EsSalud

GERENCIA CENTRAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Sub Gerencia de Comunicaciones

TÉRMINOS DE REFERENCIA

CONTRATACIÓN DEL SERVICIO DE SEGURIDAD GESTIONADA PARA ESSALUD

V°B°
Ing. Ricardo Sandoval C.
Sub Gerente (e)
SUB GERENCIA DE COMUNICACIONES GP-GCTIC
ESSALUD

LIMA, 2021

ÍNDICE

SUB GERENCIA DE COMUNICACIONES GP-GTIC V°B° Ing. Ricardo Sierras C. Sub Gerente (e) ESSALUD

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

GERENCIA DE COMUNICACIONES GP-GCTIC
V°B°
Ing. Ricardo Silvicas C.
Sub Gerente (e)
ESSALUD

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

1. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del Servicio de Seguridad Gestionada para EsSalud.

2. FINALIDAD PÚBLICA

Mejorar las capacidades de infraestructura y gestión de la seguridad informática para EsSalud a nivel nacional, garantizando la protección a la red de datos institucional contra los ataques internos y externos que puedan poner en riesgo la confidencialidad, disponibilidad de información y acceso a las aplicaciones críticas de forma local o remota, con el control de políticas de seguridad y accesos configurados para un eficiente uso de los recursos y ancho de banda de la red de EsSalud.

3. ANTECEDENTES

3.1 EsSalud es una institución de Seguridad Social de Salud que persigue el bienestar de los asegurados y su acceso oportuno a las prestaciones de salud, económicas y sociales, integrales y de calidad, mediante una gestión transparente y eficiente. En tal sentido, es función de la Gerencia de Producción de la GCTIC, asegurar el correcto funcionamiento y disponibilidad de la infraestructura de seguridad de Essalud, sistemas y servicios informáticos instalados en el Centro de Datos de la Sede Central, basados en buenas prácticas en seguridad de información y continuidad operativa, así como la adecuada gestión de proveedores de servicios TI.

3.2 En cumplimiento del Decreto Supremo Nº 004-2013-PCM, respecto a desarrollar y emplear intensivamente las tecnologías de información y comunicación (TIC) con la aplicación de buenas prácticas en seguridad de información exigidos en la "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición"; la Subgerencia de Comunicaciones a través de la Gerencia de Producción de la GCTIC, definió una arquitectura tecnológica de seguridad informática para la contratación de un servicio con dicha plataforma por un periodo de 12 meses que incluiría el soporte de nivel 3 y 4. La misma que actualmente está implementada y es gestionada por los especialistas de seguridad de la Sub Gerencia de Comunicaciones de la GCTIC de EsSalud.

3.2 A través del servicio contratado para la seguridad informática, la Subgerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, cuenta con una infraestructura tecnológica de seguridad perimetral que permite asegurar la protección de la red de datos y sistemas de información de ESSALUD a nivel nacional, ante posibles ataques maliciosos que puedan poner en riesgo la seguridad de los accesos, así como la integridad y disponibilidad de la información institucional.

3.3 Por el impacto que ha tenido la infraestructura actual de seguridad informática a nivel de performance, como producto del estado de emergencia sanitaria, se ha visto conveniente considerar el fortalecimiento de las capacidades de hardware a la infraestructura de seguridad requerida para el servicio, con el propósito de responder a una alta demanda de requerimientos de accesos remotos y procesamiento de reglas y/o políticas de seguridad, para el acceso a los servicios que brinda EsSalud a su población de asegurados.

www.essalud.gob.pe

Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

4. OBJETIVOS DE LA CONTRATACIÓN

4.1 Objetivo General

Contratar los servicios de una persona jurídica especializada en la implementación, configuración, gestión y resolución de problemas de plataforma de seguridad, para realizar un Servicio de Seguridad Gestionada para EsSalud a nivel nacional.

4.2 Objetivos Específicos

- Instalar y configurar la solución de seguridad propuesta.
- Integrar el equipamiento existente de EsSalud a la solución propuesta.
- Migración de las políticas y/o reglas de seguridad a la solución propuesta.
- Estabilizar las funcionalidades de la Infraestructura instalada.
- Brindar soporte y gestión de los sistemas de Seguridad Perimetral, Seguridad Nacional y Servidores.
- Garantizar la protección a la red de datos institucional contra los ataques internos y externos que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de información y servicios críticos que se acceden de forma local y/o remota.
- Optimizar oportunamente los parámetros de configuración de la solución.
- Atender eficientemente las solicitudes de requerimientos de soporte e incidencias bajo una metodología y nivel de SLA.
- Asegurar una adecuada performance de la solución propuesta.
- Mantener una disponibilidad de 24x7x365 de la solución instalada.

5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO A CONTRATAR

El alcance del servicio a contratar, comprende la siguiente Plataforma de Seguridad.

5.1 Prestación Principal

La contratación tiene un alcance que incluye el servicio de seguridad gestionada total para la plataforma de Seguridad Perimetral, Seguridad Nacional y Servidores para EsSalud.

El contratista proporcionará un servicio de seguridad gestionada que incluya dentro de sus componentes el equipamiento necesario de acuerdo a lo detallado en el presente documento, así como el soporte gestionado del equipamiento provisto y de los equipos de seguridad de la institución.

La implementación de la plataforma de seguridad en su integridad es responsabilidad del contratista, además debe facilitar los componentes nuevos en año de fabricación y vigentes tecnológicamente que sean necesarios para atender las necesidades que se describen en los presentes términos de referencia.

El contratista para cumplir con el servicio mínimo debe utilizar las siguientes herramientas:

- Equipos de Seguridad perimetral, Seguridad Nacional y Seguridad de Servidores.
- Administración centralizada de firewalls.
- Plataforma de Seguridad para Correo Electrónico

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

- Plataforma de Protección de infraestructura DNS.
- Plataforma de detección, investigación y respuesta de endpoints y analítica de comportamiento de la red.
- Switches para conectividad de plataforma de seguridad.
- Implementación solución integral de seguridad y conectividad propuesta.
- Seguridad gestionada de solución ofertada
- Seguridad gestionada de equipos de seguridad de Essalud.

Es de indicar, que la totalidad de los componentes o equipos para el servicio pertenecen al contratista durante la ejecución del servicio y los mantenimientos de todos los componentes o equipos corre a cuenta del contratista, así como mantener la correcta operatividad de los mismos. Adicionando que, en el caso de los equipos estos deben tener la garantía del fabricante por el plazo de ejecución del servicio.

El contratista debe realizar todas las gestiones y configuraciones necesarias para la integración de toda la plataforma ofertada con los equipos de la entidad. El contratista será encargado de configurar lo necesario en la plataforma a fin de garantizar las mayores funcionalidades del servicio, debe incluir las mejores prácticas de configuración y diseño para la implementación de los equipos ofertados.

Para garantizar un mínimo impacto en la continuidad de las operaciones del Servicio de Seguridad Gestionada a brindar, el contratista debe seguir sus propios procedimientos y las recomendaciones de la marca o fabricante.

Durante la implementación y ejecución del servicio, todas las migraciones, integraciones y/o actualizaciones a la plataforma del presente servicio que el Contratista requiera realizar, se deben llevar a cabo sin costo para ESSALUD. La realización de estos trabajos será coordinada y autorizadas por el personal de la Sub Gerencia de Comunicaciones de la GCTIC responsable de la supervisión.

La solución ofertada deberá de ser integrada a los equipos de propiedad de Essalud detallada a continuación:

Item	Marca	Modelo / N-Serie	Versión S.O.	Cantidad	Garantía
1	CISCO	Firepower 2130 N/S: JMX2342Z09H	v6.4.0.4	1	12/12/2022
2	F5	F5-BIG-AFM-I2800 BIG-IP N/S: f5-vkgn-xpjv	BIG-IP 14.1.0 Build 0.0.116 Final	1	12/05/2022
3	F5	F5-BIG-AFM-I2800 BIG-IP N/S: f5-iyug-txze	BIG-IP 14.1.0 Build 0.0.116 Final	1	12/10/2022

Tabla N° 1. Equipamiento de seguridad (Propiedad EsSalud).

Las características detalladas a continuación incluyen las características del servicio solicitado y los componentes que el postor debe proveer para llevar a cabo su ejecución.

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

No se aceptarán en la ejecución del servicio los componentes reciclados, reensamblados o reacondicionados, o su equivalente comercial como por ejemplo aquellos que tenga la denominación "refurbished", "remarketing".

Los componentes del servicio no deberán contar, a la fecha de presentación de propuestas, con anuncio de Fin de Ciclo Vital (End of Life) del fabricante con el fin de asegurar un mayor periodo de vigencia tecnológica.

5.1.1 Características técnicas mínimas del Servicio

- El propósito del presente documento es establecer un estándar de calidad, funciones y características para el servicio. Es responsabilidad del contratista asegurar que la solución propuesta cumpla lo requerido en las características mínimas requeridas.
- El contratista debe contar con un sistema de gestión a través de una ventanilla única y/o Centro de atención de averías, es decir un único punto de contacto para ESSALUD para el reporte de fallas, atención de nuevas solicitudes o tratamiento de reclamos en un formato 24x7x365.
- El tiempo de respuesta máximo por parte del contratista para la atención de un problema (avería o incidente) será de treinta (30) minutos, contados desde que ESSALUD reporte el incidente por medio de una llamada telefónica o un correo electrónico.
- El contratista debe informar los puntos de contacto directo que ESSALUD podrá emplear para la gestión adecuada del servicio.
- El tiempo máximo de subsanación de una avería a satisfacción de ESSALUD contado desde la llamada telefónica o él envió del correo electrónico, que comprende desde el reporte de la incidencia por la entidad a la ventanilla del contratista el cuál asignará un ticket de atención, será según lo siguiente:
  - Para subsanación de averías que corresponden a una atención remota los tiempos máximos de atención serán de 4 Horas y para una atención presencial los tiempos máximos de atención serán de 8 Horas.
  - En circunstancias donde la plataforma que soporta el servicio ofrecido esté comprometido para su correcto funcionamiento, tales como averías de hardware o aquellas donde los tiempos de diagnóstico o reemplazo dependan de terceros (por ejemplo, escalamiento de soporte a la marca o garantía del fabricante), el contratista, en un plazo no mayor de 4 horas luego del diagnóstico del primer nivel de soporte[1], deberá entregar e implementar sin costo para ESSALUD, los equipos y/o componentes requeridos con similares o mayores características para la continuidad de los servicios ofrecidos, hasta que concluya con la solución de la avería de manera definitiva.
- ESSALUD brindará todas las facilidades técnicas para que la resolución de averías concluya de manera efectiva y en el menor tiempo posible. Se podrá habilitar acceso remoto a los equipos para su diagnóstico y la ejecución de herramientas de diagnóstico, identificación y ejecución de programas para solución de problemas.

GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD

5.1.1.1 Servicio de Seguridad Perimetral

[1] Absolución de Consultas y Observaciones N° 169, ITALTEL PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

5.1.1.1.1 Consideraciones Generales

a. El contratista deberá facilitar como parte del servicio una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
b. Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance o chassis y que deban ser del mismo fabricante. No se aceptarán servidores o máquinas virtuales
c. La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad una solución redundante de por lo menos 2 (dos) appliances o chassis tanto externos como internos.
d. El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 3 (tres) años en la modalidad 7x24x365, la misma que iniciará luego de la firma del Acta de aprobación de la Implementación de la Solución Anexo "C". Dicha vigencia será verificada a través de una declaración jurada del Contratista.[2]
e. En relación al RMA, el CONTRATISTA por medio de un servicio del fabricante (el cual deberá contar con depósito de partes o equipos completos con presencia local en el país), ofrezca mínimamente reemplazo de partes en un tiempo máximo de 24 horas, para garantizar el funcionamiento de la solución en caso no haya afectación de servicios. En caso que el/los equipos provoquen degradación o pérdida del servicio contratado, el tiempo máximo de reemplazo deberá ser de 4 horas [3][4][5][6][7].
f. El contratista deberá proveer una solución que sea miembro activo de la organización global conocida como la "Alianza de Ciberamenazas" la cual garantiza un intercambio de inteligencia de amenazas entre terceros para acelerar la detección y mitigación de ataques globales.
g. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support (Fin de Vida o Fin de Ventas o Fin de Soporte) y no deberán tener reemplazo tecnológico anunciado. Se deberá adjuntar el link público de los equipos propuestos donde se verifique que los modelos propuestos no están en ese listado o sustentado mediante carta del fabricante dirigido al proceso.
h. Los equipos deben poder ser administrados desde una plataforma centralizada de gestión.
i. Los equipos deben poder seguir siendo administrados de manera independiente aun si pierden la comunicación con la plataforma de gestión centralizada. Los equipos deben permitir al menos las siguientes acciones a través de su propia

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Serrano C. Sub Gerente (e) ESSALUD

[2] Absolución de Consultas y Observaciones N° 93, VERIFICACIÓN Y CONTROL DE DATOS SAC
[3] Absolución de Consultas y Observaciones N° 18, N° 35, GRUPO ELECTRODATA SAC
[4] Absolución de Consultas y Observaciones N° 98, VERIFICACIÓN Y CONTROL DE DATOS SAC
[5] Absolución de Consultas y Observaciones N° 103, VERIFICACIÓN Y CONTROL DE DATOS SAC
[6] Absolución de Consultas y Observaciones N° 145, INDRA PERÚ SAC
[7] Absolución de Consultas y Observaciones N° 181, ITALTEL PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

GUI: crear/modificar/borrar objetos y políticas, reglas de calidad de servicio, monitoreo de estado general y de seguridad.

