



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

11

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

## TÉRMINOS DE REFERENCIA

### CONTRATACIÓN DEL SERVICIO DE ALOJAMIENTO CLOUD PARA SERVIDORES DE SALUDPOL

#### I. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del servicio de alojamiento cloud para servidores de SALUDPOL.

#### II. FINALIDAD PÚBLICA

La contratación del servicio permitirá disponer de recursos de cómputo, almacenamiento, redes y seguridad de rápido aprovisionamiento, para la publicación y/o alojamiento de aplicaciones y servicios de TI, en ambientes de alta disponibilidad, confidencialidad y seguridad que permitan el normal desarrollo de las actividades diarias, contribuyendo con una Gestión Pública eficiente y de calidad que repercute en la atención oportuna de las necesidades de las áreas usuarias.

#### III. REQUERIMIENTOS TÉCNICOS MÍNIMOS

##### III.1 CARACTERÍSTICAS GENERALES

- El contratista tiene la obligación de realizar el servicio de acuerdo a lo establecido en los Términos de Referencia, teniendo responsabilidad total sobre la ejecución del servicio contratado.
- El contratista será responsable de todo el despliegue y los elementos necesarios para realización de lo solicitado. Para la realización del servicio, SALUDPOL a través del responsable de la Oficina de Tecnología de la Información brindará las facilidades y accesos necesarios.
- Cualquier omisión en las características técnicas, no eximirá de responsabilidad al contratista, no podrá tomarse como base para reclamos, pues se entiende que el personal a cargo está técnicamente capacitado y especializado en la materia y que al realizar la propuesta técnica ha examinado cuidadosamente todos los documentos y se ha informado de todas las condiciones que puedan afectar sus servicios, costo y plazo de entrega.
- Las labores que involucren el corte de algún servicio en producción no podrán ser efectuados en horario de oficina para no interrumpir las labores del personal, en caso contrario, se realizarán en horario a coordinar con el responsable de la Oficina de Tecnología de la Información.
- El contratista deberá contemplar como parte del servicio esquemas de continuidad, alta disponibilidad y escalabilidad, así como la exclusividad de los recursos asignados al servicio.
- El contratista deberá contemplar y asegurar como parte del servicio, altos niveles en la confidencialidad y privacidad de la información alojada, acorde a normativas y estándares vigentes.
- El contratista del servicio deberá contar con un Centro de Datos cual este implementado con los mecanismos y niveles de seguridad física y lógica necesarios para brindar un servicio de excelentes condiciones y adecuado nivel de disponibilidad, durante todo el periodo de la contratación del servicio.
- El contratista deberá de cumplir con los "Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano".
- El contratista brindará una disponibilidad mínima sobre el servicio cloud del 99.95% anual.
- El Centro de Datos deberá contar con al menos dos conexiones de salida internacional hacia internet, las cuales se deberán comutar de manera automática.
- El contratista deberá mantener secreto profesional respecto de los datos a los que acceda en virtud del servicio ofertado, así como asegurar el respaldo de los mismos, obligaciones que subsistirán aún después de finalizar su relación con la persona contratante.
- El "Datacenter" o "Centro de Datos" del proveedor deberán contar como mínimo con certificación TIER-III otorgada por el UpTime Institute.
- El contratista deberá asegurar el que el Datacenter del servicio Cloud ofertado cumpla mínimamente con las siguientes certificaciones internacionales de seguridad y privacidad: ISO 27001, ISO 27017, ISO 27018, ISO 27701, CSA STAR, NIST Cybersecurity Framework (CSF).
- El contratista deberá contar con una mesa de ayuda con la capacidad de registrar incidentes por Teléfono, por correo electrónico o por sistema de ticket para reportar incidencias o requerimientos.

##### III.2 DISPONIBILIDAD Y BALANCEO DE CARGA DEL SERVICIO

- El contratista debe revisar y asegurar que los servicios de cómputo y memoria del servicio nube a ofertar tenga un SLA mínimo de 99.95%.
- El contratista debe revisar y asegurar que el servicio de nube ofertado permita balancear la carga de trabajo y distribuir un tipo específico de tráfico (http: o https: o ftp:) proveniente





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

de internet entre los servidores de la solución, considerando que la aplicación si soporta un escenario de alta disponibilidad.

### III.3 CARACTERÍSTICAS DE LA INFRAESTRUCTURA

- Debe contar con un portal de autoaprovisionamiento vía web compatible con diferentes navegadores por el cual la entidad accederá a los servicios requeridos. Este portal de auto-aprovisionamiento debe ser protegido por un mecanismo de doble autenticación, además de un usuario y contraseña.
- Debe contar con un servicio que permita gestionar el control de los accesos e identidades de los usuarios a la cuenta de nube otorgada. Permitirá a la entidad gestionar cuentas de usuario y autorizar permisos para los recursos de la nube.
- Debe contar con la provisión de servicios Infraestructura como servicio (IaaS) y Plataforma como Servicio (PaaS) como mínimo.
- Debe contar un servicio de cómputo que permitirá desplegar ambientes virtuales con CPU y memoria. Asimismo, debe soportar el despliegue de Windows y de Linux.
- Debe permitir desplegar máquinas virtuales usando imágenes privadas con el propósito de reducir el servicio de despliegue.
- La plataforma debe permitir el uso de base de datos relacionales y no relacionales (noSQL) como servicio.
- Debe contar con un servicio de APIs de alto rendimiento para construir, gestionar y desplegar APIs, que deberá desplegarse desde el portal de la nube.
- Debe contar con un servicio de almacenamiento de bloques basado en arquitectura distribuida. Se deben operar estos servicios sin detener los servicios de la solución de nube. Puede utilizarse para sistemas de archivos, bases de datos, y otro software de sistema o aplicaciones que necesiten almacenamiento de bloques. Este servicio debe permitir configurar almacenamiento en discos SATA y SSD (base de datos) desde el mismo portal de autoaproxisionamiento.
- Los discos admitirán el cifrado de datos para garantizar la seguridad de los datos.
- El servicio debe soportar la expansión de capacidad de los discos, sin detener las máquinas virtuales.
- Debe contar con un servicio de almacenamiento de objetos de tipo S3 o S3 compatible, con una disponibilidad del 99.9% y durabilidad del 11 9's (99.999999999%) anual. Así mismo, este servicio debe contar con servicio de almacenamiento de modo frecuente, no frecuente y para archivado de información.
- Debe contar con un servicio de alarmas. Estas alarmas podrán utilizarse para recopilar y seguir métricas, definir alarmas y reaccionar de modo automático ante los cambios en sus recursos. Estas alarmas revisarán el estado de los servicios de cómputo, almacenamiento, balanceo de carga. Estos servicios deberán estar disponibles desde el portal de autoaproxisionamiento y permitirán conocer el estado de funcionamiento y el rendimiento de los objetos monitorizados de cada servicio, en tiempo real.
- Debe permitir habilitar notificaciones al crear reglas de alarma. Cuando el estado del servicio en la nube cambia y los datos de monitoreo de la métrica alcanzan el umbral especificado en una regla de alarma, el servicio lo notificará mediante mensajes de texto, correos electrónicos o enviando mensajes a las direcciones del servidor. De esta manera, puede monitorear el estado de los recursos y los cambios en tiempo real.
- Debe contar con un servicio de compartición de archivos con alta confiabilidad (99.95%), alto rendimiento (IOPS: 4,000 hasta IOPS: 16,000), para las instancias virtuales que se creen en la plataforma de nube y debe desplegarse desde el portal de autoaproxisionamiento vía web.
- Debe incluir el aprovisionamiento de direcciones IP públicas a demanda desde el mismo portal de auto-provisionamiento, que permitirán la publicación de las aplicaciones por Internet.
- Debe contar con un servicio de VPN Site to Site para la conexión segura desde el datacenter de SALUDPOL al nodo de nube.
- La plataforma debe permitir crear, borrar o editar capacidades de procesamiento, almacenamiento, de red (ancho de banda) y sistemas operativos en una infraestructura a la que accede para su administración.
- La plataforma de nube debe permitir por lo menos 99.95% de disponibilidad mensual en los servicios de cómputo y memoria.
- La plataforma de nube a proponer debe tener una latencia promedio máxima de 60 ms desde el nodo a ofrecer hasta Perú.
- Debe contar servicios de seguridad de pago por uso como Anti-DDoS y web application firewall, a configurarse desde el portal de auto-aprovisionamiento.
- Los centros de datos que se usan para alojar los nodos de la nube a considerar en este requerimiento deben contar con certificación de TIER 3 del Uptime Institute como mínimo.
- Durante toda la vigencia del servicio, el contratista deberá activar y mantener un servicio de soporte especializado proporcionado directamente por el proveedor del servicio de nube pública.



