



**BASES PARA LA CONTRATACIÓN DIRECTA DE
SERVICIOS EN GENERAL**

CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA

CONTRATACIÓN DE SERVICIOS:

**“SERVICIO DE SEGURIDAD DE LAS COMUNICACIONES
DEL CCFFAA, DE LA MARCA CHECK POINT O
EQUIVALENTE”**

PAC N° 88

2024



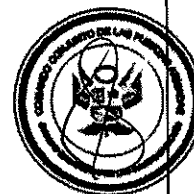
DEBER DE COLABORACIÓN

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista, deben conducir su actuación conforme a los principios previstos en la Ley de Contrataciones del Estado.

En este contexto, se encuentran obligados a prestar su colaboración al OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI, en todo momento según corresponda a sus competencias, a fin de comunicar presuntos casos de fraude, colusión y corrupción por parte de los funcionarios y servidores de la Entidad, así como los proveedores y demás actores que participan en el proceso de contratación.

De igual forma, deben poner en conocimiento del OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión de Conductas Anticompetitivas", o norma que la sustituya, así como las demás normas de la materia.

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir al OSCE o a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información referida a las contrataciones del Estado que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.



SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

(ESTA SECCIÓN NO DEBE SER MODIFICADA EN NINGÚN EXTREMO, BAJO SANCIÓN DE NULIDAD)

CAPÍTULO III DEL CONTRATO



3.1. PERFECCIONAMIENTO DEL CONTRATO

Los plazos y el procedimiento para perfeccionar el contrato se realiza conforme a lo indicado en el artículo 141 del Reglamento.

El contrato se perfecciona con la suscripción del documento que lo contiene, salvo en los contratos cuyo monto del valor estimado no supere los doscientos mil Soles (S/ 200,000.00), en los que se puede perfeccionar con la recepción de la orden de servicios, conforme a lo previsto en la sección específica de las bases.

Importante

El órgano encargado de las contrataciones o el comité de selección, según corresponda, debe consignar en la sección específica de las bases la forma en que se perfeccionará el contrato, sea con la suscripción del contrato o la recepción de la orden de servicios. En caso la Entidad perfeccione el contrato con la recepción de la orden de servicios no debe incluir la proforma del contrato establecida en el Capítulo V de la sección específica de las bases.

Para perfeccionar el contrato, el postor ganador de la buena pro debe presentar los documentos señalados en el artículo 139 del Reglamento y los previstos en la sección específica de las bases.

3.2. GARANTÍAS

Las garantías que deben otorgar los postores y/o contratistas, según corresponda, son las de fiel cumplimiento del contrato y por los adelantos.

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

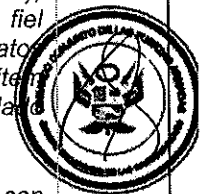
Como requisito indispensable para perfeccionar el contrato, el postor ganador debe entregar a la Entidad la garantía de fiel cumplimiento del mismo por una suma equivalente al diez por ciento (10%) del monto del contrato original. Esta se mantiene vigente hasta la conformidad de la recepción de la prestación a cargo del contratista.

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación accesorio, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

- En los contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados no superen el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.
- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y el numeral 151.2 del artículo 151 del Reglamento.



3.2.3. GARANTÍA POR ADELANTO

En caso se haya previsto en la sección específica de las bases la entrega de adelantos, el contratista debe presentar una garantía emitida por idéntico monto conforme a lo estipulado en el artículo 153 del Reglamento.

3.3. REQUISITOS DE LAS GARANTÍAS

Las garantías que se presenten deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la Entidad. Asimismo, deben ser emitidas por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

Importante

Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro y/o contratista cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.

Advertencia

Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente:

1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).
2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.
3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.
4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.

En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.

De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza>).

Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.



3.4. EJECUCIÓN DE GARANTÍAS

La Entidad puede solicitar la ejecución de las garantías conforme a los supuestos contemplados en el artículo 155 del Reglamento.

3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento.

3.6.2. OTRAS PENALIDADES

La Entidad puede establecer penalidades distintas a la mencionada en el numeral precedente, según lo previsto en el artículo 163 del Reglamento y lo indicado en la sección específica de las bases.

Estos dos tipos de penalidades se calculan en forma independiente y pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

3.7. INCUMPLIMIENTO DEL CONTRATO

Las causales para la resolución del contrato, serán aplicadas de conformidad con el artículo 36 de la Ley y 164 del Reglamento.

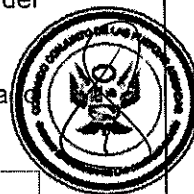
3.8. PAGOS

El pago se realiza después de ejecutada la respectiva prestación, pudiendo contemplarse pagos a cuenta, según la forma establecida en la sección específica de las bases o en el contrato.

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

La conformidad se emite en un plazo máximo de siete (7) días de producida la recepción salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad del funcionario que debe emitir la conformidad.

En el caso que se haya suscrito contrato con un consorcio, el pago se realizará de acuerdo a lo que se indique en el contrato de consorcio.



Advertencia

En caso de retraso en los pagos a cuenta o pago final por parte de la Entidad, salvo que se deba a caso fortuito o fuerza mayor, esta reconoce al contratista los intereses legales correspondientes, de conformidad con el artículo 39 de la Ley y 171 del Reglamento, debiendo repetir contra los responsables de la demora injustificada.

3.9. DISPOSICIONES FINALES

Todos los demás aspectos del presente procedimiento no contemplados en las bases se regirán supletoriamente por la Ley y su Reglamento, así como por las disposiciones legales vigentes.

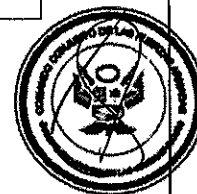


SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

(EN ESTA SECCIÓN LA ENTIDAD DEBERÁ COMPLETAR LA INFORMACIÓN EXIGIDA, DE ACUERDO A LAS INSTRUCCIONES INDICADAS)

CAPÍTULO I GENERALIDADES



1.1. ENTIDAD CONVOCANTE

Nombre : COMANDO CONJUNTO DE LAS FUERZAS ARMADAS
RUC N° : 20131380870
Domicilio legal : Jr. Nicolas Corpancho N° 289 – Urb. Santa Beatriz – Cercado de Lima - Lima
Teléfono: : 315-1030 anexo: 2477
Correo electrónico: : logistica@ccffaa.mil.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del “**Servicio de seguridad de las comunicaciones del CCFFAA, de la marca Check Point o equivalente**”.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado Formato de Solicitud y Aprobación de Expediente de Contratación N° 049, de fecha 16 de octubre del 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios.

Importante

La fuente de financiamiento debe corresponder a aquella prevista en la Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal en el cual se convoca el procedimiento de selección.

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de A SUMA ALZADA, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. MODALIDAD DE EJECUCIÓN

Llave en Mano.

1.7. DISTRIBUCIÓN DE LA BUENA PRO

No aplica.

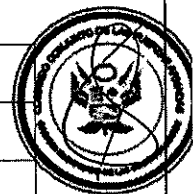
1.8. ALCANCES DEL REQUERIMIENTO

El alcance de la prestación está definido en el Capítulo III de la presente sección de las bases.

1.9. PLAZO DE PRESTACIÓN DEL SERVICIO

Plazos en los que se ejecutará el servicio

Detalle	Plazo
Entrega de Licenciamiento	Cinco (05) días
Entrega en almacén, Instalación y puesta en funcionamiento del Equipamiento	Setenta (70) días
Capacitación	Cinco (05) días
TOTAL	Ochenta (80) días calendario



Computados a partir del día siguiente de la suscripción del contrato, en concordancia con lo establecido en el expediente de contratación.

El plazo de ejecución de las prestaciones accesorias es de tres (03) años, equivalente a mil noventa y cinco (1095) días calendario, contando a partir del día siguiente de la suscripción del contrato y activación del servicio.

PLAZO DE LA PRESTACIÓN PRINCIPAL

Plazo de entrega del Licenciamiento, Equipamiento y Capacitación

Como plazo máximo cinco (05) días calendarios posteriores de la suscripción del contrato y la entrega formal al área y equipos a intervenir para las renovaciones indicadas del numeral 5.2.1 al 5.2.3.

5.2.1
Licenciamiento y soporte del fabricante

Cuadro N° 1

SKU	Nombre del producto	Cant
CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01

5.2.2
Licenciamiento y soporte del fabricante

Cuadro N° 2

SKU	Nombre del producto	Cant
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02

5.2.3
Licenciamiento y suscripción a las siguientes soluciones

Cuadro N° 3

SKU	Nombre del producto	Cant
CP-HAR-EP-COMplete	Harmony Endpoint Complete	450
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400

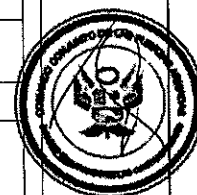
5.2.4
Equipamiento

Cuadro N° 4

N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS
01	Equipo Firewall Perimetral	01	ANEXO A
02	Equipo Firewall DataCenter	01	ANEXO B
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C

Como plazo máximo para la entrega, instalación y configuración del equipamiento del numeral 5.2.4, será de setenta (70) días calendario contados a partir del día siguiente de suscrito el contrato y sin perjuicio de realizar

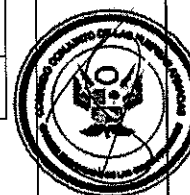
entregas parciales. Asimismo, para dicho efecto se suscribirá un acta de instalación y configuración del equipamiento.	04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D
	05	Equipo Firewall Perimetral Remoto	03	ANEXO E
	06	Switch Acceso Remoto	02	ANEXO F
	07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G
	08	Equipo virtual para protección de aplicaciones web	01	ANEXO H
	09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I
	10	Gabinete Autocontenido	01	ANEXO J
	11	Equipo de AA Confort	01	ANEXO K
	12	Equipo UPS	01	ANEXO L
Para el Numeral 5.2.5, la capacitación tendrá un plazo máximo de CINCO (05) días, posterior a la implementación total del equipamiento, y esta se sustentará bajo un acta de conformidad de la unidad usuaria.	5.2.5 Capacitación			
	Cuadro N° 5			
	N°	ITEM	MODALIDAD	Cant.
	01	Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)	Presencial	10 Personas
	02	Curso de la solución de seguridad de firewall a nivel de administración y/o experto	Curso no oficial	05 Personas
03	Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall	Voucher de Certificación	05 Personas	



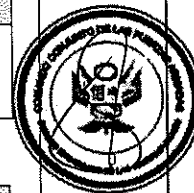
PLAZO DE LA PRESTACIÓN ACCESORIA

El periodo de la prestación accesoria, tendrá un periodo de tres (03) años, equivalente a mil noventa y cinco (1095) días calendario, para lo cual el proveedor deberá brindar los servicios consignados en el numeral 5.3 de los Términos de Referencia del Capítulo III de la Sección Específica de las bases.

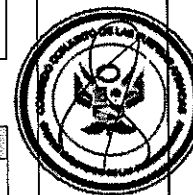
PRESTACIÓN ACCESORIA	PERIODO	EQUIPAMIENTO A INTERVENIR		
Servicio de mantenimiento preventivo para todo el equipamiento detallado en el cuadro N° 1, N° 2, N° 3, N° 4.	AF-2024	Cuadro N° 1 (Pre-existent)		
		SKU	Nombre del producto	Cant
		CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01
		Cuadro N° 2 (Pre-existent)		
		SKU	Nombre del producto	Cant
		CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02



		<table><tr><th colspan="3">Cuadro N° 3 (Pre-existent)</th></tr><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CP-HAR-EP-COMLETE</td><td>Harmony Endpoint Complete</td><td>450</td></tr><tr><td>CP-INFINITY-XPR</td><td>Extended Detection/Prevention & Response.</td><td>400</td></tr></table>	Cuadro N° 3 (Pre-existent)			SKU	Nombre del producto	Cant	CP-HAR-EP-COMLETE	Harmony Endpoint Complete	450	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																																																																										
Cuadro N° 3 (Pre-existent)																																																																																								
SKU	Nombre del producto	Cant																																																																																						
CP-HAR-EP-COMLETE	Harmony Endpoint Complete	450																																																																																						
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																																																																																						
AF-2025		<table><tr><th colspan="3">Cuadro N° 1 (Pre-existent)</th></tr><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CPSB-NGTP-1600-3Y</td><td>1600 Base Appliance with Threat Prevention (NGTP) subscription package</td><td>01</td></tr></table> <table><tr><th colspan="3">Cuadro N° 2 (Pre-existent)</th></tr><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CON-SNTP-C93002TA</td><td>Catalyst 9300 SNTC 24X7X4</td><td>02</td></tr></table> <table><tr><th colspan="3">Cuadro N° 3 (Pre-existent)</th></tr><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CP-HAR-EP-COMLETE</td><td>Harmony Endpoint Complete</td><td>450</td></tr><tr><td>CP-INFINITY-XPR</td><td>Extended Detection/Prevention & Response.</td><td>400</td></tr></table> <table><tr><th colspan="4">Cuadro N° 4 (1er Mantenimiento)</th></tr><tr><th>N°</th><th>Nombre del producto</th><th>Cant</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr><tr><td>01</td><td>Equipo Firewall Perimetral</td><td>01</td><td>ANEXO A</td></tr><tr><td>02</td><td>Equipo Firewall DataCenter</td><td>01</td><td>ANEXO B</td></tr><tr><td>03</td><td>Equipo Virtual para Administración y Correlación de Eventos y Reportes</td><td>01</td><td>ANEXO C</td></tr><tr><td>04</td><td>Equipo Sandboxing para Emulación de Amenazas de día cero</td><td>01</td><td>ANEXO D</td></tr><tr><td>05</td><td>Equipo Firewall Perimetral Remoto</td><td>03</td><td>ANEXO E</td></tr><tr><td>06</td><td>Switch Acceso Remoto</td><td>02</td><td>ANEXO F</td></tr><tr><td>07</td><td>Equipo virtual para Protección de Correo Electrónico onpremise</td><td>01</td><td>ANEXO G</td></tr><tr><td>08</td><td>Equipo virtual para protección de aplicaciones web</td><td>01</td><td>ANEXO H</td></tr><tr><td>09</td><td>Equipo virtual para protección de bases de datos en reposo</td><td>01</td><td>ANEXO I</td></tr><tr><td>10</td><td>Gabinete Auto contenido</td><td>01</td><td>ANEXO J</td></tr><tr><td>11</td><td>Equipo de AA Confort</td><td>01</td><td>ANEXO K</td></tr><tr><td>12</td><td>Equipo UPS</td><td>01</td><td>ANEXO L</td></tr></table>	Cuadro N° 1 (Pre-existent)			SKU	Nombre del producto	Cant	CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01	Cuadro N° 2 (Pre-existent)			SKU	Nombre del producto	Cant	CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02	Cuadro N° 3 (Pre-existent)			SKU	Nombre del producto	Cant	CP-HAR-EP-COMLETE	Harmony Endpoint Complete	450	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400	Cuadro N° 4 (1er Mantenimiento)				N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS	01	Equipo Firewall Perimetral	01	ANEXO A	02	Equipo Firewall DataCenter	01	ANEXO B	03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C	04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D	05	Equipo Firewall Perimetral Remoto	03	ANEXO E	06	Switch Acceso Remoto	02	ANEXO F	07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G	08	Equipo virtual para protección de aplicaciones web	01	ANEXO H	09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I	10	Gabinete Auto contenido	01	ANEXO J	11	Equipo de AA Confort	01	ANEXO K	12	Equipo UPS	01	ANEXO L
	Cuadro N° 1 (Pre-existent)																																																																																							
	SKU	Nombre del producto	Cant																																																																																					
	CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01																																																																																					
	Cuadro N° 2 (Pre-existent)																																																																																							
	SKU	Nombre del producto	Cant																																																																																					
	CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02																																																																																					
	Cuadro N° 3 (Pre-existent)																																																																																							
	SKU	Nombre del producto	Cant																																																																																					
	CP-HAR-EP-COMLETE	Harmony Endpoint Complete	450																																																																																					
	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																																																																																					
	Cuadro N° 4 (1er Mantenimiento)																																																																																							
N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS																																																																																					
01	Equipo Firewall Perimetral	01	ANEXO A																																																																																					
02	Equipo Firewall DataCenter	01	ANEXO B																																																																																					
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C																																																																																					
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D																																																																																					
05	Equipo Firewall Perimetral Remoto	03	ANEXO E																																																																																					
06	Switch Acceso Remoto	02	ANEXO F																																																																																					
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G																																																																																					
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H																																																																																					
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I																																																																																					
10	Gabinete Auto contenido	01	ANEXO J																																																																																					
11	Equipo de AA Confort	01	ANEXO K																																																																																					
12	Equipo UPS	01	ANEXO L																																																																																					



AF-2026	Cuadro N° 1 (Pre-existent)			
	SKU		Nombre del producto	Cant
	CPSB-NGTP-1600-3Y		1600 Base Appliance with Threat Prevention (NGTP) subscription package	01
	Cuadro N° 2 (Pre-existent)			
	SKU		Nombre del producto	Cant
	CON-SNTP-C93002TA		Catalyst 9300 SNTC 24X7X4	02
	Cuadro N° 3 (Pre-existent)			
	SKU		Nombre del producto	Cant
	CP-HAR-EP-COMplete		Harmony Endpoint Complete	450
	CP-INFINITY-XPR		Extended Detection/Prevention & Response.	400
	Cuadro N° 4 (2do Mantenimiento)			
	N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS
	01	Equipo Firewall Perimetral	01	ANEXO A
02	Equipo Firewall DataCenter	01	ANEXO B	
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C	
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D	
05	Equipo Firewall Perimetral Remoto	03	ANEXO E	
06	Switch Acceso Remoto	02	ANEXO F	
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G	
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H	
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I	
10	Gabinete Autocontenido	01	ANEXO J	
11	Equipo de AA Confort	01	ANEXO K	
12	Equipo UPS	01	ANEXO L	
Servicio de soporte e incidentes para todo el equipamiento detallado en el cuadro N° 1, N° 2 N° 3 N° 4	AF-2024 AF-2025 AF-2026	Cuadro N° 1 (Pre-existent)		
		SKU	Nombre del producto	Cant
		CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01



Cuadro N° 2 (Pre-existent)

SKU	Nombre del producto	Cant
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02

Cuadro N° 3 (Pre-existent)

SKU	Nombre del producto	Cant
CP-HAR-EP-COMPLETE	Harmony Endpoint Complete	450
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400

Cuadro N° 4

N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS
01	Equipo Firewall Perimetral	01	ANEXO A
02	Equipo Firewall DataCenter	01	ANEXO B
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D
05	Equipo Firewall Perimetral Remoto	03	ANEXO E
06	Switch Acceso Remoto	02	ANEXO F
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I
10	Gabinete Auto contenido	01	ANEXO J
11	Equipo de AA Confort	01	ANEXO K
12	Equipo UPS	01	ANEXO L

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

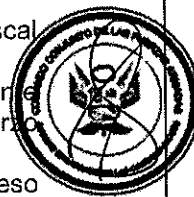
Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar TRECE CON 70/100 SOLES (S/ 13.70) de acuerdo a lo establecido en el TUPA del Ministerio de Defensa – Comando Conjunto de las Fuerzas Armadas. El pago se realizará en el Banco de la Nación en la Cuenta Corriente N° 0000-298220 a favor del Comando Conjunto de las Fuerzas Armadas. Pudiendo recabarlas en la Unidad de Logística del CCFFAA, en Jr. Nicolás Corpancho N° 289 – Urb. Santa Beatriz – Lima, en el horario de 08:00 horas a 16:00 horas.

Importante

El costo de entrega de un ejemplar de las bases no puede exceder el costo de su reproducción.

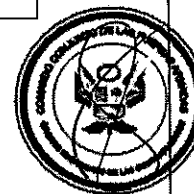
1.11. BASE LEGAL

- Ley N° 31953, Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N° 31954, Ley de Equilibrio Financiero del Presupuesto del Sector Público del Año Fiscal 2024.
- Texto Único Ordenado de la Ley N° 30225, aprobado mediante Decreto Supremo N° 082-2019-EF y publicado en el Diario Oficial El Peruano el 13 de marzo de 2019.
- Decreto Supremo N° 021-2019-JUS, TUO de la Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública
- Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Ley N° 30999, Ley de Ciberdefensa.
- Ley N° 31246, Ley que modifica la Ley N° 29783, Ley de Seguridad y Salud en el Trabajo.
- Decreto legislativo N° 295, Código Civil.
- Decreto Legislativo N° 1440, Decreto Legislativo del Sistema Nacional de Presupuesto Público.
- Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento. Modificado por Decreto Supremo N° 377-2019-EF, Decreto Supremo N° 168-2020-EF y Decreto Supremo N° 051-2024-EF.
- Decreto Supremo N° 008-2008-TR, Reglamento de la Ley MYPE.
- Decreto Supremo N° 005-2012-TR, Reglamento de la Ley de Seguridad y Salud en el Trabajo.
- Decreto Supremo N° 013-2013-PRODUCE - Texto Único Ordenado de la Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial.
- Decreto Supremo N° 004-2019-JUS, TUO de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 103-2020-EF, que establece disposiciones reglamentarias para la tramitación de los procedimientos de selección que se reinicien en el marco del TUO de la Ley 30225.
- Directivas y Opiniones emitidas por el OSCE.



Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN



2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

Según el cronograma de la ficha de selección de la convocatoria publicada en el SEACE.

2.2. CONTENIDO DE LAS OFERTAS

La oferta se presentará debidamente foliada y conteniendo la rúbrica del postor invitado o de su representante legal, debiendo ser remitida al correo electrónico logistica@ccffaa.mil.pe y de manera física presentada en UN (1) sobre cerrado en original, dirigido a la Unidad de Logística de la Oficina de Administración del Comando Conjunto de las Fuerzas Armadas para la CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA, conforme al siguiente detalle:

Señores
COMANDO CONJUNTO DE LAS FUERZAS ARMADAS
Atención: Unidad de Logística de la Oficina de Administración del CCFFAA

Jr. Nicolás Corpancho N° 289 – Urb. Santa Beatriz – Cercado de Lima – Lima

CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA

Denominación de la convocatoria: **SERVICIO DE SEGURIDAD DE LAS
COMUNICACIONES DEL CCFFAA, DE LA MARCA CHECK POINT O EQUIVALENTE**

OFERTA
[NOMBRE / DENOMINACIÓN O RAZÓN SOCIAL DEL POSTOR]

La oferta contendrá, además de un índice de documentos¹, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

- Declaración jurada de datos del postor. (**Anexo N° 1**)
- Documento que acredite la representación de quien suscribe la oferta.

En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.

En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.

En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

¹ La omisión del índice no determina la no admisión de la oferta.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE² y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.



- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento (Anexo N°2)
- d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo N° 3)
- e) Declaración jurada de plazo de prestación del servicio. (Anexo N° 4)³
- f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (Anexo N° 5)
- g) El precio de la oferta en SOLES. Adjuntar obligatoriamente el Anexo N° 6.

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

Importante

- El órgano encargado de las contrataciones o el comité de selección, según corresponda, verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.
- En caso de requerir estructura de costos o análisis de precios, esta se presenta para el perfeccionamiento del contrato.

2.2.1.2. Documentos para acreditar los requisitos de calificación

Incorporar en la oferta los documentos que acreditan los “Requisitos de Calificación” que se detallan en el numeral 3.2 del Capítulo III de la presente sección de las bases.

2.2.2. Documentación de presentación facultativa:

- a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad⁴.
- b) Solicitud de bonificación por tener la condición de micro y pequeña empresa. (Anexo N° 11)

² Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

³ En caso de considerar como factor de evaluación la mejora del plazo de prestación del servicio, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

⁴ Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

Advertencia

El órgano encargado de las contrataciones o el comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápite "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".



2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

- Garantía de fiel cumplimiento del contrato.
- Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁵ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- Domicilio para efectos de la notificación durante la ejecución del contrato.
- Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁶. (**Anexo N° 12**).
- Detalle de los precios unitarios del precio ofertado⁷.
- Estructura de costos⁸.
- Copia de la Certificación CheckPoint Security Expert (CCSE) ya sea la versión R80 o R81 y/o CheckPoint Security Master (CCSM) ya sea la versión R80 o R81 y/o la Certificación Check Point Certified Endpoint Specialist (CCES); o equivalente, con la que debe contar Un (01) especialista en soporte (Personal Clave).

Importante

- En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva Participación de Proveedores en Consorcio en las Contrataciones del Estado.*

⁵ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

⁶ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁷ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

⁸ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.



- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 y el numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.
- En los contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados no supere el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

Importante

- Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.
- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya⁹.
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en la Mesa de Partes del Comando Conjunto de las Fuerzas Armadas, sito en Jr. Nicolás Corpancho N° 289 – Santa Beatriz – Lima, en el horario de 08:00 a 16:00 horas.

2.5. FORMA DE PAGO

La Entidad realizará el pago de las contraprestaciones (Prestación Principal y Prestación Accesoría) pactadas a favor del contratista en TRES (03) PAGO PARCIALES, durante el periodo de tres (03) años de la siguiente manera:

PAGO	PORCENTAJE	CONDICIONES PARA EL PAGO
Primer pago AF-2024	30% del monto adjudicado	Se realizará previa conformidad de la activación de las licencias, soporte y suscripción indicadas del numeral 5.2.1 al 5.2.3: 5.2.1 Licenciamiento y soporte del fabricante

⁹ Según lo previsto en la Opinión N° 009-2016/DTN.