5.1.1.1.2 Performance

- Los firewalls perimetrales deben soportar un throughput de 10 Gbps. Se deberá considerar tráfico real para el dimensionamiento de los equipos, o mediciones con tráfico HTTP de 64 KB o transacciones usando tráfico empresarial mixto (Enterprise Mix)[8] [9] [10] [11]. No serán permitidas mediciones bajo condiciones ideales o tráfico UDP. Dicha medición debe contemplar las siguientes funcionalidades habilitadas simultáneamente:
    - Firewall (capa4).
    - Control de aplicaciones.
    - Sistema de Prevención de Intrusos (IPS).
    - Antivirus o Antimalware.
    - Filtrado de comando y control, antibot o antispyware.
    - Logging Activo.
    - Sandbox.
- El postor deberá sustentar el cumplimiento del performance con información pública del fabricante o mediante carta del fabricante dirigido al proceso.

5.1.1.1.3 Conexiones Simultaneas

a. Los firewalls perimetrales deberán soportar como mínimo 12 millones de sesiones concurrentes medidas utilizando tráfico TCP.
b. Deberán soportar 300 mil conexiones por segundo.

5.1.1.1.4 Interfaces de Cobre

a. Los firewalls perimetrales e internos deberán contar con un mínimo de 4 interfaces de cobre (formato RJ-45). Estas interfaces no deberán ser utilizadas para funciones de alta disponibilidad u otras funciones de gestión.

5.1.1.1.5 Interfaces fibra óptica

a. Los firewalls perimetrales deberán contar con un mínimo de 8 interfaces ópticos de 10gb (SFP+). Estas interfaces deberán también trabajar a 1Gbps.
b. Los firewalls perimetrales deben poder utilizar una interfaz de 10GB adicional para la sincronización de sesiones del clúster. Se deben incluir los transceivers y cables necesarios.
c. Todas las interfaces requeridas (1 Gbps y 10 Gbps) deberán incluir los transceivers para fibra multimodo.

[8] Absolución de Consultas y Observaciones N° 19, GRUPO ELECTRODATA SAC
[9] Absolución de Consultas y Observaciones N° 95, VERIFICACIÓN Y CONTROL DE DATOS SAC
[10] Absolución de Consultas y Observaciones N° 142 y N° 148, INDRA PERÚ SAC
[11] Absolución de Consultas y Observaciones N° 176, ITALTEL PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

5.1.1.1.6 Características de Hardware

a. Cada equipo debe contar con una interfaz de red 10/100/1000 dedicada para administración.
b. Cada equipo debe poder ser montado en un rack de 19''. Debe incluir todos los elementos necesarios para su montaje.
c. Los equipos deben soportar sistemas virtuales, entornos o contextos virtuales. Debe contar con licenciamiento mínimo para 5 entornos virtuales.

5.1.1.1.7 Características de Red

a. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames (opcional), sub-interfaces ethernet lógicas, NAT de origen y destino.
b. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);
c. El dispositivo debe soporta direccionamiento IPv6 basado: direccionamiento en interfaces; IPv6 rutas estáticas; IPv6 lista de acceso o regla de acceso. Debe contar con alguna certificación para IPv6.
d. El dispositivo debe soportar la operación en modo transparente y enrutado; además en modos debe de soportar IPv6 para futuras implementaciones.
e. El dispositivo debe tener la capacidad de soportar el protocolo Netflow o similares para poder tener información de seguridad y troubleshooting.
f. Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de instancias o dominios virtuales:
    - Modo Sniffer o Pasiva, para inspección vía puerto espejo del tráfico de datos de la red;
    - Modo Capa – 2 (L2) o Bridge, para inspección de datos en línea o dentro de un mismo segmento de red
    - Modo Capa – 3 (L3) o Routed, para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default gateway de las redes protegidas;
    - Modo Transparente o Inline, para poder inspeccionar datos en línea y tener visibilidad del control de tráfico a nivel de aplicación sobre 2 puertos en modo bridge/transparente.
g. Modo mixto de trabajo Sniffer o Pasiva, Transparente, L2 y L3 simultáneamente en diferentes interfaces físicas del mismo equipo.

5.1.1.1.8 Alta Disponibilidad

GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siccha C. Sub Gerente (e) SUB GERENCIA DE REDES Y SEGURIDAD - ESSALUD

www.essalud.gob.pe

Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

a. Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo o modo, cluster con despliegues de los equipos en modo capa 3 (L3)
b. La configuración en alta disponibilidad debe sincronizar:
   - Sesiones;
   - Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red;
   - Asociaciones de Seguridad de las VPNs;
   - El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.

5.1.1.1.9 Características de Firewall

a. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, grupos y categorías de aplicaciones.
b. Control, inspección y descifrado de SSL o TLS por política para tráfico de entrada (Inbound) y salida (Outbound).
c. Debe soportar inspección de tráfico encriptado con TLS 1.2 y de manera opcional TLS 1.3.
d. Soportar el control de tiempo sobre las políticas de control de acceso con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
e. El equipo debe incorporar herramientas para troubleshooting avanzado como la capacidad de visualizar la trazabilidad de los paquetes y realizar capturas de tráfico en tiempo real desde el propio equipo.
f. Debe contar con mecanismos que faciliten la optimización de reglas de seguridad:
   - Mostrar la cantidad de veces que una política ha sido aplicada para medir la eficiencia de la misma
   - Mostrar a través de un filtro, las reglas de seguridad que no han sido utilizadas, a fin de tener una depuración de reglas sin usar.

5.1.1.1.10 Control de Aplicaciones

a. Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
b. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares, firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo.
c. Debe ser capaz de inspeccionar aplicaciones que viajen por tráfico cifrado como HTTPS y de manera opcional SSH.
d. Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la entidad.

GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD

e. Debe ser posible la creación de grupos de aplicaciones basados en características de las aplicaciones como: • Tecnología cliente-servidor. • Nivel de riesgo de las aplicaciones. • Categoría de aplicaciones. f. Debe contar y tener la funcionalidad de filtro URL basado en una base de datos de URLs en cache en el equipo o en la nube del fabricante, evitando retrasos de comunicación/validación de direcciones URL. Esta funcionalidad debe funcionar al menos durante el periodo del servicio[12].
5.1.1.1.11 Prevención de Amenazas
a. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Anti-malware de red, Antibot, DNS Filtering o DNS Sinkhole integrados en el propio appliance. b. El equipo debe proteger de amenazas avanzadas que utilizan conexiones DNS, de manera que permita filtrar las consultas de DNS de los hosts para bloquear conexiones hacia sitios maliciosos, conexiones de botnet, ya sea en base a categorías o firmas. c. La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca. d. Las firmas de IPS deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo. e. Debe soportar granularidad en las políticas de IPS, Antimalware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, aplicación, usuario y grupo de usuarios y la combinación de todos esos ítems. f. Permitir el bloqueo de malware por lo menos en los siguientes protocolos: HTTP, IMAP, FTP, SMB, SMTP y POP3 g. Identificar y bloquear comunicaciones con amenazas clasificadas como atacantes, Bots, Comando y Control, Exploitkit, Malware, OpenProxy, OpenRelay, Phishing, SPAM y Nodos de salida de TOR.
5.1.1.1.12 Prevención de amenazas desconocidas

SUB GERENCIA DE COMUNICACIONES GPGCTIC VºBº Ing. Ricardo Serrate C. Sub Gerente (e) ESSALUD

[12] Absolución de Consultas y Observaciones N° 26, GRUPO ELECTRODATA SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

a. Poseer la capacidad de análisis de amenazas no conocidas.
b. La plataforma de seguridad de sandboxing debe ser basada en una plataforma on-premise o local con soporte de Inteligencia de Amenazas compartidas En caso de caída del equipo de sandbox local, los equipos firewall deben poder enviar los archivos a un servicio de sandboxing en nube del mismo fabricante.
c. Debe contar, de manera opcional con una plataforma de API para poder integrarse a herramientas de terceros.
d. El equipo de Sandboxing tenga la capacidad de explotar el malware en un ambiente controlado (VM) con sistema operativo Windows 7, Windows 8, Windows 10 , MacOS o Android[13].
e. Debe soportar el monitoreo de archivos transferidos por internet (FTP, HTTP, SMTP, IMAP y POP3) como también archivos transferidos internamente en los servidores de archivos usando SMB.
f. Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, archivos comprimidos (ZIP, TAR) archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), en el ambiente controlado.
g. El firewall propuesto debe poder enviar a la solución de sandbox (del mismo fabricante) como mínimo 80,000 archivos por día, para el caso de los archivos desconocidos (para los que no tenga firma).

5.1.1.1.13 Identificación de Usuarios

a. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de directorio, autenticación vía LDAP, Active Directory, o base de datos local.
b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente instalado en un equipo del dominio.
c. Debe soportar la recepción de eventos de autenticación de al menos una de las siguientes formas: controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows para la identificación de direcciones IP y usuarios, o agentes de seguridad de endpoint.
d. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación a futuro.
e. Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes citrix y microsoft terminal server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios.

5.1.1.1.14 Calidad de Servicio

a. Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, o Netflix por ejemplo), se requiere que la solución

[13] Absolución de Consultas y Observaciones N° 190, ITALTEL PERU SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto audio como vídeo streaming y todo el inventario de aplicaciones soportadas por la solución de seguridad. b. Soportar la creación de políticas de QoS por: dirección de origen, dirección de destino, por usuario y grupo de LDAP/AD, por aplicaciones, por puerto. c. El QoS debe permitir la definición de clases o reglas por: ancho de banda máximo, garantizado y prioridades.
5.1.1.1.15 Filtro de Datos
a. Los archivos deben ser identificados por extensión; b. Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones o tráfico HTTP. c. Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo o del mensaje, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.
5.1.1.1.16 Funcionabilidad a nivel de Firewall VPN
a. El dispositivo debe contar con licencias que permitan la conexión remota mínima de 3,500 usuarios concurrentes de tipo SSL. Se requiere como mínimo que 1,500 usuarios puedan conectarse sin agente. b. Al término del servicio los dos (02) equipos de seguridad perimetral quedarán en propiedad de EsSalud.

5.1.1.2 Servicio de Seguridad Nacional y Seguridad de Servidores

5.1.1.2.1 Consideraciones Generales
a. Provisionar una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial. b. Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance o chassis y que deban ser del mismo fabricante. No se aceptarán servidores o máquinas virtuales. c. La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad una solución redundante de por lo menos 2 (dos) appliances o chassis tanto externos como internos. d. El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 3 (tres) años en la modalidad 7x24x365, la misma que iniciará luego de la firma del Acta de aprobación de la Implementación de la Solución Anexo "C". Dicha vigencia será verificada a través de una declaración jurada del postor. e. En relación al RMA, el CONTRATISTA por medio de un servicio del fabricante (el cual deberá contar con depósito de partes o equipos completos con presencia local en el país), ofrezca mínimamente reemplazo de partes en un tiempo máximo

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

de 24 horas, para garantizar el funcionamiento de la solución en caso no haya afectación de servicios. En caso que el/los equipos provoquen degradación o pérdida del servicio contratado, el tiempo máximo de reemplazo deberá ser de 4 horas [14] [15] [16] [17] [18].

f. El contratista deberá proveer una solución que sea miembro activo de la organización global conocida como la "Alianza de Ciberamenazas" la cual garantiza un intercambio de inteligencia de amenazas entre terceros para acelerar la detección y mitigación de ataques globales.
g. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support (Fin de Vida o Fin de Ventas o Fin de Soporte). Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado o sustentado mediante carta del fabricante dirigido al proceso.
h. Los equipos deben poder ser administrados desde una plataforma centralizada de gestión.
i. Los equipos deben poder seguir siendo administrados de manera independiente aun si pierden la comunicación con la plataforma de gestión centralizada. Los equipos deben permitir al menos las siguientes acciones a través de su propia GUI: crear/modificar/borrar objetos y políticas, reglas de calidad de servicio, monitoreo de estado general y de seguridad.