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

10

**III.4 COMPONENTES DE LA SOLUCIÓN – REQUISITOS MÍNIMOS**

Los servicios a considerar descritos anteriormente serán usados al 100% de utilización al año, estos servicios deben ser como mínimo:

Item	Descripción	Cantidad
1	Linux Centos x64 8.x o superior -Procesador 8 vCPU -Memoria RAM 16GB -Disco duro 2000GB Nvme SSDs	1
2	Linux Centos x64 7.x o superior -Procesador 8 vCPU -Memoria RAM 16GB -Disco duro 1200GB Nvme SSDs	1
3	Windows Server x64 2016 Standard -Procesador 2 vCPU -Memoria RAM 4GB -Disco duro 50GB Nvme SSDs	1
4	Linux Centos x64 8.x o superior -Procesador 24v CPU -Memoria RAM 48GB -Disco duro 500GB Nvme SSDs	1
5	Windows Server 2016 x64 Std o superior - Procesador 02 vCPU - Memoria RAM 4GB - Disco duro 50GB Nvme SSDs	1
6	Oracle Linux x64 7 o superior - Procesador 08 vCPU - Memoria RAM 32GB - Disco duro 550GB Nvme SSDs	1
7	CentOS Linux x64 8 o superior - Procesador 08 vCPU - Memoria RAM 16GB - Disco duro 3200GB Nvme SSDs	1
8	CentOS Linux x64 8 o superior - Procesador 08 vCPU - Memoria RAM 16GB - Disco duro 500GB Nvme SSDs	1
9	CentOS Linux x64 8 o superior - Procesador 08 vCPU - Memoria RAM 16GB - Disco duro 500GB Nvme SSDs	1
10	CentOS Linux x64 8 o superior - Procesador 08 vCPU - Memoria RAM 16GB - Disco duro 500GB Nvme SSDs	1
11	CentOS Linux x64 8 o superior - Procesador 04 vCPU - Memoria RAM 8GB - Disco duro 2000GB Nvme SSDs	1
12	CentOS Linux x64 8 o superior - Procesador 02 vCPU - Memoria RAM 8GB - Disco duro 50GB Nvme SSDs	1
13	CentOS Linux x64 7 o superior - Procesador 08 vCPU - Memoria RAM 16GB - Disco duro 500GB Nvme SSDs	1
14	- Linux Centos 8.x o superior - Procesador 16v CPUs - Memoria RAM 32GB - Disco duro 1000GB Nvme SSDs	1
15	Servicio de AntiDDos.	1





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

16	Servicio WAF PaaS o SaaS (Según TDR)	1
17	Servicio de Network Firewall PaaS o SaaS (Según TDR)	1
18	Servicio de Protección de servidores PaaS o SaaS o Agente (Según TDR)	1
19	Servicio de Backup	1
20	Servicio de monitoreo y alarmas de cpu, memoria y disco.	1
21	Ips públicas estáticas	15
22	Servicio de vpn site – site	15
	Servicio de vpn site - client	15
23	Servicio de Soporte del Contratista en modalidad 24x7. Este servicio incluirá la devolución de la llamada para la atención de la incidencia.	1
24	Servicio de Soporte Business en modalidad 24x7. Este servicio deberá ser exclusivo de la marca.	1

### III.5 DEL MONITOREO

- El contratista deberá realizar el monitoreo de cada servidor considerando:
  - ✓ Monitoreo 24x7: Servidor
  - ✓ Uso de espacio en Disco
  - ✓ Uso de Memoria RAM
  - ✓ Uso de Procesamiento
- Así mismo, el contratista deberá de brindar un acceso web a SALUDPOL para visualizar el estado de los servidores y servicios.

### III.6 DE LA CONECTIVIDAD

- El contratista deberá proporcionar una salida a Internet en su "Datacenter" o "Centro de Datos" con un ancho de banda de 40 Mbps o superior, con overbooking de 1:1.
- El servicio deberá contar con un firewall para filtrar todo el tráfico para evitar que archivos infectados, malware o virus entren en la red.

### III.7 DEL RESPALDO DE INFORMACIÓN

- El servicio de respaldo para las máquinas virtuales debe tener una disponibilidad mínima del 99.9%.
- El servicio de respaldo para las máquinas virtuales permite la copia de seguridad y restauración con un clic para el servicio de almacenamiento de bloques a través de la plataforma.
- El servicio deberá usar la solución nativa de respaldo que ofrece la plataforma. No deberá necesitar de la instalación de agentes en el ambiente virtual o máquinas virtuales para poder realizar las tareas de respaldo y recuperación.
- El contratista deberá garantizar la disponibilidad de la información alojada en los servidores, mediante una política de respaldo que contemple por lo menos:
  - ✓ Respaldo a disco del total de GB de almacenamiento contratados.
  - ✓ Deberá programarse un (01) respaldo completo (Full) y catorce (14) incrementales, con lo que se podrá acceder y recuperar información dentro de los últimos quince (15) días.
  - ✓ Deberá programarse un (01) respaldo completo (Full) mensual el último día de cada mes, con lo que se podrá acceder y recuperar información dentro de los últimos dos (02) meses.

### III.8 DEL ACCESO REMOTO

- El contratista deberá brindar como parte del servicio:
  - ✓ El servicio de acceso remoto al servidor vía conexión directa y/o internet y/o vpn, con acceso de administrador o root sobre cada servidor.
  - ✓ Cuentas estables durante la contratación del servicio.
  - ✓ Soporte para conexiones sobre IPv4.

### III.9 DE LOS SERVICIOS DE SEGURIDAD

Deberá contar con:

- a. **Network Firewall:** El contratista deberá proporcionar un Network Firewall como servicio PaaS o SaaS del fabricante cloud. El servicio debe cumplir con las siguientes especificaciones mínimas, tomando como referencia un servicio de firewall en la nube avanzado.



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

09

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

#### Características y Especificaciones:

##### 2. Capacidad de Protección Adicional (EIP Protection Capacity):

- Protección para 15 EIPs: El servicio debe incluir la capacidad de proteger al menos 15 direcciones IP elásticas (EIP), garantizando la protección de las instancias críticas expuestas a Internet.