Cuadro N° 1

SKU	Nombre del producto	Cant
CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01

5.2.2 Licenciamiento y soporte del fabricante

Cuadro N° 2

SKU	Nombre del producto	Cant
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02

5.2.3 Licenciamiento y suscripción a las siguientes soluciones

Cuadro N° 3

SKU	Nombre del producto	Cant
CP-HAR-EP-COMplete	Harmony Endpoint Complete	450
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400

Así mismo a la entrega, instalación y configuración del equipamiento detallados en el numeral 5.2.4 y a la capacitación del personal de acuerdo al 5.2.5:

5.2.4 Equipamiento

Cuadro N° 4

N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS
01	Equipo Firewall Perimetral	01	ANEXO A
02	Equipo Firewall DataCenter	01	ANEXO B
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D
05	Equipo Firewall Perimetral Remoto	03	ANEXO E
06	Switch Acceso Remoto	02	ANEXO F
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I
10	Gabinete Autocontenido	01	ANEXO J
11	Equipo de AA Confort	01	ANEXO K
12	Equipo UPS	01	ANEXO L

5.2.5 Capacitación



		<div>Cuadro N° 5</div> <table><tr><th>N°</th><th>ITEM</th><th>MODALIDAD</th><th>Cant.</th></tr><tr><td>01</td><td>Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)</td><td>Presencial</td><td>10 Pers onas</td></tr><tr><td>02</td><td>Curso de la solución de seguridad de firewall a nivel de administración y/o experto</td><td>Curso no oficial</td><td>05 Pers onas</td></tr><tr><td>03</td><td>Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall</td><td>Voucher de Certificación</td><td>05 Pers onas</td></tr></table>	N°	ITEM	MODALIDAD	Cant.	01	Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)	Presencial	10 Pers onas	02	Curso de la solución de seguridad de firewall a nivel de administración y/o experto	Curso no oficial	05 Pers onas	03	Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall	Voucher de Certificación	05 Pers onas																																					
N°	ITEM	MODALIDAD	Cant.																																																				
01	Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)	Presencial	10 Pers onas																																																				
02	Curso de la solución de seguridad de firewall a nivel de administración y/o experto	Curso no oficial	05 Pers onas																																																				
03	Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall	Voucher de Certificación	05 Pers onas																																																				
Segundo pago AF-2025	35% del monto adjudicado	<div>Al culminar el primer año del contrato, asimismo, luego de la conformidad por parte del área usuaria del correcto funcionamiento, soporte y mantenimiento de los productos solicitados.</div> <div>Cuadro N° 1 (Pre-existent)</div> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CPSB-NGTP-1600-3Y</td><td>1600 Base Appliance with Threat Prevention (NGTP) subscription package</td><td>01</td></tr></table> <div>Cuadro N° 2 (Pre-existent)</div> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CON-SNTP-C93002TA</td><td>Catalyst 9300 SNTC 24X7X4</td><td>02</td></tr></table> <div>Cuadro N° 3 (Pre-existent)</div> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CP-HAR-EP-COMplete</td><td>Harmony Endpoint Complete</td><td>450</td></tr><tr><td>CP-INFINITY-XPR</td><td>Extended Detection/Prevention & Response.</td><td>400</td></tr></table> <div>Cuadro N° 4 (1er Mantenimiento)</div> <table><tr><th>N°</th><th>Nombre del producto</th><th>Cant</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr><tr><td>01</td><td>Equipo Firewall Perimetral</td><td>01</td><td>ANEXO A</td></tr><tr><td>02</td><td>Equipo Firewall DataCenter</td><td>01</td><td>ANEXO B</td></tr><tr><td>03</td><td>Equipo Virtual para Administración y Correlación de Eventos y Reportes</td><td>01</td><td>ANEXO C</td></tr><tr><td>04</td><td>Equipo Sandboxing para Emulación de Amenazas de día cero</td><td>01</td><td>ANEXO D</td></tr><tr><td>05</td><td>Equipo Firewall Perimetral Remoto</td><td>03</td><td>ANEXO E</td></tr><tr><td>06</td><td>Switch Acceso Remoto</td><td>02</td><td>ANEXO F</td></tr><tr><td>07</td><td>Equipo virtual para Protección de Correo Electrónico onpremise</td><td>01</td><td>ANEXO G</td></tr></table>	SKU	Nombre del producto	Cant	CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01	SKU	Nombre del producto	Cant	CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02	SKU	Nombre del producto	Cant	CP-HAR-EP-COMplete	Harmony Endpoint Complete	450	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400	N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS	01	Equipo Firewall Perimetral	01	ANEXO A	02	Equipo Firewall DataCenter	01	ANEXO B	03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C	04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D	05	Equipo Firewall Perimetral Remoto	03	ANEXO E	06	Switch Acceso Remoto	02	ANEXO F	07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G
SKU	Nombre del producto	Cant																																																					
CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01																																																					
SKU	Nombre del producto	Cant																																																					
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02																																																					
SKU	Nombre del producto	Cant																																																					
CP-HAR-EP-COMplete	Harmony Endpoint Complete	450																																																					
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																																																					
N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS																																																				
01	Equipo Firewall Perimetral	01	ANEXO A																																																				
02	Equipo Firewall DataCenter	01	ANEXO B																																																				
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C																																																				
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D																																																				
05	Equipo Firewall Perimetral Remoto	03	ANEXO E																																																				
06	Switch Acceso Remoto	02	ANEXO F																																																				
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G																																																				



		<table><tr><td>08</td><td>Equipo virtual para protección de aplicaciones web</td><td>01</td><td>ANEXO H</td></tr><tr><td>09</td><td>Equipo virtual para protección de bases de datos en reposo</td><td>01</td><td>ANEXO I</td></tr><tr><td>10</td><td>Gabinete Autocontenido</td><td>01</td><td>ANEXO J</td></tr><tr><td>11</td><td>Equipo de AA Confort</td><td>01</td><td>ANEXO K</td></tr><tr><td>12</td><td>Equipo UPS</td><td>01</td><td>ANEXO L</td></tr></table>	08	Equipo virtual para protección de aplicaciones web	01	ANEXO H	09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I	10	Gabinete Autocontenido	01	ANEXO J	11	Equipo de AA Confort	01	ANEXO K	12	Equipo UPS	01	ANEXO L																																						
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H																																																									
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I																																																									
10	Gabinete Autocontenido	01	ANEXO J																																																									
11	Equipo de AA Confort	01	ANEXO K																																																									
12	Equipo UPS	01	ANEXO L																																																									
Tercer pago AF-2026	35% del monto adjudicado	<p>Al culminar el segundo año del contrato, asimismo, luego de la conformidad por parte del área usuaria del correcto funcionamiento, soporte y mantenimiento de los productos solicitados.</p> <p>Cuadro N° 1 (Pre-existentes)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CPSB-NGTP-1600-3Y</td><td>1600 Base Appliance with Threat Prevention (NGTP) subscription package</td><td>01</td></tr></table> <p>Cuadro N° 2 (Pre-existentes)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CON-SNTP-C93002TA</td><td>Catalyst 9300 SNTC 24X7X4</td><td>02</td></tr></table> <p>Cuadro N° 3 (Pre-existentes)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CP-HAR-EP-COMLETE</td><td>Harmony Endpoint Complete</td><td>450</td></tr><tr><td>CP-INFINITY-XPR</td><td>Extended Detection/Prevention & Response.</td><td>400</td></tr></table> <p>Cuadro N° 4 (2do Mantenimiento)</p> <table><tr><th>N°</th><th>Nombre del producto</th><th>Cant</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr><tr><td>01</td><td>Equipo Firewall Perimetral</td><td>01</td><td>ANEXO A</td></tr><tr><td>02</td><td>Equipo Firewall DataCenter</td><td>01</td><td>ANEXO B</td></tr><tr><td>03</td><td>Equipo Virtual para Administración y Correlación de Eventos y Reportes</td><td>01</td><td>ANEXO C</td></tr><tr><td>04</td><td>Equipo Sandboxing para Emulación de Amenazas de día cero</td><td>01</td><td>ANEXO D</td></tr><tr><td>05</td><td>Equipo Firewall Perimetral Remoto</td><td>03</td><td>ANEXO E</td></tr><tr><td>06</td><td>Switch Acceso Remoto</td><td>02</td><td>ANEXO F</td></tr><tr><td>07</td><td>Equipo virtual para Protección de Correo Electrónico onpremise</td><td>01</td><td>ANEXO G</td></tr><tr><td>08</td><td>Equipo virtual para protección de aplicaciones web</td><td>01</td><td>ANEXO H</td></tr></table>		SKU	Nombre del producto	Cant	CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01	SKU	Nombre del producto	Cant	CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02	SKU	Nombre del producto	Cant	CP-HAR-EP-COMLETE	Harmony Endpoint Complete	450	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400	N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS	01	Equipo Firewall Perimetral	01	ANEXO A	02	Equipo Firewall DataCenter	01	ANEXO B	03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C	04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D	05	Equipo Firewall Perimetral Remoto	03	ANEXO E	06	Switch Acceso Remoto	02	ANEXO F	07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G	08	Equipo virtual para protección de aplicaciones web	01	ANEXO H
SKU	Nombre del producto	Cant																																																										
CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01																																																										
SKU	Nombre del producto	Cant																																																										
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02																																																										
SKU	Nombre del producto	Cant																																																										
CP-HAR-EP-COMLETE	Harmony Endpoint Complete	450																																																										
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																																																										
N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS																																																									
01	Equipo Firewall Perimetral	01	ANEXO A																																																									
02	Equipo Firewall DataCenter	01	ANEXO B																																																									
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C																																																									
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D																																																									
05	Equipo Firewall Perimetral Remoto	03	ANEXO E																																																									
06	Switch Acceso Remoto	02	ANEXO F																																																									
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G																																																									
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H																																																									

		09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I
		10	Gabinete Autocontenido	01	ANEXO J
		11	Equipo de AA Confort	01	ANEXO K
		12	Equipo UPS	01	ANEXO L



Cronograma de Pago

AF-2024	AF-2025	AF-2026	TOTAL
DIC - 30%	DIC - 35%	DIC - 35%	100%

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

- Acta de Conformidad suscrita por el encargado de la Seguridad Informática y la Jefatura de la Oficina de Soporte Informática y Estadística (OSIE).
- Informe del funcionario responsable de la Oficina de Soporte Informática y Estadística (OSIE), emitiendo la conformidad de la prestación efectuada.
- Entregables de la Prestación Principal y Prestación Accesorio detallados en el numeral 10 de los Términos de Referencia del Capítulo III de la Sección Específica de las bases.
- Comprobante de pago. (Factura).

Dicha documentación se debe presentar en la Mesa de Partes de la Oficina de Administración del Comando Conjunto de las Fuerzas Armadas, sito en Jr. Nicolás Corpancho N° 289 – Santa Beatriz – Lima, en el horario de 08:00 a 16:00 horas.

CAPÍTULO III REQUERIMIENTO

Importante

De conformidad con el numeral 29.8 del artículo 29 del Reglamento, el área usuaria es responsable de la adecuada formulación del requerimiento, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.



3.1. TÉRMINOS DE REFERENCIA

TÉRMINOS DE REFERENCIA PARA EL SERVICIO DE SEGURIDAD DE LAS COMUNICACIONES DEL CCFFAA, DE LA MARCA CHECK POINT O EQUIVALENTE

1. DENOMINACIÓN DE LA CONTRATACIÓN:

Servicio de seguridad de las comunicaciones del CCFFAA, de la marca Check Point o equivalente.

2. FINALIDAD PÚBLICA:

El servicio tiene como objetivo establecer el soporte y mantenimiento de todos los equipos del servicio de seguridad de las comunicaciones de datos del CCFFAA e incrementar las capacidades de ciberseguridad, el cual permitirá garantizar la confiabilidad, integridad y disponibilidad de la información, así mismo la continuidad operativa y seguridad de las redes del Comando Conjunto de las Fuerzas Armadas.

3. ANTECEDENTES

Actualmente el Comando Conjunto de las Fuerzas Armadas, posee una infraestructura de equipamiento de seguridad con la marca Check Point y Cisco, para cubrir las necesidades de protección perimetral a los diferentes sistemas de Información.



La infraestructura de seguridad perimetral existente, permite realizar las siguientes acciones:

- Proteger el perímetro de la red interna y externa de datos institucional, mediante la aplicación de reglas automatizadas, que minimizan y mitigan los ataques informáticos.
- Comunicación segura de la red de datos entre el CE-VRAM, IIAA y CCFFAA.
- Proteger los servicios informáticos, que son accesibles desde la red interna y externa.
- Establecer conexiones remotas seguras a través de VPN, para realizar trabajo remoto al personal del CCFFAA.
- Mitigar y reducir los riesgos de envío de información maliciosa, en el buzón de correo electrónico del CCFFAA.
- Contar con un monitoreo permanente de la red de datos del CCFFAA.

El 31 de octubre del 2018, mediante Contrato N°033-2018-MD/CCFFAA derivado del procedimiento de selección Licitación Pública N° 012-2018-DPC-ACDDAA-1 se realizó la contratación de la "ADQUISICIÓN E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD PERIMETRAL DE LA INFORMACIÓN DEL ÁREA DEL CE-VRAEM", por un periodo de TRES (03) años, contabilizados a partir del día calendario siguiente de la suscripción del contrato y cuya fecha fin del servicio se cumplió el 31 de diciembre del 2021, tanto para el licenciamiento y soporte por parte del proveedor del servicio.



Con el Contrato N° 009-2022-MD/CCFFAA del 19 de mayo del 2022, se suscribió el proceso contractual para el "SERVICIO DE SOPORTE Y MANTENIMIENTO DEL SISTEMA DE SEGURIDAD PARA LAS COMUNICACIONES DEL CE-VRAEM Y EL CCFFAA", por un periodo de CUATRO (04) MESES, con la finalidad de mantener actualizado las licencias y el servicio de soporte de la solución de seguridad del CCFFAA actual, la cual no contempla el esquema de seguridad en las instalaciones del VRAEM y el esquema de seguridad en la Nube.

Mediante resolución del Comando Conjunto de las Fuerzas armadas N° 384 CCFFAA/OA de fecha 12 de octubre del 2022, se aprueba el proceso de estandarización para la renovación de la garantía del equipo, licenciamiento, mantenimiento, soporte técnico y equipamiento adicional firewall perimetral e interno de marca CheckPoint, por un periodo de tres (03) años.

Con el contrato N° 001-2da DIEMCFAA – PROTECCION WARI – 2022, del 25 de octubre del 2022, se suscribió el proceso contractual para el "SERVICIO DE SEGURIDAD DE LAS COMUNICACIONES DEL CE-VRAEM Y CCFFAA", por un periodo de SIETE (07) MESES, con la finalidad de mantener actualizado las licencias y el servicio de soporte de la solución de seguridad del CCFFAA.

Mediante el Contrato N° 001-2da DIEMCFAA – CHIQAQ-2023 "SERVICIO DE SEGURIDAD DE LAS COMUNICACIONES DEL CE-VRAEM Y CCFFAA" del 20 de junio del 2023, se renovó el servicio para el soporte y mantenimiento, así como la inclusión de un firewall de la Marca Checkpoint en el CE VRAEM, por un periodo de DOCE (12) MESES, con la finalidad de continuar con una solución que permita dar seguridad a las comunicaciones en entrada y salida de la información del CCFFAA.

4. OBJETIVO(S) DE LA CONTRATACIÓN

Contratar el servicio de soporte, mantenimiento y equipamiento adicional (necesario para brindar el servicio) que permitirán la operatividad del sistema de seguridad de las comunicaciones de datos del CCFFAA (anexo M), así como la correlación de todos los equipos bajo una sola plataforma de gestión, por un periodo de TREINTA Y SEIS (36) MESES.

5. ALCANCE Y DESCRIPCIÓN DE LOS SERVICIOS A CONTRATAR

5.1 Descripción del servicio

Contratación del servicio de soporte, mantenimiento y equipamiento adicional (necesario para brindar el servicio) que



permitirá la operatividad del sistema de seguridad de las comunicaciones de datos del CCFFAA, así como la correlación de todos los equipos bajo una sola plataforma de gestión, por el periodo de TREINTA Y SEIS (36) MESES o equivalente a 1095 días calendario.

5.2 Alcance del servicio (PRESTACIÓN PRINCIPAL):

Se requiere contratar soporte, que incluyan actualizaciones de release y parches de seguridad Check Point o equivalente y Cisco (switch core pre existente) para el equipamiento de seguridad detallados en el Cuadro N° 1, 2 y 3.

5.2.1 Licenciamiento y soporte del fabricante

Cuadro N° 1

SKU	Nombre del producto	Cant
CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01

5.2.2 Licenciamiento y soporte del fabricante

Cuadro N° 2

SKU	Nombre del producto	Cant
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02

5.2.3 Licenciamiento y suscripción a las siguientes soluciones

Cuadro N° 3

SKU	Nombre del producto	Cant
CP-HAR-EP-COMPLETE	Harmony Endpoint Complete	450
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400

5.2.4 Equipamiento

Para el óptimo funcionamiento de la red de datos y la ampliación de la cobertura de seguridad, el proveedor instalará como parte del servicio, el siguiente equipamiento de primer uso, que permita garantizar la protección de la red LAN interna y WAN externa de la entidad (sede principal en Lima y sedes remotas).

Cuadro N° 4

N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS
01	Equipo Firewall Perimetral	01	ANEXO A
02	Equipo Firewall DataCenter	01	ANEXO B
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D
05	Equipo Firewall Perimetral Remoto	03	ANEXO E
06	Switch Acceso Remoto	02	ANEXO F
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I
10	Gabinete Autocontenido	01	ANEXO J
11	Equipo de AA Confort	01	ANEXO K
12	Equipo UPS	01	ANEXO L



5.2.5 Capacitación

Para la transferencia de conocimiento, el proveedor pondrá a disposición del área usuaria lo siguiente:

Cuadro N° 5

N°	ITEM	MODALIDAD	Cant.
01	Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)	Presencial	10 Personas
02	Curso de la solución de seguridad de firewall a nivel de administración y/o experto	Curso no oficial	05 Personas
03	Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall	Voucher de Certificación	05 Personas

En caso de brindar algún curso adicional a lo solicitado, se considerará una mejora al servicio, en beneficio de los usuarios finales de las herramientas propuestas.

5.3 PRESTACION ACCESORIA

Se requiere contratar:

- Servicio de mantenimiento preventivo para todo el equipamiento detallado en el cuadro N° 1, N° 2, N° 3, N° 4.
- Servicio de soporte e incidentes para todo el equipamiento detallado en el cuadro N° 1, N° 2, N° 3, N° 4.

El periodo de la prestación accesoria, tendrá un periodo de TREINTA Y SEIS (36) MESES, para lo cual el proveedor deberá de brindar los siguientes servicios:

5.3.1 Servicio de mantenimiento preventivo

El proveedor deberá realizar el servicio de Mantenimiento Preventivo al equipamiento de seguridad de las comunicaciones de datos del CE-VRAEM y el CCFFAA, detallado en el **cuadro N° 1, N° 2, N° 3 y N° 4**, los cuales se encuentran en las instalaciones del CCFFAA, y se deberá realizar tres (03) veces, durante el tiempo de prestación del servicio. Se considera mantenimiento preventivo en sitio para los equipos ubicado en Lima. Para los equipos ubicados en sedes remotas, el mantenimiento preventivo se realizará de manera presencial y con apoyo de CCFFAA.

El servicio es a todo costo debe ser asumido íntegramente por el proveedor y debe comprender, como mínimo lo siguiente: mano de obra, materiales para limpieza, lubricación, partes y piezas; y ajustes necesarios sobre los incidentes detallados en la realización del servicio. El suministro de repuestos de partes y piezas es por cuenta y cargo del proveedor.

El proveedor deberá poner una etiqueta (donde precisará la fecha del mantenimiento preventivo) en cada equipo en donde se haya realizado el servicio.

5.3.2 Servicio de soporte técnico

El servicio de soporte técnico consiste en solicitar al proveedor realizar configuraciones sobre todos los equipos detallados en el **cuadro N° 1, N° 2, N° 3 y N° 4** a solicitud de la Oficina de Soporte Informática y Estadística del CCFFAA. Se considera atención remota o en sitio para los equipos ubicado en Lima. Para los equipos ubicados en sedes remotas, se realizará de manera remota con apoyo de CCFFAA.

El servicio de soporte técnico, con el fabricante deberá estar disponible de lunes a domingo (24 horas, 7 días a la semana).

El servicio de soporte técnico se realizará de acuerdo a los niveles de servicios establecidos en siguiente **numeral 5.3.4**.



5.3.3 Servicio de incidentes

El servicio de respuesta ante incidentes, será requerido ante una interrupción del servicio que soporta los equipos detallados en el **cuadro N° 1, N° 2, N° 3 y N° 4**, por lo cual se realizará la notificación al proveedor para que identifique la falla del incidente.

De requerir el cambio de equipos y/o algún componente ante cualquier desperfecto que se presente, el proveedor deberá de gestionar y escalar la reposición de los equipos o componentes al fabricante. Para garantizar la continuidad operativa, el proveedor deberá de reponer de manera temporal el equipamiento que permita continuar con las operaciones en el CCFFAA.

El servicio de incidentes por parte del proveedor, deberá estar disponible de lunes a domingo (24 horas, 7 días a la semana).

El servicio de soporte técnico se realizará de acuerdo a los niveles de servicios establecidos en siguiente **numeral 5.3.4**.

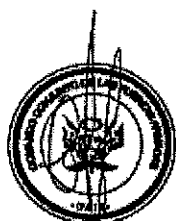
5.3.4 Niveles de servicio

El proveedor deberá proporcionar un número telefónico y correo electrónico para contactar a su mesa de ayuda, para solicitar el soporte técnico e incidentes, considerando los siguientes niveles de servicio:

Cuando se publiquen actualizaciones de fábrica del equipamiento ofertado, los fabricantes por intermedio del contratista, deberán informar y aplicar las actualizaciones de sistema operativo, parches del software o módulos publicados recientemente, utilizados en los respectivos equipos implementados, así mismo estos deberán estar disponible para descarga y/o actualización en los equipos durante toda la vigencia del soporte técnico.

El fabricante y/o proveedor deberá ser responsable de la operatividad, disponibilidad y actualizaciones de la plataforma SOC, durante toda la vigencia del soporte técnico, así mismo deberá de comunicar por los canales oficiales al área usuaria, sobre las actualizaciones emitidas, para su actualización o upgrade correspondiente.

La atención de las solicitudes de soporte o incidente se realizará de manera presencial y/o remota por el proveedor, en las



instalaciones del CCFFAA, por los especialistas propuestos por el proveedor.

5.4 Garantía del Servicio:

El proveedor deberá brindar la garantía del servicio por igual período de vigencia del soporte técnico (por el período de 03 años), con el fin de asegurar el óptimo funcionamiento del servicio solicitado y detallado en el numeral 5.2.

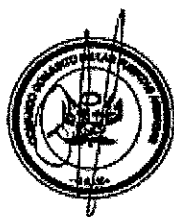
5.5 Disponibilidad de servicios y repuestos:

Tiempo de respuesta: tiempo que transcurre desde el momento de reportado la solicitud de soporte técnico o incidente por parte de la OSIE (el reporte de la solicitud será vía telefónica y/o por correo electrónico), hasta que el proveedor responda consignando el Ticket de la solicitud (teniendo como plazo de respuesta máximo de dos (02) horas), para dar inicio a la solución, el cual deberá ser comunicado al correo electrónico de la persona que reporto el incidente. En caso supere el tiempo de atención se aplicará la penalidad indicada **en el numeral 12 (OTRAS PENALIDADES).**

Tiempo de atención: Tiempo que transcurre desde que se consigna el ticket de incidente por parte del proveedor a la persona que reporto el incidente (OSIE), hasta la solución del mismo (presencial y/o remoto). En caso supere el tiempo de solución se aplicará la penalidad indicada **en el numeral 12 (OTRAS PENALIDADES).**

El tiempo de atención para el caso de requerimientos de soporte técnico (configuraciones, asesoramiento): no deberá exceder las veinte cuatro (24) horas, contabilizadas desde que se consigna el ticket de la solicitud al proveedor hasta la solución del mismo. En caso supere el tiempo de solución se aplicará la penalidad indicada **en el numeral 12 (OTRAS PENALIDADES).**

El tiempo de solución para los incidentes, no debe superar las ocho (08) horas. Los incidentes que ameriten la interacción del fabricante, se atenderán de acuerdo con el nivel de servicio con el cual cuenta la entidad. En caso de que el equipo de soporte determine el reemplazo de equipos o repuestos, deberá de comunicar a la OSIE, y tendrá un plazo no mayor a cuatro (04) horas en Lima, adicionales a partir de la determinación que se necesita equipo de reemplazo. Para realizar el remplazo de equipos o repuestos, estos repuestos o equipos, podrán ser soluciones virtualizadas o equipos similares que cumplan como mínimo las



mismas características del equipo original, no se acepta soluciones basadas en nube. Para el caso de equipos fuera de Lima, la atención será remota con apoyo de personal de CCFFAA y el plazo se cumplirá con la entrega del equipo en Lima.

Se indica que, la OSIE brindará las facilidades técnicas de acceso remoto o presencial hacia los equipos de seguridad para que el proveedor pueda desarrollar las labores de soporte, resolución de incidentes y mantenimiento técnico del equipamiento.



5.6 Lugar, plazo de entrega y plazo de prestación del servicio:

Lugar donde se desarrollará el servicio.

1. La prestación principal se implementará en el Data Center de la Oficina de Soporte Informática y Estadística del Comando Conjunto de las Fuerzas Armadas, situado en Jr. Nicolás Corpancho 289 Santa Beatriz – Lima (OSIE).
2. Para la instalación de los Equipos Firewall Perimetral Remotos y sus accesorios para su buen funcionamiento y correcta prestación del servicio, se realizarán en el Comando Operacional del Sur (Arequipa), Comando Operacional del Norte (PIURA) y Comando Operacional de la Amazonia (IQUITOS).



Plazos en los que se ejecutará el servicio

Los servicios materia de la presente convocatoria se prestarán en el plazo de tres (03) años equivalente a 1095 días calendario, contando a partir del día siguiente de la suscripción del contrato y activación del servicio.

Plazo de entrega del servicio

- Como plazo máximo cinco (05) días calendarios posteriores de la suscripción del contrato y la entrega formal al área y equipos a intervenir para las renovaciones indicadas del numeral 5.2.1 al 5.2.3.
- Como plazo máximo para la entrega, instalación y configuración del equipamiento del numeral 5.2.4 será de setenta (70) días calendario contados a partir del día siguiente de suscrito el contrato y sin perjuicio de realizar entregas parciales. Asimismo, para dicho

efecto se suscribirá un acta de instalación y configuración del equipamiento.

- Para el Numeral 5.2.5, la capacitación tendrá un plazo máximo de CINCO (05) días, posterior a la implementación total de la solución, y esta se sustentará bajo un acta de conformidad de la unidad usuaria.



6. CONFIDENCIALIDAD:

El Contratista es consciente de la importancia de su responsabilidad en cuanto a guardar confidencialidad de la información, ya sea dentro o fuera de las instalaciones del CCFFAA. Por lo tanto, el Contratista manifiesta haber leído, entendido y se compromete a cumplir todas las disposiciones que nome la confidencialidad, cualquiera sea su fuente o registro; oral, escrito, impreso, digital, eléctrico, fax, fotografía, video o cualquier otro medio de conservación. Del mismo modo declara que, durante su vinculación en el CCFFAA, no intentara tener acceso, copiar, compartir o hacer conocer a terceros ninguna información a través de cualquier medio de comunicación y/o redes sociales.

El Contratista se compromete a utilizar los medios razonables para proteger a la información confiada a su persona y a no hacer uso de sus privilegios de acceso a la información más allá de lo estrictamente necesario para el cumplimiento de sus funciones; del mismo modo, no comprometerá la confidencialidad de la información contenida en ella.

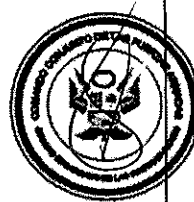
El CONTRATISTA no transportará información clasificada fuera de las instalaciones del CCFFAA, cuando por razones de servicio se requiere trasladar la misma, lo hará solo con autorización del Oficial de Seguridad, adoptando los medios necesarios para garantizar la confidencialidad. El CONTRATISTA acepta que la terminación de su vinculación con el CCFFAA, cualquiera que sea la causa, no determinará la terminación de su vinculación devolverá toda la información que se le haya sido concedido, cualquiera sea su fuente, escrito, impreso, magnético y/o cualquier modo de soporte de información, y que su incumplimiento ocasionará, el inicio a la determinación de la responsabilidad civil y/o penal en que pueda incurrir.

7. CONFORMIDAD DE LA PRESTACIÓN.

La Oficina de Soporte Informática y Estadística (OSIE), es la responsable de otorgar la conformidad de la prestación y deberá hacerlo en un plazo que no excederá (10) días calendario, contabilizado a partir del día calendario

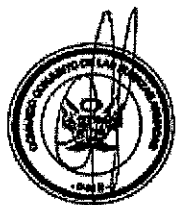


siguiente de la recepción de los entregables detallados en el numeral 10 para la prestación principal y accesorio, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario. El mismo plazo resulta aplicable para que el CCFFAA se pronuncie sobre el levantamiento de observaciones, según corresponda.



MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

- **ÁREAS QUE SUPERVISAN:** La Sección de Seguridad de Redes de la Oficina de Soporte Informática y Estadística del CCFFAA.
- **ÁREAS QUE COORDINAN CON EL PROVEEDOR:** La Sección de Seguridad de Redes de la Oficina de Soporte Informática y Estadística del CCFFAA será la responsable de la coordinación con el proveedor del presente servicio.
- **ÁREAS QUE BRINDAN LA CONFORMIDAD:** La conformidad será otorgada por el encargado de la Seguridad Informática y la Jefatura de la Oficina de Soporte Informática y Estadística.