5.1.1.2.2 Performance

a. Los firewalls deben soportar un throughput de 15 Gbps. Se deberá considerar tráfico real para el dimensionamiento de los equipos o mediciones con tráfico HTTP de 64 KB o transacciones usando tráfico empresarial mixto (Enterprise Mix)[19] [20] [21], no serán permitidas mediciones bajo condiciones ideales o tráfico UDP. Dicha medición debe contemplar las siguientes funcionalidades habilitadas simultáneamente:
   - Firewall (capa 4).
   - Control de aplicaciones.
   - Sistema de Prevención de Intrusos (IPS).
   - Antivirus o Antimalware
   - Filtrado de comando y control, antibot o antispyware
   - Logging Activo.
   - Sandbox.

V°B° Ing. Ricardo Siancas C. Sub Gerente (e) SUB GERENCIA DE COMUNICACIONES GP-GCTIC ESSALUD

[14] Absolución de Consultas y Observaciones N° 18, N° 35, GRUPO ELECTRODATA SAC
[15] Absolución de Consultas y Observaciones N° 98, VERIFICACIÓN Y CONTROL DE DATOS SAC
[16] Absolución de Consultas y Observaciones N° 103, VERIFICACIÓN Y CONTROL DE DATOS SAC
[17] Absolución de Consultas y Observaciones N° 145, INDRA PERÚ SAC
[18] Absolución de Consultas y Observaciones N° 181, ITALTEL PERU SAC
[19] Absolución de Consultas y Observaciones N° 36, GRUPO ELECTRODATA SAC
[20] Absolución de Consultas y Observaciones N° 101, VERIFICACIÓN Y CONTROL DE DATOS SAC
[21] Absolución de Consultas y Observaciones N° 183, ITALTEL PERU SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

b. El postor deberá sustentar el cumplimiento del performance con información pública del fabricante o mediante carta del fabricante dirigido al proceso.
5.1.1.2.3 Conexiones Simultaneas
a. Los firewalls deberán soportar 15 millones de sesiones concurrentes. b. Deberán soportar 400 mil conexiones por segundo.
5.1.1.2.4 Interfaces de Cobre
a. Los firewalls perimetrales e internos deberán contar con un mínimo de 4 interfaces de cobre (formato RJ-45).
5.1.1.2.5 Interfaces fibra óptica
a. Los firewalls deberán contar con un mínimo de 4 interfaces RJ45 u ópticos (SFP) 1GB y 8 interfaces ópticos de 10gb (SFP+) b. Los firewalls deben poder utilizar una interface de 10 GB adicional para la sincronización de sesiones del clúster, se deben incluir los transceivers y cables necesarios. c. Todas las interfaces requeridas (1 Gbps y 10 Gbps) deberán incluir los transceivers para fibra multimodo.
5.1.1.2.6 Características de Hardware
a. Cada equipo debe contar con una interfaz de red 10/100/1000 dedicada para administración. b. Cada equipo debe poder ser montado en un rack de 19''. Debe incluir todos los elementos necesarios para su montaje. c. Los equipos deben soportar sistemas virtuales, entornos o contextos virtuales. Debe contar con licenciamiento para al menos 10 entornos virtuales.
5.1.1.2.7 Características de Red
a. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino. b. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2); c. El dispositivo debe soporta direccionamiento IPv6 basado: direccionamiento en interfaces; IPv6 rutas estáticas; IPv6 lista de acceso o regla de acceso. Debe contar con alguna certificación para IPv6. d. El dispositivo debe soportar la operación en modo transparente y enrutado; además en ambos modos debe de soportar IPv6 para futuras implementaciones. e. El dispositivo debe tener la capacidad de soportar el protocolo Netflow o similares para poder tener información de seguridad y troubleshooting. f. Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de instancias o dominios virtuales:

V°B° Ing. Ricardo Siancas Sub Gerente (e) SUB GERENCIA DE COMUNICACIONES GP-GCTIC - ESSALUD -

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

- Modo Sniffer o Pasiva, para inspección vía puerto espejo del tráfico de datos de la red.
- Modo Capa – 2 (L2) Bridge, para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación o dentro de un mismo segmento de red.
- Modo Capa – 3 (L3) o Routed, para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default gateway de las redes protegidas.
- Modo Transparente o Inline, para poder inspeccionar datos en línea y tener visibilidad del control de tráfico a nivel de aplicación sobre 2 puertos en modo bridge/transparente.

a. Modo mixto de trabajo Sniffer o Pasiva, Transparente, L2 y L3 simultáneamente en diferentes interfaces físicas del mismo equipo.

5.1.1.2.8 Alta Disponibilidad

a. Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo o modo, clúster con despliegues de los equipos en modo capa 3 (L3)
b. La configuración en alta disponibilidad debe sincronizar:
   - Sesiones;
   - Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red;
   - Asociaciones de Seguridad de las VPNs;
   - El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.

SUB GERENCIA DE COMUNICACIONES GP-CTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD

5.1.1.2.9 Características de Firewall

a. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, grupos y categorías de aplicaciones.
b. Control, inspección y descifrado de SSL o TLS por política para tráfico de entrada (Inbound) y salida (Outbound).
c. Debe soportar inspección de tráfico encriptado con TLS 1.2 y de manera opcional TLS 1.3.
d. Soportar el control de tiempo sobre las políticas de control de acceso con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
e. El equipo debe incorporar herramientas para troubleshooting avanzado como la capacidad de visualizar la trazabilidad de los paquetes y realizar capturas de tráfico en tiempo real desde el propio equipo.
f. Debe contar con mecanismos que faciliten la optimización de reglas de seguridad:
g. Mostrar la cantidad de veces que una política ha sido aplicada para medir la eficiencia de la misma
h. Mostrar a través de un filtro, las reglas de seguridad que no han sido utilizadas, a fin de tener una depuración de reglas sin usar.

5.1.1.2.10 Control de Aplicaciones

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

a. Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
b. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares, firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo.
c. Debe ser capaz de inspeccionar aplicaciones que viajen por tráfico cifrado como HTTPS y de manera opcional SSH.
d. Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la entidad.
e. Debe ser posible la creación de grupos de aplicaciones basados en características de las aplicaciones como:
f. Tecnología cliente-servidor.
g. Nivel de riesgo de las aplicaciones.
h. Categoría de aplicaciones.

5.1.1.2.11 Prevención de Amenazas

a. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Anti-malware de red, Antibot, DNS Filtering o DNS Sinkhole integrados en el propio appliance.
b. El equipo debe proteger de amenazas avanzadas que utilizan conexiones DNS, de manera que permita filtrar las consultas de DNS de los hosts para bloquear conexiones hacia sitios maliciosos, conexiones de botnet, ya sea en base a categorías o firmas.
c. La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca.
d. Las firmas de IPS deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo.
e. Debe soportar granularidad en las políticas de IPS, Antimalware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, aplicación, usuario y grupo de usuarios y la combinación de todos esos ítems.
f. Permitir el bloqueo de malware por lo menos en los siguientes protocolos: HTTP, IMAP, FTP, SMB, SMTP y POP3
g. Identificar y bloquear comunicaciones con amenazas clasificadas como atacantes, Bots, Comando y Control, Exploitkit, Malware, OpenProxy, OpenRelay, Phishing, SPAM y Nodos de salida de TOR.

5.1.1.2.12 Prevención de amenazas desconocidas

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

a. Poseer la capacidad de análisis de amenazas no conocidas.
b. La plataforma de seguridad de sandboxing debe ser basada en una plataforma on-premise o local con soporte de Inteligencia de Amenazas compartidas En caso de caída del equipo de sandbox local, los equipos firewall deben poder enviar los archivos a un servicio de sandboxing en nube del mismo fabricante.
c. Debe contar, de manera opcional con una plataforma de API para poder integrarse a herramientas de terceros.
d. El equipo de Sandboxing tenga la capacidad de explotar el malware en un ambiente controlado (VM) con sistema operativo Windows 7, Windows 8, Windows 10 , MacOS o Android[22].
e. Debe soportar el monitoreo de archivos transferidos por internet (FTP, HTTP, SMTP, IMAP y POP3) como también archivos transferidos internamente en los servidores de archivos usando SMB.
f. Deberá soportar el análisis de archivos ejecutables /EXE), DLLs, Archivos comprimidos (obligatorios ZIP y TAR, opcionalmente GZIP), archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx(en el ambiente controlado.[23]
g. El firewall propuesto debe poder enviar a la solución de sandbox (del mismo fabricante) al menos 80,000 archivos por día, para el caso de los archivos desconocidos (para los que no tenga firma).

5.1.1.2.13 Identificación de Usuarios

a. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de directorio, autenticación vía LDAP, Active Directory, o base de datos local.
b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente instalado en un equipo del dominio.
c. Debe soportar la recepción de eventos de autenticación de al menos una de las siguientes formas: controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows para la identificación de direcciones IP y usuarios, o agentes de seguridad de endpoint.
d. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación a futuro.
e. Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes citrix y microsoft terminal server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios.

5.1.1.2.14 Calidad de Servicio

[22] Absolución de Consultas y Observaciones N° 190, ITALTEL PERU SAC
[23] Absolución de Consultas y Observaciones N° 163, ADEXUS PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

a. Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, o Netflix por ejemplo), se requiere que la solución tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto audio como vídeo streaming y todo el inventario de aplicaciones soportadas por la solución de seguridad. b. Soportar la creación de políticas de QoS por: dirección de origen, dirección de destino, por usuario y grupo de LDAP/AD, por aplicaciones, por puerto. c. El QoS debe permitir la definición de clases o reglas por: ancho de banda máximo, garantizado y prioridades.
5.1.1.2.15 Filtro de Datos
a. Los archivos deben ser identificados por extensión; b. Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones o tráfico HTTP. c. Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo o del mensaje, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular. d. Al término del servicio los dos (02) equipos de seguridad nacional y seguridad de servidores quedarán en propiedad de EsSalud.

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Gamarra C. Sub Gerente (e) ESSALUD

5.1.1.3 Servicio de Administración Centralizada de Firewalls

5.1.1.3.1 Consideraciones Generales
a. La gestión de los firewalls debe realizarse desde una solución en appliance provista por el mismo fabricante de los firewalls. No se aceptarán soluciones en software o máquinas virtuales montadas sobre servidores o hipervisores. b. El almacenamiento de logs deberá tener un almacenamiento de al menos 10Tb neto sea en RAID 1, o 5, o 6, o 10. El almacenamiento de los logs debe ser provisto en un equipo adicional con capacidad para generar las vistas y reportes solicitados. Este equipo puede ser de una marca distinta al fabricante de los firewalls. c. La solución debe tener la capacidad de ingestar por lo menos 10,000 logs/flujos por segundo. d. La administración de las políticas de seguridad debe realizarse sobre hardware dedicado para dicho propósito y provisto por el mismo fabricante de los firewalls. e. La solución debe contar con interface gráfica de usuario (GUI), vía Web por HTTP y/o HTTPS compatible al menos con, Windows, Linux y Mac OS. f. La solución debe contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

g. La solución debe poseer una interface basada en línea de comando (CLI) usando SSH, Telnet o puerto serial dedicado.
h. La solución debe permitir importar los cambios realizados directamente en los firewalls para sincronizarlos con la configuración existente en la plataforma de gestión.
i. La caída o falla de la plataforma de gestión no debe impedir el acceso a los firewalls para realizar cambios en la configuración.
j. La solución debe mostrar los indicadores de compromiso y comportamiento detectados por los diferentes motores de inspección habilitados en los NGFW.
k. La solución debe contar con la capacidad de asignar un perfil de administración basado en roles (RBAC) que permita delimitar las funciones del equipo que pueden gerenciar y afectar.
l. Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración;
m. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema, por tipo de log o por equipos administrados.
n. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de Anti-malware de red, IPS, control de aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
o. Generar alertas automáticas vía:
p. Email;
q. SNMP;
r. Syslog;
s. La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en JSON o XML.
t. Al término del servicio el appliance (01) de administración centralizada de firewalls quedará en propiedad de EsSalud.

