- *Acta de conformidad de puesta en producción*

Dicha documentación se debe presentar en en la Sub Gerencia de Adquisiciones de la Gerencia de Abastecimiento de la Gerencia Central de Logística, sitio en Av. Arenales N° 1402- Jesus Maria – 5 Piso, en horario de 08:00 horas a 16:00 p.m.

(...)

CAPÍTULO III
(...)
5.23 Forma de pago
5.23.1 *El pago de la contraprestación pactada a favor del contratista será en pagos parciales, luego de la emisión de las conformidades de entregables, según lo descrito en el numeral 5.13 según detalle siguiente:*
(...)"

(El subrayado y resaltado es agregado)

Al respecto, de la revisión de los extremos citados de las Bases, se aprecia que, la Entidad ha previsto que la forma de pago considere condiciones, acciones, además de documentación diversa; que deben ser acreditadas conforme al numeral 5.13; no obstante, de la revisión del numeral 2.5 de las Bases integradas, se aprecian exigencias diferentes a las requeridas por el área usuaria, por lo que dichas divergencias podrían generar confusión a los participantes, vulnerando lo establecido en el Principio de Transparencia.

En ese contexto, mediante el documento Nota N° 07-2025-CP-SM-11-2024-ESSALUD/GCL-1[13], el área usuaria de la Entidad precisó lo siguiente:

"(...)
Forma de pago
El pago de la contraprestación pactada a favor del contratista será en pagos parciales, luego de la emisión de las conformidades de entregables, ***según lo descrito en el numeral 5.13 según el siguiente detalle****:(...)"*

(El subrayado y resaltado es agregado)

En ese sentido, considerando lo indicado en el informe técnico de la Entidad y con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se adecuará** el contenido del numeral 2.5 del Capítulo II y del acápite 5.13 del numeral 3.1 del Capítulo III, de la Sección Específica de las Bases Integradas Definitivas, conforme a lo siguiente:

  *"**CAPÍTULO II***
  (...)
  2.5. FORMA DE PAGO

[13] Mediante Trámite Documentario N° 2025-008868, de fecha 17 de enero de 2025.

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS PARCIALES.

PRIMER ENTREGABLE

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- ***EL PROVEEDOR** deberá presentar el informe técnico inicial correspondiente, donde describirá la metodología que utilizará para la configuración de los componentes de la solución de seguridad que se está proponiendo y la cual será adecuada a la necesidad operacional de **ESSALUD.***
- *Acta de conformidad de puesta en producción.*
- *Presentación del informe detallado sobre las labores de implantación y migración.*
- *Se deberán presentar informes técnicos indicando los incidentes presentados y requerimientos atendidos durante el periodo de 30 días, y las actividades de soporte realizadas, estos informes se entregarán mensualmente, y el periodo de inicio se contabilizará desde el día siguiente de suscrito el contrato; Estos informes deberán ser entregados en formato digital, vía la mesa de partes institucional (virtual: https://mpv.essalud.gob.pe/Login/Index).*
- *En caso de que se presente algún incidente dentro del periodo del entregable en relación a la atención de requerimientos, se deberá generar el informe técnico correspondiente de la incidencia en cualquier momento en que se presente y/o a demanda de ESSALUD; este informe técnico deberá indicar al menos lo siguiente:*
  - *Incidentes presentados durante el periodo de la implementación y servicio.*
  - *Actividades realizadas para la resolución del incidente.*
  - *El informe técnico se entregará en formato digital, adjuntando anexos para obtener la mayor cantidad de información de los incidentes ocurridos vía la mesa de partes virtual (https://mpv.essalud.gob.pe/Login/Index) de ESSALUD, inmediatamente después de solucionada la incidencia.*
  - *Así mismo, el Informe Técnico deberá estar dirigido al jefe de la Oficina de Seguridad Informática, indicando detalladamente las actividades realizadas según los tiempos establecidos en el numeral 5.10.1., los mismos que deberán ser requisito indispensable para las conformidades mensuales de atención de requerimientos y el pago de los mismos.*
- *Informe de Implementación del Sistema de Gestión de Seguridad de la Información – SGSI, en cumplimiento de lo establecido en la etapa N°1 del numeral 5.2.3.2 del presente termino de referencia.*
- *Informe de Capacitación, que contenga el syllabus de los temas tratados, los certificados para cada uno de los asistentes, el listado de asistencia firmado por los asistentes y el instructor y una copia de los materiales entregados en formato digital, dentro del plazo establecido en el numeral 5.2.2. literal f.*