8. FORMA DE PAGO:

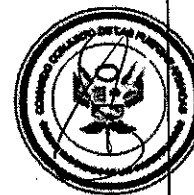
LA ENTIDAD debe efectuar el pago de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

El pago se realizará en forma parcial en 03 pagos durante el periodo de tres (03) años de la siguiente manera:

- Primer pago AF-2024: 30% del monto adjudicado y se realizará previa conformidad de la activación de las licencias, soporte y suscripción indicadas del numeral 5.2.1 al 5.2.3, así mismo a la entrega, instalación y configuración del equipamiento detallados en el numeral 5.2.4 y a la capacitación del personal de acuerdo al 5.2.5.
- Segundo pago AF-2025: 35% del monto adjudicado al culminar el primer año del contrato, asimismo luego de la conformidad por parte del área usuaria del correcto funcionamiento de los productos solicitados.
- Tercer pago AF 2026: 35% del monto adjudicado al culminar el segundo año del contrato, asimismo luego de la conformidad por parte del área usuaria del correcto funcionamiento de los productos solicitados.

Cronograma de Pago

AF-2024	AF-2025	AF-2026	TOTAL
DIC - 30%	DIC - 35%	DIC - 35%	100%

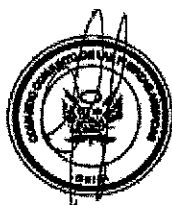


9. RESPONSABILIDAD POR VICIOS OCULTOS:

El Contratista será responsable por la calidad ofrecida y los vicios ocultos por la prestación brindada, conforme a lo indicado en el artículo 40° de la Ley de Contrataciones del Estado, por un plazo de tres (03) años a partir de la firma del Contrato.

10. ENTREGABLES

La presentación de los entregables, se realizará a través de la Oficina de Soporte Informático y Estadística del Comando Conjunto de las Fuerzas Armadas o a los correos electrónicos: segurinfo@ccffaa.mil.pe y salva@ccffaa.mil.pe según corresponda, de lunes a viernes en horario de 08:30 horas a las 16:30 horas, dirigido a la Jefatura de la Oficina de Soporte Informática y Estadística.



10.1. Prestación principal

El contratista debe ser un representante autorizado en el Perú para brindar la comercialización y soporte técnico del hardware/software Check Point o equivalente y Cisco (equipamiento pre existente) vigente. El contratista debe acreditar este requisito mediante:

Carta de Soporte

Carta del fabricante o sucursal local del fabricante, que acredite que el contratista es representante autorizado en el Perú para la comercialización y soporte técnico del hardware/software Check Point o equivalente (pre existente y adicional).

Carta de Soporte o Entregable del fabricante de lo solicitado en el Numeral 5.2.1. y 5.2.3, emitido por el fabricante CheckPoint o equivalente (pre existente), el cual debe precisar la fecha de inicio y fin, por el periodo MIL NOVENTA Y CINCO (1095) días calendario. Contabilizados dentro de los cinco (05) días posteriores de la firma del contrato para el caso de renovación de componentes actuales.

Carta del fabricante o sucursal local del fabricante, que acredite que el contratista es representante autorizado en Cisco para la comercialización y soporte técnico del hardware/software Cisco (equipamiento pre existente).

Carta de Soporte o Entregable del fabricante Cisco solicitado en el Numeral 5.2.2, emitido por el fabricante Cisco (equipamiento pre existente), el cual debe precisar la fecha de inicio y fin, por el periodo MIL NOVENTA Y CINCO (1095) días calendario. Contabilizados dentro de los cinco (05) días posteriores de la firma del contrato para el caso de renovación de componentes actuales.

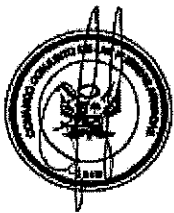
En el caso de nuevos equipos, se deberá considerar el inicio desde la entrega de equipos por el periodo MIL NOVENTA Y CINCO (1095) días calendario.

Carta del fabricante o sucursal local del fabricante, que acredite que el contratista es representante autorizado para la comercialización y soporte técnico del equipamiento ofertado a nivel de la solución de Firewall, Endpoint, Switches y Protección de datos en reposo.

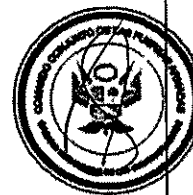
Entregable del fabricante de los equipos solicitados en el Numeral 5.2.4 el cual debe precisar la fecha de inicio y fin, por el periodo MIL NOVENTA Y CINCO (1095) días calendario. Contabilizados a partir de la entrega de equipos por el periodo MIL NOVENTA Y CINCO (1095) días calendario.

Plazo de entrega: deberá ser presentado por el contratista para el inicio efectivo del servicio. En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito, teniendo en cuenta que el servicio materia de la presente convocatoria se prestarán en el plazo de tres (03) años equivalente a 1095 días calendario, contando a partir del día siguiente de la suscripción del contrato y activación del servicio.

- Como plazo máximo de cinco (05) días calendario posteriores de la suscripción del contrato y la entrega formal al área y equipos a intervenir para las renovaciones indicadas del numeral 5.2.1 al 5.2.3.
- Como plazo máximo para la entrega, instalación y configuración del equipamiento del numeral 5.2.4 será de setenta (70) días calendario contados a partir del día siguiente de suscrito el contrato y sin perjuicio de realizar entregas parciales. Asimismo, para dicho efecto se suscribirá un acta de instalación y configuración del equipamiento.



- Para el Numeral 5.2.5, la capacitación tendrá un plazo máximo de CINCO (05) días, posterior a la implementación total de la solución, y esta se sustentará bajo un acta de conformidad de la unidad usuaria.



10.2. Prestación accesoría

a) Plan de trabajo: Debe contener como mínimo lo siguiente:

- Número telefónico, correo electrónico para contactar a su mesa de ayuda y los niveles de escalamiento de incidentes.
- Cronograma de mantenimiento preventivo.

Plazo de entrega: Como máximo a los quince (15) días calendario, contabilizados a partir del día calendario siguiente de suscripción del contrato.

Forma de entrega: De manera física y digital.

b) Informe del mantenimiento preventivo: debe contener como mínimo lo siguiente:

- Inventario de todos los equipos.
- Fecha de ejecución del mantenimiento.
- Estado situacional por cada equipo y sus componentes.
- Nombre del equipo
- Recomendaciones.

Plazo: plazo máximo hasta TREINTA (30) días antes de finalizar la prestación del servicio de mantenimiento preventivo.

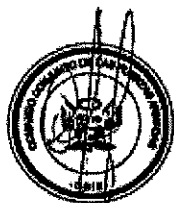
Forma de entrega: De manera física y digital.

c) Informes del soporte técnico, debe considerar como mínimo lo siguiente:

Informe detallado de cada ocurrencia realizada (ticket, solicitante, hora de registro, técnico asignado, tiempo de atención, tiempo de solución, descripción y detalle de la solución).

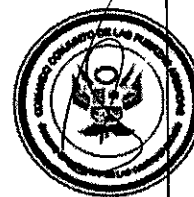
Plazo: como máximo a los cinco (05) días calendario siguiente de culminado cada requerimiento de soporte técnico o incidente reportado.

Forma de entrega: De manera digital.



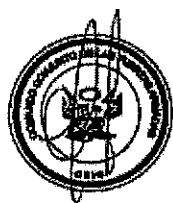
11. PENALIDAD POR MORA

De conformidad con el artículo 162° del Reglamento de la Ley de Contrataciones del Estado, en el caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad aplicará automáticamente una penalidad por mora por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10 %) del monto del contrato vigente.



12. OTRAS PENALIDADES

Cualquier retraso para la atención y solución de los requerimientos de soporte técnico o incidentes, de los Niveles de Servicio (numeral 5.3.2 al numeral 5.3.4), implicará que se aplique las siguientes penalidades:



N°	Supuestos de aplicación de penalidad	Monto por hora o fracción adicional a lo señalado en los niveles de servicio	Procedimiento
01	Por retraso en la atención o solución de los requerimientos de soporte técnico o incidentes solicitados.	S/. 90	Se aplicará cuando se supere el tiempo máximo de atención, solución de incidentes y requerimiento de soporte técnico o incidentes, para tal efecto la OSIE elaborará un informe detallado de los retrasos incurridos en el mes de acuerdo a los niveles de servicio.
02	Por retraso en reemplazo de equipos	S/. 90	Se aplicará cuando se supere el tiempo máximo para el reemplazo de equipos, para tal efecto la OSIE elaborará un informe detallado los retrasos incurridos en el mes, de acuerdo a los niveles de servicio.

13. ANTICORRUPCIÓN

El Contratista declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e Integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.



Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

14. REQUISITOS DE CALIFICACIÓN:

14.1. Calificación del Personal Clave

Formación Académica

El Contratista deberá contar con un equipo de trabajo (personal calificado) para la ejecución de la bolsa de horas de soporte solicitado en el numeral 5.3, por lo que deberá considerar como personal claves diferentes de acuerdo a lo siguiente:

- a) **Un (01) Jefe de Proyecto:** Para el perfil del jefe de proyecto debe presentar lo siguiente:



- o Título Profesional en las especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica o afines.
- o Copia de la Certificación PMP (Project Management Profesional) vigente.

b) Tres (03) Especialistas de Implementación: Para el perfil del especialista de implementación debe presentar lo siguiente:

- o Título y/o bachiller en las especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica, Telecomunicaciones o afines.
- o Copia de la Certificación a nivel Profesional y/o Expert del equipamiento ofertado a nivel de la solución de Firewall, Endpoint, Switches y Protección de datos en reposo, las cuales deben estar vigentes

c) Dos (02) Especialista en soporte: Para el perfil de especialista debe presentar lo siguiente:

- o Bachiller universitario y/o técnico en especialidades de Ingeniería de Sistemas, Cómputo, Informática y Electrónica, Telecomunicaciones, informática o afines.
- o Un (01) especialista debe contar con la copia de la Certificación CheckPoint Security Expert (CCSE) ya sea la versión R80 o R81 y/o CheckPoint Security Master (CCSM) ya sea la versión R80 o R81 y/o la Certificación Check Point Certified Endpoint Specialist (CCES); o equivalente, vigente y lo debe acreditar para la suscripción del contrato.
- o Un (01) especialista debe contar con Certificación en redes empresariales de equipamiento pre existente.
- o Copia de la Certificación a nivel Profesional y/o Expert del equipamiento ofertado a nivel de la solución de Firewall, Endpoint y Protección de datos en reposo, las cuales deben estar vigentes.

Nota:

Todos los documentos de presentación indicados se presentarán como Requisitos de Calificación y serán parte de la propuesta.

14.2. Experiencia del Personal clave:

Requisitos:

a. Jefe de Proyecto:



Tres (03) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación en equipamientos de seguridad perimetral CheckPoint o equivalente.

b. Especialistas de Implementación:

Tres (03) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación en equipamientos de redes empresariales (Networking Enterprise).

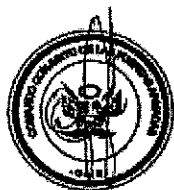
c. Especialista en soporte:

Dos (02) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación en equipamientos de seguridad perimetral CheckPoint o equivalente.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos:

- (i) Copia simple de contratos y su respectiva conformidad o
- (ii) Constancias o
- (iii) Certificados o
- (iv) Cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.



14.3. Experiencia del Postor en la Especialidad

Requisitos:

Experiencia; el postor debe acreditar un monto facturado acumulado hasta dos (02) veces el valor estimado, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computaran desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se considerarán servicios similares: Adquisición de equipamiento Firewall CheckPoint y/o similares, Seguridad de Red Perimetral, Solución de Firewalls Perimetral, Firewall o cortafuegos de aplicaciones web y/o similares en donde el servicio principal este la marca CheckPoint.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con

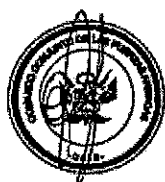
voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondiente a un máximo de veinte (20) contrataciones.

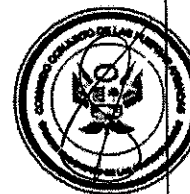
Se adjunta la Resolución del Comando Conjunto de las Fuerzas armadas N° 384 CCFFAA/OA de fecha 12 de octubre del 2022, Resolución vigente de estandarización de la marca CheckPoint, por el periodo de Tres (03) años,



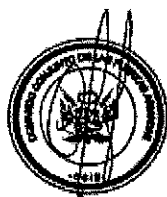
14.4. REQUISITOS DE CALIFICACIÓN

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>Un (01) Jefe de Proyecto: Para el perfil del jefe de proyecto debe presentar lo siguiente:</p> <ul style="list-style-type: none">o Título Profesional en las especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica o afines. <p>Tres (03) Especialistas de Implementación: Para el perfil del especialista de implementación debe presentar lo siguiente:</p> <ul style="list-style-type: none">o Título y/o bachiller en las especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica, Telecomunicaciones o afines. <p>Dos (02) Especialista en soporte: Para el perfil de especialista debe presentar lo siguiente:</p> <ul style="list-style-type: none">o Bachiller universitario y/o técnico en especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica, Telecomunicaciones, informática o afines.





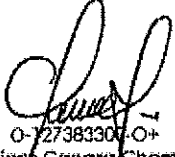
	<p>Acreditación:</p> <p>El Título Profesional requerido será verificado por el comité de selección o el órgano contratado de las contrataciones en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el Título Profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
<p>B.3.2</p>	<p>CAPACITACIÓN</p>
	<p>Requisitos:</p> <p>Un (01) Jefe de Proyecto: Para el perfil del jefe de proyecto debe presentar lo siguiente:</p> <ul style="list-style-type: none"> o Copia de la Certificación PMP (Project Management Profesional) vigente. <p>Tres (03) Especialistas de Implementación: Para el perfil del especialista de implementación debe presentar lo siguiente:</p> <ul style="list-style-type: none"> o Copia de la Certificación a nivel Profesional y/o Expert del equipamiento ofertado a nivel de la solución de Firewall, Endpoint, Switches y Protección de datos en reposo, las cuales deben estar vigentes <p>Dos (02) Especialista en soporte: Para el perfil de especialista debe presentar lo siguiente:</p> <ul style="list-style-type: none"> o Un (01) especialista debe con la copia de la Certificación CheckPoint Security Expert (CCSE) ya sea la versión R80 o R81 y/o CheckPoint Security Master (CCSM) ya sea la versión R80 o R81 y/o la Certificación Check Point Certified Endpoint Specialist (CCES); o equivalente y lo debe acreditar para la suscripción del contrato.

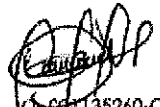



	<ul style="list-style-type: none"> o Un (01) especialista debe contar con la copia de la Certificación en redes empresariales (Network Enterprise) o equivalente. o Copia de la Certificación a nivel Profesional y/o Expert del equipamiento ofertado a nivel de la solución de Firewall, Endpoint y Protección de datos en reposo, las cuales deben estar vigentes. <p>Se acreditará con copia simple de Constancias, Certificados u otros documentos, según corresponda.</p>
B.4	<p>EXPERIENCIA DEL PERSONAL CLAVE</p> <p><u>Requisitos:</u></p> <p>a. Jefe de Proyecto:</p> <p>Tres (03) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación en equipamientos de seguridad perimetral CheckPoint o equivalente.</p> <p>b. Especialistas de Implementación:</p> <p>Tres (03) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación con equipamientos en redes empresariales (Networking Enterprise) o equivalente.</p> <p>c. Especialista en soporte:</p> <p>Dos (02) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación en equipamientos de seguridad perimetral CheckPoint o equivalente.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p>



C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>Experiencia; el postor debe acreditar un monto facturado acumulado hasta dos (02) veces el valor estimado, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computaran desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se considerarán servicios similares: Adquisición de equipamiento Firewall CheckPoint y/o similares, Seguridad de Red Perimetral, Solución de Firewalls Perimetral, Firewall o cortafuegos de aplicaciones web y/o similares en donde el servicio principal este la marca CheckPoint.</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondiente a un máximo de veinte (20) contrataciones.</p>


O-227383300-O+
Wilians Canaza Chambi
TTE EP
Ejecutivo accidental de la OSIE


O-881135260-O+
Leidy QUIROZ Bazán
Oficial de Mar 1°
OSIE


O-03106482-O+
Jonalhan RAMOS Garcia
Oficial de Mar 2°
OSIE

ANEXO A

CARACTERÍSTICAS TÉCNICAS: SEGURIDAD PERIMETRAL



Nº	ITEM	TIPO	Cant
01	Equipo Firewall Perimetral	Hardware	01

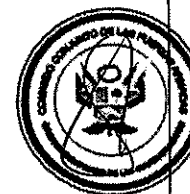
I. UN EQUIPO DE SEGURIDAD

1.2. Hardware, Performance e interfaces

- Cantidad: Una (01) unidad.
- Appliance de firewall de nueva generación/Gateway.
- Rendimiento (throughput) de 9 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, URL Filtering, Antivirus, Anti-Bot o Antispyware y Emulación Malware día-cero.
- Rendimiento (throughput) de 28 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones e IPS).
- Conexiones concurrentes: 16 millones como mínimo.
- Cantidad de conexiones por segundo: 300 000 como mínimo.
- Almacenamiento local: 480 GB SSD como mínimo.
- 08 puertos de red 1GB (RJ45)
- 04 interfaces 10 GB SFP+
- Capacidad de soportar ampliación para 02 interfaces 40 GB QSFP+
- Soporte de alta disponibilidad.
- Debe soportar (capacidad incluida sin costo adicional) IPSec VPN Client-to-Site hasta 200 usuarios concurrentes y Site-to-Site capacidad de túneles ilimitada.

1.3 Consideraciones generales

- El sistema operativo deberá ser del fabricante de la solución de firewall ofertado, el mismo deberá venir de fábrica con el "hardening" necesario. El fabricante deberá desarrollar las actualizaciones de sistema operativo, parches del software o módulos utilizados, estos deberán estar disponible para descarga y/o actualización en los equipos durante toda la vigencia del soporte técnico contratado
- Los equipos deben ser nuevos y de primer uso.
- En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Este requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.
- El fabricante de la solución de seguridad debe estar presente en los últimos 08 reportes de Gartner (Magic Quadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.



- El fabricante de la solución de seguridad debe tener un porcentaje de efectividad de seguridad igual o superior al 99% y calificación de AAA, en la última evolución de Enterprise Firewall Report de CyberRatings para el año 2023.
- El fabricante de la solución de seguridad debe tener un porcentaje de efectividad de seguridad igual o superior al 99%, en la última evolución de Miercom Next-Generation Firewall Security Benchmark (2024).
- Los sistemas operativos (SO) que operan en los equipos de seguridad firewall ofertados, no deberá tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas.

1.4 Consideraciones generales

- Los firewalls ofertados deben poder implementarse y operar en modalidad de Alta Disponibilidad en modo Activo-Activo y modo Activo-Pasivo.
- La solución de seguridad debe permitir la configuración de clúster en modo de operación en alta disponibilidad (HA), tanto para IPv4 como para IPv6.
- Debe soportar redundancia de hasta 10 enlaces ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- La redundancia de ISP puede ser a nivel de "compartición de carga" (load sharing) y detección de falla enlace (primary/backup).
- Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster, así como contar con mecanismos de detección de fallas y detección de pérdida de enlaces.



1.5 Funcionalidades de red:

- La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
- Debe soportar enrutamiento con IPv4 e IPv6.
- Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
- Debe soportar control de ancho de banda basado en prioridades de pesos.
- Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación.
- Soporte de rutas estáticas, PBR (policy based routing), LACP, OSPF (IPv4 e IPv6), RIP, BGP, IGMP, PIM, Ipsec Routing y Dual Stack IPv4 e IPv6, NAT64, NAT46 y NAT66.
- La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- El soporte a políticas de ruteo permite que, ante la presencia de dos enlaces, se pueda decidir por que enlace egresa tráfico determinado.
- La solución debe soportar políticas de ruteo estático en IPv6.
- La solución debe soportar registro de tablas ARP estáticas y dinámicas,

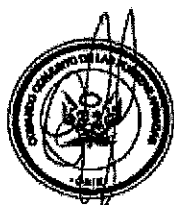
definiendo cantidad de entradas ARP y el tiempo de duración.

- Debe incluir la posibilidad de crear NAT permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.



1.6 Gestión de Políticas

- El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, comunidad de VPN, direcciones de URL y aplicaciones.
- Sobre la base de la políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final
- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora).
- Debe tener capacidad de crear reglas de firewall en base a objetos dinámicos, los cuales son basados en fuentes de URL externas (HTTP/HTTPS) que contengan archivos CSV o Json, con la finalidad de automatizar las reglas de acceso, no siendo necesario publicar y/o compilar reglas en el firewall.



1.7 Otras funcionalidades

- Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
- La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups (configuración del sistema operativo) en el tiempo deseado.
- Los backups pueden ser almacenados localmente y el administrador puede transferirlos vía FTP, TFTP y SCP de manera programada.
- La comunicación entre los servidores de administración y el equipo de seguridad (firewall), debe ser cifrada y autenticada.
- Debe tener la opción de negar los parámetros de origen o destino, es decir que para una regla dada permite todas las conexiones de origen / destino excepto la especificada en la regla.
- La solución debe permitir integración con analizadores de tráfico mediante el protocolo NetFlow.
- Integración mediante API REST de Terceros.
- Los firewalls deben permitir manejo de ancho de banda de distintos protocolos y/o aplicaciones, permitiendo la definición de niveles de ancho de banda tanto para carga (upload) y descarga (download).
- Debe soportar y proteger protocolos de VoIP (SIP, H.323, MGCP, SCCP)

Incluyendo soporte de NAT para cada uno de esos protocolos.

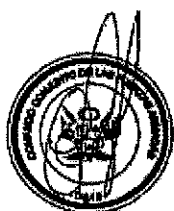
1.8 Geolocalización

- Soportar la creación de políticas basada en Geo-localización, permitiendo que el tráfico de determinado País/Países sean bloqueados o permitidos.
- Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- Las actualizaciones de las direcciones o rangos de IP pública por cada país, debe realizarse periódicamente y de manera automática.



1.9 Prevención de Intrusos - IPS

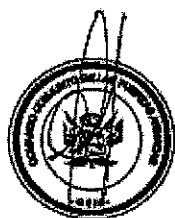
- La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.
- Debe tener protección contra ataques DoS (Denial of Service).
- A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, SQL Injection, Command Injection e injection protection para DN (Distinguished Names).
- El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.
- Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) y nivel consumo de recursos.
- Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
- Debe poder realizar captura de paquetes para protecciones específicas.
- Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, IMAP, DNS tunneling, FTP, SNMP, IMAP, SMB.
- Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.
- Debe detectar y bloquear intentos de tuneles, a fin de evitar fuga de datos o problemas de seguridad web.
- Debe proteger contra ataques tipo DNS Cache Poisoning cuando reutilizan los puertos de origen.
- Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.
- La solución debe tener capacidades de detección y prevención de ataques tunelizados en tráfico DNS.
- Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.





- Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.
- La funcionalidad de IPS debe tener las siguientes capacidades:
- Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos.
- Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial.
- Detección y prevención de comunicaciones de malware salientes.
- Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.
- Detección, prevención o restricción de ciertas aplicaciones que pueden causar amenazas a la seguridad de la red, como las aplicaciones P2P o de mensajería instantánea.

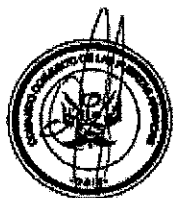
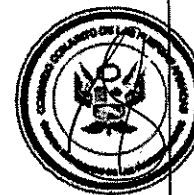
1.10 Anti-Bot o Antispyware



- La solución debe proveer una herramienta que haga descubrimiento de "bots" dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados "bots" hacia las redes de los atacantes en Internet (botnet).
- La solución debe incluir al menos los siguientes métodos de identificación:
 - ✓ Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
 - ✓ Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
 - ✓ Identificación de comportamiento de bots.
- La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de "botnet". El Anti-Bot se debe actualizar continuamente de manera automática.
- La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
- La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltración de información mediante DNS Tunneling.
- La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

1.11 Control de aplicaciones y Filtro de URL

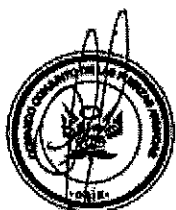
- La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.
- Se requiere que capacidad de detección de 10,000 aplicaciones



- en la base de datos de control de aplicaciones para la aplicación de políticas.
- La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
 - Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
 - Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
 - Solución debe soportar como mínimo 100 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Artificial Intelligence (AI) Hacking, Inactive Sites y Spyware/ Malicious Sites.
 - La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.
 - Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
 - Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
 - La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
 - Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
 - La solución debe proporcionar un mecanismo para limitar el uso de aplicaciones basadas en el consumo de ancho de banda (upload / download) por el tipo de aplicación y/o servicio de red definido.
 - Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
 - Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
 - Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2.
 - Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

1.12 Prevención de amenazas

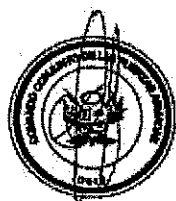
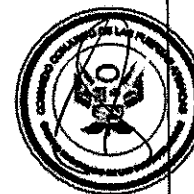
- Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
- Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el



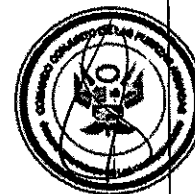
- rendimiento de la red.
- Los equipos deben tener integrada la detección y prevención de virus y amenazas (anti-malware).
 - La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
 - Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
 - Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
 - Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.
 - Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
 - Debe soportar inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
 - Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
 - Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
 - Bloquear ataques en canal SSH.
 - Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
 - Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
 - Prevenir el reenvío de puertos SSH (Port Forwarding).
 - Prevenir el uso de criptografía vulnerable en el canal SSH.
 - Prevenir el uso de clientes y servidores SSH vulnerables.
 - Prevenir el uso del puerto 22 para otros protocolos que no sean SSH.
 - Debe soportar el manejo personalizado (añadir, borrar o modificar) para la alimentación de IoC (Indicadores de Compromiso), en formato CSV y Structured Threat Information Expression (STIX XML).
 - Debe tener capacidad de integración con fuente de IoC de terceros (External IoC) a través de direcciones web URL, con capacidades de detección y prevención. La aplicación y prevención de seguridad, en base a los IoC incluidos, debe ser de manera automática, sin interacción del usuario administrador.

1.13 Prevención de amenazas desconocidas o de día-cero (Emulación y Extracción de malware)

- La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables.
- La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (sandbox).