V°B° GERENCIA DE COMUNICACIONES GP-GCTIC Ing. Ricardo Slanicas C. Sub Gerente (e) ESSALUD

5.1.1.4 Servicio para Conectividad de Plataforma de Seguridad

5.1.1.4.1 Especificaciones Generales
a. Cantidad: 02 unidades (Switches). b. Rackeable de 01 RU hasta 3RU c. 32MB de buffer de sistema d. Memoria de 16GB e. Almacenamiento 64GB SSD

5.1.1.4.2 Capacidades
a. Desempeño de 3.6Tbps non-blocking b. 2.5 bpps c. Latencia menor o igual a 5 microsegundos
5.1.1.4.3 Fuentes de Poder y Ventiladores
a. Fuentes redundantes con capacidad de intercambio en caliente b. Mínimo 2, (Incluir todas las fuentes de poder soportadas). c. Ventiladores redundantes (Incluir todos los ventiladores o bandejas de ventiladores soportados por el equipo). d. Ventiladores deben soportar la inserción y el retiro en operación (en caliente) sin afectación del servicio.
5.1.1.4.4 Cantidad de Puertos
a. 48 x 10 de fibra SFP+, considerar 24 transceivers multimodo 10GE y 8 transceivers de cobre 1GB por switch.
5.1.1.4.5 Funcionalidades Capa 2
a. 802.1Q (VLAN Trunking) b. Soporte hasta 3960 VLANs c. 802.1d (STP) d. 802.1w (RSTP) e. 802.1s (MSTP) f. 802.3ad (LACP) g. El switch debe tener la funcionalidad habilitada de formar con otro switch una entidad virtual en la que ambos se presenten como un solo switch hacia otros dispositivos de red.
5.1.1.4.6 Funcionalidades Capa 3
a. Enrutamiento Estático habilitado b. VRRP habilitado c. Soporte OSPFv3 d. Soporte BGP e. Soporte enrutamiento IPv6
5.1.1.4.7 Funcionalidades de Calidad de Servicio
a. 8 colas por puerto b. 802.1p (COS) c. DSCP d. Capacidad de manejo QoS del tráfico previamente clasificado.
5.1.1.4.8 Mecanismos de Seguridad
a. DHCP Relay b. DHCP Snooping

SUB GERENCIA DE COMUNICACIONES GP-GGTIC V°B° Ing. Ricardo Sporrat C. Sub Gerente (e) ESSALUD

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

c. IP Source Guard d. Dynamic ARP Inspection o ARP Attack Protection e. Mecanismo de protección contra ataques DoS al procesador del equipo f. Port Security g. RADIUS h. Listas de Control de Acceso (ACL)
5.1.1.4.9 Características de Gestión
a. Administración por línea de comandos vía consola b. SNMPv3 c. SSHv2 d. TACACS+ e. RMON f. LLDP g. NTP h. TFTP o FTP i. Soporte de espejamiento ("mirroring") de puertos que permita el análisis de red con dispositivos externos como detectores de intrusos j. Debe soportar gestión vía interfaces Programables de Aplicación (APIs) k. Debe soportar Configuración automatizada mediante scripts
5.1.1.4.10 Características de Sistema Operativo
a. El sistema operativo del switch debe ser de diseño modular. b. El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software. c. Se deben poder instalar parches del software en línea. d. Todos los componentes a ofertar deben ser de un mismo fabricante a fin de garantizar una total compatibilidad entre ellos. e. No se aceptarán soluciones con gestión basada en nube o fuera de la red de ESSALUD. f. La solución ofertada debe incluir el licenciamiento necesario para lo solicitado. g. Soporte de desencriptación en línea para tráfico SSL/TLS. h. Soporte de 802.1AE AES-256 para encriptación de tráfico. i. Al término del servicio los dos (02) equipos switches para conectividad de plataforma de seguridad quedarán en propiedad de EsSalud.

SUB GERENCIA DE COMUNICACIONES GPGCTIC V°B° Ing. Ricardo Sanchez C. Sub Gerente (e) ESSALUD

5.1.1.5 Servicio de Seguridad para Correo Electrónico

5.1.1.5.1 Consideraciones Generales
a. El equipo de seguridad para correo electrónico deberá ser nuevo sin uso en su integridad: chassis, componentes internos, cables de energía, patch cords, transceivers, entre otros componentes que forman parte del equipo y de los

componentes necesarios para la operatividad de acuerdo al servicio a atender por la herramienta de seguridad.

b. Solución debe basarse en "appliance" de propósito específico (Virtual o Físico). No se tendrán en cuenta los equipos de uso general (PCs o servidores) en la que se puede instalar y / o ejecutar un sistema operativo regular, como Microsoft Windows, FreeBSD, Solaris de Sun o GNU / Linux. En caso la solución sea provista en Virtual Appliance, el servidor deberá cumplir con los siguientes requerimientos mínimos:
   - Procesadores: Dos procesadores 3.2GHz, 25M Cache, 9.60GT/s QPI, Turbo, HT, 8C/16T (135W)
   - Memoria RAM: 64GB de RAM 2400MHz o superior
   - Almacenamiento: 4TB SSD SAS. Discos Duros SAS 12Gbps 2.5in con Tecnología: Hot-plug Hard Drive de escritura intensa o superior en capacidad de almacenamiento (GB) por disco duro. Deberá soportar configuraciones RAID de fabricante.
   - Conectividad: 04 puertos 1Gb RJ45, 02 puertos 10Gb SFP+, incluir transceivers
   - Puerto de Consola: Serial o RJ45
   - Energía: Fuentes redundantes 1+1 de 1100W cada una, Hot-plug
   - Montaje: En rack de 19". Rieles y administrador de cables del mismo fabricante. Debe incluir todo lo necesario para su montaje.
   - La versión Virtual Appliance debe poder desplegarse sobre VMware ESX/ESXi.
c. Tener al menos 2TB de almacenamiento local.
d. Permitir configurar por lo menos 4 dominios.
e. Soportar crear al menos 300 políticas por recipiente por dominio.
f. Soportar crear al menos 1000 políticas por recipiente por sistema.
g. Soportar enrutar al menos 600,000 mensajes por hora.
h. Soportar como mínimo 500,000 mensajes por hora con el análisis de antispam y antivirus habilitados.

5.1.1.5.2 Funcionalidades de Seguridad

a. La solución debe tener características antispam, antivirus, anti-spyware y anti-phishing y poder inspeccionar correo entrante y saliente hacia internet.
b. La solución debe contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger.
c. La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam.
d. La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb
e. La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como anti-spam, anti-virus, autenticación, entre otros.
f. La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

g. La solución debe ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados. h. La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail. i. La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico. j. La solución debe ser capaz de realizar análisis bayesiano para determinar si un correo es spam. k. La solución debe ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje. l. La solución debe ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM. m. La solución debe ser compatible con el enrutamiento en IPv4 e IPv6. n. La solución debe ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6. o. La solución debe ser capaz de detectar las direcciones IP falsificadas (Forged IP). p. La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent). q. La solución debe ser compatible con Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) y Domain Based Message Authentication (DMARC). r. La solución debe poder retrasar el envío de correo sobredimensionados a horarios que sean de menos carga. s. La solución debe poder definir el reenvío de correo (relay) a una Ip específica con base a la IP origen del mensaje. t. La solución debe permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto. u. La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica. v. La solución debe soportar cuarentena por usuario, permitiendo que cada usuario puede gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se debe acceder a través de la página web o POP3. w. La solución debe ser capaz de programar el envío de informes de cuarentena. x. La solución debe ser capaz de realizar el almacenamiento de correo electrónico (Archivado/archiving), basado en el envío y recepción de políticas, con el apoyo también de almacenamiento remoto. y. La solución debe ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega. z. Debe permitir el envío de correo cifrado punto a punto.
5.1.1.5.3 Protección contra Amenazas Avanzadas
a. La solución debe contar con capacidades de evaluar, retener y/o bloquear correos que cuentes con amenazas avanzadas, Dia zero mediante el análisis de archivos con herramientas de Sandboxing.

SUB GERENCIA DE COMUNICACIONES GP-GSTIC
V°B°
Ing. Ricardo Stancas C.
Sub Gerente (e)
ESSALUD

b. La herramienta de Sandboxing debe ser provista de manera local. No se aceptarán soluciones basadas en nube.
5.1.1.5.4 Prevención de Fuga de Información
a. La funcionalidad DLP debe permitir definir la información a detectar como palabras, frases y expresiones regulares. b. La funcionalidad DLP debe tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros. c. La funcionalidad DLP debe permitir la creación y almacenamiento de impresiones digitales (Fingerprint) de documentos.
5.1.1.5.5 Gestión
a. La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS). b. La solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen. c. La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only) d. La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog) o SIEM. e. Al término del servicio, la solución que brinda el Servicio de Seguridad para Correo Electrónico, quedará en propiedad de EsSalud.

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Richard Sparrow C. Sub Gerente (e) ESSALUD

5.1.1.6 Servicio de Visibilidad y Gestión de Riesgo en la Red

5.1.1.6.1 Consideraciones Generales
a. Se requiere una solución que permita identificar ataques y amenazas basado en el comportamiento de la red mediante el análisis del tráfico y/o eventos. b. La solución debe estar basada en la recolección de eventos o flujos de red mediante los protocolos IPFIX, Netflow, puerto espejo o en su defecto mediante la recolección de logs de dispositivos de red y seguridad. c. La solución debe ser capaz de procesar los flujos y/o eventos recogidos de la red, para ofrecer una vista completa de la seguridad y disponibilidad de la red. Debe soportar al menos 100 dispositivos. d. La solución debe soportar la recolección de tráfico de al menos 10,000 flujos por segundo y/o más de 10,000 eventos por segundo. e. La solución debe contar con una consola de gestión, desde la cual permita ejecutar tareas de administración, y reportería. f. La solución debe estar en capacidad de analizar tráfico cifrado, bien mediante la captura de datos de telemetría enviados por switches con capacidad para ello, o bien mediante la integración con los firewalls o incorporación de elementos habilitados para el sensaje de flujos.

g. El modelamiento de datos, para establecer la analítica de comportamiento de usuario, debe realizarse a partir de información recogida de los elementos activos de la misma red.
h. La solución debe poderse integrarse con una solución de control de acceso a la red o con un sistema de gestión de identidades.
i. La solución debe contar con APIs del tipo Web Services, las cuales deben estar en compliance con el Simple Object Access Protocol (SOAP) o soportar JSON API o XML API, con el fin de que se puedan usar aplicaciones externas como SIEM, ticketing, reportería de terceros, etc, para acceder datos de la consola de administración.
j. La solución debe recolectar y analizar la información de los dispositivos de red integrándose con la capa de red o acceso.
k. La solución debe perfilar y analizar el comportamiento de la red, para que los administradores puedan reconocer inmediatamente el impacto de cualquier evento inesperado sobre la misma, en cualquier lugar de la organización.
l. La solución debe trazar el volumen de tráfico, la utilización de ancho de banda, la composición y otras tendencias, en una línea de tiempo.
m. La solución debe proporcionar visibilidad de servicios, puertos y aplicaciones en toda la red, para el análisis del tráfico.
n. La solución debe detectar ataques altamente dirigidos y sofisticados que puedan evadir la defensa de seguridad, moverse sigilosamente a través de la red y robar datos confidenciales. Adicionalmente, debe detectar los diversos estados de los ataques avanzados, incluyendo: Reconocimiento de Red. Comunicaciones Botnet/ Command and Control. Filtración de datos. Movimientos laterales como la propagación de malware.
o. La solución debe identificar las fuentes de ataque de DoS o DDoS antes de que causen una interrupción de servicio.
p. La interfaz gráfica debe permitir identificar de manera rápida las amenazas de red, indicando al menos su criticidad, origen y tipo.
q. La solución debe recopilar, analizar y almacenar grandes cantidades de datos de flujos/eventos, llevando un registro de auditoria completo de todas transacciones de la red, para detectar tráfico anómalo y realizar investigaciones forenses (retrospectiva), más efectivas.
r. La solución debe incluir motor de Analítica o Machine Learning para identificar comportamientos anómalos y posibles amenazas para la institución.
s. Todo el análisis debe realizarse de manera local y sin necesidad de enviar información a la nube. Además, la solución debe recibir actualizaciones desde la nube del mismo fabricante al menos de manera diaria.
t. Debe permitir crear acciones de respuesta automática ante incidentes para mitigar o eliminar la amenaza. Estas acciones deben poder ser aplicadas sobre los equipos de red.
u. Debe garantizar la retención de información histórica por lo menos durante 12 meses.
v. La solución puede estar compuesta por varios componentes siempre y cuando cumplan con el requerimiento.

SUB GERENCIA DE COMUNICACIONES GDGCTIC V°B° Ing. Ricardo Silencar C. Sub Gerente (e) ESSALUD

5.1.1.6.2 Especificaciones del Hardware
a. La solución debe ser provista en appliance o virtual appliance. El postor debe incluir el hardware y software necesario para la instalación de la plataforma virtual. No se aceptarán soluciones que corran sobre sistemas de virtualizacón abiertos o opensources. b. Al término del servicio los equipos de visibilidad y gestión de riesgo de la red quedarán en propiedad de EsSalud.