##### 3. Tráfico de Protección Máxima (Peak Protection Traffic):

- 50 Mbit/s de Tráfico Máximo de Protección en Internet: El firewall debe ser capaz de gestionar y proteger un tráfico de hasta 50 Mbit/s en su pico, asegurando la continuidad operativa y la seguridad de los servicios públicos durante períodos de alto tráfico.

##### 1. Protección Integral contra Amenazas:

- Detección y Mitigación de Amenazas Avanzadas: Detección y mitigación de ataques DDoS, inyecciones SQL, troyanos, gusanos, spyware y ataques de phishing. Proporciona un sistema de prevención de intrusiones (IPS) que incluye un motor de inteligencia artificial para la detección en tiempo real.

##### 2. Gestión y Monitorización Centralizada:

- Consola de Administración: Ofrece herramientas de gestión centralizada que incluyen dashboards en tiempo real, reportes detallados sobre incidentes y rendimiento, y estadísticas de tráfico.

##### 3. Actualizaciones Automáticas:

- Actualización y Parcheo de Seguridad: Implementa parches de seguridad y actualizaciones automáticas para mantener el firewall siempre actualizado contra las últimas amenazas conocidas.

##### 5. Alta Disponibilidad y Resiliencia:

- Despliegue en Clúster: Los motores y componentes del firewall están desplegados en configuraciones redundantes para asegurar la continuidad del servicio en caso de fallos.

##### 6. Facilidad de Integración:

- Compatibilidad con Otros Servicios Cloud: El firewall debe ser compatible con otros servicios en la nube, facilitando su integración en un entorno híbrido o multi-cloud.

##### 7. Escalabilidad:

- Escalabilidad Automática: Permite la escalabilidad automática para adaptarse a cambios en la demanda de tráfico y recursos, sin afectar el rendimiento o la seguridad.

##### 8. Filtrado de Paquetes y Control de Acceso:

- Reglas de Filtrado Personalizadas: Control del tráfico basado en IPs, puertos y protocolos. Incluye control de acceso basado en el 5-tuple (dirección IP de origen, puerto de origen, dirección IP de destino, puerto de destino y protocolo).

##### 9. Protección de Aplicaciones Web (WAF):

- Firewall de Aplicaciones Web: Proporciona protección contra amenazas a nivel de aplicación, como ataques XSS y CSRF, asegurando la seguridad de las aplicaciones.





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

web.

10. Monitorización en Tiempo Real:

- Alertas y Notificaciones: Ofrece alertas en tiempo real para actividades sospechosas o incidentes de seguridad, permitiendo una respuesta rápida y eficaz.

11. Auditoría de Logs:

- Registro de Eventos: Registra logs detallados de eventos de ataque, control de acceso y tráfico, facilitando la auditoría y el análisis de seguridad.

12. Captura de Paquetes de Red:

- Análisis de Paquetes: Herramienta para la captura y análisis de paquetes, ayudando en la localización de fallos de red y en el análisis de ataques.

13. Protección en el Borde de la Red:

- Seguridad en el Borde: Ofrece protección de tráfico en el borde de la red y entre VPCs, asegurando la integridad y seguridad de los datos en tránsito.

14. Integración con Servicios de Log y Monitoreo:

- Servicio de Logs y Monitoreo: Integración con servicios como Log Tank Service (LTS) y SecMaster para la recolección y análisis de logs en tiempo real.

15. Defensa de Directorios Sensibles:

- Protección de Directorios: Defensa contra escaneos de directorios sensibles en los servidores, asegurando la privacidad y seguridad de los datos.

16. Defensa contra Shell Reversa:

- Protección contra Shell Reversa: Prevención de ataques de shell reversa, protegiendo contra intentos de acceso no autorizados.

17. Políticas de Seguridad Automatizadas:

- Implementación de Políticas: Facilita la importación y aplicación automatizada de políticas de seguridad, mejorando la eficiencia de gestión.

18. Notificaciones de Alarma:

- Configuración de Alertas: Permite la configuración de notificaciones para logs de ataques y advertencias de tráfico, proporcionando alertas por correo electrónico o SMS.

19. Análisis Inteligente de Amenazas:

- Motor de IA: Utiliza un motor de inteligencia artificial para el análisis y defensa contra amenazas, proporcionando una capa adicional de seguridad inteligente.

20. Acceso Controlado por ACL:

- Listas de Control de Acceso (ACL): Implementación de políticas de acceso basadas en listas negras y blancas, permitiendo un control detallado del acceso a la red.



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

08

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

- b. **Web Application Firewall:** El contratista deberá proporcionar un Web Application Firewall (WAF) como servicio PaaS o SaaS del fabricante cloud, en el contexto de una implementación en el sector público en Perú. El servicio debe cumplir con las siguientes especificaciones mínimas, tomando como referencia un servicio de WAF en la nube avanzado.

#### Características y Especificaciones:

##### 2. Capacidad de Protección:

- **Número de Dominios Protegidos:** Capacidad para proteger al menos 60 dominios.
- **Número de Reglas de Protección:** Soporte para al menos 20 reglas de protección configurables.
- **Capacidad de Manejo de Solicitudes:** Capacidad para manejar hasta 200 millones de solicitudes mensuales.

#### Detalles Técnicos Principales:

##### 1. Protección Integral contra Amenazas:

- **Detección y Mitigación de Amenazas Avanzadas:** Protección contra inyecciones SQL, cross-site scripting (XSS), cargas de shells web, inyecciones de comandos/código, inclusión de archivos, acceso a archivos sensibles y explotación de vulnerabilidades de terceros.
- **Prevención de Ataques DDoS y CC:** Identificación de usuarios reales, configuración de limitación de tasas y bloqueo de usuarios falsos para mitigar ataques de denegación de servicio Challenge Collapsar (CC).

##### 2. Gestión y Monitorización Centralizada:

- **Consola de Administración:** Herramientas de gestión centralizada que incluyen dashboards en tiempo real, reportes detallados sobre incidentes y rendimiento, y estadísticas de tráfico.

##### 3. Actualizaciones Automáticas:

- **Actualización y Parcheo de Seguridad:** Implementación de parches de seguridad y actualizaciones automáticas para mantener el WAF siempre actualizado contra las últimas amenazas conocidas.

##### 5. Alta Disponibilidad y Resiliencia:

- **Despliegue en Clúster:** Los motores y componentes del WAF están desplegados en configuraciones redundantes para asegurar la continuidad del servicio en caso de fallos.

##### 6. Facilidad de Integración:

- **Compatibilidad con Otros Servicios Cloud:** El WAF debe ser compatible con otros servicios en la nube, facilitando su integración en un entorno híbrido o multi-cloud.

##### 7. Escalabilidad:

- **Escalabilidad Automática:** Permite la escalabilidad automática para adaptarse a cambios en la demanda de tráfico y recursos, sin afectar el rendimiento o la seguridad.

##### 8. Protección de Aplicaciones Web:

- **Cobertura de OWASP Top 10:** El WAF debe ofrecer protección integral contra las





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

principales amenazas de seguridad web identificadas por OWASP, incluyendo pero no limitado a:

**Inyección:** Prevención de ataques de inyección, como inyección SQL, que permiten a los atacantes ejecutar comandos no autorizados en la base de datos.

**Autenticación Rota:** Protección contra debilidades en los mecanismos de autenticación que podrían ser explotadas para obtener acceso no autorizado.

**Exposición de Datos Sensibles:** Prevención de la exposición de datos sensibles a través de protección de datos en tránsito y en reposo.