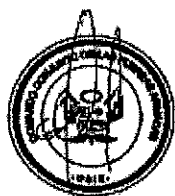
- La solución debe proteger a los usuarios internos, de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo es benigno se entrega el archivo original al usuario y si el archivo es maligno se deniega su acceso o descarga.
- La solución debe proporcionar la capacidad de protección contra ataques de malware desconocido y de día cero antes de que se hayan creado protecciones de firmas estáticas.
- La solución debe proveer prevención en tiempo real de malware desconocido en las descargas web y canal de correo electrónico.
- La solución deberá poder emular archivos para la identificación de malware que viajan en los protocolos: HTTP, HTTPS, SMTP, IMAP, CIFS, SMBv3, SMBv3 multi-channel y FTP.
- La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de MacOS (APP, DMG, PKG).
- Cada archivo emulado en el sandbox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo, basado en las técnicas y tácticas del framework de ciberseguridad MITRE ATT&CK.
- El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
- El motor de emulación debe analizar y emular los URL contenidos en documentos Microsoft Office y PDF, para detectar y prevenir descargas maliciosas de malware.
- El motor de emulación debe emplear mecanismos de ML para detectar y prevenir ataques ocultos sobre archivos LNK (accesos directos) tales como: Icon Spoofing, File Attribute Manipulation, Shortened URLs.
- El motor de emulación debe contar con tecnologías de ML basadas en Redes Neuronales (Neural Networks) para la detección de amenazas en los archivos Microsoft Office y PDF.
- El motor de emulación debe admitir varios sistemas operativos, como Windows XP, Windows7, Windows 10 y Windows 11.
- Las soluciones deben admitir motores de detección automatizados basados en machine learning.
- La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware.
- La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectaran la existencia de un entorno virtual.
- La solución deberá tener capacidad de extracción de amenazas o CDR (Content Disarm Reconstruction), en las descargas de archivos desde Internet inclusive sobre canal cifrado HTTPS para prevenir el riesgo al interior de la red corporativa. Debe tener la capacidad de limpiar archivo durante su análisis, extrayendo el componente activo de riesgo o malicioso que encuentran dentro de los archivos, y, además, poder transformar el archivo en un formato



PDF. Esta funcionalidad debe soportar como mínimo los siguientes tipos de archivo para el canal web y correo:

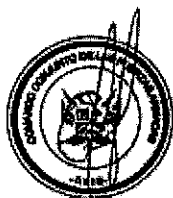
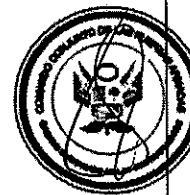
- Microsoft Excel (XLS, XLSX, XLSB, XLSM, XLTX, SLTM)
- Microsoft Word (DOC, DOCX, DOCM, DOTX, DOTM, DOT)
- Microsoft Power Point (PPT, PPS, PPTX, PPTM, POTX, POTM, PPSX)
- Adobe PDF (PDF, FDF)
- Así mismo, la capacidad de extracción y/o transformación de los archivos para prevención de amenazas, debe ser efectuada a los archivos adjuntos en canal de correo (modo MTA) para los formatos:
- Imágenes (JPEG, JPG, BMP, PSD, GIF, TIF, PNG)
- XML, TXT, HTML, JS.
- La extracción de malware deberá retirar los componentes de riesgo de los documentos tales como: Macros, Objetos Embebidos, Enlaces (Linked Objects), PDF JavaScripts y PDF Launch.

1.14 Identificación de usuarios



- La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
 - ✓ Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
 - ✓ Con agente implementado en los servidores de Directorio Activo Microsoft.
 - ✓ Empleando un Portal Cautivo.
 - ✓ Empleando un Proveedor de Identidad (IdP) basado en SAML.
- La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
- La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
- Debe proveer un "Portal Cautivo", para autenticar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
- La solución debe proveer configuración de acceso basado reglas de tiempo, en las cuales los usuarios puedan entrar a los recursos de la red.
- Cuando se detecte que los usuarios no se han autenticado, la solución tiene que re-direccionarlos a un Portal Cautivo, a través del protocolo HTTP.
- Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos Interna del equipo, servidor de LDAP y servidor de RADIUS.
- La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP.
- La solución debe integrarse con el Directorio Activo Microsoft sin la necesidad de instalar un agente en el Servidor de Dominio o en los equipos de los usuarios finales.
- La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

1.15 VPN IPSec

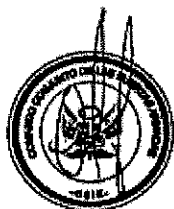
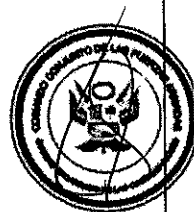


- Debe soportar IPSec VPN Client-to-Site con capacidad de XXX usuarios concurrentes.
- Debe soportar túneles VPN punto a punto Site-to-Site de manera ilimitada o hasta la máxima capacidad soportada por el equipamiento.
- Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: Tokens (Ejemplo: SecureID), TACACS, RADIUS y Certificados Digitales.
- Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Deben ser soportados 3DES y AES-256 para las fases I y II de IKE.
- Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit)
- Debe soportar integridad de datos con MD5 y SHA1.
- Debe incluir soporte a las topologías VPNs site-to-site: Todos a todos, Oficinas Remotas a Sitio Central y Sitio remoto a través del sitio central hacia otro sitio remoto.
- Soporte a VPNs client-to-site basadas en IPSEC.
- Debe poder establecer VPNs con Firewalls con direcciones IP dinámicas públicas o resolución de DNS.
- Debe poder integrarse con Directorio Activo Microsoft u Open LDAP para crear reglas de control de acceso a través de VPN, empujando: usuarios, grupos de usuarios, máquinas, dirección IP y redes.
- Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN.
- El cliente VPN, debe instalarse sobre sistemas operativos Windows, Linux y MacOS.
- La solución debe contar con autenticación de doble factor mediante el certificado del cliente y el usuario/contraseña.
- La solución VPN, debe ser capaz de evaluar la configuración del dispositivo cliente antes de otorgar el acceso a la red corporativa, por lo menos las siguientes condiciones:
 - Verificar el sistema operativo.
 - Verifica si el usuario logeado en el equipo es miembro de grupos específicos.
 - Verifica si procesos específicos se están ejecutando o no.
 - Verifica las llaves de registro, valores y su contenido.
 - Verifica el hardware de CPU, tipo y modelo.
 - Verifica los componentes de Windows Security Center, se puede elegir que componente y si es que están instalados y ejecutándose.

1.16 QoS

- Debe contar con un módulo integrado de Calidad de Servicio o QoS, que permita principalmente:
- Priorización de tráfico crítico para el negocio, sobre el tráfico de menor prioridad (no crítico).
- Garantice el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.

- Otorgue acceso garantizado o prioritario a empleados específicos, incluso si acceden de forma remota a los recursos de la red.
- El QoS debe permitir la definición:
 - Porcentaje del ancho de banda disponible, basado en prioridad de regla.
 - Ancho de banda mínimo garantizado
 - Ancho de banda máximo, basado en límites
- Deberá permitir aplicar reglas de QoS para el tráfico cifrado de VPN.
- Debe tener capacidad de QoS Queuing para servicio de baja latencia (Low Latency) para poder definir clases especiales de servicio para aplicaciones "sensibles a demoras" como voz y video.



ANEXO B

CARACTERÍSTICAS TÉCNICAS: SEGURIDAD DATA CENTER



Nº	ITEM	TIPO	Cant.
01	Equipo Firewall Data Center	Hardware	01

1. UN EQUIPO DE SEGURIDAD

1.2. Hardware, Performance e Interfaces

- ☐ Cantidad: Una (01) unidad.
- ☐ Appliance de firewall de nueva generación/Gateway.
- ☐ Rendimiento (throughput) de 11 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, URL Filtering, Antivirus, Anti-Bot o Antispyware y Emulación Malware día-cero.
- ☐ Rendimiento (throughput) de 33 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones e IPS).
- ☐ Conexiones concurrentes: 16 millones como mínimo.
- ☐ Cantidad de conexiones por segundo: 355 000 como mínima.
- ☐ Almacenamiento local: 480 GB SSD como mínimo.
- ☐ 08 puertos de red 1GB (RJ45)
- ☐ 04 interfaces 10 GB SFP+
- ☐ Capacidad de soportar ampliación para 02 interfaces 40 GB QSFP+
- ☐ Soporte de alta disponibilidad.

1.3 Consideraciones generales

- ☐ El sistema operativo deberá ser del fabricante de la solución de firewall ofertado, el mismo deberá venir de fábrica con el "hardening" necesario. El fabricante deberá desarrollar las actualizaciones de sistema operativo, parches del software o módulos utilizados, estos deberán estar disponible para descarga y/o actualización en los equipos durante toda la vigencia del soporte técnico contratado
- ☐ Los equipos deben ser nuevos y de primer uso.
- ☐ En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Este requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.
- ☐ El fabricante de la solución de seguridad debe estar presente en los últimos 08 reportes de Gartner (Magic Quadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.
- ☐ El fabricante de la solución de seguridad debe tener un porcentaje

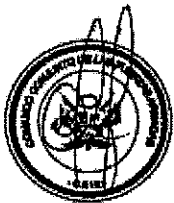
de efectividad de seguridad igual o superior al 99% y calificación de AAA, en la última evaluación de Enterprise Firewall Report de CyberRatings para el año 2023.

- ☐ El fabricante de la solución de seguridad debe tener un porcentaje de efectividad de seguridad igual o superior al 99%, en la última evaluación de Miercom Next-Generation Firewall Security Benchmark (2024).
- ☐ Los sistemas operativos (SO) que operan en los equipos de seguridad firewall ofertados, no deberá tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante los últimos 12 meses anteriores a la fecha de presentación de propuestas.



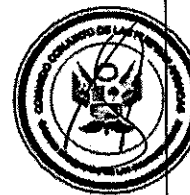
1.4 Consideraciones generales

- ☐ Los firewalls ofertados deben poder implementarse y operar en modalidad de Alta Disponibilidad en modo Activo-Activo y modo Activo-Pasivo.
- ☐ La solución de seguridad debe permitir la configuración de clúster en modo de operación en alta disponibilidad (HA), tanto para IPv4 como para IPv6.
- ☐ Debe soportar redundancia de hasta 10 enlaces ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- ☐ La redundancia de ISP puede ser a nivel de "compartición de carga" (load sharing) y detección de falla enlace (primary/backup).
- ☐ Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster, así como contar con mecanismos de detección de fallas y detección de pérdida de enlaces.



1.5 Funcionalidades de red:

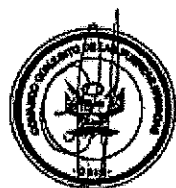
- ☐ La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- ☐ Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
- ☐ Debe soportar enrutamiento con IPv4 e IPv6.
- ☐ Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
- ☐ Debe soportar control de ancho de banda basado en prioridades de pesos.
- ☐ Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación.
- ☐ Soporte de rutas estáticas, PBR (policy based routing), LACP, OSPF (IPv4 e IPv6), RIP, BGP, IGMP, PIM, Ipsec Routing y Dual Stack IPv4 e IPv6, NAT64, NAT46 y NAT66.
- ☐ La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- ☐ El soporte a políticas de ruteo permite que, ante la presencia de dos enlaces, se pueda decidir por que enlace egresa tráfico determinado.
- ☐ La solución debe soportar políticas de ruteo estatico en IPv6.



- ❑ La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración.
- ❑ Debe incluir la posibilidad de crear NAT permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.

1.6 Gestión de Políticas

- ❑ El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, comunidad de VPN, direcciones de URL y aplicaciones.
- ❑ Sobre la base de la políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final
- ❑ Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- ❑ Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- ❑ Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora).
- ❑ Debe tener capacidad de crear reglas de firewall en base a objetos dinámicos, los cuales son basados en fuentes de URL externas (HTTP/HTTPS) que contengan archivos CSV o Json, con la finalidad de automatizar las reglas de acceso, no siendo necesario publicar y/o compilar reglas en el firewall.



1.7 Otras funcionalidades

- ❑ Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
- ❑ La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups (configuración del sistema operativo) en el tiempo deseado.
- ❑ Los backups pueden ser almacenados localmente y el administrador puede transferirlos vía FTP, TFTP y SCP de manera programada.
- ❑ La comunicación entre los servidores de administración y el equipo de seguridad (firewall), debe ser cifrada y autenticada.
- ❑ Debe tener la opción de negar los parámetros de origen o destino, es decir que para una regla dada permite todas las conexiones de origen / destino excepto la especificada en la regla.
- ❑ La solución debe permitir integración con analizadores de tráfico mediante el protocolo NetFlow.
- ❑ Integración mediante API REST de Terceros.
- ❑ Los firewalls deben permitir manejo de ancho de banda de distintos protocolos y/o aplicaciones, permitiendo la definición de niveles de

- ancho de banda tanto para carga (upload) y descarga (download).
- ☐ Debe soportar y proteger protocolos de VoIP (SIP, H.323, MGCP, SCCP) incluyendo soporte de NAT para cada uno de esos protocolos.

1.8 Geolocalización

- ☐ Soportar la creación de políticas basada en Geo-localización, permitiendo que el tráfico de determinado País/Países sean bloqueados o permitidos.
- ☐ Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- ☐ Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- ☐ Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.

1.9 Prevención de Intrusos - IPS

- ☐ La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- ☐ El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.
- ☐ Debe tener protección contra ataques DoS (Denial of Service).
- ☐ A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, SQL Injection, Command Injection e Injection protección para DN (Distinguished Names).
- ☐ El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.
- ☐ Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) y nivel consumo de recursos.
- ☐ Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
- ☐ Debe poder realizar captura de paquetes para protecciones específicas.
- ☐ Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, IMAP, DNS tunneling, FTP, SNMP, IMAP, SMB.
- ☐ Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.
- ☐ Debe detectar y bloquear intentos de tuneles, a fin de evitar fuga de datos o problemas de seguridad web.
- ☐ Debe proteger contra ataques tipo DNS Cache Poisoning cuando reutilizan los puertos de origen.
- ☐ Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.
- ☐ La solución debe tener capacidades de detección y prevención de ataques tunelizados en tráfico DNS.



- ☐ Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.
- ☐ Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.
- ☐ La funcionalidad de IPS debe tener las siguientes capacidades:
- ☐ Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos.
- ☐ Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial.
- ☐ Detección y prevención de comunicaciones de malware salientes.
- ☐ Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.
- ☐ Detección, prevención o restricción de ciertas aplicaciones que pueden causar amenazas a la seguridad de la red, como las aplicaciones P2P o de mensajería instantánea.

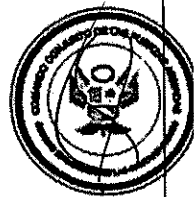
1.10 Anti-Bot o Antispyware



- ☐ La solución debe proveer una herramienta que haga descubrimiento de "bots" dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados "bots" hacia las redes de los atacantes en Internet (botnet).
- ☐ La solución debe incluir al menos los siguientes métodos de identificación:
- ☐ Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
- ☐ Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
- ☐ Identificación de comportamiento de bots.
- ☐ La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de "botnet". El Anti-Bot se debe actualizar continuamente de manera automática.
- ☐ La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
- ☐ La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltración de información mediante DNS Tunneling.
- ☐ La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

1.11 Control de aplicaciones y Filtro de URL

- ☐ La solución debe ser capaz de identificar, permitir o bloquear



- aplicaciones y páginas Web.
- ☐ Se requiere que capacidad de detección de 10,000 aplicaciones en la base de datos de control de aplicaciones para la aplicación de políticas.
- ☐ La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
- ☐ Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
- ☐ Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
- ☐ Solución debe soportar como mínimo 100 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Artificial Intelligence (AI) Hacking, Inactive Sites y Spyware/ Malicious Sites.
- ☐ La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.
- ☐ Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
- ☐ Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
- ☐ La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
- ☐ Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- ☐ La solución debe proporcionar un mecanismo para limitar el uso de aplicaciones basadas en el consumo de ancho de banda (upload / download) por el tipo de aplicación y/o servicio de red definido.
- ☐ Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
- ☐ Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
- ☐ Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2.
- ☐ Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

1.12 Prevención de amenazas

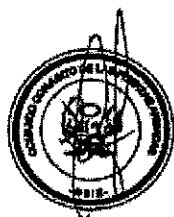
- ☐ Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
- ☐ Debe tener capacidad de clasificación y análisis de archivos y



- posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
- ☐ Los equipos deben tener integrada la detección y prevención de virus y amenazas (anti-malware).
 - ☐ La Inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
 - ☐ Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
 - ☐ Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
 - ☐ Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.
 - ☐ Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
 - ☐ Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
 - ☐ Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
 - ☐ Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
 - ☐ Bloquear ataques en canal SSH.
 - ☐ Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
 - ☐ Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
 - ☐ Prevenir el reenvío de puertos SSH (Port Forwarding).
 - ☐ Prevenir el uso de criptografía vulnerable en el canal SSH.
 - ☐ Prevenir el uso de clientes y servidores SSH vulnerables.
 - ☐ Prevenir el uso del puerto 22 para otros protocolos que no sean SSH.
 - ☐ Debe soportar el manejo personalizado (añadir, borrar o modificar) para la alimentación de IoC (Indicadores de Compromiso), en formato CSV y Structured Threat Information Expression (STIX XML).
 - ☐ Debe tener capacidad de integración con fuente de IoC de terceros (External IoC) a través de direcciones web URL, con capacidades de detección y prevención. La aplicación y prevención de seguridad, en base a los IoC incluidos, debe ser de manera automática, sin interacción del usuario administrador.

1.13 Identificación de usuarios

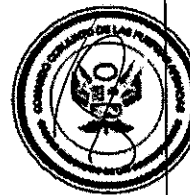
- ☐ La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
 - ☐ Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
 - ☐ Con agente implementado en los servidores de Directorio Activo Microsoft.
- ☐ Empleando un Portal Cautivo.



- ☐ Empleando un Proveedor de Identidad (IdP) basado en SAML.
- ☐ La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
- ☐ La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
- ☐ Debe proveer un "Portal Cautivo", para autenticar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
- ☐ La solución debe proveer configuración de acceso basado reglas de tiempo, en las cuales los usuarios puedan entrar a los recursos de la red.
- ☐ Cuando se detecte que los usuarios no se han autenticado, la solución tiene que re-direccionarlos a un Portal Cautivo, a través del protocolo HTTP.
- ☐ Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos Interna del equipo, servidor de LDAP y servidor de RADIUS.
- ☐ La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP.
- ☐ La solución debe integrarse con el Directorio Activo Microsoft sin la necesidad de instalar un agente en el Servidor de Dominio o en los equipos de los usuarios finales.
- ☐ La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

1.14 VPN IPSec

- ☐ Debe soportar IPSec VPN Client-to-Site con capacidad de XXX usuarios concurrentes.
- ☐ Debe soportar túneles VPN punto a punto Site-to-Site de manera ilimitada o hasta la máxima capacidad soportada por el equipamiento.
- ☐ Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: Tokens (Ejemplo: SecureID), TACACS, RADIUS y Certificados Digitales.
- ☐ Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- ☐ Deben ser soportados 3DES y AES-256 para las fases I y II de IKE.
- ☐ Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit)
- ☐ Debe soportar integridad de datos con MD5 y SHA1.
- ☐ Debe incluir soporte a las topologías VPNs site-to-site: Todos a todos, Oficinas Remotas a Sitio Central y Sitio remoto a través del sitio central hacia otro sitio remoto.
- ☐ Soporte a VPNs client-to-site basadas en IPSEC.
- ☐ Debe poder establecer VPNs con Firewalls con direcciones IP dinámicas públicas o resolución de DNS.
- ☐ Debe poder integrarse con Directorio Activo Microsoft u Open LDAP para crear reglas de control de acceso a través de VPN, emplando:



- usuarios, grupos de usuarios, máquinas, dirección IP y redes.
- ☐ Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN.
- ☐ El cliente VPN, debe instalarse sobre sistemas operativos Windows, Linux y MacOS.
- ☐ La solución debe contar con autenticación de doble factor mediante el certificado del cliente y el usuario/contraseña.
- ☐ La solución VPN, debe ser capaz de evaluar la configuración del dispositivo cliente antes de otorgar el acceso a la red corporativa, por lo menos las siguientes condiciones:
- ☐ Verifica el sistema operativo,
- ☐ Verifica si el usuario logeado en el equipo es miembro de grupos específicos.
- ☐ Verifica si procesos específicos se están ejecutando o no.
- ☐ Verifica las llaves de registro, valores y su contenido.
- ☐ Verifica el hardware de CPU, tipo y modelo.
- ☐ Verifica los componentes de Windows Security Center, se puede elegir que componente y si es que están instalados y ejecutándose.

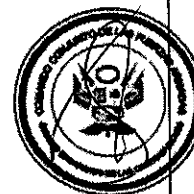
1.15 QoS



- ☐ Debe contar con un módulo integrado de Calidad de Servicio o QoS, que permita principalmente:
- ☐ Priorización de tráfico crítico para el negocio, sobre el tráfico de menor prioridad (no crítico).
- ☐ Garantice el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
- ☐ Otorgue acceso garantizado o prioritario a empleados específicos, incluso si acceden de forma remota a los recursos de la red.
- ☐ El QoS debe permitir la definición:
 - Porcentaje del ancho de banda disponible, basado en prioridad de regla.
 - Ancho de banda mínimo garantizado
 - Ancho de banda máximo, basado en límites
- ☐ Deberá permitir aplicar reglas de QoS para el tráfico cifrado de VPN.
- ☐ Debe tener capacidad de QoS Queuing para servicio de baja latencia (Low Latency) para poder definir clases especiales de servicio para aplicaciones "sensibles a demoras" como voz y video.

ANEXO C

CARACTERÍSTICAS TÉCNICAS: Administración y Correlación de Eventos y Reportes



N°	ITEM	TIPO	Cant
01	Equipo Virtual para Administración y Correlación de Eventos y Reportes	Virtual	01

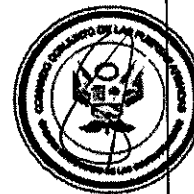
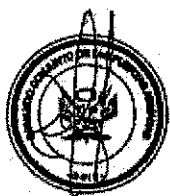
1. UN EQUIPO DE SEGURIDAD

1.2. Especificaciones

- ☐ Cantidad: Una (01) unidad.
- ☐ Appliance virtual.
- ☐ La entidad proporcionará los recursos de cómputo para el despliegue de la plataforma

1.3 Consideraciones generales

- ☐ La consola centralizada deberá tener la capacidad licenciada para gestionar todos los firewalls ofertados.
- ☐ La consola centralizada debe permitir el despliegue de actualizaciones y parches de seguridad en los firewalls gestionados.
- ☐ La consola centralizada debe permitir revisar los cambios históricos en las políticas de seguridad, quien realizó los cambios y revertir los cambios a una versión específica.
- ☐ Debe contar con un motor de tareas específicas, que permita automatizar las notificaciones por correo electrónico en base los estados de los cambios en las políticas de seguridad, antes y después de:
 - ☐ Publicación de política de seguridad
 - ☐ Aprobación de política de seguridad
 - ☐ Rechazo de una política de seguridad
 - ☐ Luego de la instalación de una política de seguridad
- ☐ La consola debe contar un flujo de aprobación de cambios. Esta función debe permitir la opción de revisar y aprobar los cambios de configuración realizados por otros administradores antes de publicarlos. Se puede definir qué administradores deben enviar sus cambios para su aprobación y qué administradores están autorizados para aprobar los cambios.
- ☐ La herramienta debe integrar en una única consola gráfica segmentando el estado general de todos los dispositivos administrados, la configuración de la política de seguridad, los logs registrados y el monitoreo de toda la plataforma.
- ☐ Debe incluir una herramienta que administre centralizadamente la licencia de todos los equipos, controlados desde la estación de administración.
- ☐ La herramienta debe permitir gestionar de forma centralizada los túneles VPN y las VPN de acceso remoto de los usuarios.



- ☐ La herramienta debe permitir sesiones concurrentes de diferentes usuarios o dispositivos para los cambios de políticas.
- ☐ La herramienta debe permitir la creación de perfiles de administradores, basados en roles, que accedan a secciones parciales de administración o a la totalidad, indicando también si los perfiles son de solo lectura o lectura/escritura.
- ☐ La herramienta debe permitir el acceso concurrente de administradores, la modificación de la política de seguridad, la publicación de los cambios realizados antes de aplicarlos y la segregación de funciones según el administrador.
- ☐ Capacidad de automatización mediante API, para organizar los flujos de trabajo, en los procesos de seguridad de TI.
- ☐ Capacidad en API de ejecutar scripts para automatizar "tareas diarias" e integrar con soluciones de terceros, como: servidores de virtualización, sistemas de tickets y sistemas de gestión de cambios.
- ☐ Capacidad de autenticación mediante API token (API key authentication), en lugar de usuario y contraseña.
- ☐ La autenticación a la consola de administración puede ser a través de: Credenciales locales, RADIUS, TACACS, SecurID, API Key, SAML.
- ☐ Se debe poder adicionar una capa adicional de seguridad, adicional a los tipos de autenticación indicados anteriormente, mediante el uso de certificado digital.
- ☐ Debe tener una herramienta o capacidad de: gestión de certificados de usuario final (ICA), crear certificados, recrear CRL (listas de revocación) y remover los certificados expirados.

1.4 Capacidad de Correlación de Eventos y reportes

- ☐ Debe contar con una consola para identificar actividades sospechosas, rastrear tendencias e investigar y mitigar eventos de seguridad, a través de plantillas gráficas y reportes.
- ☐ Debe contar con capacidad de análisis desde eventos de alto hacia los detalles específicos, tales como tipo de ataque, tiempo, tipo de aplicación y el origen.
- ☐ Debe permitir el análisis de datos en tiempo real y los registros de eventos de manera personalizada, también notificación inmediata a los administradores para permitir una acción rápida y/o remediación.
- ☐ Debe tener capacidad de mitigación (reacción) automatizada, en base a los eventos de seguridad identificados. Las capacidades deben ser tales como: Enviar un correo electrónico de alerta, bloquear por política la IP origen o múltiples IP Origen (ataque distribuido) relacionados al evento de seguridad en una ventana de tiempo configurable y generar un SNMP Trap.
- ☐ Capacidad de habilitar un "horario laboral" para detectar intentos no autorizados de accesos a sistemas protegidos y otras operaciones prohibidas fuera del horario laboral.
- ☐ Capacidad de realizar excepciones y parametrizar los umbrales para evitar "falsos positivos" en las acciones de mitigación automática.
- ☐ Capacidad de investigación forense y de amenazas, basadas en las técnicas y tácticas del framework de MITRE ATT&CK.
- ☐ Debe contar con un mapa de calor de MITRE ATT&CK, para ubicar las

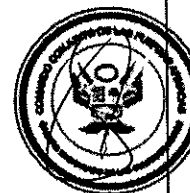
técnicas principales, y capacidad de drill-down para comprender dónde se produjeron los daños causados por archivos maliciosos.

- ☐ Debe contar con un catálogo propio de vistas interactivas y reportes, para poder explotar la información en periodos personalizados.
- ☐ Debe poder crear vistas y reportes propios (custom) empleando tablas, charts, línea de tiempo (timeline), mapa, infografías y textos enriquecidos.
- ☐ Debe soportar como tipos de eventos por lo menos: ataques de denegación de servicio, anomalías de red, actividad basada en host y/o rastreos no autorizados y/o logins no autorizados.
- ☐ Los eventos deben poder tener niveles de seguridad/criticidad asignados de manera automática.
- ☐ Posibilidad de calendarizar reportes predefinidos o customizados, para su entrega automática vía correo electrónico.
- ☐ Debe permitir exportar en formato XLSX o PDF los reportes generados.
- ☐ El sistema de reportes debe proveer información consolidada sobre al menos:
 - ☐ Eventos por Origen, Destino o Usuario
 - ☐ Eventos en una línea de tiempo.
 - ☐ Lista de ataques por severidad y producto.



ANEXO D

CARACTERÍSTICAS TÉCNICAS: SEGURIDAD SANDBOXING



N°	ITEM	TIPO	Cant.
01	Equipo Sandboxing para Emulación de Amenazas de día cero	Hardware	01

1. UN EQUIPO DE SEGURIDAD

1.2. Hardware, Performance e Interfaces

- Equipo de seguridad de propósito específico, del mismo fabricante de la solución de los firewalls ofertados.
- La solución debe integrarse y operar con los firewalls de seguridad ofertados.
- Cantidad: Una (01) unidad.
- 1,300 archivo únicos por hora
- 1 Gbps de throughput
- Almacenamiento 960 GB SSD
- 10 puertos de red 1 GB (RJ45)
- 02 fuentes de poder redundante.