5.1.2 Implementación de la Solución

Se suscribirá mediante Acta de aprobación de la Implementación de la Solución **Anexo C**, con una duración máxima de 90 días calendario contados a partir del día siguiente de suscrito el Contrato para la prestación del servicio, de acuerdo al siguiente detalle:

DESCRIPCIÓN	PLAZO
Plan de Trabajo	Un plazo máximo de 05 días calendarios, contados a partir del día siguiente de suscrito el contrato, donde se suscribirá el Aprobación de Plan de Trabajo – **Anexo A.**
Plan de Implementación	Un plazo máximo de 15 días calendarios, contados a partir del día siguiente de suscrita el Acta de Aprobación de Plan de Trabajo – **Anexo A.** Asimismo, se suscribirá mediante Acta de Aprobación del Plan de Implementación– **Anexo B.**
Implementación del Servicio	Un plazo máximo de 70 días calendarios, contados a partir del día siguiente de suscrita el Acta de Aprobación del Plan de Implementación– **Anexo B.** Asimismo, se suscribirá mediante Acta de aprobación de la Implementación de la Solución **Anexo C.**

5.1.2.1 Plan de Trabajo

El contratista debe presentar a ESSALUD en un plazo de cinco (05) días calendarios un Plan de Trabajo, contados a partir del día siguiente de suscrito el contrato, detallando el inicio de trabajos y actividades de la implementación que contenga la siguiente información:

- ✓ Lista de actividades y su descripción.
- ✓ Personal propuesto y responsables por actividad
- ✓ Procedimiento de Trabajo.
- ✓ Cronograma de Trabajo en Project.
- ✓ Plan de Seguridad y Medio Ambiente.
- ✓ Lista de Personal.
- ✓ Organigrama del equipo de trabajo.
- ✓ SCTR (Salud y Pensión) vigente del personal.

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

ESSALUD a través de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC revisará el Plan de Trabajo en un plazo conforme a los señalado en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

Cabe señalar que para la aprobación de dicha documentación se suscribirá el Acta de Aprobación de Plan de Trabajo – **Anexo A.**

El contratista, deberá presentar los documentos en dos copias. La entrega se realizará mediante documento físico firmado y en formato digital (Word), remitido a la Sub Gerencia de Comunicaciones de la Gerencia Central de Tecnologías de la Información y Comunicaciones.

5.1.2.2 Plan de Implementación

El contratista debe presentar a ESSALUD en un plazo de quince (15) días calendarios un Plan de Implementación, contados a partir del día siguiente de suscrito el Acta de Aprobación del Plan de Trabajo – **Anexo A**, detallando la siguiente información:

- Plan de Implementación de la Solución (componentes de seguridad y conectividad).
- Arquitectura de la solución que se utilizará para brindar el servicio.
- Diagramas de seguridad y conectividad.
- Plan de Migración de la Solución.
- Plan de Protocolo de Pruebas de la Solución.
- Elaboración del plan de trabajo (Gantt), conteniendo como mínimo lo siguiente: objetivo, metas y cronograma de actividades.

ESSALUD a través de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC revisará el Plan de Implementación en un plazo conforme a los señalado en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

Cabe señalar que para la aprobación de dicha documentación se suscribirá el Acta de Aprobación del Plan de Implementación– **Anexo B.**

El contratista, deberá presentar los documentos en dos copias. La entrega se realizará mediante documento físico firmado y en formato digital (Word), remitido a la Sub Gerencia de Comunicaciones de la Gerencia de producción de la GCTIC.

5.1.2.3 Implementación del Servicio

Se suscribirá mediante Acta de aprobación de la Implementación de la Solución **Anexo C**, y contará con un plazo de duración de setenta (70) días calendario, contados a partir del día siguiente de suscrito el Acta de Aprobación del Plan de Implementación – **Anexo B.**

El contratista es responsable de realizar las configuraciones necesarias en los equipos provistos y en los equipos detallados en la **Tabla N° 1 (página 34)**. Equipamiento de seguridad adicional a Gestionar para la integración de la solución de seguridad de la ENTIDAD.

- Coordinación permanente con el responsable de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la Gerencia Central de Tecnologías de la Información y Comunicaciones, o con quien éste designe, acerca de las consideraciones a tener en

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

cuenta, para cumplir con el entregable requerido.

- Realización de visitas al Datacenter y sectores en donde se instalarán los equipos en coordinación con el responsable de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la Gerencia Central de Tecnologías de la Información y Comunicaciones, o con quien éste designe.
- Implementación de componentes de seguridad y conectividad.
- El contratista deberá presentar un plan de implementación, el mismo que estará sujeto a la revisión y ratificación por parte del ESSALUD, de tal modo que cubra todas las tareas a llevar a cabo desde la firma del contrato hasta la aceptación definitiva de la solución.
- El plan de implementación deberá incluir siguiente:
  - ✓ La documentación del diseño descriptivo de la solución de seguridad, indicando en forma detallada los componentes a ser implementados.
  - ✓ Las especificaciones técnicas que deben cumplir las instalaciones físicas para el correcto montaje y funcionamiento de los componentes de la solución
  - ✓ Los plazos mínimos y máximos para cada una de las tareas a cumplir desde el otorgamiento de la buena Pro hasta la puesta en producción de los equipos, debiéndose discriminar las que debe cumplir ESSALUD, el proveedor en forma exclusiva, y las que deben asumir en forma compartida.
  - ✓ La metodología a utilizar en las pruebas de implementación.
- ESSALUD proporcionará los gabinetes requeridos para la instalación de los equipos, así como las condiciones de energía estabilizada y aire acondicionado. El proveedor es responsable de implementar todo el cableado de red (UTP Categoría 6A y Fibra) que sea requerido, de conformidad con el estándar empleado en ESSALUD.
- La entrega de los componentes de la solución se realizará en la Gerencia Central de Tecnologías de la Información y Comunicaciones, ubicada en el Jr. Domingo Cueto Nº 120, sexto piso, del distrito de Jesús María, referencia altura de la cuadra 14 de la Av. Arenales.
- Durante la implementación, deberá ser realizada por personal certificado del proveedor.
- Al finalizar la implementación, entregar a ESSALUD, en formato electrónico:
  - ✓ Documento del fabricante, donde se establezca el período de vigencia del licenciamiento, la garantía de hardware y el mantenimiento del software.
  - ✓ El informe técnico de implementación, el mismo que deberá incluir la documentación descriptiva de la solución de seguridad implementada, así como los resultados de las pruebas efectuadas durante la implementación y detalles de la configuración establecida.
  - ✓ Toda bibliografía considerada necesaria para utilizar los elementos (hardware y software) que forman parte de la solución, actualizada a la última versión. La documentación deberá contener los manuales de administración de los componentes de la solución.
  - ✓ Desarrollo del informe con los resultados de los trabajos realizados que incluya detalles diseño e implementación.

Cabe señalar que, la implementación es sin costo para la Entidad.

5.1.2.3.1 Metodología de trabajo de la Implementación

Dentro de la metodología de trabajo se considerarán los siguientes aspectos:

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

- Elaboración del plan de trabajo (Gantt), conteniendo como mínimo lo siguiente: objetivo, metas y cronograma de actividades.
- Coordinación permanente con el responsable de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, o con quien éste designe, acerca de las consideraciones a tener en cuenta, para cumplir con el entregable requerido.
- Realización de visitas al Datacenter y sectores en donde se instalarán los equipos en coordinación con el responsable de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, o con quien éste designe.
- Implementación de componentes de seguridad y conectividad.
- Desarrollo del informe con los resultados de los trabajos realizados que incluya detalles diseño e implementación.

5.1.2.3.2 Entregables de la Implementación

- Plan de Trabajo.
- Plan de Implementación de la Solución (componentes de seguridad y conectividad)
- Diagramas de seguridad y conectividad.
- Plan de Migración de la Solución
- Plan de Protocolo de Pruebas de la Solución
- Informe Técnico Final, que contendrá la descripción de los trabajos realizados, incluyendo imágenes, conclusiones y recomendaciones.

El contratista, deberá presentar el informe final en dos copias. La entrega se realizará mediante documento físico firmado y en formato digital (Word), remitido a la Sub Gerencia de Comunicaciones de la Gerencia Central de Tecnologías de la Información y Comunicaciones.

ESSALUD a través de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC revisará el Plan de Implementación de la Solución en un plazo conforme a los señalado en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

Cabe señalar que para la aprobación de dicha documentación se suscribirá el Acta de Aprobación de Implementación de la Solución – **Anexo C**.

El contratista, deberá presentar el informe final de la implementación en dos copias. La entrega se realizará mediante documento físico firmado y en formato digital (Word), remitido a la Sub Gerencia de Comunicaciones de la Gerencia Central de Tecnologías de la Información y Comunicaciones.

5.1.3 Soporte Gestionado de Seguridad

El contratista deberá encargarse de gestionar, auditar, supervisar, alertar, optimizar y agregar políticas bajo demanda y a requerimiento de EsSalud para los equipos provisionados y los equipos señalados en la **Tabla N° 01**, en un horario del 24x7x365 días a través de una mesa de servicio con personal altamente capacitado y entrenado.

Se requiere como parte del Soporte Gestionado de Seguridad lo siguiente:

- Deberá enviar personal en sitio de lunes a sábado (en las instalaciones de EsSalud) en el horario de lunes a viernes de 8:00 a.m. - 8:00 p.m. y sábado de 8:00 a.m. – 1:00 p.m. El personal asignado a soporte en sitio, ejecutará todos los trabajos relacionados a la Gestión y Soporte de la infraestructura tecnológica descritos en el presente TDR.

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

- Deberá enviar alertas tempranas vía correo electrónico ante alguna eventualidad o incidente sobre la red de la Entidad.
- Realizar análisis mensuales de amenazas a través de los componentes ofertados para mitigar el impacto de ataques sobre la red, con su respectiva documentación.
- El personal que brindará el servicio, deberá estar certificado en la solución ofertada.
- Contar con las siguientes características:
  - ✓ Administración de requerimientos.
  - ✓ Administración de incidentes.
  - ✓ Gestión de eventos, problemas.
  - ✓ Gestión de cambios de la configuración.
  - ✓ Gestión de acceso a los servicios de seguridad y protección.
  - ✓ Reportes semanales y mensuales: informes operativos, gerenciales y de gestión.
- Debe dar respuesta a los incidentes de seguridad asociados a las plataformas monitorizadas.
- Debe cumplir cabalmente los siguientes objetivos:
  - ✓ Detección oportuna de amenazas de seguridad que estén en proceso de materializarse o se hayan materializado a través de las plataformas monitorizadas.
  - ✓ Respuesta a incidente que permita mitigar el riesgo al cliente.
  - ✓ Entrega de información de contexto al cliente durante el incidente.
  - ✓ Identificación de nuevas amenazas asociadas al ámbito del servicio.
- Debe brindar soporte in-situ o remoto ante los requerimientos que demanden una ejecución de las actividades solicitadas referentes a la solución propuesta, para los incidentes de prioridad baja o normal.
- Debe brindar soporte in-situ ante requerimientos que demanden ejecución de actividades solicitadas para los incidentes de prioridad media o alta.
- Debe brindar la capacidad de control, permitiendo la identificación y bloqueo de situaciones de riesgo previamente identificadas.
- Debe de comunicar de inmediato vía llamada telefónica y por correo ante algún evento o incidente encontrado durante el monitoreo al personal supervisor de la entidad y empezar a trabajar para brindar solución oportuna.
- El tiempo máximo de atención de una incidencia de seguridad corresponde al tiempo transcurrido desde que EsSalud reporta la incidencia al NOC y se le asigna un ticket de atención, hasta la atención completa de la misma a satisfacción de EsSalud, será bajo el siguiente detalle:
  - ✓ Prioridad alta: Tiempo máximo de cuarenta (40) minutos.
  - ✓ Prioridad media: Tiempo máximo de una (01) hora.
  - ✓ Prioridad normal: Tiempo máximo de dos (02) horas.
  - ✓ Prioridad baja: Tiempo máximo de cuatro (04) horas.
- El tiempo máximo de atención de un requerimiento de seguridad corresponde al tiempo transcurrido desde que EsSalud solicita el requerimiento al NOC y se le asigna un ticket de atención, hasta la atención completa de la misma a satisfacción de EsSalud, será bajo el siguiente detalle:
  - ✓ Prioridad alta: Tiempo máximo de dos (02) horas.
  - ✓ Prioridad media: Tiempo máximo de cuatro (04) horas.
  - ✓ Prioridad normal: Tiempo máximo de ocho (08) horas.
  - ✓ Prioridad baja: Tiempo máximo de doce (12) horas.
- Se proveerá en modalidad 24x7x365 asimismo el contratista deberá contar con una

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Storgie C. Sub Gerente (e) ESSALUD

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

plataforma para apertura de tickets para la atención de incidentes de seguridad relacionada con la gestión de los equipos, así como un 0800 habilitado 24x7x365 con personal especializado y debidamente certificado en la solución propuesta.