**Entidades Externas XML (XXE):** Bloqueo de ataques que exploten vulnerabilidades en el procesamiento de XML.

**Control de Acceso Roto:** Implementación de controles estrictos para evitar el acceso no autorizado a recursos restringidos.

**Configuración de Seguridad Incorrecta:** Garantía de configuraciones seguras por defecto y capacidad para monitorear y corregir configuraciones inseguras.

**Cross-Site Scripting (XSS):** Prevención de ataques XSS que inyecten scripts maliciosos en las páginas web.

**Deserialización Insegura:** Protección contra la deserialización de datos no confiables que podrían llevar a la ejecución remota de código.

**Uso de Componentes con Vulnerabilidades Conocidas:** Detección y mitigación de riesgos asociados con el uso de bibliotecas y componentes con vulnerabilidades conocidas.

**Registro y Monitoreo Insuficientes:** Provisión de capacidades avanzadas de monitoreo y registro para la detección y respuesta a incidentes de seguridad.

#### 9. Monitorización en Tiempo Real:

- Alertas y Notificaciones:** Ofrece alertas en tiempo real para actividades sospechosas o incidentes de seguridad, permitiendo una respuesta rápida y eficaz.

#### 10. Auditoría de Logs:

- Registro de Eventos:** Registra logs detallados de eventos de ataque, control de acceso y tráfico, facilitando la auditoría y el análisis de seguridad.

#### 11. Captura de Paquetes de Red:

- Análisis de Paquetes:** Herramienta para la captura y análisis de paquetes, ayudando en la localización de fallos de red y en el análisis de ataques.

#### 12. Protección en el Borde de la Red:

- Seguridad en el Borde:** Ofrece protección de tráfico en el borde de la red y entre VPCs, asegurando la integridad y seguridad de los datos en tránsito.

#### 13. Integración con Servicios de Log y Monitoreo:

- Servicio de Logs y Monitoreo:** Integración con servicios para la recolección y análisis de logs en tiempo real.

#### 14. Defensa de Directorios Sensibles:





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

07

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

- **Protección de Directorios:** Defensa contra escaneos de directorios sensibles en los servidores, asegurando la privacidad y seguridad de los datos.

#### 15. Defensa contra Shell Reversa:

- **Protección contra Shell Reversa:** Prevención de ataques de shell reversa, protegiendo contra intentos de acceso no autorizados.

#### 16. Políticas de Seguridad Automatizadas:

- **Implementación de Políticas:** Facilita la importación y aplicación automatizada de políticas de seguridad, mejorando la eficiencia de gestión.

#### 17. Notificaciones de Alarma:

- **Configuración de Alertas:** Permite la configuración de notificaciones para logs de ataques y advertencias de tráfico, proporcionando alertas por correo electrónico o SMS.

#### 18. Análisis Inteligente de Amenazas:

- **Motor de IA:** Utiliza un motor de inteligencia artificial para el análisis y defensa contra amenazas, proporcionando una capa adicional de seguridad inteligente.

#### 19. Acceso Controlado por ACL:

- **Listas de Control de Acceso (ACL):** Implementación de políticas de acceso basadas en listas negras y blancas, permitiendo un control detallado del acceso a la red.

#### 20. Protección Anti-Crawler:

- **Defensa contra Crawlers Maliciosos:** Análisis dinámico del comportamiento de los bots y protección contra rastreadores web no autorizados.

#### 21. Geolocalización y Control de Acceso:

- **Control de Acceso por Geolocalización:** Reglas personalizadas para controlar el acceso basado en la ubicación geográfica de las direcciones IP.

#### 22. Protección contra Manipulación de Páginas Web:

- **Anti-Defacement:** Configuración de caché para páginas web estáticas con verificaciones aleatorias para detectar y prevenir la manipulación de contenido.

#### 23. Prevención de Fugas de Información:

- **Protección contra Fugas de Información:** Detección y prevención de la divulgación de información sensible como números de identificación, números de teléfono y direcciones de correo electrónico.

#### 24. Protección IPv6:

- **Compatibilidad con IPv6:** Garantiza que el WAF pueda manejar y proteger el tráfico que utiliza el protocolo IPv6.

#### 25. Protección Anti-Crawler:

- **Defensa contra Crawlers Maliciosos:** Identificación precisa del comportamiento de los bots y medidas de defensa basadas en sistemas de identificación de bots y control de riesgos.





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

- c. **Servicio de protección de servidores:** El contratista deberá proporcionar un servicio de protección contra amenazas y vulnerabilidades para todas las máquinas virtuales y contenedores que sean parte de la solución desplegada en el cloud (HSS) como servicio PaaS o SaaS o agente del fabricante cloud, en el contexto de una implementación en el sector público en Perú. El servicio debe cumplir con las siguientes especificaciones mínimas:

#### Características y Especificaciones:

##### Capacidad de Protección

- **Prevención de Ransomware:** El servicio deberá proteger contra más del 99% de los tipos conocidos de ransomware, utilizando motores de detección de ransomware y honeypots dinámicos.
- **Protección Integral contra Amenazas:** El servicio deberá detectar y mitigar amenazas avanzadas, incluyendo inyecciones SQL, cross-site scripting (XSS), cargas de shells web, inyecciones de comandos/código, inclusión de archivos, acceso a archivos sensibles y explotación de vulnerabilidades de terceros.

##### Gestión y Monitorización Centralizada:

- **Consola de Administración:** El servicio deberá incluir herramientas de gestión centralizada con dashboards en tiempo real, reportes detallados sobre incidentes y rendimiento, y estadísticas de tráfico.
- **Actualización y parcheo de Seguridad:** El servicio deberá implementar parches de seguridad y actualizaciones automáticas para mantener el HSS siempre actualizado contra las últimas amenazas conocidas.

##### Cumplimiento y Conformidad:

- **Conformidad con Normativas y Estándares Internacionales:** El servicio deberá cumplir con normativas y estándares internacionales de seguridad, así como con las regulaciones específicas del gobierno peruano.

##### Alta Disponibilidad y Resiliencia:

- **Despliegue en Clúster:** Los motores y componentes del HSS deberán estar desplegados en configuraciones redundantes para asegurar la continuidad del servicio en caso de fallos.

##### Facilidad de Integración:

- **Compatibilidad con Otros Servicios Cloud:** El HSS deberá ser compatible con otros servicios en la nube, facilitando su integración en un entorno híbrido o multi-cloud.

##### Escalabilidad:

- **Escalabilidad Automática:** El servicio deberá permitir la escalabilidad automática para adaptarse a cambios en la demanda de tráfico y recursos, sin afectar el rendimiento o la seguridad.

##### Detalles Técnicos Principales:

1. **Detección de intrusiones:** El servicio deberá detectar y bloquear más de 35 tipos de intrusiones diferentes.
2. **Protección de Ransomware:** El servicio deberá incluir una capacidad avanzada de prevención y mitigación de ransomware, incluyendo la implementación de políticas de



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

06

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

protección contra ransomware y la configuración de backups permanentes a nivel de hora.