1.3 Protocolos

- HTTP, HTTPS e ICAP para inspección de descargas de Internet, capacidad de inspección tráfico cifrado SSL/TLS.
- SMTP, IMAP, POP3 y SMTPS para inspección de archivos adjuntos en correos electrónicos en modalidad MTA.
- CIFS, SMB, SMBv3, SMBv3 multi-channel y FTP

1.4 Características

- Los firewalls ofertados deben poder implementarse y operar en modalidad de Alta Disponibilidad en modo Activo-Activo y modo Activo-Pasivo.
- Capacidad de detección de malware resistente a la evasión, con capacidad de inspección a nivel de CPU, para detectar el malware antes de que tenga la oportunidad de implantarse y evadir la detección.
- Debe contar con un motor de emulación de amenazas, para detectar malware en la fase de explotación, incluso antes de que los hackers informáticos puedan aplicar técnicas de evasión para intentar eludir el entorno limitado (sandbox), combinando inspección a nivel de CPU y a nivel del sistema operativo.
- Cada emulación de archivo debe genera un informe forense detallado.
- El informe forense debe incluir informacion sobre cualquier intento

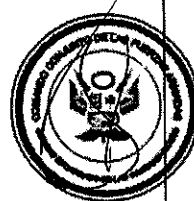
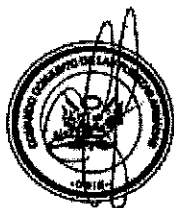
malicioso originado al ejecutar este archivo y proporcionar capturas de pantalla reales (mediante videos) sobres de los entornos simulados mientras se ejecuta el archivo.

1.5 Tipos de archivos

- Deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de MacOS (APP, DMG, PKG).
- Análisis de malware en archivos comprimidos
- Análisis de malware en archivos protegidos por contraseña.

1.6 Extracción de Amenazas

- Capacidad de eliminar contenido explotable (contenido activo) y objetos incrustados.
- Debe poder, reconstruir los archivos para eliminar amenazas potenciales y entrega rápidamente archivos desinfectados.
- Capacidad de extracción de contenido activo en los archivos, tales como: Macros y Código, Objetos Embebidos, Linked Objects, PDF JavaScript Actions y PDF Launch Actions
- La capacidad de extracción de amenazas debe soportar los siguientes tipos de archivos: Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Adobe PDF e Imágenes.



ANEXO E

CARACTERÍSTICAS TÉCNICAS: SEGURIDAD PERIMETRAL REMOTO



N°	ITEM	TIPO	Cant.
01	Equipo Firewall Perimetral Remoto	Hardware	03

1. UN EQUIPO DE SEGURIDAD

1.2. Hardware, Performance e Interfaces

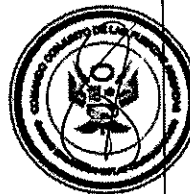
- Cantidad: Una (01) unidad.
- Appliance de firewall de nueva generación/Gateway.
- Firewall Throughput: 4.5 Gbps como mínimo.
- Firewall + IPS + Control de Aplicaciones Throughput: 3 Gbps como mínimo.
- Firewall + IPS+ Control de Aplicaciones + Antivirus + URL Filtering Throughput + Anti-Bot o Antispyware + Emulación Malware Día Cero: 1.3 Gbps como mínimo.
- Conexiones concurrentes: 2 millones como mínimo.
- Cantidad de conexiones por segundo: 50 000 como mínimo.
- Almacenamiento local: 32 GB como mínimo.
- Dieciséis (16) interfaces de red LAN 10/100/1000Base-T RJ-45.
- Una (01) interfaz de red DMZ 10/100/1000Base-T RJ-45 o 1000BaseF SFP.
- Una (01) interfaz de red WAN 10/100/1000Base-T RJ-45 o 1000BaseF SFP.
- Soporte de alta disponibilidad.

1.3 Funcionalidades de red:

- La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
- Debe soportar enrutamiento con IPv4 e IPv6.
- Debe soportar DHCP en modos: Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
- Debe soportar control de ancho de banda basado en prioridades de pesos.
- Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación.
- Debe tener mecanismos de detección de engaños de IP, donde paquetes externos a la red usan direcciones internas para saltarse los controles de seguridad.
- La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.

1.4 Gestión de Políticas

- El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, comunidad de VPN, direcciones de URL y aplicaciones.
- Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final
- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora).

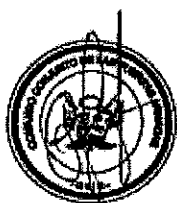


1.5 Geolocalización

- Soportar la creación de políticas basada en Geo-localización, permitiendo que el tráfico de determinado País/Países sean bloqueados o permitidos.
- Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.

1.6 Prevención de Intrusos - IPS

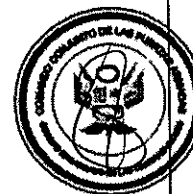
- La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.
- A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, SQL Injection, Command Injection e Injection protection para DN (Distinguished Names).
- El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.
- Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) y nivel consumo de recursos.
- Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o



- mediante las reglas de seguridad configuradas.
- Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.
 - Debe detectar y bloquear intentos de túneles, a fin de evitar fuga de datos o problemas de seguridad web.
 - Debe proteger contra ataques tipo DNS Cache Poisoning cuando reutilizan los puertos de origen.
 - Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.
 - Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.
 - La funcionalidad de IPS debe tener las siguientes capacidades:
 - Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos.
 - Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial.
 - Detección y prevención de comunicaciones de malware salientes.
 - Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.
 - Detección, prevención o restricción de ciertas aplicaciones que pueden causar amenazas a la seguridad de la red, como las aplicaciones P2P o de mensajería instantánea.

1.7 Anti-Bot o Antispyware

- La solución debe proveer una herramienta que haga descubrimiento de "Bots" dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados "Bots" hacia las redes de los atacantes en Internet (botnet).
- La solución debe incluir al menos los siguientes métodos de identificación:
- Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los Bots.
- Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de Bots.
- Identificación de comportamiento de Bots.
- La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de "botnet". El Anti-Bot se debe actualizar continuamente de manera automática.
- La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
- La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).



1.8 Control de aplicaciones y Filtro de URL

- La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.
- Se requiere que la detección de aplicaciones sea basada en APP-ID (decodificación de protocolos y aplicaciones, junto a detección heurística), o en base a firmas. En el caso que la solución sea basada en firmas, la base de datos de control de aplicaciones debe contener al menos 10,000 aplicaciones.
- La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
- Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
- Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
- Solución debe soportar como mínimo 100 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Hacking, Inactive Sites y Spyware/ Malicious Sites.
- La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.
- Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías.
- Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
- Debe permitir la categorización de los sitios basado en el contenido del campo SIN (Server Name Indication).

1.9 Prevención de amenazas

- Los equipos deben tener integrada la detección y prevención de virus y amenazas (antimalware).
- La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
- Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
- Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
- Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.
- Base de datos local de firmas de malware locales que contiene las firmas comúnmente usadas, URL y sus reputaciones.
- Utiliza el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar el



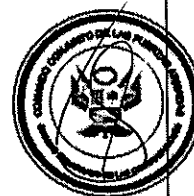
repositorio para la reputación de URL y la clasificación antivirus. Las actualizaciones de firmas de antivirus, se realiza de manera automatizada y programable.

- Debe soportar Inspección de tráfico cifrado/encryptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
- Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
- Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware. Debe contar con un mecanismo de almacenamiento en caché para verificar las URL a las cuales se acceden, o en su defecto, enviar al repositorio de inteligencia de amenazas en nube del propio fabricante para determinar si estas URLs están permitidas o no, parase detener el intento antes de que se produzcan daños en la red.



1.10 Prevención de amenazas desconocidas o de día-cero (Emulación y Extracción de malware)

- La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables.
- La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (sandbox).
- La solución debe proteger a los usuarios internos, de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo es benigno se entrega el archivo original al usuario y si el archivo es maligno se deniega su acceso o descarga.
- La solución debe proporcionar la capacidad de protección contra ataques de malware desconocido y de día cero antes de que se hayan creado protecciones de firmas estáticas.
- La solución debe proveer prevención en tiempo real de malware desconocido en las descargas web y canal de correo electrónico.
- La solución deberá poder emular archivos para la identificación de malware que viajan en los protocolos: HTTP, HTTPS, SMTP, IMAP, CIFS, SMBv3, SMBv3 multi-channel y FTP.
- La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de MacOS (APP, DMG, PKG).
- Cada archivo emulado en el sandbox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo, basado en las técnicas y tácticas del framework de ciberseguridad MITRE ATT&CK.



- El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
- El motor de emulación debe analizar y emular los URL contenidos en documentos Microsoft Office y PDF, para detectar y prevenir descargas maliciosas de malware.
- El motor de emulación debe emplear mecanismos de ML para detectar y prevenir ataques ocultos sobre archivos LNK (accesos directos) tales como: Icon Spoofing, File Attribute Manipulation, Shortened URLs.
- El motor de emulación debe contar con tecnologías de ML basadas en Redes Neuronales (Neural Networks) para la detección de amenazas en los archivos Microsoft Office y PDF.
- El motor de emulación debe admitir varios sistemas operativos, como Windows XP, Windows7, Windows 10 y Windows 11.
- Las soluciones deben admitir motores de detección automatizados basados en machine learning.
- La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware.
- La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectaran la existencia de un entorno virtual.
- La solución deberá tener capacidad de extracción de amenazas o CDR (Content Disarm Reconstruction), en las descargas de archivos desde Internet inclusive sobre canal cifrado HTTPS para prevenir el riesgo al interior de la red corporativa. Debe tener la capacidad de limpiar archivo durante su análisis, extrayendo el componente activo de riesgo o malicioso que que encuentran dentro de los archivos, y, además, poder transformar el archivo en un formato PDF. Esta funcionalidad debe soportar como mínimo los siguientes tipos de archivo para el canal web y correo:
 - Microsoft Excel (XLS, XLSX, XLSB, XLSM, XLTX, SLTM)
 - Microsoft Word (DOC, DOCX, DOCM, DOTX, DOTM, DOT)
 - Microsoft Power Point (PPT, PPS, PPTX, PPTM, POTX, POTM, PPSX)
 - Adobe PDF (PDF, FDF)
- Así mismo, la capacidad de extracción y/o transformación de los archivos para prevención de amenazas, debe ser efectuada a los archivos adjuntos en canal de correo (modo MTA) para los formatos:
 - Imágenes (JPEG, JPG, BMP, PSD, GIF, TIF, PNG)
 - XML, TXT, HTML, JS.
- La extracción de malware deberá retirar los componentes de riesgo de los documentos tales como: Macros, Objetos Embebidos, Enlaces (Linked Objects), PDF JavaScripts y PDF Launch.

1.11 VPN IPsec

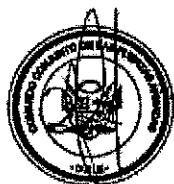
- Debe soportar IPsec VPN (Client-to-Site y Site-to-Site) y capacidad de usuarios ilimitada o hasta el de usuarios que permita la capacidad del equipo.
- Debe soportar túneles VPN punto a punto (Site-to-Site) y túneles de



- acceso remoto para usuario final (Client-to-Site).
- Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Deben ser soportados 3DES y AES-256 para las fases I y II de IKE.
- Debe soportar integridad de datos con MD5 y SHA1.
- Soporte a VPNs client-to-site basadas en IPSEC.
- El cliente VPN, debe instalarse sobre sistemas operativos Windows.
- La solución debe contar con autenticación de doble factor.

1.12 QoS

- Debe contar con un módulo integrado de Calidad de Servicio o QoS, que permita principalmente:
 - Priorización de tráfico crítico para el negocio, sobre el tráfico de menor prioridad (no crítico).
 - Garantice el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y Tráfico VPN.



1.13 Gestión

- Servicio gestionado desde la propia nube del fabricante.
- Servicio MaaS (Management as a Service)
- Consola unificada, una política de control de acceso unificado para los usuarios, aplicaciones, datos y redes.
- La gestión de amenazas está completamente integrada, con los registros, monitoreo, correlación de eventos e informes en un solo lugar.
- Contiene tableros visuales que proporcionan una visibilidad completa de la seguridad en toda la red.
- Con capacidad de 100GB de retención y hasta 03Gb de logs diarios.

1.14 Otras Funcionalidades

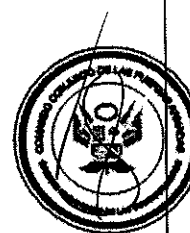
- Administración accesible a través de SSH y de Interfaz Web segura (HTTPS).
- La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups (configuración del sistema operativo) en el tiempo deseado.
- Los backups pueden ser almacenados localmente y el administrador puede transferirlos vía TFTP o FTP o RCP o SCP o sFTP, o funcionalidades similares que cubran dicha especificación.
- La comunicación entre los servidores de administración y el equipo de seguridad (firewall), debe ser cifrada y autenticada.
- Debe incluir la posibilidad de crear NAT permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.
- Debe tener la opción de negar los parámetros de origen o destino, es decir que para una regla dada permite todas las conexiones de

- origen / destino excepto la especificada en la regla.
- Los firewalls deben permitir manejo de ancho de banda de distintos protocolos y/o aplicaciones, permitiendo la definición de niveles para carga (upload) y descarga (download).



ANEXO F

CARACTERÍSTICAS TÉCNICAS:
SWITCH ACCESO

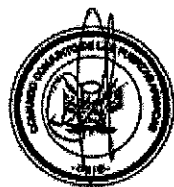


Nº	ITEM	TIPO	Cant
01	Switch Acceso	Hardware	02

1. **Switch Acceso**

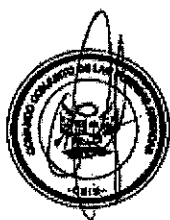
El modelo de switch deberá ser nuevo y cumplir como mínimo las siguientes características técnicas:

1. El switch deberá ser de 1 RU.
2. Soporte a 24 puertos 10/100/1000 en cobre y contar con uplink modular o integrado con un mínimo de 04 puertos 1G SFP+. Los puertos de uplink no deben bloquear puertos de acceso(downlink), maximizando así la cantidad de puertos totales por switch.
3. Leds indicadores de operación por puerto.
4. Fuente de poder con alimentación de 110 a 220VAC, 50 o 60Hz
5. Mínima capacidad de reenvío: 40 Mpps
6. Ancho de banda de switching: 50 GB
7. Soporte para 4000 VLAN IDs como mínimo
8. Soporte de Spanning Tree IEEE 802.1d.
9. Soporte a IEEE 802.1Q para entregar streams de audio y video de forma sincronizada y con baja latencia sobre redes Ethernet capa 2.
10. Capacidad de operación de puertos en half y full dúplex
11. Soporte de NTP
12. Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
13. Soporte de IGMP.
14. Software actualizable. Incluir la última versión disponible.



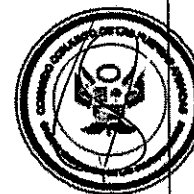


15. Soporte de Telnet, HTTP y SSH para gestión remota
16. Soporte de SNMP v1, SNMP v2c y/o SNMP v3.
17. Soporte del estándar IEEE 802.1AB (LLDP: Link Layer Discovery Protocol) para intercambio de información de dispositivos en redes multivendor.
18. Soportar múltiples niveles de privilegios de acceso por puerto de consola o Telnet para administración.
19. Procesos de debug para análisis en caso de fallas.
20. Soporte de diagnóstico en línea del switch, que permita verificar el hardware usando diferentes pruebas predefinidas en demanda o calendarizadas
21. El switch debe tener la capacidad de limitar la cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.
22. Soporte de autenticación 802.1x con asignación dinámica de VLAN y asignación dinámica de listas de control de acceso (ACL).
23. Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentican vía 802.1x.
24. Autenticación, Autorización y Accounting para administradores de red usando RADIUS/TACACS+.
25. Soporte de Calidad de Servicio QoS.
26. Marcado y clasificación de paquetes.
27. El switch deberá ofrecer mecanismos de booteo seguro para verificar la secuencia de arranque del equipo y protegerlo contra firmware no original o manipulado.



ANEXO G

CARACTERÍSTICAS TÉCNICAS: SEGURIDAD DE CORREO ELECTRONICO



N°	ITEM	TIPO	Cant
01	Equipo virtual para Protección de Correo Electrónico onpremise	Virtual	01

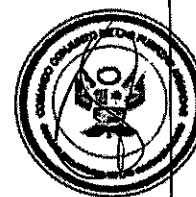
1. CARACTERISTICAS

1.2. Especificaciones Generales

- La entidad proporcionará los recursos de cómputo para el despliegue de la plataforma.
- Se requiere una solución para la protección del buzón de correo electrónico on-premise en mínimo 500 usuarios.
- Tener la capacidad de generar políticas al tráfico entrante y al tráfico saliente, de forma independiente.
- Contar con múltiples opciones de respuesta:
 - Eliminar Mensaje
 - Enviar Mensaje a un recipiente especificado
 - Guardar el Mensaje en una Cuarentena
 - Enviar Notificación
- Tener la flexibilidad de establecer distintas configuraciones de seguridad de correo electrónico, como políticas, a usuarios y grupos basados en sus direcciones de correo y dominios.
- Tener la capacidad para encontrar rápidamente sobre qué política cae un mensaje, dependiendo del remitente o destinatario.
- Tener criterios para selección de política - basado en remitente, destinatario, direcciones de e-mail o LDAP Group Queries.
- Realizar el descartado, cuarentena y entrega de mensajes sospechosos de ser spam.

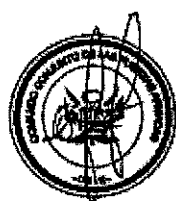
1.3 Capacidades de reporte y análisis de la plataforma

- Deberá contar un sistema para revisar los correos en tiempo real a medida que pasan por el sistema de correo. Este sistema deberá entregar la siguiente información:
 - Estado de Mensajes
 - Estado de Conexión
 - Estado de entrega de Mensajes
 - Resultado del análisis del Mensaje
- Deberá contar con diferentes tipos de Dashboards que incluyen:
 - Reportes asociados al valor de producto en términos de seguridad.
 - Dashboard asociados al correo entrante (Top Mensajes Entrantes, Top Recipients, Throughput, resumen)
 - Dashboard asociados al correo saliente (Top Mensajes Entrantes, Top Outbound Senders, Resumen, etc.)
- Personalizar el dashboard usando "My Reports", agregar múltiples



- reportes con capacidad de drill-down y usar drag-and-drop para acomodarlos. Las vistas se podrán personalizar en rangos de tiempo.
- Tener habilidad de tener reportes y gráficas de estado de mensajes entrantes/salientes por dominio.
- Reportes de alto volumen de correo en base a diferentes parámetros como remitente, top subjects, top filtros de mensaje.
- Reportes para verificar la capacidad y carga del sistema en diferentes rangos de tiempo, que describen cantidad de conexiones totales entrantes/salientes, promedio de tamaño de correo entrante/saliente, tamaño total de correos, utilización de recursos.
- Reportes de los estados de las diferentes cuarentenas, con opciones para tomar acción sobre mensajes determinados.
- Rastreo detallado de correos electrónicos: Capacidad de poder hacer búsqueda de un mensaje procesado y poder ver sus características/composición y detalle cronológico del procesamiento recibido durante el flujo.

1.4 Manejo de Correo de Alto Volumen



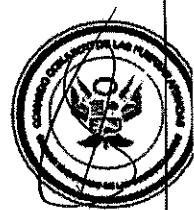
- Capacidad de crear filtros de mensajes en base a múltiples parámetros, que permitan la detección de e-mail en alto volumen y aplicar acciones como cuarentena y descartado (drop).
- Poder aplicar rate-limiting selectivo tanto en flujos entrantes como salientes.
- Poder aplicar throttling de mensajes por remitente, destino o Gateway Virtual, en base a límites configurables.
- Poder aplicar excepciones a este tipo de reglas.
- Poder manejar y aplicar diferentes perfiles de rebotado de correo (Bounce).

1.5 Outbreak Filters y Anti-Phishing

- Debe tener protección de amenazas emergentes, Outbreak Filters que defiende ante nuevos outbreaks.
- Debe crear un disclaimer o aviso de OVF en base a una plantilla predefinida y variables de sustitución. Este disclaimer se desplegará sobre el cuerpo del correo. Tener también que se puede modificar el Subject del correo.
- Debe proteger ante ataques mezclados "Blended Threats" por medio de reescribir URLs dentro de mensajes sospechosos. Cuando se da clic, los URL se redireccionan automáticamente a la solución de Web Security del mismo fabricante, el contenido se escanea, y se desplegará una pantalla de bloqueo si el sitio contiene malware.
- Debe realizar selectivamente por medio de las políticas de e-mail, poder habilitar el reescribir los URLs para todos los mensajes o bien de únicamente para mensajes no autenticados por DKIM.
- Ciertos dominios, direcciones IP, hostnames pueden ser omitidos de la modificación de URL, a través de listas blancas.
- Las URLs reescritas seguirán teniendo efecto y aun cuando el usuario hace forward del mensaje a alguien dentro de la organización.
- Los mensajes identificados como Phishing serán enviados a una

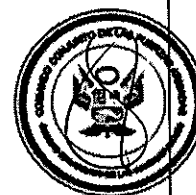
cuarentena específica.

- Tener cómo los URLs dentro de los correos pueden ser sujetos a filtrado y categorización web en base a reputación y contenido del sitio. Sitios con URLs identificados como inapropiados según las categorías seleccionadas por el administrador (por ejemplo Apuestas, Freeware, Hacking, Juegos, Adultas, etc.), pueden ser modificados o bloqueados. De esta manera, si el URL viola la política, el correo podrá ser puesto en cuarentena, descartado, o únicamente el URL modificada o bloqueado.



ANEXO H

CARACTERÍSTICAS TÉCNICAS: SEGURIDAD APLICACIONES WEB



Nº	ITEM	TIPO	Cant
01	Equipo WAF	Virtual	01

1. CARACTERÍSTICAS

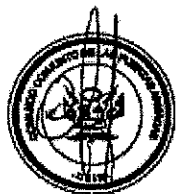
1.2. Especificaciones Técnicas.

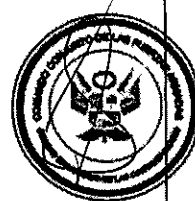
- La entidad proporcionará los recursos de cómputo para el despliegue de la plataforma.
- Se requiere una solución para la protección automatizada de aplicaciones web y API, la misma debe de cumplir con las siguientes características o especificaciones.
- Incorporar las siguientes tecnologías de protección.
 - Web Application Protection
 - API Security
 - Bot Prevention
 - Intrusion Prevention (IPS)
 - File Security
- La solución deberá ser capaz de proteger ataques de día cero en el aplicativo protegido, sin la capacidad de contar con firmas de IPS relacionadas.
- La protección de día cero deberá ser realizada a través del aprendizaje del aplicativo y su comportamiento evitando ataques por headers o formularios web.
- La solución deberá de permitir una cantidad ilimitada de aplicaciones y de ancho de banda, ya que la solución brindara protección a diferentes ambientes WEB y API y la cantidad de estas aplicaciones es muy dinámica al igual que la cantidad del ancho de banda y su ubicación (nube/on-premise).
- La solución deberá brindar en conjunto una protección de al menos 200 Millones de solicitudes (request) web por año.
- La solución debe poder prevenir ciberataques conocidos y desconocidos.
- La implementación debe ser flexible y poderse realizar en diferentes ambientes en nube y en premisas.
- La solución deberá de ser administrada desde un portal en la nube.
- La solución debe poder proteger las aplicaciones en diferentes entornos construidos en cualquier arquitectura (on-premise, nube, containers) administrado desde un único portal centralizado.
- La solución debe poder analizar cada solicitud entrante y se debe analizar en contexto esta solicitud.
- El motor de inteligencia artificial de la solución debe poder llevar a cabo un análisis de riesgos mediante el examen de parámetros como:





- el perfil del usuario
 - los patrones observados en la sesión del usuario
 - la forma en que otros usuarios interactúan típicamente con la aplicación.
- A cada solicitud se le debe asignar una puntuación que determine la probabilidad de que sea maliciosa.
 - El motor se debe poder adaptar automáticamente a los cambios de la aplicación al perfilar continuamente el usuario, la aplicación y el contenido.
 - El motor deberá contar con un aprendizaje asistido donde el operador con una simple decisión pueda asegurar el tráfico.
 - La solución debe poder detener los ataques contra aplicaciones que incluyen:
 - Cross Site Request Forgery
 - XML External Entity
 - Remote Code Execution
 - Evasion Techniques
 - LDAP Injection
 - Path Traversal
 - Vulnerability Scanning
 - SQL Injection
 - Métodos HTTP ilegales Entrada no válida para formularios y APIs
 - Bot Scraping Brute Force Attacks
 - La solución deberá proporcionar protecciones basadas en firmas para al menos 2,800 CVE, vulnerabilidades y exposiciones comunes para aplicaciones Web.
 - La solución deberá poder limitar los siguientes parámetros
 - Los Bytes en el tamaño de URL
 - La profundidad de los objetos de HTTP
 - El tamaño del body de una petición
 - El tamaño del encabezado en una petición
 - Deberá contar con una protección de CSRF
 - La solución debe contar con un motor de análisis de archivos maliciosos, que eviten que se carguen archivos maliciosos en los servidores de la organización. El motor de seguridad de archivos escanea el tráfico HTTP que ingresa a la organización.
 - La solución debe contar con capacidad de emulación de amenazas no conocidas en una zona de pruebas ubicada en la nube de amenazas del propio fabricante, para evitar ataques en la etapa más temprana. La capacidad de emulación debe analizar varios tipos de archivos conocidos: Word, Excel, PowerPoint, PDF y archivos ejecutables.
 - La solución deberá ser capaz de configurar excepciones tales como:
 - expresión regular que determina el uri que debe coincidir. Por ejemplo: /login/.*
 - expresión regular y CIDR que determina el identificador de fuente que debe coincidir. Por ejemplo: 192.168.24.0/24 o .*@Acme.com]
 - CIDR que determina la IP de origen físico que debe coincidir. Por ejemplo: 192.168.24.0/16
 - expresión regular que determina el nombre del parámetro que

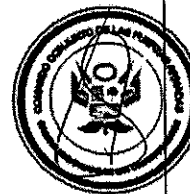




- debe coincidir. Por ejemplo: * Contraseña. *
- expresión regular que determina el nombre del parámetro que debe coincidir. Por ejemplo: ^ 4 [0-9] {12} (? : [0-9] {3}) ? \$
- el indicador que debe coincidir. Si es necesario, usa una lista separada por comas.
- La solución deberá ser capaz de configurar excepciones y modificar la acción que toma la herramienta de forma predeterminada, la solución deberá permitir aceptar o bloquear el tráfico cuando el mismo haga match a algunas de las condiciones mencionadas en el punto anterior.
- La solución deberá permitir subir certificados para poder proteger sitios https de la institución.
- La solución deberá incluir un motor de aprendizaje que ayude a disminuir la cantidad de eventos críticos y altos a lo largo del tiempo a medida que aprende el tráfico del sitio y comprende el comportamiento del usuario.
- El aprendizaje de la solución debe de funcionar de manera continua y no solo tener un "modo aprendizaje"
- La solución deberá clasificar cada solicitud y decidir sus posibilidades de ataque a través de un motor de inteligencia artificial inteligente
- Las políticas de la solución deberán de poder operar en al menos los siguientes modos:
 - Prevención
 - Aprendizaje/detección
 - Deshabilitado
- La solución deberá incluir políticas predefinidas que sean Best Practice (o la practica recomendada del fabricante). Estas políticas deberán de poder ser editadas en caso de ser necesario.
- La solución debe poder ser instalada en diferentes ambientes, algunos actualmente implementados en la institución y otros que se implementaran en el futuro, al menos debe poder ser instalada en:
 - Nube: Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, VMware
 - Contenedores: Docker, Kubernetes, Kubernetes Ingress, Openshift
 - Un agente que funcione sobre NGINX Web Server o un proxy reverso de NGINX

1.3 Funcionalidades para la seguridad WEB

- La solución deberá permitir aplicar políticas para definir los límites en los mensajes del protocolo HTTP. Incluir al menos los siguientes parámetros:
 - Tamaño del cuerpo (Body Size): tamaño máximo del cuerpo del mensaje HTTP
 - Tamaño de URL (URL Size): tamaño máximo de la URL, esto incluye todos los campos de consulta.
 - Tamaño del encabezado (Header Size): tamaño máximo del encabezado HTTP
 - Profundidad máxima del objeto (Object Depth): tamaño de profundidad máxima del objeto JSON / XML, esto incluye XML incrustado en JSON y lo contrario.