- ~~*Informe del funcionario responsable de la Gerencia Central de Tecnología de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada previo informe de la Oficina de Seguridad Informática.*~~
- *Comprobante de pago.*
- ~~*Acta de conformidad de puesta en producción*~~

Dicha documentación se debe presentar en en la Sub Gerencia de Adquisiciones de la Gerencia de Abastecimiento de la Gerencia Central de Logística, sitio en Av. Arenales N° 1402- Jesus Maria – 5 Piso, en horario de 08:00 horas a 16:00 p.m.

A PARTIR DEL SEGUNDO ENTREGABLE

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Se deberán presentar informes técnicos indicando los incidentes presentados y requerimientos atendidos durante el periodo de 30 días, y las actividades de soporte realizadas; estos informes se entregarán mensualmente. Estos informes deberán ser entregados en formato digital, vía la mesa de partes institucional (virtual: https://mpv.essalud.gob.pe/Login/Index), de ESSALUD.

- En caso de que se presente algún incidente en la atención de requerimientos, se deberá generar el informe técnico correspondiente de la incidencia en cualquier momento en que se presente y/o a demanda de ESSALUD; este informe técnico deberá indicar al menos lo siguiente:

- *Incidentes presentados durante el periodo de la implementación y servicio.*
- *Actividades realizadas para la resolución del incidente.*
- *El informe técnico se entregará en formato digital, adjuntando anexos para obtener la mayor cantidad de información de los incidentes ocurridos vía la mesa de partes virtual (https://mpv.essalud.gob.pe/Login/Index) de ESSALUD, inmediatamente después de solucionada la incidencia.*
- *Así mismo, el Informe Técnico deberá estar dirigido al jefe de la Oficina de Seguridad Informática, indicando detalladamente las actividades realizadas según los tiempos establecidos en el numeral 5.10.1., los mismos que deberán ser requisito indispensable para las conformidades mensuales de atención de requerimientos y el pago de los mismos.*
- *Informe de Capacitación, que contenga el syllabus de los temas tratados, los certificados para cada uno de los asistentes, el listado de asistencia firmado por los asistentes y el instructor y una copia de los materiales entregados en formato digital, dentro del plazo establecido en el numeral 5.2.2. literal f.*

- Informe de Implementación del Sistema de Gestión de Seguridad de la Información – SGSI

- ~~Informe del funcionario responsable de la Gerencia Central de Tecnología de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada previo informe de la Oficina de Seguridad Informática.~~

- Comprobante de pago.

- ~~Acta de conformidad de puesta en producción~~

ENTREGABLE	***PLAZO DE ENTREGA***
*Informe con la documentación asociada al desarrollo de la **Etapa 2**, según lo establecido en el numeral 5.2.3.2 del presente termino de referencia.*	*Hasta los 90 días calendarios.*
*Informe con la documentación asociada al desarrollo de la **Etapa 3** según lo establecido en el numeral 5.2.3.2 del presente termino de referencia.*	*Hasta los 180 días calendarios.*
*Informe con la documentación asociada al desarrollo de la **Etapa 4** según lo establecido en el numeral 5.2.3.2 del presente termino de referencia.*	*A los 240 días calendarios.*
Informe final de implementación del SGSI	*A los 240 días calendarios.*

Dicha documentación se debe presentar en en la Sub Gerencia de Adquisiciones de la Gerencia de Abastecimiento de la Gerencia Central de Logística, sitio en Av. Arenales N° 1402- Jesus Maria – 5 Piso, en horario de 08:00 horas a 16:00 p.m.