3. **Análisis Inteligente de Amenazas:** El servicio deberá utilizar un motor de inteligencia artificial para el análisis y defensa contra amenazas, proporcionando una capa adicional de seguridad inteligente.
4. **Protección de Aplicaciones Web:** El servicio deberá incluir un Firewall de Aplicaciones Web (WAF) integrado para proteger contra amenazas a nivel de aplicación, como ataques XSS y CSRF.
5. **Auditoría de Logs:** El servicio deberá registrar logs detallados de eventos de ataque, control de acceso y tráfico, facilitando la auditoría y el análisis de seguridad.
6. **Captura de Paquetes de Red:** El servicio deberá incluir una herramienta para la captura y análisis de paquetes, ayudando en la localización de fallos de red y en el análisis de ataques.
7. **Control de Acceso Basado en ACL:** El servicio deberá implementar políticas de acceso basadas en listas negras y blancas, permitiendo un control detallado del acceso a la red.
8. **Protección Anti-Crawler:** El servicio deberá incluir análisis dinámico del comportamiento de los bots y protección contra rastreadores web no autorizados.
9. **Protección de Contenedores:** El servicio deberá ser capaz de detectar vulnerabilidades en imágenes de contenedores y proteger contra escapes de contenedores.
10. **Protección de Integridad de Archivos:** El servicio deberá monitorizar archivos críticos del sistema y alertar sobre modificaciones no autorizadas.
11. **Defensa contra Shell Reversa:** El servicio deberá prevenir ataques de shell reversa, protegiendo contra intentos de acceso no autorizados.
12. **Integración con Servicios de Log y Monitoreo:** El servicio deberá integrarse con servicios para la recolección y análisis de logs en tiempo real.
13. **Configuración de Alertas:** El servicio deberá permitir la configuración de notificaciones para logs de ataques y advertencias de tráfico, proporcionando alertas por correo electrónico o SMS.
14. **Políticas de Seguridad Automatizadas:** El servicio deberá facilitar la importación y aplicación automatizada de políticas de seguridad, mejorando la eficiencia de gestión.
15. **Protección en el Borde de la Red:** El servicio deberá ofrecer protección de tráfico en el borde de la red y entre VPCs, asegurando la integridad y seguridad de los datos en tránsito.
16. **Registro de Eventos:** El servicio deberá registrar logs detallados de eventos de ataque, control de acceso y tráfico.
17. **Compatibilidad con IPv6:** El servicio deberá garantizar que puede manejar y proteger el tráfico que utiliza el protocolo IPv6.
18. **Protección contra Fugas de Información:** El servicio deberá detectar y prevenir la divulgación de información sensible.
19. **Control de Acceso por Geolocalización:** El servicio deberá incluir reglas





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

personalizadas para controlar el acceso basado en la ubicación geográfica de las direcciones IP.

**20. Protección contra Manipulación de Páginas Web:** El servicio deberá ofrecer configuración de caché para páginas web estáticas con verificaciones aleatorias para detectar y prevenir la manipulación de contenido.

### III.10 DEL SERVICIO DE DDoS

- El contratista del servicio de cloud público debe ofrecer una solución en modalidad PaaS o SaaS o nativa Anti-DDoS integrada que cumpla con los siguientes requisitos mínimos:

- ✓ Protección Básica: Provisión de protección contra ataques DDoS con un límite de hasta 5 Gbps de tráfico. La solución debe mitigar automáticamente los ataques detectados sin intervención manual.
- ✓ Detección y Mitigación: La solución debe incluir monitoreo continuo y análisis en tiempo real del tráfico para detectar y mitigar anomalías asociadas con ataques DDoS.
- ✓ Reportes y Alertas: Debe proporcionar notificaciones en tiempo real y reportes detallados después de un ataque, incluyendo la descripción del ataque y las medidas mitigadoras aplicadas.
- ✓ Configuración y Gestión: La solución debe ser fácil de configurar y gestionar a través de un panel de control centralizado que permita una gestión eficiente de las políticas de defensa.
- ✓ Escalabilidad: Capacidad de escalar automáticamente para manejar incrementos en el tráfico durante un ataque, con políticas de defensa que se puedan ajustar a las necesidades del cliente.
- ✓ Compatibilidad y Rendimiento: La solución debe ser compatible con múltiples protocolos de red y tener un impacto mínimo en el rendimiento de las aplicaciones protegidas.
- ✓ Soporte Técnico y Actualizaciones: Provisión de soporte técnico 24/7 y actualizaciones regulares para mantener la efectividad de la solución Anti-DDoS.

### III.11 SERVICIO DE DESPLIEGUE DE LA SOLUCIÓN

- El contratista deberá desplegar los servicios requeridos en un máximo de 30 días calendario en coordinación con la entidad. La entidad entregará la información necesaria antes del inicio del despliegue de los servicios.
- El servicio incluye la implementación de los servidores y servicios de TI, así como la migración de aplicaciones, sin embargo, se requiere un acompañamiento durante 30 días del personal de SALUDPOL para el despliegue de sus aplicaciones.
- Las particiones de los servidores serán realizadas conforme el personal de la Oficina de Tecnología de la Información lo indique en coordinación con el contratista.
- El contratista del servicio se compromete a firmar y entregar al inicio del servicio el acuerdo de confidencialidad y cumplimiento de la Política de Seguridad de la Información del SALUDPOL.

### III.12 SOPORTE TÉCNICO y CAPACITACIÓN

#### 3.12.1 SOPORTE TÉCNICO DE LA MARCA

- Este soporte debe cumplir con las siguientes características mínimas, inspiradas en los niveles de servicio ofrecidos en el "Soporte Business" de proveedores de nubes públicas.

- ✓ Disponibilidad 24/7: El soporte debe estar disponible 24 horas al día, 7 días a la semana, incluyendo días festivos, para asegurar una respuesta continua a cualquier problema o incidente que pueda surgir.

- **Tiempo de Respuesta Prioritario:**

- ✓ Incidentes Críticos: El soporte debe proporcionar un tiempo de respuesta inicial máximo de 15 minutos para incidentes que tengan un impacto severo en la operatividad del servicio, tales como caídas completas del sistema o interrupciones significativas en los servicios críticos.
- ✓ Incidentes Importantes: Un tiempo de respuesta inicial máximo de 1 hora para incidentes que afectan significativamente la operación, como problemas que degradan el rendimiento del sistema, pero no lo detienen completamente.



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

05

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

- ✓ Incidentes Menores: Un tiempo de respuesta inicial máximo de 2 horas para problemas de menor impacto que afectan parcialmente la funcionalidad del servicio pero permiten que las operaciones continúen con algunas restricciones.
- Asistencia Técnica Especializada:
  - ✓ Acceso a ingenieros y expertos técnicos del proveedor del servicio de nube que pueden proporcionar soluciones avanzadas y soporte detallado para resolver problemas complejos, incluidos aquellos relacionados con la infraestructura y la seguridad.
- Gestión Proactiva y Mantenimiento:
  - ✓ Apoyo en la implementación de actualizaciones críticas, parches de seguridad y prácticas de mantenimiento proactivo para asegurar la continuidad del servicio y la integridad de la infraestructura. Esto incluye la supervisión y la recomendación de acciones preventivas para evitar futuros problemas.
- Consultoría en Mejores Prácticas:
  - ✓ Orientación continua sobre las mejores prácticas en la gestión y optimización de los recursos en la nube, incluyendo asesoría para la mejora de la eficiencia operativa, el rendimiento y la seguridad del servicio.
- Informes y Auditorías Detalladas:
  - ✓ Provisión de informes regulares y detallados sobre las actividades de soporte, incluyendo análisis de incidentes, resolución de problemas y recomendaciones para la prevención de futuros incidentes. También se debe incluir auditorías periódicas para asegurar el cumplimiento de los niveles de servicio acordados.
- El contratista deberá proporcionar evidencia de la activación de este soporte especializado al inicio del contrato y mantener dicha activación durante todo el periodo de vigencia del servicio. Este soporte es esencial para asegurar que los servicios gestionados en la nube pública cumplan con los más altos estándares de calidad, disponibilidad y seguridad.
- El soporte business deberá permitir reportar incidencias por un lado por parte del contratista como segundo nivel si se trata de una cuestión relacionada con la nube. Por otro lado SALUDPOL también puede reportar directamente lo que proporciona una mayor flexibilidad

### 3.12.2 SOPORTE TÉCNICO DEL CONTRATISTA

El contratista deberá proporcionar soporte técnico integral y continuo para la gestión del servicio de cloud público, abarcando aspectos clave como la administración de recursos de cómputo, políticas de backup, networking, monitoreo y seguridad. El enfoque será la gestión completa de la nube, incluyendo la protección Anti-DDoS como uno de los componentes de seguridad.