- Métodos válidos HTTP (RFP): Aceptar o bloquear métodos https no standard.
- La solución deberá soportar métodos para poder distinguir a los usuarios entre sí. Deberá soportar al menos los siguientes mecanismos:
 - X-Forwarded-For
 - IP Origen
 - Cookie
 - Header Only
- La solución deberá poder inspeccionar la carga de archivos al sitio protegido evitando que estos cuenten con malware incrustado
 - Los archivos inspeccionados deberán emularse en la nube del fabricante proveedor del servicio
- La solución deberá soportar la integración de firmas de SNORT con el fin de poder integrar indicadores de compromiso adicionales

1.4 Funcionalidades para la seguridad de API

- La solución debe ofrecer protección preventiva para posibles vulnerabilidades de API a través de un procedimiento de validación de esquema (schema).
- La solución deberá integrarse a través de un API con el SDLC e integrar una validación de esquema de json, para conocer el comportamiento esperado del aplicativo.
- La solución debe revisar las solicitudes de API entrantes con estos esquemas (schema) para bloquear todas las solicitudes de API no válidas.
- La solución deberá también utilizar las funciones de WAF para detectar y bloquear automáticamente los payloads maliciosos en la API.
- La solución debe poder proteger las API utilizando técnicas como la validación automatizada mediante archivos de esquema Open API.

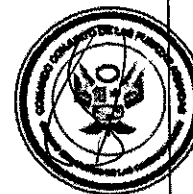
1.5 Funcionalidades para la protección anti-bot

- La solución deberá poder inyectar scripts en páginas de aplicaciones web, como páginas de inicio de sesión o utilizar algún otro mecanismo para recopilar datos sobre patrones de entrada y canalice secuencias de pulsaciones de teclas, movimientos del ratón y toques con los dedos. Esto con el fin de poder diferenciar a un humano de un bot.
- La solución deberá poder identificar estos patrones en caso de que un bot los utilice.
- La solución deberá poder tomar una decisión si la entrada es ingresada por un humano o por un script automático (como un bot), y bloquear esta actividad.
- La solución debe poder detener el relleno de credenciales (credential stuffing), los ataques de fuerza bruta y el site scraping con la protección avanzada de bots.



ANEXO I

CARACTERÍSTICAS TÉCNICAS: SEGURIDAD BASES DE DATOS

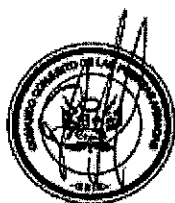


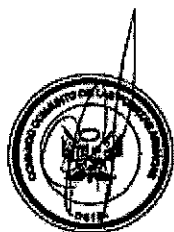
Nº	ITEM	TIPO	Cant.
01	Equipo para protección de bases de datos en reposo	Virtual	01

1. ESPECIFICACIONES TECNICAS

1.2. Consola de Administración

- ☐ La entidad proporcionará los recursos de cómputo para el despliegue de la plataforma.
- ☐ La solución deberá de permitir almacenar y gestionar llaves criptográficas y certificados digitales.
- ☐ La solución debe presentarse bajo la modalidad de suscripción.
- ☐ La solución debe contar con una consola de administración web la cual permita cifrar la comunicación mediante TLS 1.2. o superior.
- ☐ La solución debe contar con una consola de administración con certificación FIPS 140-2 Nivel 1.
- ☐ La solución deberá de permitir establecer control de acceso basados en roles.
- ☐ La solución debe gestionar y asegurar las llaves de cifrado de tal forma que los usuarios del sistema no tengan acceso a las mismas.
- ☐ La solución debe contar con una consola de comandos para administración.
- ☐ La solución debe contar con una API REST de administración y criptografía.
- ☐ La solución debe contar con una API REST con autenticación simple y avanzada como el uso de certificados del lado del cliente.
- ☐ La solución debe permitir la realización de copias de seguridad de sus configuraciones de forma automática o manual.
- ☐ Debe tener capacidad para soportar un mínimo de 20.000 llaves criptográficas.
- ☐ Debe ser compatible con certificados digitales (X.509) PKCS # 7, PKCS # 8 y PKCS # 12, llaves de cifrado simétrico: algoritmos 3DES, AES (128, 192, 256), ARIA (128, 192, 256) y asimétrico: RSA (1024,2048,4096) y algoritmos de curva elíptica.
- ☐ Debe permitir almacenar secretos genéricos en forma de binario o codificado en base64.
- ☐ Debe ser escalable para admitir la administración de agentes de múltiples servicios en un marco de múltiples dominios. Para



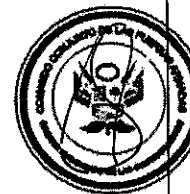


- ello, debe ser posible configurar diferentes llaves criptográficas según cada área de operación, si es necesario.
- ☐ Debe soportar integración con LDAP.
 - ☐ La solución deberá permitir visualizar los logs de auditoría mediante la plataforma de gestión.
 - ☐ Debe soportar configurar un servidor syslog con formatos: RFC-5424, CEF, LEEF.
 - ☐ Debe soportar integración con herramientas de monitoreo SNMP v2c, v3.
 - ☐ Debe permitir integrar con un servidor de tiempo usando protocolo NTP.
 - ☐ Debe ser compatible con PKCS#11 (Estándares de criptografía de llave pública), JCE (Extensión de criptografía de Java), Microsoft CNG (API de criptografía de próxima generación), Administración extensible de llaves de Microsoft (EKM), REST API, KMIP.
 - ☐ La solución debe permitir realizar respaldos seguros de las llaves de forma manual o automatizada.
 - ☐ La solución debe proporcionar una única consola que permita la gestión centralizada de todos los agentes criptográficos, sus llaves criptográficas, políticas de configuración, publicación y control de acceso de los datos a proteger.
 - ☐ La solución debe tener la capacidad de generar registros de auditoría para trazar los accesos a datos confidenciales.
 - ☐ La solución debe tener la capacidad de generar registros de auditoría para intentos fallidos de acceder a datos confidenciales.
 - ☐ La solución debe permitir integrarse con productos SIEM para agregar y monitorear registros.
 - ☐ Debe permitir implementar la segregación de funciones para que ninguna persona tenga una autonomía innecesaria sobre un proceso de aprobación o acceso a datos.
 - ☐ El sistema debe facilitar la auditoría de los cambios en la Administración de usuarios ya sea mediante la generación de un informe o en el sistema con la capacidad de indicar que la acción fue auditada.
 - ☐ A cada usuario se le debe asignar una identificación (ID) única para garantizar que las acciones realizadas por cada usuario se puedan registrar y rastrear.
 - ☐ La solución deberá permitir establecer criterios de complejidad para las contraseñas.
 - ☐ Capacidad para almacenar volúmenes/períodos significativos de registros.
 - ☐ Capacidad para consultar y buscar fácilmente registros.
 - ☐ Capacidad para proporcionar informes de auditoría personalizables.

1.3 Licenciamiento – Cifrado Transparente de Datos



- ❑ La solución debe contar con dos (02) licencias como mínimo para ejecutar el cifrado transparente de datos en dos (02) servidores.
- ❑ La solución debe realizar gestión de llaves centralizada y cifrado de datos no estructurados en reposo a nivel de file system.
- ❑ La solución debe soportar múltiples sistemas de archivos, incluidos, entre otros, EXT3, EXT4, XFS, NFS V3, NFS v4, NTFS, CIFS, ReFS, AWS EFS.
- ❑ La solución debe soportar múltiples sistemas operativos, incluidos, entre otros, Windows, Red Hat Linux, CentOS, SLES, Ubuntu y AIX.
- ❑ La solución debe permitir la gestión de llaves centralizada y cifrado de datos estructurados en reposo, específicamente en archivos de base de datos.
- ❑ La solución debe soportar múltiples sistemas de bases de datos en todas las versiones, incluidas, entre otras, Microsoft SQL, DB2, MySQL, Oracle, MongoDB, SAP HANA, Teradata, Informix y bases de datos del tipo Big Data.
- ❑ La solución debe ofrecer características para asegurar y controlar el acceso a bases de datos, archivos y contenedores.
- ❑ La solución debe permitir la transformación de datos en vivo, lo que permite que las aplicaciones puedan continuar utilizando los datos sin interrupción mientras los mismos se cifran.
- ❑ El proceso de cifrado debe ser realizado por agentes o equivalentes que deben estar instalados en los servidores donde resida los datos a cifrar.
- ❑ El agente o equivalente debe residir en el sistema operativo o en la capa del dispositivo, y el cifrado y descifrado deben ser transparentes para todas las aplicaciones que se ejecutan por encima de él.
- ❑ Los agentes deben tener la certificación FIPS 140-2 Nivel 1.
- ❑ Los agentes que serán instalados en los servidores deben operar de manera autónoma a la consola de gestión con excepción de las instancias de su inicialización (boot) en los servidores. Estos deben operar de manera ininterrumpida, aplicando el proceso de cifrado y descifrado, incluso si las consolas son apagadas.
- ❑ Los agentes deben permitir la rotación/cambio de llaves en vivo, sin interrumpir el servicio o la disponibilidad de los datos.
- ❑ Los agentes deben registrar y rastrear el acceso de los usuarios del sistema a los archivos y poder bloquear o restringir este acceso.
- ❑ Las políticas de control de acceso deben poder aplicarse a los usuarios privilegiados del sistema y no deben tener la autoridad para deshacer la política de acceso en un intento de aumentar su privilegio nuevamente.
- ❑ Las políticas deben permitir el control basado en el usuario, el proceso y el tipo de archivo.



- ☐ Las políticas deben poder aplicarse a los usuarios locales o integrarse eventualmente a un Active Directory o servidor LDAP.
- ☐ Las políticas permitirán implementar el uso de tecnologías de autenticación multifactor (MFA) para acceso control de acceso a repositorios con datos confidenciales.
- ☐ La solución debe contar con registros para identificar a qué datos se accedió, quién accedió, cómo se accedió y dónde se accedió.
- ☐ La solución permitirá a los usuarios privilegiados realizar su trabajo sin acceso a información en texto claro.
- ☐ La solución debe generar registros de auditoría para intentos de inicio de sesión fallidos o exitosos en la aplicación de cifrado de datos.
- ☐ La solución debe registrar cambios confidenciales realizados y generar un registro de auditoría. La traza de auditoría debe contener quién realizó el cambio, cuándo se realizó y qué se modificó.
- ☐ El proveedor deberá validar la compatibilidad del agente con el sistema operativo de los servidores donde se encuentran instaladas las bases de datos. De requerir realizar alguna actualización o migración, esta deberá ser realizada por el proveedor. La entidad brindará los recursos de cómputo de ser necesarios.
- ☐ No se aceptarán soluciones de diferentes fabricantes.

ANEXO J

CARACTERÍSTICAS TÉCNICAS: GABINETE AUTOCONTENIDO



N°	ITEM	TIPO	Cant.
01	Gabinete	Físico	01

1. ESPECIFICACIONES TÉCNICAS

1.2. Características

- Micro Datacenter con equipamiento nativo instalado, compuesto por:
- Tablero eléctrico integrado de fábrica en el gabinete.
- UPS 6KVA con fp1.
- Batería de litio LFP.
- Unidad de refrigeración rackeable con condensador incorporado, 3.5kW de capacidad de refrigeración.
- Unidad compacta contra incendios, rackeable, con agente limpio FK5112 o NOVEC1230 integrado.
- Unidad de gestión y centralización nativa.
- Control de acceso con reconocimiento biométrico.



1.3 Gabinetes de convergencia

- Aplicación: Alberga el equipamiento de la sala de comunicaciones.
- Cantidad: un (1) sistema convergente conformado por gabinetes de las siguientes medidas:
- Dimensiones requeridas.
 - Altura: 200cm.
 - Ancho: 60cm.
 - Profundidad: 110cm
 - Pasillos frío y caliente autocontenidos en el gabinete
- Fabricado en acero al carbono clase A, recubrimiento zincado o galvanizado y acabado con pintura RAL9005 o similar. Cumplimiento IEC 60297-2.
- Altura 42RU.
- Fabricante con certificación ISO14001 e ISO9001.
- Rieles ajustables de 19" según EIA 310.
- Capacidad de carga estática de al menos 1500kg y 1000kg de carga dinámica.
- Grado de protección IP20
- Puerta frontal de vidrio y puerta trasera de acero con aislamiento térmico para evitar la condensación por la diferencia de temperatura entre el interior y el exterior.
- Sistema de apertura automática instalada con brazo retráctil.
- 2 PDU de 16A, versión conmutable, con al menos 8 tomas C13.
- Pantalla frontal extraíble, con interacción gráfica para la

administración nativa de toda la infraestructura (ups, control de acceso, refrigeración, monitoreo ambiental y alarmas.)

1.4 Tablero eléctrico (rackeado de fábrica)

- Alimentación a 220VAC, 1f+neutro + tierra, 60hz.
- Interruptor termomagnético principal y llaves ITM independientes para el sistema de refrigeración, UPS, bypass y rPDU instalados en el sistema autocontenido. SPD Switch incorporado.

1.5 UPS integrado

- Se requiere un sistema UPS de 6KVA/6KW, rackeado de fábrica.
- Eficiencia de al menos 96%.
- Montaje rackeable en 1RU.
- Alimentación 220VAC, 1ph, 60hz.
- Doble conversión.
- Factor de potencia de salida 1.
- Precisión del voltaje de salida de +/- 1%.
- Capacidad de sobre carga del inverter:
 - $105\% \leq \text{carga} < 125\%$ □ transferencia a modo bypass después de 10 minutos.
 - $125\% \leq \text{carga} < 150\%$ □ transferencia a modo bypass después de 30 segundos
- Cumplimiento CE.

1.6 Tablero eléctrico (rackeado de fábrica)

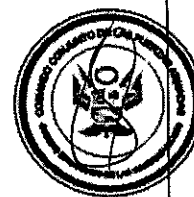
- Alimentación a 220VAC, 1f+neutro + tierra, 60hz.
- Interruptor termomagnético principal y llaves ITM independientes para el sistema de refrigeración, UPS, bypass y rPDU instalados en el sistema autocontenido. SPD Switch incorporado.

1.7 Baterías rackeables

- 1 Banco de batería VRLA rackeable de 9Ah, 240V.
- Debe ser de la misma marca del UPS para asegurar compatibilidad.
- Dimensionada para 2kW, 30min.
- No deberá ocupar más de 3RU.

1.8 Sistema monitoreo y gestión centralizada

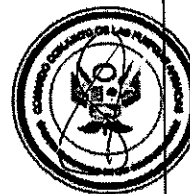
- Sistema de monitoreo rackeable que concentre de manera nativa el monitoreo y gestión del sistema de refrigeración, distribución eléctrica, UPS, seguridad y sensores ambientales.
- Unidad de gestión:
 - Rackeable en 1RU, módulo de potencia y módulo de control extrables del chasis para un fácil reemplazo o upgrade.
 - Temperatura de trabajo -20 a 50°C.
 - Humedad relativa 5-95%HR.
 - Puerto para SIM card para el envío de alertas.



- Antena direccional.
- Alimentación 200-240VAC.
- Suministro de salida para la alimentación de periféricos y equipos conectados. Alimentación de salida DC y entrada AC.
- Puertos LAN y WAN con autonegociación 10/100/1000Mbps/s.
- Puerto RS485 para expansión.
- Puertos AIDI con conector RJ45 para la conexión de sensores de humo, agua y NTC.
- Puerto USB para la instalación del módulo Wifi para el monitoreo con smartphone o Tablet, que permita revisar el layout de distribución de equipos, alarmas y demás variables.
- Detecta y recolecta la estadística de la temperatura y humedad al interior del sistema autocontenido.
- Apertura automáticamente las puertas en caso del ingreso de clave.
- En caso de emplear sistema de extinción de sala, las puertas traseras se abren automáticamente al detectar humo en el sistema autocontenido. En caso de emplear la extinción interior, el sistema se mantiene confinado para permitir la extinción adecuada.
- Detecta fuga de agua en la base del autocontenido y provee señales de alarma en tiempo real.
- Se interconecta con el UPS de manera nativa para el monitoreo de las variables eléctricas (voltaje, frecuencia, corriente, etc.)
- Monitoreo del sistema de refrigeración:
 - Monitoreo del suministro y la temperatura del aire de retorno.
 - Monitoreo del estado del compresor.
- Video vigilancia: Conexión con la cámara del sistema, provee alimentación PoE, acceso real a las imágenes en el gestor web (WebUI).
- App View:
 - Generación de vistas al menos en 2D que muestren la distribución actual del gabinete, indicando la ubicación de tablero eléctrico rackeable, la unidad de refrigeración y el UPS.
 - Muestra el estado actual de alarmas de los sensores de ambientales.
 - Debe contar con reconocimiento facial a través de la Tablet de monitoreo de al menos 10", instalada en la puerta del gabinete.
- Alarmas:
 - El sistema debe monitorear de manera nativa el estado de los equipos de refrigeración, unidades UPS y dispositivos ambientales. En caso de una alerta o error, el sistema deberá generar una alarma en tiempo real. La cual puede ser visualizada en la pantalla de gestión en el gabinete de gestión. La alarma debe ser mostrada, así como la sugerencia de solución.
 - Alarmas clasificadas en crítico, mayor, menor y warning. Dichas alarmas deberán poder ser filtrada.
 - La iluminación cambiará de color según el nivel de severidad de la alarma.
 - Envío de alarmas por email y SMS. Al menos 500 alarmas deben ser soportadas.
- Sensores requeridos: temperatura, humo y sensor de inundación.
- 1 Cámara domo fijo de 2MP, IR, con accesorio de montaje para el

gabinete y grabación de 7 días con tarjeta SD.

- 1.9 Sistema de Climatización de expansión directa (Aire Acondicionado de precisión interno y rackeable.
- Cantidad: Un (1) sistema de refrigeración rackeado de fábrica.
 - Capacidad de. Enfriamiento para carga TI de al menos 3kW, bajo las siguientes condiciones
 - Temperatura de bulbo seco 37°C y bulbo húmedo de 24°C.
 - Temperatura de bulbo seco (externo) 35°C.
 - Refrigerante: R410A.
 - Monitoreo: Local a través de la pantalla táctil extraíble tipo tablet instalada en el gabinete de infraestructura y remoto haciendo uso del gestor web que integra la solución de monitoreo ambiental, sistema de refrigeración, tablero y control de acceso.
 - Condensador y Evaporador Integrados
 - Control de temperatura con precisión +/-1°C.
 - Disponibilidad de operación 24x7
 - Rackeable, no mayor a 10RU.
 - Flujo de aire: frontal o soplado superior.
 - Alimentación eléctrica: 208-240VAC / 1 fase / 60 Hz
 - Flujo promedio: 600m3/h mínimo.
 - Unidad condensadora integrada, para evitar la implementación de tuberías de refrigerante externas.
 - Capacidad de refrigeración variable en función a la demanda.



ANEXO K

CARACTERÍSTICAS TÉCNICAS: AIRE ACONDICIONADO



N°	ITEM	TIPO	Cant
01	AA CONFORT	Físico	01

1. ESPECIFICACIONES TÉCNICAS

1.2. Características

- Tecnología en línea con dos etapas de conversión de potencia
- Factor de potencia DE 0.9 como mínimo.
- Capacidad de Enfriamiento
- Min - 1,365Btu/h
- Nominal - 11,942Btu/h
- Max - 13,751 Btu/h
- EER 3.14 W/W10.71 (Btu/h)/W
- Consumo, Enfriamiento 186 kWh/año
- Fase / Voltaje / Frecuencia 1 Ø, 220V, 60Hz
- Refrigerante, R410A
- Compresor tipo Twin Rotary



ANEXO L

CARACTERÍSTICAS TÉCNICAS:
UPS



N°	ITEM	TIPO	Cant
01	UPS	Físico	01

1. ESPECIFICACIONES TECNICAS

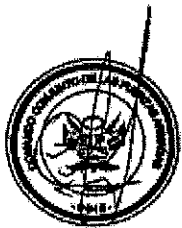
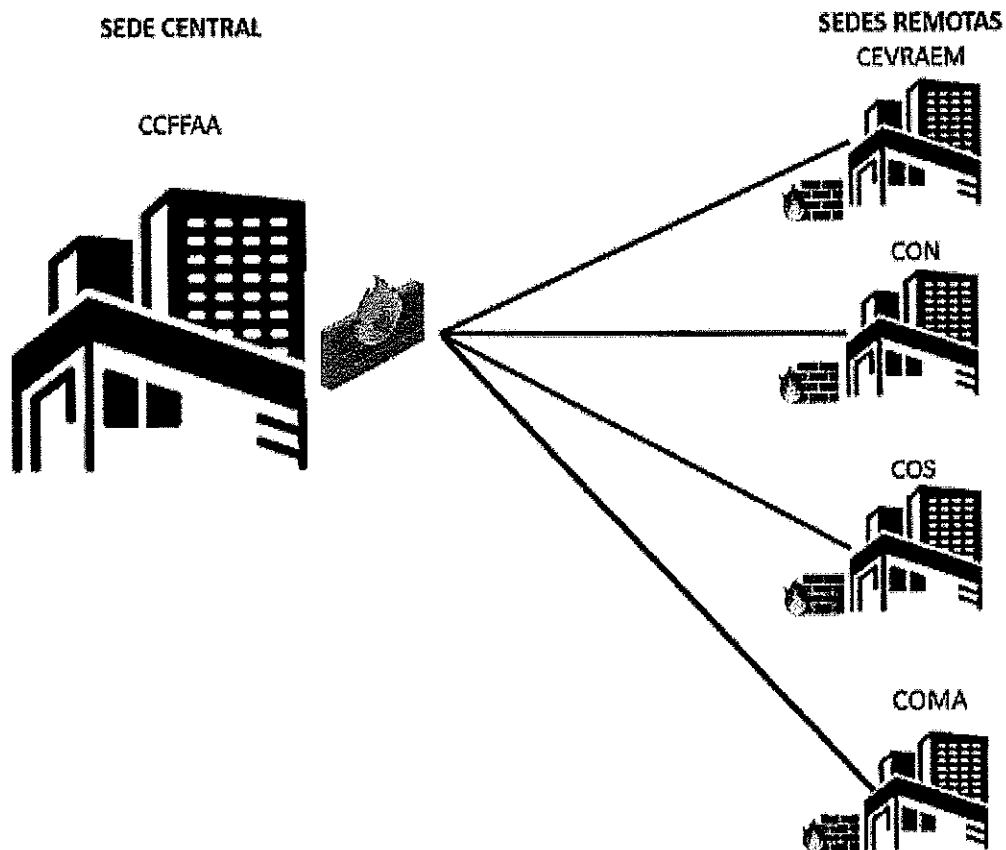
1.2. Características


- Tecnología en línea con dos etapas de conversión de potencia
- Factor de potencia DE 0.9 como mínimo.
- Deberá ser instalada de modo rack/torre.
- Pantalla de cristal líquido (LCD).
- Deberá contar con un modo de operación configurable que le permita ahorro de energía no menor a 80%
- Operación con un amplio voltaje de entrada (120-300 VCA)
- Conector de entrada, IEC60320 C20
- Salidas, IEC60320 C13 x 6 IEC60320 C19 x1.
- Autonomía de 10.5 minutos a 50% de carga.
- Seguridad, IEC/EN 62040-1: 2014.

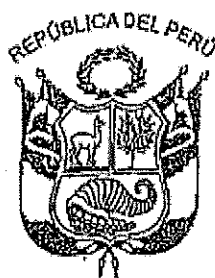


ANEXO M

DISEÑO DE LA SEGURIDAD PERIMETRAL DE LA ENTIDAD




O-2165784070-04
Alfredo Javier RODRIGUEZ Arizola
Jefe de la Oficina de Administración del
Comando Conjunto de las Fuerzas Armadas



Resolución Comando Conjunto de las Fuerzas Armadas

Lima, 12 OCT 2022

N° 384 CCFFAA/OA

VISTO:

El Informe Técnico N° 006 - 2022/CCFFAA/OSIE/ADM del Jefe de la Oficina de Soporte Informático y Estadística del Comando Conjunto de las Fuerzas Armadas, de fecha 06 de Setiembre de 2022;


CONSIDERANDO:

Que, los artículos 2° y 6° del Decreto Legislativo N° 1136, Decreto Legislativo del Comando Conjunto de las Fuerzas Armadas, establecen que el Comando Conjunto de las Fuerzas Armadas tienen naturaleza jurídica de órgano ejecutor, dependiente del Ministerio de Defensa, cuya Jefatura es el órgano de Comando del más alto nivel, quien depende del Ministerio de Defensa, de la cual establece que constituye su más alta autoridad.



Que, el artículo 1° del Texto Único Ordenado de la Ley de Contrataciones del Estado, Ley N° 30225, aprobado por el Decreto Supremo N° 082-2019-EF, establece que este dispositivo legal tiene como finalidad establecer normas orientadas a maximizar el valor de los recursos públicos que se intervienen y a promover la actuación bajo el enfoque gestión por resultados en las contrataciones de bienes, servicios y obras; de tal manera que estas se efectúen en forma oportuna y bajo las mejores condiciones de precio y calidad, permitan el cumplimiento de los fines públicos y tengan una repercusión positiva en las condiciones de vida de los ciudadanos;

Que, el numeral 16.1 del artículo 16 del Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado, establece que: "El área usuaria requiere los bienes, servicios u obras a contratar, siendo responsable de formular las especificaciones técnicas, términos de referencia o expediente técnico, respectivamente, así como los requisitos de calificación; además de justificar la


O-2024-784070-O+
Alfredo Javier RODRIGUEZ Aulestiano
Coronel EF
Jefe de la Oficina de Administración del
Comando Conjunto de las Fuerzas Armadas



finalidad pública de la contratación. Los bienes, servicios u obras que se requieran deben estar orientados al cumplimiento de las funciones de la Entidad.";

Que el numeral 29.4 del artículo 29 del Reglamento de la Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 344-2018-EF, señala que en la definición de requerimiento no se hace referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados, ni descripción que oriente la contratación hacia ellos, salvo que la entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por el Titular de Entidad, en cuyo caso deben agregarse las palabras "o equivalente" a continuación de dicha referencia;

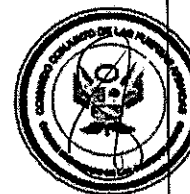
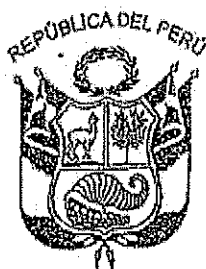
Que, el Anexo N° 1 de Definiciones del citado Reglamento define la Estandarización como el "Proceso de racionalización consistente en ajustar a un determinado tipo o modelo los bienes o servicios a contratar, en atención a los equipamientos preexistentes";

Que, el numeral 16.2 del artículo 16 del Texto Único Ordenado por la Ley N° 30225, Ley de Contrataciones del Estado, aprobado mediante Decreto Supremo N° 082-2019-EF, señala que las especificaciones técnicas, términos de referencia o expediente técnico deben formularse de forma objetiva y precisa por el área usuaria; alternatively pueden ser formulados por el órgano a cargo de contrataciones y aprobados por el área usuaria. Dichas las especificaciones técnicas, términos de referencia o expediente técnico deben proporcionar acceso al proceso de contratación en condiciones de igualdad y no llenen por efecto la creación de obstáculos ni direccionamiento que perjudiquen la competencia en el mismo. Salvo las excepciones previstas en el reglamento, en el requerimiento no se hace referencia a una fabricación o una procedencia determinada, o aun procedimiento concreto que caracterice a los bienes y servicios ofrecidos por un proveedor determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados con la finalidad de favorecer o descartar ciertos proveedores o ciertos productos.