- E contratista deberá facilitar a EsSalud, acceso de consultas a las herramientas de gestión de la plataforma ofertada, con el propósito de realizar el seguimiento de los tickets y monitoreo de operación de la solución ofertada.
- Deberá remitir los números de contacto y la lista de escalamiento para la atención de requerimientos relacionados a la gestión de la solución, el cual deberá ser presentado al inicio del periodo del servicio. Asimismo, dicha información debe estar disponible en todo momento en la web de mesa de ayuda para una comunicación fluida y obtener una trazabilidad del estado de los tickets generados.
- El contratista deberá contar con un sistema de gestión a través de un centro de operaciones de red; es decir, un único punto de contacto para EsSalud para el reporte de fallas, atención a nuevas solicitudes o tratamiento de reclamos.
- El centro de Operaciones del Contratista (NOC) deberá tener la capacidad de escalamiento interno a otros niveles de servicio sin la necesidad de que EsSalud informe sobre la demora o falta de atención de un evento o incidente informado por cualquier canal de atención (teléfono, correo, etc).
- El Ingeniero en sitio deberá contar con su SCTR habilitado durante todo el periodo de ejecución del servicio.
- El contratista mantendrá la administración y gestión permanente de todo para los equipos provisionados y los equipos señalados en la Tabla N° 01. Asimismo, deberá de garantizar el soporte del fabricante y las licencias de estos equipos hasta el periodo de duración del servicio, para ello deberá de presentar los sustentos de los números de contratos con el fabricante, EsSalud podrá realizar validaciones de estos contratos con el fabricante. A continuación, se detallan los equipos propios de EsSalud.

Item	Marca	Modelo / N-Serie	Versión S.O.	Cantidad	Garantía
1	CISCO	Firepower 2130 N/S: JMX2342Z09H	v6.4.0.4	1	12/12/2022
2	F5	F5-BIG-AFM-I2800 BIG-IP N/S: f5-vkgn-xpjv	BIG-IP 14.1.0 Build 0.0.116 Final	1	12/05/2022
3	F5	F5-BIG-AFM-I2800 BIG-IP N/S: f5-iyug-txze	BIG-IP 14.1.0 Build 0.0.116 Final	1	12/10/2022

Tabla N° 1. Equipamiento de seguridad adicional a Gestionar (Propiedad EsSalud).

- El contratista deberá ejecutar revisiones del nivel de adopción de mejores prácticas con la finalidad de mejorar la postura de seguridad de los equipos cubiertos por su servicio.
- El contratista deberá ejecutar la evaluación de mejores prácticas de forma trimestral buscando cumplir al menos el promedio de la industria en la cual se encuentra la Entidad, teniendo que subsanar (con autorización del cliente) cualquier recomendación de mejora y documentar los motivos por las cuales no pueden ser subsanados en caso no puedan realizarlo.

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

5.1.3.1 Gestor de la Plataforma de Seguridad

El contratista debe asignar un personal con conocimientos profesionales y avanzados, con certificaciones vigentes nivel profesional de la marca o fabricante ofertado para ejecutar las tareas de operación complejas, elaboración de reportes, configuración avanzada, actualización, administración y troubleshooting. Así mismo será el responsable de la trasferencia de conocimientos hacia el personal encargado de la supervisión, control y gestión de la plataforma. Algunas actividades se podrán realizar de manera remota y otras on site dependiendo de la severidad de los casos. La asignación de tiempo de este recurso deberá ser de 10 horas por cada semana como mínimo por el primer año de servicio, este recurso deberá contar con la certificación nivel profesional de la marca propuesta.

5.2 Capacitación

El contratista se obliga a prestar las siguientes capacitaciones:

Un programa especializado para dos (02) personas que designe la Sub Gerencia de Comunicaciones de la GCTIC, orientado a brindar conocimientos, desarrollar las competencias y habilidades necesarias para planificar y ejecutar eficientemente proyectos de TI y gerencia del conocimiento y alinear las estrategias de TI con la estrategia empresarial todo esto orientado al marco conceptual del presente servicio público; con una duración de (60) horas como mínimo. Debe incluir la entrega de certificado de asistencia.

Curso de capacitación oficial nivel asociado en la solución ofertada para tres (03) personas que designe la Sub Gerencia de Comunicaciones de la GCTIC, con una duración de (40) horas como mínimo. Debe incluir la entrega de certificado de asistencia.

El contratista deberá gestionar los recursos necesarios para el correcto dictado de las capacitaciones, como sistema de proyección, una PC por alumno, manuales, físicos o digitales, para lo cual el capacitador deberá estar certificado en la marca de los productos ofertados.

Todas las capacitaciones podrán ser dictadas bajo la modalidad presencial y/o virtual, los horarios y las fechas programadas se realizarán previa coordinación con la Sub Gerencia de Comunicaciones de la GCTIC, el plazo para iniciar la capacitación será máximo a los noventa (90) días calendario, contados a partir de la suscripción del contrato.

5.3 Garantía Comercial de la Solución

La garantía de los componentes para la prestación de los servicios será entregada por el contratista a ESSALUD. Para este fin, el contratista presentará la Carta de Garantía del Fabricante especificando la garantía de la marca, modelo, número y el tiempo de la garantía de cada uno de los componentes nuevos implementados. Este documento se presentará una vez culminada la implementación.

5.3.1 Alcance de la Garantía

La garantía del servicio ofertado por el contratista debe cubrir defectos de diseño y/o fabricación, averías o fallas de funcionamiento, y no detectable al momento que se otorgó la conformidad. Para lo cual deberá de cubrir los componentes y mano de obra asociados

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

con el reemplazo de cualquier componente que fallará, dentro del período de garantía ofrecido por el contratista.

Incluirá el reemplazo de los equipos y/o suministros y/o accesorios y/o materiales que se encuentren defectuosos por causas de fabricación por originales y nuevos dentro del plazo de garantía ofertado (3 años mínimo).

5.3.2 Condiciones de la Garantía

Todas las actividades a las que está obligado a realizar el contratista para cumplir con lo indicado a continuación serán sin costo para ESSALUD (incluye mano de obra y fletes) hasta la sede donde los componentes estarán implementados:

- En circunstancias donde la plataforma que soporta el servicio ofrecido esté comprometido para su correcto funcionamiento, tales como averías de hardware por causas de fabricación y/o vicios ocultos o aquellas donde los tiempos de diagnóstico o reemplazo dependan de terceros (por ejemplo, escalamiento de soporte a la marca o garantía del fabricante), el contratista, en un plazo no mayor de 4 horas luego del diagnóstico del primer nivel de soporte[24], deberá entregar e implementar sin costo para ESSALUD, los equipos y/o componentes requeridos con similares o mayores características para la continuidad de los servicios ofrecidos, hasta que concluya con la solución de la avería de manera definitiva.
- El contratista deberá contar con depósito de partes o equipos completos con presencia local en el país, y poder ofrecer mínimamente reemplazo de partes en un tiempo máximo de 24 horas, para poder garantizar el funcionamiento de la solución en caso no haya afectación de servicios. En caso que el/los equipos provoquen degradación o pérdida del servicio contratado, el tiempo máximo de reemplazo deberá ser de 4 horas.
- Al finalizar el servicio los equipos solicitados deberán quedar como propiedad de EsSalud.

5.3.3 Periodo de la Garantía

El contratista debe garantizar los productos a suministrar según el siguiente detalle:

Componentes de Seguridad y Conectividad	Garantía del Fabricante
• Servicio de Seguridad perimetral • Servicio de Seguridad Nacional y Servidores • Servicio de Administración centralizada de firewalls • Servicio para conectividad de plataforma de seguridad • Servicio de Seguridad para Correo Electrónico • Servicio de Visibilidad y Gestión de Riesgo en la Red • Licencias de Software de la Solución	3 años

[24] Absolución de Consultas y Observaciones N° 169, ITALTEL PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

El inicio del cómputo del periodo de garantía será a partir del día siguiente de suscrita el Acta de aprobación de la Implementación de la Solución **Anexo C.**

5.3.4 Disponibilidad de Servicios

En las contrataciones que conlleven la ejecución de prestaciones, tales como mantenimiento, reparación o actividades afines, el CONTRATISTA debe otorgar una garantía adicional por este concepto, mediante una Declaración Jurada, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas, no pudiendo eximirse su presentación en ningún caso. [25]

6 REQUISITOS DEL CONTRATISTA Y/O PERSONAL

6.1. Del Contratista

El Contratista deberá ser una empresa jurídica del rubro de tecnologías de información y/o telecomunicaciones, especializada en la implementación, configuración, gestión y resolución de problemas de plataforma de seguridad. El contratista debe acreditar mediante una carta del fabricante o representante de la marca ofertada en el cual precise si cumple con Certificación Vigente en:

CALIFICACIONES DEL CONTRATISTA	
Partnership en la marca ofertada	Permite demostrar la experiencia y capacidad de desarrollar las soluciones empresariales de seguridad, routing & switching, con profunda experiencia en los productos de la marca y tecnología propuesta, que permiten obtener el más alto servicio por parte del contratista garantizando la continuidad de los servicios de ESSALUD para el servicio solicitado.
Acreditación en especialización en la Arquitectura de Seguridad en la marca ofertada	Demuestra la experiencia en la solución de arquitectura de seguridad por parte del contratista con las marcas propuestas, con la cual nos garantiza una alta especialización en la implementación, configuración y resolución de problemas de la plataforma de seguridad.

Las cartas deben de presentarse como parte de la documentación para suscribir el contrato.

6.2. Del Personal Clave

El personal del Contratista debe estar conformado por los siguientes perfiles y contar con los siguientes conocimientos y experiencia, las cuales deberán ser sustentadas y adjuntadas dentro de su propuesta técnica:

CALIFICACIONES DEL PERSONAL CLAVE

[25] Absolución de Consultas y Observaciones N° 136, INDRA PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

UN (01) **JEFE DE PROYECTO Y SUPERVISOR DE PROYECTO**	Requisitos: **Profesional titulado o Bachiller en:** Ingeniería de Sistemas e Informática, o Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. Actividades a Realizar: Estará a cargo de la dirección general del proyecto, será el encargado de efectuar las coordinaciones directas con el Coordinador – EsSalud y/o con la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, durante la etapa de la implementación.
UN (01) **LIDER TÉCNICO – IMPLEMENTACIÓN**	Requisitos: **Técnico o Bachiller en:** Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, Computación e Informática, o Redes y Comunicaciones de Datos[26] [27] o, Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. Actividades a Realizar: El líder técnico estará a cargo de supervisión de las tareas de instalación, configuración y puesta en funcionamiento, durante la etapa de la implementación.

V°B° Ing. Ricardo Silvera C. Sub Gerente (e) – GERENCIA DE COMUNICACIONES GPGCTIC – ESSALUD

[26] Absolución de Consultas y Observaciones N° 1, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[27] Absolución de Consultas y Observaciones N° 76, VERIFICACIÓN Y CONTROL DE DATOS SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

DOS (02) ESPECIALISTAS TÉCNICOS – IMPLEMENTACIÓN	Requisitos: **Técnico o Bachiller en:** Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Computación e Informática, o Redes y Comunicaciones de Datos[28] [29], o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. Actividades a Realizar: Los especialistas técnicos estarán a cargo de las tareas de instalación, configuración y puesta en funcionamiento, durante la etapa de la implementación.
UN (01) GESTOR DE PLATAFORMA DE SEGURIDAD	Requisitos: **Técnico o Bachiller en:** Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, o Computación e Informática, o Redes y Comunicaciones de Datos[30] [31], o Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. Actividades a Realizar: El Gestor de la plataforma de Seguridad debe ejecutar las tareas de operación complejas, elaboración de reportes, configuración avanzada, actualización, administración y troubleshooting. Así mismo será el responsable de la trasferencia de conocimientos hacia el personal

GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Santos C. Sub Gerente (e) SUB GERENCIA - ESSALUD

[28] Absolución de Consultas y Observaciones N° 2, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[29] Absolución de Consultas y Observaciones N° 77, VERIFICACIÓN Y CONTROL DE DATOS SAC
[30] Absolución de Consultas y Observaciones N° 3, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[31] Absolución de Consultas y Observaciones N° 78, VERIFICACIÓN Y CONTROL DE DATOS SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

	encargado de la supervisión, control y gestión de la plataforma. Algunas actividades se podrán realizar de manera remota y otras on site dependiendo de la severidad de los casos.
DOS (02) ESPECIALISTAS DE SEGURIDAD	Requisitos: **Técnico o Bachiller en:** Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, o Computación e Informática, o Redes y Comunicaciones de Datos[32] [33] o Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. Actividades a Realizar: Estarán a cargo de las tareas configuración, soporte y operación del servicio, durante la ejecución del servicio.

Acreditación:

El grado de Bachiller y el título profesional requerido, 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.

Importante para la Entidad
El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.

En caso que, el grado de Bachiller y el título profesional requerido 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.

NOTA: Un mismo PERSONAL CLAVE no puede postularse a más de un perfil requerido.

[32] Absolución de Consultas y Observaciones N° 4, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[33] Absolución de Consultas y Observaciones N° 79, VERIFICACIÓN Y CONTROL DE DATOS SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

NOTA: La forma de acreditación del perfil y la experiencia, se encuentran detalladas en los REQUISITOS DE CALIFICACIÓN.

NOTA: Se acreditará con copia simple de certificados, u otros documentos, según corresponda, las certificaciones requeridas del personal clave, en la presentación de ofertas.