#### a. Disponibilidad del Soporte Técnico

- ✓ Soporte Remoto a Demanda: El soporte técnico debe estar disponible 24 horas al día, 7 días a la semana, para abordar cualquier problema o incidente relacionado con la infraestructura en la nube.
- ✓ Soporte Telefónico y por Correo Electrónico: Acceso a soporte a través de llamadas telefónicas y correos electrónicos para consultas urgentes y no urgentes.
- ✓ Sistema de Tickets: Una plataforma en línea para registrar y seguir el progreso de incidentes y solicitudes, accesible para el personal de SALUDPOL.

#### b. Tipos de Atención y Servicios Cubiertos

##### • Gestión de Máquinas Virtuales (VMs)

- ✓ Creación y Configuración de VMs: Asistencia en la creación y configuración de máquinas virtuales, incluyendo la instalación de sistemas operativos estándar y la configuración inicial de recursos.
- ✓ Escalado de Recursos: Apoyo en la ampliación o reducción de recursos (CPU, memoria, almacenamiento) asignados a las VMs según las necesidades operativas.





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

- ✓ Snapshots y Clonación: Realización de snapshots para la recuperación de estado y clonación de VMs para entornos de desarrollo y pruebas.

- **Políticas de Backup y Recuperación**

- ✓ Implementación de Backups: Configuración y administración de políticas de backup para asegurar la protección de los datos.
- ✓ Recuperación ante desastres: Desarrollo y ejecución de planes de recuperación ante desastres para minimizar la pérdida de datos y el tiempo de inactividad.
- ✓ Verificación de Backups: Realización de pruebas periódicas para asegurar la efectividad de los backups y su capacidad de restauración.

- **Networking y Seguridad**

- ✓ Configuración de Redes Virtuales: Asistencia en la configuración de redes virtuales, incluyendo VPCs, subredes, y direccionamiento IP.
- ✓ Gestión de Firewalls: Configuración y mantenimiento de reglas de firewall, listas de control de acceso (ACLs) y políticas de seguridad para proteger los recursos.
- ✓ VPN y Enrutamiento: Configuración y soporte para conexiones VPN y enrutamiento para asegurar la conectividad segura entre diferentes entornos.

- **Monitoreo y Alarmas**

- ✓ Configuración de alarmas: Establecimiento de alarmas para monitorear el rendimiento y la disponibilidad de recursos clave (CPU, memoria, red, etc.).
- ✓ Respuesta a Alertas: Gestión proactiva y resolución de alertas generadas por el sistema de monitoreo para prevenir o mitigar problemas.
- ✓ Análisis de Rendimiento: Evaluación y reporte periódico sobre el rendimiento de la infraestructura y los servicios, incluyendo recomendaciones para la mejora continua.

- **Administración y Mantenimiento de la Plataforma**

- ✓ Actualización de Sistemas y Aplicaciones: Coordinación y gestión de la instalación de actualizaciones y parches de sistemas operativos y aplicaciones para mantener la seguridad y la operatividad.
- ✓ Optimización de Recursos: Revisión y recomendación de estrategias para optimizar el uso de recursos en la nube, minimizando costos operativos sin comprometer el rendimiento.
- ✓ Auditorías de Seguridad: Realización de auditorías para asegurar que la infraestructura cumple con las políticas de seguridad y regulaciones vigentes.

- **Protección Anti-DDoS (Como uno de los componentes de seguridad)**

- ✓ Monitoreo de Tráfico y Mitigación de Ataques: Supervisión continua y mitigación de ataques DDoS para asegurar la disponibilidad de los servicios.
- ✓ Ajuste de Políticas de Defensa: Modificación de las políticas de defensa Anti-DDoS según sea necesario para adaptarse a nuevas amenazas.
- ✓ Reportes de Incidentes de Seguridad: Análisis detallado y reporte de los ataques DDoS y las medidas tomadas para mitigar su impacto.

- **Administración de los servicios implementados en Huawei Cloud**

- ✓ Se incluyen como parte del soporte todos los componentes implementados sobre Huawei Cloud como parte de la definición de este TDR.

- **Exclusiones del Soporte Técnico**

El soporte técnico proporcionado no incluirá:

- ✓ Gestión de Sistemas Operativos: Administración y resolución de problemas internos de los sistemas operativos dentro de las VMs.
- ✓ Aplicaciones de terceros: Instalación, configuración, y soporte para aplicaciones de terceros no incluidas en los servicios nativos de Huawei Cloud.
- ✓ Problemas Internos de la Red del Cliente: Soporte para problemas de red que ocurren dentro de la infraestructura del cliente y no en el entorno de la nube.
- ✓ Desarrollo de Software: Actividades relacionadas con el desarrollo, prueba, y mantenimiento de aplicaciones personalizadas que no forman parte de los servicios cloud.



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

04

#### c. Gestión de Tickets

El contratista debe manejar un sistema de tickets que permita registrar y gestionar tanto solicitudes de servicio (requerimientos) como incidentes.

#### d. Tiempos de Respuesta y Solución

**Tiempo de Respuesta:** El contratista debe comenzar la atención a cualquier incidente o solicitud en un máximo de 15 minutos desde el registro del mismo.

#### Tiempos de Solución por Nivel de Urgencia:

- **Alta Urgencia:** Máximo 1 hora para resolver incidentes que afectan críticamente la operación de los servicios. Son incidentes que necesitan un tratamiento especial para la organización por su alto impacto; su inatención inmediata afecta o podría afectar significativamente la operación de algún componente de la infraestructura tecnológica.
- **Media Urgencia:** Máximo 3 horas para incidentes que tienen un impacto moderado en los servicios. Son incidentes con un tiempo de atención intermedio; su inatención afecta o podría afectar moderadamente a la operación de algún componente de la infraestructura tecnológica.
- **Baja Urgencia:** Máximo 4 horas para incidentes de impacto leve. Son incidentes con un tiempo de atención menor; su inatención afecta o podría afectar levemente a la operación de algún componente de la infraestructura tecnológica.

La clasificación de la urgencia la realizará el personal del SALUDPOL en el registro del incidente.

El personal del SALUDPOL verificará que se haya dado la solución al incidente antes de aceptar el fin del tiempo de solución.

#### e. Gestión de Incidentes

- **Sistema de Gestión de Incidencias:** El contratista debe proporcionar una plataforma web para la gestión de incidencias, problemas y solicitudes.
- **Automatización:** Utilización de herramientas para la automatización de la priorización y el seguimiento de incidentes.

#### f. Medios de Comunicación para el Registro de Incidentes

- **Sistema de Tickets:** Principal medio para el registro y seguimiento de incidentes.
- **Teléfono y Correo Electrónico:** Canales adicionales para asegurar la comunicación efectiva y rápida.