Que, la Directiva N° 004-2016-OSCE/CD "Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo en particular", aprobada por el Organismo Supervisor de las Contrataciones con el Estado, a través de la Resolución N° 011-2016-OSCE/PRE, establece los lineamientos que las entidades deben observar para hacer referencia en la definición de requerimiento, a marca o tipo particular de bienes o servicios a contratar.

Que, la citada Directiva en su numeral 7.1 señala que la estandarización debe responder a criterios técnicos y objetivos que la sustenten, debiendo ser necesaria para garantizar la funcionalidad, operatividad o valor económico del equipamiento o infraestructura preexistente de la Entidad; asimismo, el numeral 7.2 establece los presupuestos que deben verificarse para que proceda la estandarización, siendo estos los siguientes: a) la preexistencia de un determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos u otro tipo de bienes, así como ciertos servicios especializados y b) los bienes o servicios que se requiere contratar sean accesorios o complementarios al equipamiento o infraestructura Preexistente, e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura;




Que, el numeral 7.4 de la Directiva antes señalada, indica que la estandarización de bienes o servicios a ser contratados será aprobada por el Titular de la Entidad, sobre la base del Informe técnico de estandarización emitido por el área usuaria, la que podrá efectuar las coordinaciones con el órgano encargado de las contrataciones de la Entidad para tal fin; precisando, adicionalmente que, dicha aprobación deberá efectuarse por escrito, mediante resolución o instrumento que haga sus veces y publicarse en la página web de la Entidad al día siguiente de producida su aprobación. Asimismo, en dicho documento deberá indicarse el período de vigencia de la estandarización, precisándose que de variar las condiciones que determinaron la estandarización, dicha aprobación quedará sin efecto;

Que, conforme al numeral 7.6 de la Directiva en mención, la estandarización no supone la existencia de un proveedor único nacional, es decir, el hecho que una Entidad apruebe un proceso de estandarización no enerva la posibilidad de que en el mercado pueda existir más de un proveedor, con lo cual, en principio la Entidad se encontraría obligada a efectuar un procedimiento de selección para determinar al proveedor con el cual celebrará el contrato;

Que, mediante el Informe Técnico N° 006 - 2022/CCFFAA/OSIE/ADM, la Oficina de Soporte Informático y Estadística del Comando Conjunto de las Fuerzas Armadas - OSIE, en su calidad de área usuaria, sustenta el pedido de estandarización, por el periodo de un (03) año, respecto a la estandarización de las soluciones "Next Generation Security Check Point" en el CCFFAA (de todos sus módulos, versiones, licencias de software, upgrade de software, garantía del equipamiento y hardware adicional y mantenimiento preventivo), incluyendo sus consolas de administración, gestión y correlación de eventos; asegurando de esta manera la protección de la red del CCFFAA, a nivel perimetral e internamente, a sus servidores y centros de datos de la institución;

Que, con respecto a los presupuestos que deben verificarse para que proceda la estandarización, el área usuaria señala que, desde el año 2018, se cuenta con el siguiente equipamiento de marca Checkpoint: UN (01) appliances Security Gateway - NGTX, modelos 5600, UN (01) appliances Security Gateway - NGTP, modelos 15400, Un (01) appliance Security SandBlast, modelo TE250X, así mismo el licenciamiento: CPSM-NGSM10 Next Generation Security Management Software for 10 gateways (SmartEvent & Compliance), CPSM-NGSM10-EVNT Next Generation


O 27/10/2024
Alfredo J. Ayala Rodríguez
Jefe de la Oficina de Asesoría Jurídica del
Comando Conjunto de las Fuerzas Armadas




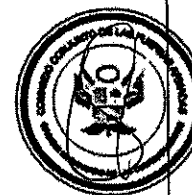
Security Management SmartEvent dedicated Server for 10 gateways, Support for Appliance Gateways; Soporte del fabricante para equipos físicos. Equipos: SN 18168A0008- SN LR201606011664- SN 1823BA0455, Security Services - Enterprise Based Protection Annuity Blades: Licenciamiento NGTP para equipo 15400, Annuity Blades: Licenciamiento NGTX para equipos 5600, 1823BA0455 Annuity Blades: Licenciamiento NGTX para equipo TE250X, CPES-CO-PREMIUM (Collaborative Enterprise Support - Premium), CPEP-COMLETE-RENEWAL, e) servicio de renovación de la garantía del equipamiento permitirá que los equipos y/o componentes puedan ser reemplazados en caso de fallas de hardware. El servicio de renovación de licenciamiento permitirá contar con actualizaciones de software y reducir el índice de fallas por problemas de vulnerabilidad, así como los servicios de mantenimiento y soporte técnico, permitirán minimizar los tiempos fuera de servicio, además de contar con un adecuado nivel de funcionamiento y operatividad del sistema de seguridad firewall perimetral. Así mismo, justifica la incidencia económica de la estandarización;



Que, por su parte, la unidad de Logística de la Oficina de Administración, a través del Informe N° 103-2022-CCFFAA/OA/ULOG de fecha 04 de octubre de 2022, en el marco de su competencia, da cuenta de la revisión y evaluación efectuada a la solicitud de estandarización presentada por la Oficina de Soporte Informático y Estadística del Comando Conjunto de las Fuerzas Armadas, para la renovación de la garantía del equipamiento, licenciamiento, mantenimiento y soporte técnico del sistema firewall perimetral e interno, el cual se encuentra comprendido por la gestión del proveedor para la renovación de la garantía y licenciamiento del equipamiento del sistema de seguridad perimetral de marca Checkpoint, así como el servicio de mantenimiento preventivo y el soporte técnico por parte del proveedor de dicho equipamiento de marca Checkpoint, por el período de tres (03) años, indicando que el Informe Técnico elaborado por el área usuaria cumple con sustentar su requerimiento con base a criterios técnicos y objetivos, conforme los presupuestos exigidos por la Directiva N° 004-2016-OSCE/CD, que establece los "Lineamientos para la Contratación en la que se hace referencia a determinada marca o tipo particular". Finalmente, concluye que considera pertinente aprobar la estandarización solicitada por el área usuaria, solicitando se gestione ante la Oficina de Asesoría Jurídica la elaboración del acto resolutivo que apruebe la estandarización requerida, a fin de contar con las herramientas necesarias para garantizar la asistencia especializada imprescindible para dar continuidad operativa a los equipos que forman parte de la plataforma tecnológica del CCFFAA. Los componentes de hardware y software del sistema firewall perimetral e internos Checkpoint son indispensables para el cumplimiento de las funciones y actividades propias de la entidad;

Que, de conformidad con lo establecido por el artículo 30 de la Ley de Contrataciones del Estado, aprobada por Ley N° 30225, el artículo 67 del Reglamento de la Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 344-2018-EF; y, la Resolución Ministerial N° 502-2019-EF/43, y estando a lo informado por el Jefe de la Oficina de Soporte Informático y Estadística; a lo opinado por el Jefe de la Unidad de Logística del Comando Conjunto de las Fuerzas Armadas; y, con opinión favorable de la Oficina de Asesoría Jurídica del Comando Conjunto de las Fuerzas Armadas.


O: 057-44070-0+
Alfredo Jarama TORREALBA
Coronel E
Jefe de la Oficina de Administración del
Comando Conjunto de las Fuerzas Armadas



SE RESUELVE:

Artículo 1.- APROBAR, el proceso de estandarización para la renovación de la garantía del equipamiento, licenciamiento, mantenimiento, soporte técnico y equipamiento adicional firewall perimetral e interno de marca Checkpoint, por un periodo de tres (03) años, contando a partir del día siguiente de su aprobación, el cual podrá ser menor en caso que varíen las condiciones que determinaron la estandarización.

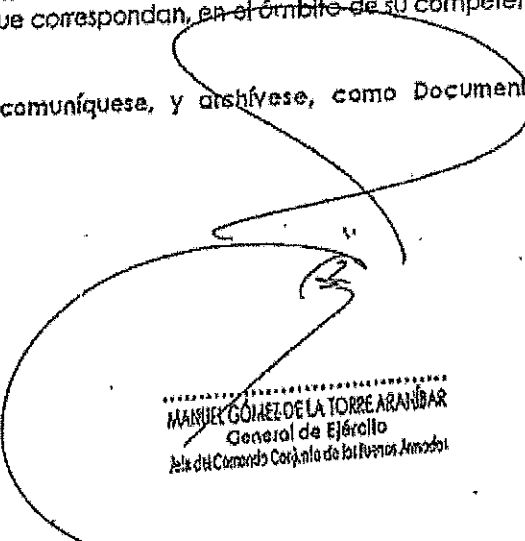
Artículo 2.- DISPONER, el registro de la presente Resolución en el Sistema Electrónico de Contrataciones del Estado, SEACE, de conformidad con el numeral 67.1 del artículo 67 del Reglamento de la Ley N° 302255 aprobado por el Decreto Supremo N° 082-2019-EF.

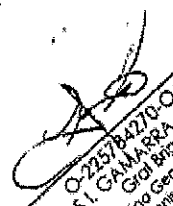
Artículo 3.- ENCARGAR, a la Oficina de Administración del Comando Conjunto de las Fuerzas Armadas, la notificación de la presente Resolución y la realización de los trámites que correspondan, en el ámbito de su competencia.

Regístrese, comuníquese, y archívese, como Documento Oficial

Público




MANUEL GÓMEZ DE LA TORRE ARANDBAR
General de Ejército
Jefe del Comando Conjunto de las Fuerzas Armadas


O-225784270-O+
CARLOS I. GAMARRA QUINTANA
Jefe de la Oficina General de Apoyo del
Comando Conjunto de las FFAA



"ES COPIA DEL ORIGINAL"

O-226490874-B+
Gustavo HERNÁNDEZ Del Castillo
Teniente Coronel EP
Fedatario del Comando Conjunto de las
Fuerzas Armadas



Resolución Comando Conjunto de las Fuerzas Armadas

190
N° CCFFAA/OGA/OSIE/SGR

Lima, 16 MAY 2023

VISTO:

El informe Técnico de Estandarización de Software N° 016-2023-CCFFAA/OGA/OSIE/SGR de fecha 08 de mayo de 2023, elaborado por la Oficina de Soporte Informática y Estadística de la Oficina General de Apoyo del Comando Conjunto de las Fuerzas Armadas.

CONSIDERANDO:

Que, el numeral 16.1 del artículo 16° de la Ley N° 39225, Ley Contrataciones del Estado de fecha 10 de julio de 2014, modificado por el Decreto Legislativo N° 1444, de fecha 16 de setiembre de 2018 y su Reglamento, aprobado por el Decreto Supremo N° 344-2018-EF, de fecha 31 de diciembre de 2018, dispone que el área usuaria requiere los bienes, servicios u obras a contratar, siendo responsable de formular las especificaciones técnicas, términos de referencia o expediente técnico, respectivamente, así como los requisitos de calificación; además de justificar la finalidad pública de la contratación. Los bienes, servicios u obras que se requieran deben estar orientados al cumplimiento de las funciones de la Entidad;

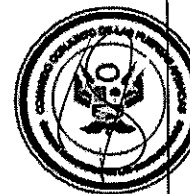
Que, las especificaciones técnicas, términos de referencia o expediente técnico deben formularse de forma objetiva y precisa, proporcionando acceso en condiciones de igualdad al proceso de contratación y no tienen por efecto la creación de obstáculos que perjudiquen la competencia en el mismo. Salvo las excepciones previstas en el reglamento, en el requerimiento no se hace referencia a una fabricación o una precedencia determinada, o a un procedimiento concreto que caracterice a los bienes o servicios ofrecidos por

O-225/04270-OF
CARLOS I. GAMARRA QUINTANA
Jefe de la Oficina General de Apoyo del
Comando Conjunto de las FFAA



"ES COPIA FIEL DEL ORIGINAL"

O-225/0874-B+
Gustavo HERNANDEZ Del Castillo
Asesoría General JEP
Fiscalía del Comando Conjunto de las
Fuerzas Armadas



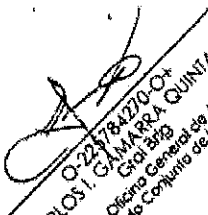
proveedor determinado, o a marcas, patentes, o a un origen o a una producción determinadas con la finalidad de favorecer o descartar ciertos proveedores o ciertos productos;

Que, el numeral 29.1 del artículo 29° del citado Reglamento de la Ley de Contrataciones del Estado, establece que las especificaciones técnicas, los términos de referencia o el expediente técnico de obra, que integran el requerimiento, contienen 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 se ejecuta, incluyendo obligaciones de levantamiento digital de información y tecnologías de posicionamiento espacial, tales como la georreferenciación, en obras y consultorías de obras. El requerimiento incluye, además, los requisitos de calificación que se consideren necesarios, así como, su posterior numeral 29.2., dispone que, para la contratación de obras, la planificación incluye la identificación y asignación de riesgos previsibles de ocurrir durante la ejecución, así como las acciones y planes de intervención para reducirlos o mitigarlos, conforme a los formatos que apruebe el OSCE. El análisis de riesgos implica clasificarlos por niveles en función a: i) su probabilidad de ocurrencia y ii) su impacto en la ejecución de la obra. Asimismo, el numeral 29.3., señala que al definir el requerimiento no se incluyen exigencias desproporcionadas al objeto de la contratación, irrazonables e innecesarios referidos a la calificación de los potenciales postores que limiten o impidan la concurrencia de los mismos u orienten la contratación hacia uno de ellos. Por su parte, el numeral 29.4., señala que, en la definición del requerimiento no se hace referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados, ni descripción que oriente la contratación hacia ellos, salvo que la Entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por su titular, en cuyo caso se agregan las palabras "o equivalente" a continuación de dicha referencia;

Que, por su parte, la estandarización es un proceso de racionalización consistente en ajustar a un determinado tipo o modelo de bienes o servicios a contratar, en atención a los equipamientos preexistentes;

Que, el Organismo Supervisor de las Contrataciones del Estado, mediante Resolución N° 358-2009-OSCE/PRE, aprobó la Directiva N° 010-2009-OSCE/CD, Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular, dicho instrumento señala que la estandarización es el proceso de racionalización que una entidad debe aplicar cuando le resulta inevitable contratar un bien o servicio de una determinada marca o tipo particular, dado que sólo este bien o servicio garantiza la funcionalidad, operatividad o valor económico del equipamiento o infraestructura preexistente en la Entidad;

Que, conforme a lo establecido en el numeral VI.2 de la VI Disposiciones Específicas de la citada Directiva, los presupuestos que deben verificarse para


O-223784270-O+
CARLOS I. GAMARRA QUINTANA
Jefe de la Oficina General de Apoyo del
Comando Conjunto de las FFAA



"ES COPIA FIEL DEL ORIGINAL"

O-226990874-B+
Gustavo HERNÁNDEZ Del Castillo
Teniente Coronel EP
Fedatario del Comando Conjunto de las
Fuerzas Armadas



que proceda la estandarización son los siguientes: a) La Entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos u otro tipo de bienes, así como ciertos servicios especializados; b) Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistentes; y c) Los bienes o servicios que se requiere contratar son imprescindibles para garantizar la funcionalidad, operatividad o valor económico del equipamiento o infraestructura preexistente;

Que, la referida Directiva, señala además que cuando el área usuaria considere que resulta inevitable solicitar determinada marca o tipo particular de los bienes a ser contratados, deberá elaborar un informe técnico de estandarización, el cual contendrá como mínimo lo siguiente: a) La descripción del equipamiento o infraestructura preexistente de la Entidad; b) La descripción del bien o servicio requerido, indicándose la marca o tipo de producto, así como las especificaciones técnicas o Términos de Referencia, según corresponda; c) El uso o aplicación que se le dará al bien o servicio requerido; d) La justificación de la Estandarización, donde se describa objetivamente los aspectos técnicos, la verificación de los presupuestos para la estandarización antes señalados y la incidencia económica de la contratación; e) Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio, y del jefe del área usuaria; f) La fecha de elaboración del Informe Técnico;



Que, conforme a lo señalado en el considerando precedente, el Jefe de la Oficina de Soporte Informático y Estadística de la Oficina General de Apoyo del Comando Conjunto de las Fuerzas Armadas, mediante Informe Técnico de Estandarización de Hardware N° 016-2023-CCFFAA/OGA/OSIE/SGR De fecha 08 de mayo de 2023, sustentó el proceso de estandarización de hardware de marca CISCO para la adquisición de equipos, repuestos, partes, piezas originales, complementos y componentes, de la estructura tecnológica preexistente, y que, permitirá contar con una oportuna solución a problemas de indisponibilidad de los servicios de comunicaciones en el Comando Conjunto de las Fuerzas Armadas, solucionando así los problemas físicos o lógicos que se presenten;



Que, el Informe citado, cumple con los requisitos establecidos en la Directiva N° 010-2009-OSCE/CD, describe los equipos preexistentes, los bienes a estandarizar, precisa el uso de los bienes requeridos y, justifica técnica y objetivamente los presupuestos para la estandarización;

O-22584220-0+
CARLOS I. GAMARRA QUINJANA
Jefe de la Oficina General de Apoyo del
Comando Conjunto de las FFAA



"ES COPIA DEL ORIGINAL"

O-225890874-8+
Gustavo HERNÁNDEZ Del Castillo
Teniente Coronel EP
Fedatario del Comando Conjunto de las
Fuerzas Armadas



Que, asimismo el informe referido, señala que la vigencia de la estandarización será de TRES (3) años, precisándose que al finalizar el periodo de vigencia se efectuará un nuevo proceso de estandarización acorde a los cambios o condiciones técnicas o tecnológicas del equipamiento o infraestructura preexistente;

Que, el numeral VI.4 de la VI Disposición Específica de la citada Directiva, señala que la estandarización de bienes y servicios a ser contratados será aprobado por el Titular de la Entidad o por el funcionario al que éste delegue dicha facultad, sobre la base del Informe técnico de estandarización emitido por el área usuaria, dicha autorización deberá efectuarse por escrito mediante resolución o instrumento que haga sus veces, y publicarse en la página web de la Entidad al día siguiente de producida su aprobación;

Que, mediante Directiva N° 020-22 /JCCFFAA/OSIE/USA de fecha 17 de mayo de 2022, se norma la Implementación y el Mantenimiento del Sistema de Gestión de Seguridad de la Información del Comando Conjunto de las Fuerzas Armadas, en su Anexo "H" subíndice 1.8.4 Mantenimiento del Equipamiento, refiere que se debe realizar un correcto mantenimiento a los equipos informáticos para asegurar su continua disponibilidad e integridad, lo cual se debe hacer en base a las recomendaciones de intervalos y especificaciones de servicio del proveedor de los equipos y de la Oficina de Soporte Informático y Estadística de la Oficina General de Apoyo del Comando Conjunto de las Fuerzas Armadas;

Que, de conformidad con lo dispuesto por la Ley N° 30225, Ley de Contrataciones del Estado de fecha 10 de julio de 2014, modificado por el Decreto Legislativo N° 1444, de fecha 16 de setiembre de 2018 y su Reglamento, aprobado por el Decreto Supremo N° 344-2018-EF, de fecha 31 de diciembre de 2018; el Decreto Legislativo N° 1136, Decreto Legislativo del Comando Conjunto de las Fuerzas Armadas, de fecha de diciembre de 2012, reglamentado por Decreto Supremo N° 007-2016-DE, de fecha 18, de julio del 2016 y modificado por Decreto Supremo N° 013-2017-DE, de fecha 22 de diciembre de 2017, la Resolución N° 358-2007-OSCE/PRE que aprueba la Directiva N° 010-2006-OSCE/CD y la Directiva N° 020-16 /JCCFFAA/D-6/DGRS/SBDS, resulta pertinente, emitir el acto de administración para la aprobación del proceso de estandarización en mención;

Estando a lo propuesto por el Jefe de la Oficina de Soporte Informático y Estadística de la Oficina General de Apoyo del Comando de las Fuerzas Armadas, a lo recomendado por el Jefe de la Oficina General de Apoyo del Comando de las Fuerzas Armadas y a lo opinado por el Jefe de la Oficina de Asesoría Jurídica del Comando Conjunto de las Fuerzas Armadas.

SE RESUELVE:

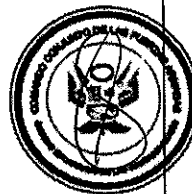
Artículo 1.- Aprobar el proceso de estandarización de hardware CISCO, por el periodo de TRES (03) años en el Comando Conjunto de las Fuerzas Armadas, conforme al Informe Técnico de Estandarización de Software N° 016-

O-225744270-O+
CARLOS I. GAMARRA QUINTANA
Jefe de la Oficina General de Apoyo del
Comando Conjunto de las FFAA



"ES COPIA DEL ORIGINAL"

O-225744270-4-B+
Gustavo HERNANDEZ Del Castillo
Teniente Coronel EP
Fedatario del Comando Conjunto de las
Fuerzas Armadas



2023-CCFFAA/OGA/OSIE/SGR de fecha 08 de mayo de 2023, elaborado por la Oficina de Soporte Informático y Estadística de la Oficina General de Apoyo del Comando Conjunto de las Fuerzas Armadas.

Artículo 2.- La aprobación de la presente estandarización a que se refiere el artículo precedente no implica la exoneración del proceso de selección correspondiente, ni exime del cumplimiento de los requisitos, condiciones, formalidades, exigencias y garantías establecidas en la Ley de Contrataciones del Estado y su Reglamento, para la realización de los actos preparatorios del proceso de selección que corresponda y la ejecución contractual respectiva.

Artículo 3.- Encargar a la Oficina de Soporte Informático y Estadística de la Oficina General de Apoyo del Comando de las Fuerzas Armadas, la verificación durante el periodo de vigencia de la presente estandarización, de las condiciones que determinaron su aprobación, debiendo informar la variación de las mismas, en cuyo caso la referida aprobación quedará sin efecto.

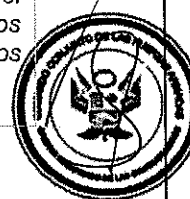
Artículo 4.- Disponer la publicación de la presente Resolución en el portal Institucional del Comando Conjunto de las Fuerzas Armadas (www.ccffao.mil.pe)

Regístrese, comuníquese y archívese, como Documento Oficial Público (D.O.P.).

MANUEL GÓMEZ DE LA TORRE ARAMBAR
General de Ejército
Jefe del Comando Conjunto de las Fuerzas Armadas

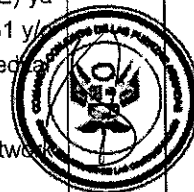
Importante

Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, el órgano encargado de las contrataciones o el comité de selección, según corresponda, incorpora los requisitos de calificación previstos por el área usuaria en el requerimiento, no pudiendo incluirse requisitos adicionales, ni distintos a los siguientes:



3.2. REQUISITOS DE CALIFICACIÓN

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none">- Un (01) Jefe de Proyecto: Para el perfil del jefe de proyecto debe presentar lo siguiente: Título Profesional en las especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica o afines.- Tres (03) Especialistas de Implementación: Para el perfil del especialista de implementación debe presentar lo siguiente: Título y/o bachiller en las especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica, Telecomunicaciones o afines.- Dos (02) Especialista en soporte: Para el perfil de especialista debe presentar lo siguiente: Bachiller universitario y/o técnico en especialidades de Ingeniería de Sistemas, Cómputo, Informática, Electrónica, Telecomunicaciones, informática o afines. <p><u>Acreditación:</u></p> <p>El Título Profesional y/o Bachiller será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el Título Profesional y/o Bachiller no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.3.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none">- Un (01) Jefe de Proyecto: Para el perfil del jefe de proyecto debe presentar lo siguiente:<ul style="list-style-type: none">o Copia de la Certificación PMP (Project Management Profesional) vigente.- Tres (03) Especialistas de Implementación: Para el perfil del especialista de implementación debe presentar lo siguiente:<ul style="list-style-type: none">o Copia de la Certificación a nivel Profesional y/o Expert del equipamiento ofertado a nivel de la solución de Firewall, Endpoint, Switches y Protección de datos en reposo, las cuales deben estar vigentes.



- **Dos (02) Especialista en soporte:** Para el perfil de especialista debe presentar lo siguiente:

- o Un (01) especialista debe con la copia de la Certificación CheckPoint Security Expert (CCSE) ya sea la versión R80 o R81 y/o CheckPoint Security Master (CCSM) ya sea la versión R80 o R81 y/o la Certificación Check Point Certified Endpoint Specialist (CCES); o equivalente y lo debe acreditar para la suscripción del contrato.
- o Un (01) especialista debe contar con la copia de la Certificación en redes empresariales (Networking Enterprise) o equivalente.
- o Copia de la Certificación a nivel Profesional y/o Expert del equipamiento ofertado a nivel de la solución de Firewall, Endpoint y Protección de datos en reposo, las cuales deben estar vigentes.

Acreditación:

Se acreditará con copia simple de Constancias, Certificados u otros documentos, según corresponda.

Importante

Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.

B.4 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

- **Jefe de Proyecto:**
Tres (03) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación en equipamientos de seguridad perimetral CheckPoint o equivalente.
- **Especialistas de Implementación:**
Tres (03) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación con equipamientos en redes empresariales (Networking Enterprise) o equivalente.
- **Especialista en soporte:**
Dos (02) años de experiencia, en servicio de soporte y/o mantenimiento y/o implementación en equipamientos de seguridad perimetral CheckPoint o equivalente.

De presentarse experiencia ejecutada paralelamente (trasape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento
- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
- Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los

	documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.
C	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 9,245,000.00 (Nueve Millones Doscientos Cuarenta y Cinco Mil con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 1,155,620.00 (Un Millón Ciento Cincuenta y Cinco Mil Seiscientos Veinte con 00/100 Soles), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran servicios similares a los siguientes: Adquisición de equipamiento Firewall CheckPoint y/o similares, Seguridad de Red Perimetral, Solución de Firewalls Perimetral, Firewall o cortafuegos de aplicaciones web y/o similares en donde el servicio principal este la marca CheckPoint.</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹⁰, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de</p>



¹⁰ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

Importante

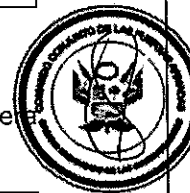
- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalente, y no mediante declaración jurada.*



CAPÍTULO IV FACTORES DE EVALUACIÓN

La evaluación se realiza sobre la base de cien (100) puntos.