IMPORTANTE: El personal propuesto por el POSTOR no podrá ser cambiado por el CONTRATISTA durante la ejecución del servicio, salvo fuerza mayor y/o caso fortuito y/o situación debidamente sustentada, la misma que será evaluada y aprobada por la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la Gerencia Central de Tecnologías de Información y Comunicaciones. [34]

7 RECURSOS A SER PROVISTOS POR EL CONTRATISTA

El contratista es responsable de asegurar todos los recursos necesarios para que la solución de seguridad asegure las funcionalidades requeridas por ESSALUD, tales como; Seguridad perimetral, Seguridad Nacional y Seguridad de Servidores, Administración centralizada de Firewalls y Switches para conectividad de plataforma de seguridad.

Incluir dos (02) estaciones para el monitoreo y gestión de la plataforma, el cual debe acondicionarse como mínimo con:

- ✓ (02) laptops, ultra ligera de última generación
- ✓ Procesador de tipo i7 de última generación
- ✓ Pantalla de 15.6
- ✓ Memoria DDR4 16GB,
- ✓ Disco Solido 512GB
- ✓ Capacidad de conexión wifi
- ✓ Conexión bluetooth
- ✓ Conexión Ethernet
- ✓ Sistema Operativo compatible con la entidad.
- ✓ Se debe incluir dos muebles (escritorio y silla ergonómica) para la instalación de estas dos estaciones de monitoreo, supervisión, troubleshooting y gestión de la solución de seguridad.

8 RECURSOS A SER PROVISTOS POR LA ENTIDAD

EsSalud proveerá el espacio en gabinete para la instalación de los componentes que el contratista estime necesarios para brindar el servicio de seguridad gestionada. Asimismo, proveerá puntos de datos y energía 220 VAC estabilizada para la implementación del servicio.

Se brindará al contratista los permisos y acceso necesario hacia el Centro de Datos de EsSalud para que puedan realizar las instalación y configuración de la solución ofertada, con las pruebas necesarias para la habilitación del servicio.

[34] Absolución de Consultas y Observaciones N° 137, INDRA PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

EsSalud coordinará con el proveedor actual de seguridad informática para brindar las facilidades en el proceso de migración de políticas y/o reglas de seguridad configuradas a la fecha de la implementación de la nueva solución. Así como en las pruebas que se realizaran previo a la salida en operación.

9 LUGAR Y PLAZO DE EJECUCIÓN

9.1 Lugar

La prestación del servicio se realizará en la Gerencia Central de Tecnologías de Información y Comunicaciones (Piso 6) de la Sede Central, ubicado en el Jr. Domingo Cueto 120 – Jesús María – Lima.

9.2 Plazo de Ejecución

El plazo de ejecución del Servicio de Seguridad Gestionada será de **mil noventa y cinco (1095) días calendarios**, contados a partir del día siguiente de suscrita el Acta de Implementación de Servicio de Seguridad Gestionada **Anexo C.**

10 ENTREGABLES

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD

El Proveedor deberá presentar los siguientes entregables:

N°	Entregable	Periodo	Procedimiento
1	Plan de Trabajo	05 días calendarios	Acta de aceptación según Anexo A suscrito por la Subgerencia de Comunicaciones de la GCTIC
2	Plan de Implementación	15 días calendario posterior a la firma del Acta - Anexo A	Acta de aceptación según Anexo B suscrito por la Subgerencia de Comunicaciones de la GCTIC
3	Informe detallado de los trabajos y actividades de implementación del Servicio de Seguridad Gestionada, con la lista de productos con versiones, topología, licencias, descripciones, equipamiento, recomendaciones y conclusiones.	90 días calendario	Acta de aceptación según Anexo C suscrito por la Subgerencia de Comunicaciones de la GCTIC
4	Información de los contactos respectivos (número de teléfonos y correos electrónicos) y un cuadro de escalamiento comercial y atención de incidentes, una vez	90 días calendario	Acta de aceptación según Anexo C suscrito por la Subgerencia de Comunicaciones de la GCTIC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

N°	Entregable	Periodo	Procedimiento
	culminada la implementación del servicio.		
5	Informe mensual detallando actividades, trabajos, incidencias y acciones realizadas durante el periodo del servicio de seguridad gestionada de la plataforma.	**Mensual** A los 5 días calendario posterior a la finalización del periodo	Acta de aceptación según Anexo D suscrito por la Subgerencia de Comunicaciones de la GCTIC

***NOTA:** El periodo de días, se contabilizará a partir del día siguiente de suscrito el contrato.*

Todos los **Entregables** deberán ser entregados en dos (02) juegos en formato impreso o digital (PDF) y editable. Toda la información debe ser a colores.

11 PENALIDAD

En caso de retraso de la entrega del plan de trabajo, de la subsanación del plan de trabajo, de la entrega del plan de implementación, de la subsanación del plan de implementación, de la implementación de la solución, de la entrega del informe mensual, por caída del servicio, retraso de la entrega de los equipos o de los certificados de la capacitación, la Entidad le aplicará al contratista una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente. Esta penalidad será deducida de los pagos a cuenta, del pago final o en la liquidación final; o si fuese necesario se cobrará del monto resultante de la ejecución de las garantías de fiel cumplimiento o por el monto diferencial de oferta.

En caso de que el contratista incumpla con lo descrito se calculará de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto Mensual}}{F \times \text{Plazo en días}}$$

Donde:

Para **plazos menores o iguales** a **sesenta días: F = 0.40**
Para **plazos mayores a sesenta días: F = 0.25**

Cuando se llegue a cubrir el monto máximo de la penalidad, la Entidad podrá resolver el contrato por incumplimiento.

12 OTRAS PENALIDADES

Ítem	Incumplimiento	Penalidad	Procedimiento
A	La no subsanación por cada avería que corresponden a una atención presencial.	50 % de la UIT por cada atención no atendida	Según informe de la Sub Gerencia de Comunicaciones – GCTIC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

B	La no subsanación por cada avería que corresponden a una atención remota	50 % de la UIT por cada atención no atendida	Según informe de la Sub Gerencia de Comunicaciones - GCTIC

13 OTRAS OBLIGACIONES

13.1 Otras obligaciones del Contratista

El contratista debe garantizar la participación de la totalidad del personal clave propuesto, descrito en su propuesta técnica, la misma que debe acreditarse con la correspondiente declaración jurada de cumplimiento. Documentos que serán presentados a la suscripción del contrato.

Al inicio de los trabajos, el contratista hará entrega de una lista con los nombres del jefe de proyecto y del equipo de trabajo a la Sub Gerencia de Comunicaciones de la Gerencia de Producción - GCTIC

El contratista es el responsable directo y absoluto de las actividades que realizara, sea directamente o a través de su personal, debiendo responder por el servicio brindado.

El contratista será responsable de los deterioros, daños, pérdidas y/o sustracciones que sufrieran los bienes de propiedad de EsSalud por acción, desconocimiento o negligencia de su personal, debiendo reparar los daños causados o reemplazar los bienes a satisfacción de la Entidad.

A EsSalud no le corresponderá ninguna responsabilidad en caso de accidentes, daños, mutilaciones, invalidez o muerte de los trabajadores del contratista o terceras personas, que pudieran ocurrir durante la ejecución del contrato, con ocasión o como consecuencia del mismo.

13.2 Otras obligaciones de la Entidad

ESSALUD, a través de la Sub Gerencia de Comunicaciones de la Gerencia de Producción - GCTIC, proporcionará (siempre y cuando disponga del área o ambiente) un espacio para el almacenaje de los componentes y demás elementos que forman parte de la implementación, cuya responsabilidad por los daños en la propiedad física, pérdida de materiales, herramientas u otros NO será atribuible a ESSALUD.

14 ANTICORRUPCIÓN

El Contratista declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a raves 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,

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

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.

15 CONFIDENCIALIDAD

El contratista se compromete a mantener en confidencialidad y reserva absoluta la información que recabe y tenga acceso de ESSALUD, quedando prohibido revelar la información que le sea proporcionada a terceros, para lo cual se suscribirá un Acta de Confidencialidad y Reserva de la Información – **Anexo** E, la misma que será presentada a la suscripción del contrato.

16 MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

Área de coordinación con el proveedor

Con el propósito de viabilizar los trabajos de configuración, la Sub Gerencia de comunicaciones, designará un "Coordinador-Essalud" cuya tarea principal estará enfocada en el control, monitoreo y seguimiento periódico de las actividades que serán ejecutadas.

El contratista programará reuniones con el Coordinador – EsSalud para revisar y exponer el avance de la implementación de acuerdo al plan de trabajo presentado, el cual será Informado a la Sub Gerencia de Comunicaciones acerca de los avances, observaciones o problemas que se susciten durante el desarrollo de la implementación, para su evaluación y aprobación correspondiente.
En el caso de que el contratista requiera efectuar el cambio del personal encargado del proyecto, este deberá de contar como con la aprobación de la Sub Gerencia de Comunicaciones Gerencia de Producción - GCTIC para lo cual deberá de presentar toda la documentación técnica (copia de títulos, certificados de cursos, certificados de trabajo, etc.) necesaria que sustente que el nuevo personal cumple con el mismo perfil del profesional inicial.

Dicha solicitud deberá ser realizada de manera formal, es decir, el contratista que requiera efectuar el cambio del profesional encargado del proyecto deberá de presentar su solicitud dirigida a la Sub Gerencia de Comunicaciones Gerencia de Producción - GCTIC a través de mesa de partes de EsSalud.

Área responsables de las medidas de control

El coordinador designado por la sub Gerencia de Comunicaciones de la Gerencia de Producción - GCTIC, efectuara el monitoreo, seguimiento y control respectivo durante el tiempo de implementación.

Área que brindará la Conformidad

De la Implementación del Servicio

La conformidad de la implementación del servicio será otorgada por la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, de acuerdo al cumplimiento

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

de las actividades descritas en el ***numeral 5.1.2 Implementación de la Solución*** y la firma del Acta de Implementación del Servicio de Seguridad Gestionada – **Anexo C.**

De la Prestación del Servicio

La conformidad de la prestación del servicio mensual será otorgada por la Subgerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, de acuerdo al cumplimiento de las actividades descritas en el ***numeral 5.1.3 Soporte Gestionado de Seguridad*** y la firma del Acta de Conformidad del Servicio – **Anexo D.**

De la Capacitación

La conformidad del servicio de capacitación, será emitida por la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, quien verificará el cumplimiento del servicio de acuerdo a lo solicitado en el ***numeral 5.2 Capacitación*** del presente términos de referencia.

De la Puesta en Funcionamiento de la Solución

Las pruebas de puesta en funcionamiento para la conformidad técnico – operativa se realizarán en presencia del personal técnico y/o profesional de la Sub Gerencia de Comunicaciones y el contratista

17 FORMA DE PAGO

El pago para la ejecución del servicio se realizará a través de **treinta y seis (36) armadas** de igual valor, previa verificación de la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC a través de Actas de Conformidad del servicio (Anexo D), para lo cual el contratista deberá presentar el informe solicitado en el **ítem 5 del numeral 10. ENTREGABLES.**

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD

El contratista deberá entregar el Informe por cada periodo por mesa de partes de ESSALUD dentro de los (05) días calendarios siguientes a la culminación de cada periodo, para ser revisado y aprobado por la Sub Gerencia de Comunicaciones de la Gerencia de Producción de la GCTIC, quien emitirá un informe y el Acta de Conformidad del Servicio (Anexo D) correspondiente al periodo.

18 RESPONSABILIDAD POR VICIOS OCULTOS

De acuerdo al artículo 40° de la Ley de Contrataciones del Estado y artículo 146° de su Reglamento, el plazo máximo de responsabilidad del contratista para esta contratación será de dos (02) años, contados a partir de la última conformidad otorgada por la entidad.

19 ANEXOS

- Anexo A: Acta de Aprobación de Plan de Trabajo.
- Anexo B: Acta de Aprobación de Plan de Implementación.
- Anexo C: Acta de Implementación del Servicio de Seguridad Gestionada.
- Anexo D: Acta de Conformidad del Servicio
- Anexo E: Compromiso de Confidencialidad y reserva de la informa.

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

ANEXO A

ACTA DE APROBACIÓN DE PLAN DE TRABAJO

Siendo las..... horas del día....., se procede a redactar la presente Acta de Aprobación de Plan de Trabajo para la "Contratación del Servicio de Seguridad Gestionada"
El contratista a la fecha, ha cumplido con elaborar y proporcionar los siguientes documentos:

- ✓ Lista de actividades y su descripción.
- ✓ Personal propuesto y responsables por actividad
- ✓ Procedimiento de Trabajo.
- ✓ Cronograma de Trabajo en Project.
- ✓ Plan de Seguridad y Medio Ambiente.
- ✓ Lista de Personal.
- ✓ Organigrama del equipo de trabajo.
- ✓ SCTR (Salud y Pensión) vigente del personal.

Firman dando fe de lo anterior.