#### 3.12.2 CAPACITACIÓN

- ✓ El contratista debe incluir un curso de capacitación oficial del proveedor de nube para la Gestión de los Servicios requeridos ofertados de 25 horas como mínimo para 12 personas indicadas por SALUDPOL.
- ✓ El contratista al finalizar el curso deberá emitir un certificado o constancia para las 12 personas que recibieron la capacitación.
- ✓ El contratista debe incluir los voucher para el examen de certificación oficial una vez culminado el curso.

#### III.13 CERTIFICADOS DE SEGURIDAD DE LA INFORMACIÓN DE LA PLATAFORMA CLOUD

- ISO 27001:2013
- Classified Cybersecurity Protection of China's Ministry of Public Security
- ISO 27017:2015
- Singapore MTCS Level 3 Certification
- ISO 20000-1:2011
- SOC audit
- ISO 27018:2014
- PCI DSS Certification





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

- ISO 22301:2012
- CSA STAR Gold Certification
- Gold O&M (TRUCS)
- Certification for the Capability of Protecting Cloud Service User Data (TRUCS)
- ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT)
- TRUCS (Trusted Cloud Service)
- Cloud Service Security Certification - Cyberspace Administration of China (CAC)
- International Common Criteria EAL 3+ Certification
- ISO 27018:2014
- ISO 29151:2017
- ISO 27701:2019
- BS 10012:2017

#### IV. CONDICIONES ADMINISTRATIVAS MÍNIMAS:

##### IV.1 PLAZO DE LA PRESTACIÓN

- El servicio de hosting será brindado por 365 días calendario, contados a partir del día siguiente de suscrita el Acta de implementación, fecha en que el pago será contabilizado.
- El Acta de implementación debe contener la siguiente información:
  - ✓ Características técnicas y configuraciones de los servidores implementados.
  - ✓ Documento firmado de confidencialidad por parte del contratista.
  - ✓ Lista de contactos para soporte del contratista. Se precisa que el servicio de soporte deberá tener la disponibilidad de 24 horas x 7 días a la semana, el tiempo que dure el contrato del servicio. Este deberá ser por los canales de atención tales como correo, número de celular y/o 0800
- En caso de falla de algún componente del servicio, el contratista deberá proceder con la reparación y/o reemplazo sin costo alguno para la entidad; asegurando la continuidad del servicio de hosting.
- El plazo máximo para la implementación del servicio será de treinta (30) días calendario, contados desde el día siguiente de la suscripción del contrato.
- El plazo de la prestación se tomará como fecha de inicio al día siguiente de suscrito Acta de Implementación.

##### IV.2 DEL PAGO

- El postor deberá ingresar la facturación e informe en forma mensual hasta los primeros quince (15) días calendarios de cada mes y será ingresada en formato físico vía mesa de partes en SALUDPOL.
- Para el pago del primer mes, el contratista deberá adjuntar a su facturación el "Acta de implementación del servicio", el "Informe mensual del estado del servicio" y "Facturación".
- Para los pagos del segundo al doceavo mes, el contratista deberá adjuntar a su facturación el informe mensual del estado del servicio.

##### IV.3 DE LA CONFORMIDAD

- La implementación del servicio contará con el "Acta de implementación", la cual será firmada por el responsable de la Oficina de Tecnología de la Información de SALUDPOL una vez finalizadas las actividades correspondientes y activadas el servicio.
- Las conformidades del servicio serán emitidas mensualmente por el responsable de la Oficina de Tecnología de la Información de SALUDPOL, previa recepción por parte del contratista del "Informe mensual del estado del servicio", con la siguiente información:
  - ✓ Reporte de Actividad Mensual: Un resumen de todos los tickets gestionados, incluyendo detalles de cada incidente y solicitud, tiempos de respuesta y solución, y análisis de tendencias.
  - ✓ Inventario y Diagramas: Un informe mensual que incluya un inventario detallado de todos los recursos en la nube y diagramas actualizados de la arquitectura de la infraestructura, reflejando cualquier cambio realizado durante el mes.
  - ✓ Informe de Rendimiento de Recursos.
  - ✓ Análisis de Seguridad: Resumen de las actividades de seguridad, incluyendo incidentes de seguridad gestionados, estado de las políticas de firewall, y análisis de amenazas detectadas.

##### IV.4 ACTIVIDADES

###### JEFE O LÍDER:

Análisis de requisitos: El líder de proyecto debe comprender los requisitos del cliente y definir claramente las necesidades y objetivos del proyecto.

Planificación del proyecto: El líder de proyecto debe desarrollar un plan detallado que incluya la configuración del servidor, la migración de datos, las pruebas de rendimiento, la





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

0

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

implementación de medidas de seguridad y el cronograma de actividades.

**Coordinación y comunicación:** Actuando como punto de contacto principal, el líder de proyecto coordinará y mantendrá una comunicación efectiva entre el proveedor de servicios de alojamiento y el cliente.

**Supervisión del proyecto:** El líder de proyecto será responsable de supervisar todo el proceso de implementación, asegurándose de que se cumplan los plazos, se alcancen los objetivos y se resuelvan los problemas que puedan surgir durante el proceso.

#### IMPLEMENTADOR:

**Configuración de servidores:** El implementador será responsable de configurar los servidores según los requisitos del cliente, instalando el sistema operativo, configurando el software y optimizando el rendimiento.

**Migración de datos:** El implementador deberá planificar y llevar a cabo la migración de los datos existentes al nuevo servicio de alojamiento de servidores, asegurándose de que se realice de manera segura y sin interrupciones.

**Pruebas y verificación:** El implementador realizará pruebas exhaustivas para garantizar que el servicio de alojamiento de servidores funcione correctamente. Esto puede incluir pruebas de rendimiento, pruebas de carga, pruebas de seguridad, etc.

**Capacitación y documentación:** El implementador proporcionará capacitación al personal del cliente en el uso y administración del servicio de alojamiento de servidores, y generará documentación técnica detallada para su referencia.

#### IV.5 DE LAS PENALIDADES

Se aplicará las penalidades según lo establecido en el Reglamento de la Ley de Contrataciones del Estado del artículo 162.

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.

#### IV.6 OTRAS PENALIDADES

Se aplicarán las penalidades según lo establecido en el Reglamento de la Ley de Contrataciones del Estado del artículo 163.

Podrán aplicarse otras penalidades, siempre y cuando sean objetivas, razonables y congruentes con el objeto de la convocatoria, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del servicio contratado.

La Oficina de Tecnología de la Información, en base a la ejecución de actividades de control informará a la Oficina de Administración si el contratista contratado incurre en una penalidad, a fin de que se ejecute la penalidad correspondiente.

Cuando se llegue a cubrir el monto máximo de la penalidad (10%), SALUDPOL podrá resolver el contrato por incumplimiento en caso lo decida.



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

Las otras penalidades son las siguientes:

Supuesto de aplicación de penalidad	Forma de cálculo Rango de Interrupción del servicio	Forma de cálculo % Deducible de la facturación mensual	Procedimiento
Disponibilidad del servicio mensual (99.9%)	> 44 minutos ≤ 90 minutos	2.5%	Para efectos del cálculo de la penalidad se acumularán los minutos en los que el servicio se haya interrumpido en el mes, contados desde que ha sido reportado a la mesa de ayuda por Teléfono o por correo electrónico o por sistema de ticket hasta la disponibilidad total del servicio.
	> 90 minutos ≤ 120 minutos	5%	
	> 120 minutos	10%	

Nota: El rango de interrupción es mensual, y en el mes se considera 30 días calendario.