Para determinar la oferta con el mejor puntaje y el orden de prelación de las ofertas, se considera lo siguiente:



FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<p><u>Evaluación:</u></p> <p>Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p>	<p>La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i= Oferta P_i= Puntaje de la oferta a evaluar O_i=Precio i O_m= Precio de la oferta más baja PMP=Puntaje máximo del precio</p> <p style="text-align: right;">80 puntos</p>
B. PLAZO DE PRESTACIÓN DEL SERVICIO¹¹	
<p><u>Evaluación:</u></p> <p>Se evaluará en función al plazo ofertado para la entrega, instalación y configuración del equipamiento del numeral 5.2.4 de los Términos de Referencia, el cual debe mejorar el plazo de ejecución establecido en los Términos de Referencia.</p> <p><u>Acreditación:</u></p> <p>Se acreditará mediante la presentación de declaración jurada de plazo de prestación del servicio. (Anexo N° 4)</p>	<p>De 50 hasta 60 días calendario: 20 puntos</p> <p>De 61 hasta 69 días calendario: 10 puntos</p>
PUNTAJE TOTAL	100 puntos

Importante

Los factores de evaluación elaborados por el órgano encargado de las contrataciones o el comité de selección, según corresponda, son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de los Términos de Referencia ni los requisitos de calificación.

¹¹ Este factor podrá ser consignado cuando del expediente de contratación se advierta que el plazo establecido para la prestación del servicio admite reducción, para lo cual deben establecerse rangos razonables para la asignación de puntaje, esto es que no suponga un riesgo de incumplimiento contractual y que represente una mejora al plazo establecido.

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, las que en ningún caso pueden contemplar disposiciones contrarias a la normativa vigente ni a lo señalado en este capítulo.



Conste por el presente documento, la contratación del **SERVICIO DE SEGURIDAD DE LAS COMUNICACIONES DEL CCFFAA, DE LA MARCA CHECK POINT O EQUIVALENTE**, que celebra de una parte el COMANDO CONJUNTO DE LAS FUERZAS ARMADAS, en adelante LA ENTIDAD, con RUC N° [...], con domicilio legal en [...], representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [...], el órgano encargado de las contrataciones, adjudicó la buena pro de la **CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA** para la contratación del **SERVICIO DE SEGURIDAD DE LAS COMUNICACIONES DEL CCFFAA, DE LA MARCA CHECK POINT O EQUIVALENTE**, a **[INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO]**, cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto la contratación del **SERVICIO DE SEGURIDAD DE LAS COMUNICACIONES DEL CCFFAA, DE LA MARCA CHECK POINT O EQUIVALENTE**.

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a **[CONSIGNAR MONEDA Y MONTO]**, que incluye todos los impuestos de Ley.

Este monto comprende el costo del servicio, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del servicio materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO¹²

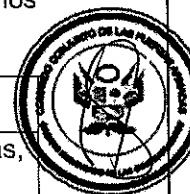
LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en **[INDICAR MONEDA]**, en TRES (03) PAGOS PARCIALES, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario.

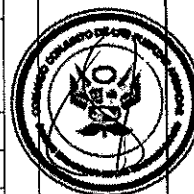
LA ENTIDAD debe efectuar el pago dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

¹² En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

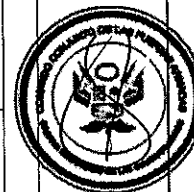
En caso de retraso en el pago por parte de LA ENTIDAD, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 39 de la Ley de Contrataciones del Estado y en el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.



PAGO	PORCENTAJE	CONDICIONES PARA EL PAGO																														
Primer pago AF-2024	30% del monto adjudicado	se realizará previa conformidad de la activación de las licencias, soporte y suscripción indicadas del numeral 5.2.1 al 5.2.3:																														
		5.2.1 Licenciamiento y soporte del fabricante																														
		Cuadro N° 1																														
		<table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CPSB-NGTP-1600-3Y</td><td>1600 Base Appliance with Threat Prevention (NGTP) subscription package</td><td>01</td></tr></table>	SKU	Nombre del producto	Cant	CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01																								
		SKU	Nombre del producto	Cant																												
		CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01																												
		5.2.2 Licenciamiento y soporte del fabricante																														
		Cuadro N° 2																														
		<table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CON-SNTP-C93002TA</td><td>Catalyst 9300 SNTC 24X7X4</td><td>02</td></tr></table>	SKU	Nombre del producto	Cant	CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02																								
		SKU	Nombre del producto	Cant																												
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02																														
5.2.3 Licenciamiento y suscripción a las siguientes soluciones																																
Cuadro N° 3																																
<table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CP-HAR-EP-COMPLETE</td><td>Harmony Endpoint Complete</td><td>450</td></tr><tr><td>CP-INFINITY-XPR</td><td>Extended Detection/Prevention & Response.</td><td>400</td></tr></table>	SKU	Nombre del producto	Cant	CP-HAR-EP-COMPLETE	Harmony Endpoint Complete	450	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																							
SKU	Nombre del producto	Cant																														
CP-HAR-EP-COMPLETE	Harmony Endpoint Complete	450																														
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																														
Así mismo a la entrega, instalación y configuración del equipamiento detallados en el numeral 5.2.4 y a la capacitación del personal de acuerdo al 5.2.5:																																
5.2.4 Equipamiento																																
Cuadro N° 4																																
<table><tr><th>N°</th><th>Nombre del producto</th><th>Cant</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr><tr><td>01</td><td>Equipo Firewall Perimetral</td><td>01</td><td>ANEXO A</td></tr><tr><td>02</td><td>Equipo Firewall DataCenter</td><td>01</td><td>ANEXO B</td></tr><tr><td>03</td><td>Equipo Virtual para Administración y Correlación de Eventos y Reportes</td><td>01</td><td>ANEXO C</td></tr><tr><td>04</td><td>Equipo Sandboxing para Emulación de Amenazas de día cero</td><td>01</td><td>ANEXO D</td></tr><tr><td>05</td><td>Equipo Firewall Perimetral Remoto</td><td>03</td><td>ANEXO E</td></tr><tr><td>06</td><td>Switch Acceso Remoto</td><td>02</td><td>ANEXO F</td></tr><tr><td>07</td><td>Equipo virtual para Protección de Correo Electrónico onpremise</td><td>01</td><td>ANEXO G</td></tr></table>	N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS	01	Equipo Firewall Perimetral	01	ANEXO A	02	Equipo Firewall DataCenter	01	ANEXO B	03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C	04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D	05	Equipo Firewall Perimetral Remoto	03	ANEXO E	06	Switch Acceso Remoto	02	ANEXO F	07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G
N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS																													
01	Equipo Firewall Perimetral	01	ANEXO A																													
02	Equipo Firewall DataCenter	01	ANEXO B																													
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C																													
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D																													
05	Equipo Firewall Perimetral Remoto	03	ANEXO E																													
06	Switch Acceso Remoto	02	ANEXO F																													
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G																													



		<table><tr><td>08</td><td>Equipo virtual para protección de aplicaciones web</td><td>01</td><td>ANEXO H</td></tr><tr><td>09</td><td>Equipo virtual para protección de bases de datos en reposo</td><td>01</td><td>ANEXO I</td></tr><tr><td>10</td><td>Gabinete Autocontenido</td><td>01</td><td>ANEXO J</td></tr><tr><td>11</td><td>Equipo de AA Confort</td><td>01</td><td>ANEXO K</td></tr><tr><td>12</td><td>Equipo UPS</td><td>01</td><td>ANEXO L</td></tr></table>	08	Equipo virtual para protección de aplicaciones web	01	ANEXO H	09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I	10	Gabinete Autocontenido	01	ANEXO J	11	Equipo de AA Confort	01	ANEXO K	12	Equipo UPS	01	ANEXO L									
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H																												
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I																												
10	Gabinete Autocontenido	01	ANEXO J																												
11	Equipo de AA Confort	01	ANEXO K																												
12	Equipo UPS	01	ANEXO L																												
		<p>5.2.5 Capacitación</p> <p>Cuadro N° 5</p> <table><tr><th>N°</th><th>ITEM</th><th>MODALIDAD</th><th>Cant.</th></tr><tr><td>01</td><td>Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)</td><td>Presencial</td><td>10 Pers onas</td></tr><tr><td>02</td><td>Curso de la solución de seguridad de firewall a nivel de administración y/o experto</td><td>Curso no oficial</td><td>05 Pers onas</td></tr><tr><td>03</td><td>Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall</td><td>Voucher de Certificación</td><td>05 Pers onas</td></tr></table>	N°	ITEM	MODALIDAD	Cant.	01	Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)	Presencial	10 Pers onas	02	Curso de la solución de seguridad de firewall a nivel de administración y/o experto	Curso no oficial	05 Pers onas	03	Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall	Voucher de Certificación	05 Pers onas													
N°	ITEM	MODALIDAD	Cant.																												
01	Curso de capacitación en el funcionamiento de la solución ofertada (36 Horas)	Presencial	10 Pers onas																												
02	Curso de la solución de seguridad de firewall a nivel de administración y/o experto	Curso no oficial	05 Pers onas																												
03	Voucher Oficiales de la marca a nivel de Administrador y/o expert de la solución de firewall	Voucher de Certificación	05 Pers onas																												
Segundo pago AF-2025	35% del monto adjudicado	<p>Al culminar el primer año del contrato, asimismo, luego de la conformidad por parte del área usuaria del correcto funcionamiento, soporte y mantenimiento de los productos solicitados.</p> <p>Cuadro N° 1 (Pre-existent)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CPSB-NGTP-1600-3Y</td><td>1600 Base Appliance with Threat Prevention (NGTP) subscription package</td><td>01</td></tr></table> <p>Cuadro N° 2 (Pre-existent)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CON-SNTP-C93002TA</td><td>Catalyst 9300 SNTC 24X7X4</td><td>02</td></tr></table> <p>Cuadro N° 3 (Pre-existent)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CP-HAR-EP-COMplete</td><td>Harmony Endpoint Complete</td><td>450</td></tr><tr><td>CP-INFINITY-XPR</td><td>Extended Detection/Prevention & Response.</td><td>400</td></tr></table> <p>Cuadro N° 4 (1er Mantenimiento)</p> <table><tr><th>N°</th><th>Nombre del producto</th><th>Cant</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr><tr><td>01</td><td>Equipo Firewall Perimetral</td><td>01</td><td>ANEXO A</td></tr></table>	SKU	Nombre del producto	Cant	CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01	SKU	Nombre del producto	Cant	CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02	SKU	Nombre del producto	Cant	CP-HAR-EP-COMplete	Harmony Endpoint Complete	450	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400	N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS	01	Equipo Firewall Perimetral	01	ANEXO A
SKU	Nombre del producto	Cant																													
CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01																													
SKU	Nombre del producto	Cant																													
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02																													
SKU	Nombre del producto	Cant																													
CP-HAR-EP-COMplete	Harmony Endpoint Complete	450																													
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																													
N°	Nombre del producto	Cant	CARACTERÍSTICAS TÉCNICAS																												
01	Equipo Firewall Perimetral	01	ANEXO A																												



		<table><tr><td>02</td><td>Equipo Firewall DataCenter</td><td>01</td><td>ANEXO B</td></tr><tr><td>03</td><td>Equipo Virtual para Administración y Correlación de Eventos y Reportes</td><td>01</td><td>ANEXO C</td></tr><tr><td>04</td><td>Equipo Sandboxing para Emulación de Amenazas de día cero</td><td>01</td><td>ANEXO D</td></tr><tr><td>05</td><td>Equipo Firewall Perimetral Remoto</td><td>03</td><td>ANEXO E</td></tr><tr><td>06</td><td>Switch Acceso Remoto</td><td>02</td><td>ANEXO F</td></tr><tr><td>07</td><td>Equipo virtual para Protección de Correo Electrónico onpremise</td><td>01</td><td>ANEXO G</td></tr><tr><td>08</td><td>Equipo virtual para protección de aplicaciones web</td><td>01</td><td>ANEXO H</td></tr><tr><td>09</td><td>Equipo virtual para protección de bases de datos en reposo</td><td>01</td><td>ANEXO I</td></tr><tr><td>10</td><td>Gabinete Autocontenido</td><td>01</td><td>ANEXO J</td></tr><tr><td>11</td><td>Equipo de AA Confort</td><td>01</td><td>ANEXO K</td></tr><tr><td>12</td><td>Equipo UPS</td><td>01</td><td>ANEXO L</td></tr></table>	02	Equipo Firewall DataCenter	01	ANEXO B	03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C	04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D	05	Equipo Firewall Perimetral Remoto	03	ANEXO E	06	Switch Acceso Remoto	02	ANEXO F	07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G	08	Equipo virtual para protección de aplicaciones web	01	ANEXO H	09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I	10	Gabinete Autocontenido	01	ANEXO J	11	Equipo de AA Confort	01	ANEXO K	12	Equipo UPS	01	ANEXO L
02	Equipo Firewall DataCenter	01	ANEXO B																																											
03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C																																											
04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D																																											
05	Equipo Firewall Perimetral Remoto	03	ANEXO E																																											
06	Switch Acceso Remoto	02	ANEXO F																																											
07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G																																											
08	Equipo virtual para protección de aplicaciones web	01	ANEXO H																																											
09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I																																											
10	Gabinete Autocontenido	01	ANEXO J																																											
11	Equipo de AA Confort	01	ANEXO K																																											
12	Equipo UPS	01	ANEXO L																																											
Tercer pago AF-2026	35% del monto adjudicado	<p>Al culminar el segundo año del contrato, asimismo, luego de la conformidad por parte del área usuaria del correcto funcionamiento, soporte y mantenimiento de los productos solicitados.</p> <p>Cuadro N° 1 (Pre-existent)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CPSB-NGTP-1600-3Y</td><td>1600 Base Appliance with Threat Prevention (NGTP) subscription package</td><td>01</td></tr></table> <p>Cuadro N° 2 (Pre-existent)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CON-SNTP-C93002TA</td><td>Catalyst 9300 SNTC 24X7X4</td><td>02</td></tr></table> <p>Cuadro N° 3 (Pre-existent)</p> <table><tr><th>SKU</th><th>Nombre del producto</th><th>Cant</th></tr><tr><td>CP-HAR-EP-COMplete</td><td>Harmony Endpoint Complete</td><td>450</td></tr><tr><td>CP-INFINITY-XPR</td><td>Extended Detection/Prevention & Response.</td><td>400</td></tr></table> <p>Cuadro N° 4 (2do Mantenimiento)</p> <table><tr><th>N°</th><th>Nombre del producto</th><th>Cant</th><th>CARACTERISTICAS TÉCNICAS</th></tr><tr><td>01</td><td>Equipo Firewall Perimetral</td><td>01</td><td>ANEXO A</td></tr><tr><td>02</td><td>Equipo Firewall DataCenter</td><td>01</td><td>ANEXO B</td></tr></table>		SKU	Nombre del producto	Cant	CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01	SKU	Nombre del producto	Cant	CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02	SKU	Nombre del producto	Cant	CP-HAR-EP-COMplete	Harmony Endpoint Complete	450	CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400	N°	Nombre del producto	Cant	CARACTERISTICAS TÉCNICAS	01	Equipo Firewall Perimetral	01	ANEXO A	02	Equipo Firewall DataCenter	01	ANEXO B										
SKU	Nombre del producto	Cant																																												
CPSB-NGTP-1600-3Y	1600 Base Appliance with Threat Prevention (NGTP) subscription package	01																																												
SKU	Nombre del producto	Cant																																												
CON-SNTP-C93002TA	Catalyst 9300 SNTC 24X7X4	02																																												
SKU	Nombre del producto	Cant																																												
CP-HAR-EP-COMplete	Harmony Endpoint Complete	450																																												
CP-INFINITY-XPR	Extended Detection/Prevention & Response.	400																																												
N°	Nombre del producto	Cant	CARACTERISTICAS TÉCNICAS																																											
01	Equipo Firewall Perimetral	01	ANEXO A																																											
02	Equipo Firewall DataCenter	01	ANEXO B																																											

		03	Equipo Virtual para Administración y Correlación de Eventos y Reportes	01	ANEXO C
		04	Equipo Sandboxing para Emulación de Amenazas de día cero	01	ANEXO D
		05	Equipo Firewall Perimetral Remoto	03	ANEXO E
		06	Switch Acceso Remoto	02	ANEXO F
		07	Equipo virtual para Protección de Correo Electrónico onpremise	01	ANEXO G
		08	Equipo virtual para protección de aplicaciones web	01	ANEXO H
		09	Equipo virtual para protección de bases de datos en reposo	01	ANEXO I
		10	Gabinete Autocontenido	01	ANEXO J
		11	Equipo de AA Confort	01	ANEXO K
		12	Equipo UPS	01	ANEXO L



Cronograma de Pago

AF-2024	AF-2025	AF-2026	TOTAL
DIC - 30%	DIC - 35%	DIC - 35%	100%

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

- Acta de Conformidad suscrita por el encargado de la Seguridad Informática y la Jefatura de la Oficina de Soporte Informática y Estadística (OSIE).
- Informe del funcionario responsable de la Oficina de Soporte Informática y Estadística (OSIE), emitiendo la conformidad de la prestación efectuada.
- Entregables de la Prestación Principal y Prestación Accesorias detallados en el numeral 10 de los Términos de Referencia del Capítulo III de la Sección Específica de las bases.
- Comprobante de pago. (Factura).

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE ÚLTIMO CASO].

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS¹³

Las prestaciones accesorias tienen por objeto [CONSIGNAR EL OBJETO DE LAS PRESTACIONES ACCESORIAS].

¹³ De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesorias, pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

El monto de las prestaciones accesorias asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

El plazo de ejecución de las prestaciones accesorias es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL CUMPLIMIENTO DE LAS PRESTACIONES PRINCIPALES, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS, DEBIENDO INDICAR LAS MISMAS EN ESTE ÚLTIMO CASO].



[DE SER EL CASO, INCLUIR OTROS ASPECTOS RELACIONADOS A LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS]

CLÁUSULA SÉTIMA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA OCTAVA: GARANTÍAS

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por los conceptos, montos y vigencias siguientes:

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE]. Monto que es equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

Importante

Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente:

"De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."

En el caso que corresponda, consignar lo siguiente:

- Garantía fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE], la misma que debe mantenerse vigente hasta el cumplimiento total de las obligaciones garantizadas.

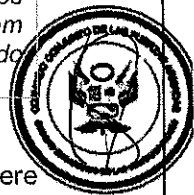
Importante

Al amparo de lo dispuesto en el numeral 151.2 del artículo 151 del Reglamento de la Ley de Contrataciones del Estado, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato de la prestación accesorio como garantía de fiel cumplimiento de prestaciones accesorias, debe consignarse lo siguiente:

"De fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."

Importante

De conformidad con el artículo 152 del Reglamento, no se constituirá garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias, en contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00). Dicha excepción también aplica a los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados no supere el monto señalado anteriormente.



CLÁUSULA NOVENA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto en el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no otorga la conformidad, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

- **ÁREAS QUE SUPERVISAN:** La Sección de Seguridad de Redes de la Oficina de Soporte Informática y Estadística del CCFFAA.
- **ÁREAS QUE COORDINAN CON EL PROVEEDOR:** La Sección de Seguridad de Redes de la Oficina de Soporte Informática y Estadística del CCFFAA será la responsable de la coordinación con el proveedor del presente servicio.
- **ÁREAS QUE BRINDAN LA CONFORMIDAD:** La conformidad será otorgada por el encargado de la Seguridad Informática y la Jefatura de la Oficina de Soporte Informática y Estadística.

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

EL CONTRATISTA declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitado para contratar con el Estado en caso de incumplimiento.

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del

contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$$

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;

F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Importante

De haberse previsto establecer penalidades distintas a la penalidad por mora, incluir dichas penalidades, los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar, conforme el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Estos dos (2) tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.

CLÁUSULA DÉCIMA CUARTA: OTRAS PENALIDADES

Cualquier retraso para la atención y solución de los requerimientos de soporte técnico o incidentes, de los Niveles de Servicio (numeral 5.3.2 al numeral 5.3.4 de los Términos de Referencia del Capítulo III de la Sección Específica de las bases), implicará que se aplique las siguientes penalidades:

N°	Supuestos de aplicación de penalidad	Monto por hora o fracción adicional a lo señalado en los niveles de servicio	Procedimiento
01	Por retraso en la atención o solución de los requerimientos de soporte técnico o incidentes solicitados.	S/ 90.00	Se aplicará cuando se supere el tiempo máximo de atención, solución de incidentes y requerimiento de soporte técnico o incidentes, para tal efecto la OSIE elaborará un informe detallado de los retrasos incurridos en el mes de acuerdo a los niveles de servicio.



02	Por retraso en reemplazo de equipos	S/ 90.00	Se aplicará cuando se supere el tiempo máximo para el reemplazo de equipos, para tal efecto la OSIE elaborará un informe detallado los retrasos incurridos en el mes, de acuerdo a los niveles de servicio.
----	-------------------------------------	----------	---



CLÁUSULA DÉCIMA QUINTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA SEXTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMA SÉTIMA: ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

CLÁUSULA DÉCIMA OCTAVA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÉCIMA NOVENA: SOLUCIÓN DE CONTROVERSIAS¹⁴

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven

¹⁴ De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

CLÁUSULA VIGÉSIMA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA PRIMERA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: [.....]

CORREO ELECTRÓNICO DE LA ENTIDAD: logistica@ccffaa.mil.pe

DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

CORREO ELECTRÓNICO DEL CONTRATISTA: [CONSIGNAR EL CORREO ELECTRÓNICO DEL CONTRATISTA]

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

"LA ENTIDAD"

"EL CONTRATISTA"

ANEXO N° 01

COMPROMISO DE CONFIDENCIALIDAD



Conste por el presente Compromiso de Confidencialidad que suscribe _____, identificado(a) con (DNI/Pasaporte) N° _____, con domicilio en _____, en adelante EL (LA) _____, lo siguiente:

PRIMERO: EI CONTRATISTA es consciente de la importancia de su responsabilidad en cuanto a guardar confidencialidad de la información, ya sea dentro o fuera de las instalaciones del CCFFAA. Por lo tanto, el **CONTRATISTA** manifiesta haber leído, entendido y se compromete a cumplir con todas las disposiciones que normen la confidencialidad, cualquiera sea su fuente o registro: oral, escrito impreso, magnético, electrónico, fax, fotografía, video o cualquier otro medio de conservación. Del mismo modo declara que, durante su vinculación en el CCFFAA, no intentará tener acceso, copiar, compartir o hacer conocer a terceros ninguna información a través de cualquier medio de comunicación y/o redes sociales.

SEGUNDO: EI CONTRATISTA se compromete a utilizar todos los medios razonables para proteger la Información confiada a su persona y a no hacer uso de sus privilegios de acceso a la información más allá de lo estrictamente necesario para el cumplimiento de sus funciones, del mismo modo, no comprometerá la confidencialidad de la información contenida en ella. El **CONTRATISTA** no transportará información clasificada fuera de las instalaciones del CCFFAA; cuando por razones de servicio se requiera trasladar la misma, lo hará sólo con autorización del Oficial de Seguridad, adoptando los medios necesarios para garantizar la confidencialidad. El **CONTRATISTA** acepta que la terminación de su vinculación con el CCFFAA, cualquiera que sea la causa, no determinará la terminación de los compromisos que asume mediante el presente documento. Al término de su vinculación devolverá toda la información que se le haya sido concedido, cualquiera sea su fuente: escrito impreso, magnético y/o cualquier medio de soporte de información; y que su incumplimiento ocasionará, el inicio de la determinación de la responsabilidad civil y/o penal en la que pueda incurrir.

TERCERO: EI CONTRATISTA declara conocer que cualquier incumplimiento del presente compromiso podrá dar lugar al inicio de las acciones administrativas, civiles o penales a que hubiera lugar.

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹⁵.

¹⁵ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>



ANEXOS

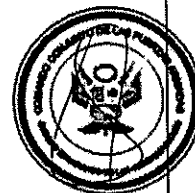
ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA

Presente.-



El que se suscribe, [.....], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ¹⁶	Sí	No	
Correo electrónico :			

Autorización de notificación por correo electrónico:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios¹⁷

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o Representante legal, según corresponda

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

¹⁶ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

¹⁷ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de servicios.

Importante

Cuando se trate de consorcios, la declaración jurada es la siguiente:

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR



Señores

ÓRGANO ENCARGADO DE LAS CONTRATACIONES

CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA

Presente.-

El que se suscribe, [...], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁸		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁹		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ²⁰		Sí	No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.

¹⁸ En los contratos periódicos de prestación de servicios, esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dichos efectos, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

¹⁹ Ibidem.

²⁰ Ibidem.

2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios²¹



Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del representante
común del consorcio**

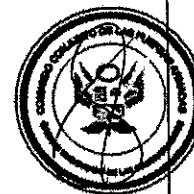
Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

²¹ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO N° 2

**DECLARACIÓN JURADA
(ART. 52 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)**



Señores
ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

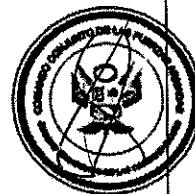
.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

Importante

En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA



Señores
ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de **[CONSIGNAR EL OBJETO DE LA CONVOCATORIA]**, de conformidad con los Términos de Referencia que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante

Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de los términos de referencia, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO



Señores
ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a prestar el servicio objeto del presente procedimiento de selección en el plazo de [CONSIGNAR EL PLAZO OFERTADO].

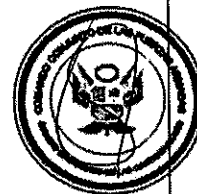
[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 5

PROMESA DE CONSORCIO

(Sólo para el caso en que un consorcio se presente como postor)



Señores

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA**

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA**.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 140 del Reglamento de la Ley de Contrataciones del Estado, bajo las siguientes condiciones:

a) Integrantes del consorcio

1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

c) Fijamos nuestro domicilio legal común en [.....].

d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]²²

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²³

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%²⁴

[CONSIGNAR CIUDAD Y FECHA]

²² Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²³ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁴ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

.....
Consortiado 1
Nombres, apellidos y firma del Consortiado 1
o de su Representante Legal
Tipo y N° de Documento de Identidad

.....
Consortiado 2
Nombres, apellidos y firma del Consortiado 2
o de su Representante Legal
Tipo y N° de Documento de Identidad

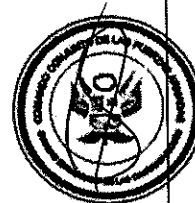


Importante

De conformidad con el artículo 52 del Reglamento, las firmas de los integrantes del consorcio deben ser legalizadas.

ANEXO N° 6

PRECIO DE LA OFERTA



Señores
ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

CONCEPTO	PRECIO TOTAL
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda**

Importante

- *El postor debe consignar el precio total de la oferta, sin perjuicio que, de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:

Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]".*
- *El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias.*

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA
Presente.-



Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD:

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁶	EXPERIENCIA PROVENIENTE ²⁷ DE:	MONEDA	IMPORTE ²⁸	TIPO DE CAMBIO VENTA ²⁹	MONTO FACTURADO ACUMULADO ³⁰
1										
2										
3										
4										

²⁵ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

²⁶ Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

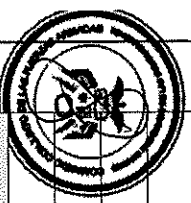
²⁷ Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN "Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz". Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, "... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe".

²⁸ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁹ El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

³⁰ Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁶	EXPERIENCIA PROVENIENTE ²⁷ DE:	MONEDA	IMPORTE ²⁸	TIPO DE CAMBIO VENTA ²⁹	MONTO FACTURADO ACUMULADO ³⁰
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										



[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 9

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**



Señores
ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA
Presente. -

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

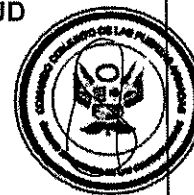
Importante

A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en <http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados>. También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.

ANEXO N° 12

AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA SOLICITUD
DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE COMUNICACIÓN

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)



Señores
ÓRGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA N° 005-2024/MD-CCFFAA
Presente.-

El que se suscribe, [.....], postor adjudicado y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo que durante la ejecución del contrato se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO] lo siguiente:

✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante

La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.