(...)

CAPÍTULO III

(...)

5.13 Entregables ***PARA EL PRIMER ENTREGABLE*** *(…)* *Comprobante de pago.* ***A PARTIR DEL SEGUNDO ENTREGABLE*** *(…)* *Comprobante de pago.* *(…)"*

- **<u>Se dejará sin efecto y/o ajustará</u>** todo extremo del pliego absolutorio, las Bases o Informe Técnico que se oponga a las disposiciones previstas en los párrafos anteriores.

3.5. Respecto de la duplicidad de requisitos de calificación

Al respecto, de la revisión de las Bases Integradas, se aprecia que la Entidad consignó los "requisitos de calificación" de forma duplicada; de forma que se encuentran tanto en el numeral 3.1 "Términos de referencia", como en el numeral 3.2 del Capítulo III, ambos pertenecientes a la Sección Específica de las Bases Integradas, los cuales podrían generar confusión en los participantes. Por lo que, con ocasión de las Bases Integradas Definitivas, se implementará la siguiente disposición:

Firmado digitalmente por LAURA SILVA Anthony David FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 06.02.2025 17:32:36 -05:00

- **<u>Se suprimirá</u>** todo extremo del numeral 3.1 del Capítulo III de la Sección Específica de las Bases Integradas Definitivas, relacionada a los "requisitos de calificación".

Firmado digitalmente por CHAMOCHUMBI CHERRE Carlos Ernesto FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 06.02.2025 17:28:06 -05:00

- **<u>Se dejará sin efecto y/o ajustará</u>** todo extremo del pliego absolutorio, las Bases o Informe Técnico que se oponga a las disposiciones previstas en los párrafos anteriores.

4. CONCLUSIONES

Firmado digitalmente por VARGAS PEREZ Wilberth FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 06.02.2025 17:24:07 -05:00

En virtud de lo expuesto, este Organismo Técnico Especializado ha dispuesto:

4.1 Se procederá a la integración definitiva de las Bases a través del SEACE, en atención a lo establecido en el artículo 72 del Reglamento.

4.2 Corresponde al Titular de la Entidad, iniciar el respectivo deslinde de responsabilidades, así como impartir las directrices pertinentes a fin de que los funcionarios encargados, en futuros procedimientos de selección, brinden atención – de manera oportuna- a los requerimientos efectuados por este Organismo Técnico Especializado.

4.3 Es preciso indicar que contra el pronunciamiento emitido por el OSCE no cabe interposición de recurso administrativo alguno, siendo de obligatorio cumplimiento para la Entidad y los proveedores que participan en el procedimiento de selección.

Adicionalmente, cabe señalar que, las disposiciones vertidas en el pliego absolutorio que generen aclaraciones, modificaciones o precisiones, priman sobre los aspectos relacionados con las Bases integradas, salvo aquellos que fueron materia del presente pronunciamiento.

4.4 Una vez emitido el pronunciamiento y registrada la integración de Bases definitivas por el OSCE, corresponderá al comité de selección **modificar** en el cronograma del procedimiento, las fechas del registro de participantes, presentación de ofertas y otorgamiento de la buena pro, teniendo en cuenta que, entre la integración de Bases y la presentación de propuestas no podrá mediar menos de siete (7) días hábiles, computados a partir del día siguiente de la publicación de las Bases integradas en el SEACE, conforme a lo dispuesto en el artículo 70 del Reglamento.

4.5 Finalmente, se recuerda al Titular de la Entidad que el presente pronunciamiento no convalida extremo alguno del procedimiento de selección.

Jesús María, 6 de febrero de 2025

Código: 6.1, 14.1

Firmado digitalmente por FLORES BAZAN Miguel Angel FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 06.02.2025 17:42:36 -05:00