Supuesto de aplicación de penalidad	Forma de cálculo Rango de respuesta a requerimientos	Forma de cálculo % Deducible de la facturación mensual	Procedimiento
Tiempo de respuesta al requerimiento de soporte técnico por vez (Máximo).	> 2 horas ≤ 3 horas	1%	Se acumularán los minutos contados desde que ha sido solicitado el requerimiento a la mesa de ayuda por Teléfono o por correo electrónico o por sistema de ticket hasta la respuesta de atención del requerimiento.
	> 3 horas ≤ 4 horas	5%	
	> 4 horas	8%	

Nota: El rango de respuesta ante requerimientos es contabilizado por cada ticket o correo enviado.

#### IV.7 SISTEMA DE CONTRATACIÓN:

A suma Alzada.

V.

#### SEGURIDAD EN EL TRABAJO

##### V.1 SEGURO COMPLEMENTARIO DE TRABAJO DE RIESGO

Los trabajadores del contratista deberán estar sujetos al Seguro Complementario de Trabajo de Riesgo.

Para lo cual el contratista deberá presentar el Seguro Complementario de Trabajo de Riesgo (SCTR) vigente del personal que trabajará en la prestación. El SCTR deberá ser presentado al inicio del servicio.

##### V.2 EQUIPOS DE PROTECCIÓN PERSONAL (EPP)

El Contratista deberá proporcionar los correspondientes equipos de protección personal (EPP) a su personal de acuerdo a la especialidad. Se entiende que el uso de dichos equipos es de carácter obligatorio mientras se encuentre laborando en las instalaciones del SALUDPOL.

##### V.3 SEGURIDAD Y SALUD EN EL TRABAJO (SST)

Se pone en conocimiento los "Lineamientos para la prevención del contagio del covid-19 durante la permanencia al interior del fondo de aseguramiento en salud de la policía nacional del Perú – SALUDPOL"



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

02

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

<https://www.gob.pe/institucion/saludpol/normas-legales/826958-065-2020-in-saludpol-ag>

#### V.4 PROTOCOLOS SANITARIOS

El Contratista se compromete a cumplir y respetar cada una de las medidas de seguridad previstas en el protocolo de SALUDPOL, el que será puesto en conocimiento de sus trabajadores al inicio de la prestación; para cuyo efecto SALUDPOL, a la firma del Contrato, cumplirá con hacer entrega de una copia legible del mismo. El Contratista deberá asegurar en todo momento que el personal que realiza el desarrollo de la prestación en las instalaciones de SALUDPOL cumpla con las disposiciones señaladas en los párrafos anteriores.

#### VI. RESPONSABILIDAD POR VICIOS OCULTOS

El plazo máximo de responsabilidad del contratista por la calidad ofrecida y por los vicios ocultos será de 365 días contados a partir de la conformidad del servicio.

#### VII. CONFIDENCIALIDAD

El contratista se compromete a no revelar, comentar suministrar o transferir de cualquier forma a terceros, información que hubiere recibido directa o indirectamente o que hubiese generado como parte del servicio.

El incumplimiento de esta obligación, dará lugar a la resolución inmediata del contrato perfeccionado mediante orden de servicio.

#### VIII. NORMA ANTICORRUPCIÓN

El contratista / contratista acepta expresamente que no llevará a cabo, acciones que están prohibidas por las leyes locales y otras leyes anticorrupción. Sin limitar lo anterior, el contratista /contratista se obliga a no efectuar ningún pago, ni ofrecerá ni trasferirá algo de valor, a un establecido de manera que pudiere violar leyes locales u otras anticorrupción, sin restricción alguna.

En forma especial, el contratista / contratista declara con carácter de declaración jurada que no se encuentra inmerso en algún proceso de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma del mismo en la orden de servicio de la que estos términos de referencia forman parte integrante.

#### IX. CLÁUSULA ANTICORRUPCIÓN

El contratista, no debe ofrecer negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general o cualquier beneficio o incentivo ilegal en relación al contrato, que pueda construir incumplimiento de la Ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o través de socios, integrantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia o a lo establecido en el art. 11 de la ley de contrataciones del estado, ley N° 30225, los artículos 7 de su reglamento aprobado mediante Decreto Supremo N° 344-2018-EF.

Así mismo el contratista se obliga a conducirse en todo momento, durante la ejecución de la orden de servicio 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 personal vinculados en virtud a lo establecido en los artículos antes citados de la Ley de Contrataciones del Estado y su Reglamento.

#### X. REQUISITOS DE CALIFICACIÓN

Los requisitos de calificación son los siguientes:

##### B CAPACIDAD TÉCNICA Y PROFESIONAL

##### B.3. CALIFICACIONES DEL PERSONAL CLAVE

##### B.3.1 FORMACIÓN ACADÉMICA

Requisitos:

##### JEFE O LÍDER DEL PROYECTO

Titulado profesional universitario en ingeniería electrónica, telecomunicaciones, computación, informática, industrial o sistemas.

##### IMPLEMENTADOR

Bachiller o profesional titulado universitario en ingeniería electrónica, telecomunicaciones, informática, computación y/o sistemas.





PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

**Acreditación:**

El BACHILLER O TÍTULO PROFESIONAL 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 : <http://www.titulosinstitutos.pe/>, según corresponda.

En caso el BACHILLER O 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.

**B.4 EXPERIENCIA DEL PERSONAL CLAVE****Requisitos:****Jefe o Líder del Proyecto**

Tres (03) años de experiencia realizando funciones como jefe o Líder de proyectos y/o coordinador en servicios de implementación de proyectos de alquiler y/o hosting de servidores.

**IMPLEMENTADOR**

Tres (03) años de experiencia liderando o implementando soluciones de virtualización de servidores, implementación de servicios en nube, almacenamiento, redes y respaldo.

De presentarse experiencia ejecutada paralelamente (traslape), 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.

**D EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD****Requisitos:**

El postor debe acreditar un monto facturado acumulado equivalente a S/ 600,000.00 (SEISCIENTOS 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.



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

01

#### "Decenio de la Igualdad de Oportunidades para mujeres y hombres"

En el caso de postores que declaran en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/45,000.00 (CUARENTA Y CINCO MIL 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.

Se consideran servicios similares a los siguientes:

- ✓ Servicio de housing o servicio de procesamiento de datos de producción y/o de contingencia, o servicio de plataforma y/o infraestructura en la nube.
- ✓ Servicio de Data Center (Housing y/o Hosting)
- ✓ Servicio de Housing de infraestructura computacional
- ✓ Servicio de Operación y Administración del Centro de Cómputo Principal y Centro de Computo de Contingencia.
- ✓ Servicio de Cloud Hosting
- ✓ Servicio de Infraestructura en la Nube
- ✓ Servicio de alojamiento en nube privada de los sistemas de información
- ✓ Servicio de Gestión de TI en Nube
- ✓ Servicio de Ciberseguridad en Nube
- ✓ Servicio de administración o gestión en Nube
- ✓ Bigdata y Analítica en Nube (AWS, Huawei Cloud o Azure)

#### 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<sup>1</sup>, correspondientes a un máximo de veinte (20) contrataciones.

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 sólo 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

En el caso de servicios de ejecución periódica o continuada, sólo 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.

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.

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 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

<sup>1</sup> 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 si se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".



PERÚ

Ministerio del Interior

Fondo de Aseguramiento en Salud  
de la Policía Nacional del Perú - SALUDPOLOficina de Tecnología  
de la Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"

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, sólo 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 documentalmente, y no mediante declaración jurada.*