.....
Lugar y Fecha

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Sánchez C. Sub Gerente (e) - ESSALUD -

.....
SELLO Y FIRMA
Sub Gerencia de Comunicaciones de la Gerencia Central de Tecnologías de la Información y Comunicaciones

.....
SELLO Y FIRMA
Contratista: Representante Legal

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

ANEXO B

ACTA DE APROBACIÓN DE PLAN DE IMPLEMENTACIÓN

Siendo las..... horas del día....., se procede a redactar la presente Acta de Aprobación de Plan de Implementación para la "Contratación del Servicio de Seguridad Gestionada"
El contratista a la fecha, ha cumplido con elaborar y proporcionar los siguientes documentos:

- Plan de Implementación de la Solución (componentes de seguridad y conectividad).
- Arquitectura de la solución que se utilizará para brindar el servicio.
- Diagramas de seguridad y conectividad.
- Plan de Migración de la Solución.
- Plan de Protocolo de Pruebas de la Solución.
- Elaboración del plan de trabajo (Gantt), conteniendo como mínimo lo siguiente: objetivo, metas y cronograma de actividades.

Firman dando fe de lo anterior.

.....
Lugar y Fecha

SUB GERENCIA DE COMUNICACIONES GPTICTIC
V°B°
Ing. Ricardo Stanzas C.
Sub Gerente (e)

.....
SELLO Y FIRMA
Sub Gerencia de Comunicaciones de la Gerencia Central de Tecnologías de la Información y Comunicaciones

.....
SELLO Y FIRMA
Contratista: Representante Legal

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

ANEXO C

ACTA DE IMPLEMENTACIÓN DEL SERVICIO DE SEGURIDAD GESTIONADA

Siendo las..... horas del día....., se procede a redactar la presente Acta de conformidad de la Implementación del Servicio - prestación principal del proceso "Contratación del de Servicio de Seguridad Gestionada.

El contratista a la fecha, ha cumplido con:

- Implementación de Servicio de Seguridad Gestionada.

Cabe indicar que la solución instalada cuenta con una garantía de bienes que puede hacerse efectivo inmediatamente después de suscribir la presente acta.

Por medio del presente informo que el contratista ..... da inicio al cómputo del periodo de garantía.

Firman dando fe de lo anterior.

.....
Lugar y Fecha

V°B° SUB GERENCIA DE COMUNICACIONES GP-GCTIC ESSALUD

.....
SELLO Y FIRMA
Sub Gerencia de Comunicaciones de la Gerencia Central de Tecnologías de la Información y Comunicaciones

.....
SELLO Y FIRMA
Contratista: Representante Legal

www.essalud.gob.pe

Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

ANEXO D

ACTA DE CONFORMIDAD DEL SERVICIO MENSUAL DE SOPORTE GESTIONADO DE SEGURIDAD

Se deja constancia que el Contratista "_____", ha cumplido con las actividades del **"SERVICIO DE SEGURIDAD GESTIONADA PARA ESSALUD"**, correspondiente al periodo del _____ Al _____ de acuerdo al numeral 5.1.3 Soporte Gestionado de Seguridad de los términos de referencia y a las condiciones contenidas en el Contrato Nº _____. Para lo cual, se adjunta el informe solicitado por EsSalud.

Firman dando fe de lo anterior.

Fecha: .....

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD

.....
SELLO Y FIRMA
Sub Gerencia de Comunicaciones de la Gerencia Central de Tecnologías de la Información y Comunicaciones

.....
SELLO Y FIRMA
Contratista: Representante Legal

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

ANEXO E

"COMPROMISO DE CONFIDENCIALIDAD Y RESERVA DE LA INFORMACIÓN"

Por medio de la presente, nos comprometemos a lo siguiente:

A mantener confidencialidad respecto de toda la información obtenida, a no divulgar ningún material o información a terceras personas sin la previa autorización escrita de EsSalud, a no utilizar la información para ningún otro propósito que no esté relacionado con el proceso "Contratación del de Servicio de Seguridad Gestionada", y a no utilizar la información de cualquier manera que pudiera generar conflictos con los intereses del Estado Peruano, sus funcionarios o dependencias.

La información obtenida será puesta a disposición de nuestro personal, ejecutivos, por motivos relacionados con el proceso "Contratación del Servicio de Seguridad Gestionada". Dicho personal conocerá este acuerdo y se encontrará igualmente obligado a mantener confidencialidad respecto de la información antes mencionada. Tomaremos todas las acciones que fuesen razonables para impedir la divulgación de cualquier información a cualquier persona, sin el previo consentimiento escrito de EsSalud.

Este acuerdo no se aplicará a la información que:

(i) A la fecha en la que fue divulgada a nosotros o a nuestros asesores era de conocimiento público o en cualquier momento a partir de esa oportunidad sea del conocimiento público (exceptuando aquel objeto del incumplimiento de este acuerdo por nosotros o nuestros asesores), o
(ii) A la fecha, ya se encuentre legalmente en nuestro poder y, por lo tanto, no esté sujeta al compromiso de confidencialidad.

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Alberto Sierra C. Sub Gerente (e) ESSALUD

Los derechos y obligaciones establecidos en este documento se regirán e interpretarán de acuerdo a lo dispuesto por las leyes peruanas y las partes acuerdan someterse irrevocablemente a la jurisdicción y competencia de los jueces y tribunales de Lima, Perú.

Lugar y fecha: ....., ... de ..... de 2021.

.....
SELLO Y FIRMA
Representante Legal
Contratista

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

3.1. REQUISITOS DE CALIFICACIÓN

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	Requisitos: **UN (01) JEFE DE PROYECTO Y SUPERVISOR DEL PROYECTO** Profesional titulado o Bachiller en: Ingeniería de Sistemas e Informática, o Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. **UN (01) LÍDER TÉCNICO – IMPLEMENTACIÓN** Técnico o Bachiller en: Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, Computación e Informática, o Redes y Comunicaciones de Datos[35] [36] o, Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. **DOS (02) ESPECIALISTAS TÉCNICOS – IMPLEMENTACIÓN** Técnico o Bachiller en: Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Computación e Informática, o Redes y Comunicaciones de Datos[37] [38], o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. **UN (01) GESTOR DE PLATAFORMA DE SEGURIDAD** Técnico o Bachiller en: Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, o Computación e Informática, o Redes y

GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD

[35] Absolución de Consultas y Observaciones N° 1, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[36] Absolución de Consultas y Observaciones N° 76, VERIFICACIÓN Y CONTROL DE DATOS SAC
[37] Absolución de Consultas y Observaciones N° 2, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[38] Absolución de Consultas y Observaciones N° 77, VERIFICACIÓN Y CONTROL DE DATOS SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

	Comunicaciones de Datos[39] [40], o Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. **DOS (02) ESPECIALISTAS DE SEGURIDAD** Técnico o Bachiller en: Redes y Comunicaciones, electrónica, Telecomunicaciones o Sistemas o Ingeniería de Sistemas e Informática, o Computación e Informática, o Redes y Comunicaciones de Datos[41] [42] o Ingeniería Electrónica y Telecomunicaciones, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería Electrónica con mención en Telecomunicaciones, o Ingeniería de Sistemas Empresariales, o Ingeniería Industrial y de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniería de Computación y de Sistemas, o Ingeniería Informática y de Sistemas, o Ingeniería de Redes y Comunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Empresarial y de Sistemas, o Ingeniería de Estadística e Informática, o Ingeniería de Sistemas y Cómputo, o Ingeniería Eléctrica. Acreditación: El Titulo, Grado de Bachiller o Título Técnico será verificado por el comité de selección 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 Titulo, Grado de Bachiller o Título Técnico 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.3.2	**CAPACITACIÓN**
	Requisitos: **UN (01) JEFE DE PROYECTO Y SUPERVISOR DEL PROYECTO** • Capacitación en Gestión de Proyectos (Mínimo 35 horas lectivas) [43] [44] • Certificación Project Management Professional (PMP) • Se acreditará con copia simple de certificados o diplomas **UN (01) LÍDER TÉCNICO – IMPLEMENTACIÓN** • De manera opcional la capacitación a nivel Experto o Arquitecto o Profesional o Nivel 4

[39] Absolución de Consultas y Observaciones N° 3, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[40] Absolución de Consultas y Observaciones N° 78, VERIFICACIÓN Y CONTROL DE DATOS SAC
[41] Absolución de Consultas y Observaciones N° 4, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[42] Absolución de Consultas y Observaciones N° 79, VERIFICACIÓN Y CONTROL DE DATOS SAC
[43] Absolución de Consultas y Observaciones N° 80, VERIFICACIÓN Y CONTROL DE DATOS SAC
[44] Absolución de Consultas y Observaciones N° 122, INDRA PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

	o Nivel Máximo según corresponda del fabricante (Mínimo 80 horas) [45] [46] [47] [48] • La Certificación deberá ser de manera obligatoria vigente a nivel Experto o Arquitecto o Profesional o Nivel 4 o Nivel Máximo del fabricante, según corresponda, en la marca propuesta [49]. [50] [51] [52] • Se acreditará con copia simple de certificados o diplomas. **DOS (02) ESPECIALISTAS TÉCNICOS – IMPLEMENTACIÓN** • De manera opcional la capacitación a nivel Profesional o Administrador o Nivel 3 (Máximo 48 horas lectivas) [53] [54] • La Certificación deberá ser de manera obligatoria vigente a nivel Profesional o Administrador o Nivel 3 en la marca propuesta en Seguridad o Routing and Switching [55] [56] • Se acreditará con copia simple de certificados o diplomas. **DOS (02) ESPECIALISTAS DE SEGURIDAD** • De manera opcional la capacitación a nivel Asociado o Profesional o Nivel 3 (Máximo 48 horas lectivas) [57] [58] [59] [60] • La Certificación deberá ser de manera obligatoria vigente a nivel Asociado o Profesional o Nivel 3 en la marca propuesta en Seguridad. [61] • Se acreditará con copia simple de certificados o diplomas. [62] [63] **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**

V°B° Ing. Ricardo Siancas C. Sub Gerente (e)

[45] Absolución de Consultas y Observaciones N° 5 y N° 6, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[46] Absolución de Consultas y Observaciones N° 81 y N° 82, VERIFICACIÓN Y CONTROL DE DATOS SAC
[47] Absolución de Consultas y Observaciones N° 123, N° 124, INDRA PERÚ SAC
[48] Absolución de Consultas y Observaciones N° 170, ITALTEL PERU SAC
[49] Absolución de Consultas y Observaciones N° 5 y N° 6, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[50] Absolución de Consultas y Observaciones N° 81 y N° 82, VERIFICACIÓN Y CONTROL DE DATOS SAC
[51] Absolución de Consultas y Observaciones N° 123, N° 124, INDRA PERÚ SAC
[52] Absolución de Consultas y Observaciones N° N°171 ITALTEL PERU SAC
[53] Absolución de Consultas y Observaciones N° 83 y N° 84, VERIFICACIÓN Y CONTROL DE DATOS SAC
[54] Absolución de Consultas y Observaciones N° 7, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[55] Absolución de Consultas y Observaciones N° 83 y N° 84, VERIFICACIÓN Y CONTROL DE DATOS SAC
[56] Absolución de Consultas y Observaciones N° 7, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[57] Absolución de Consultas y Observaciones N° 8, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[58] Absolución de Consultas y Observaciones N° 85 y N° 86, VERIFICACIÓN Y CONTROL DE DATOS SAC
[59] Absolución de Consultas y Observaciones N° 125, INDRA PERÚ SAC
[60] Absolución de Consultas y Observaciones N° 172, ITALTEL PERÚ SAC
[61] Absolución de Consultas y Observaciones N° 8, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[62] Absolución de Consultas y Observaciones N° 85 y N° 86, VERIFICACIÓN Y CONTROL DE DATOS SAC
[63] Absolución de Consultas y Observaciones N° 125, INDRA PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

Requisitos:

UN (01) JEFE DE PROYECTO Y SUPERVISOR DEL PROYECTO
Experiencia no menor a cinco (05) años en gestión de proyectos de tecnología, supervisión de proyectos, gerente o sub gerente o jefe de Redes y Comunicaciones y/o Seguridad Informática.

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

UN (01) LÍDER TÉCNICO – IMPLEMENTACIÓN
Experiencia no menor a tres (03) [64] años como líder técnico o responsables en la implementación de Soluciones de Seguridad informática o Seguridad Perimetral o Seguridad Gestionada.

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

DOS (02) ESPECIALISTAS TÉCNICOS – IMPLEMENTACIÓN
Experiencia no menor de un (01) año [65] como especialistas en la implementación de Soluciones de Seguridad informática o Seguridad Perimetral o Seguridad Gestionada.

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

UN (01) GESTOR DE PLATAFORMA DE SEGURIDAD
Experiencia no menor a tres (03) años como Gestor de Plataforma de Seguridad o Solucione de Seguridad Informática o Seguridad Perimetral o Seguridad Gestionada.

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

DOS (02) ESPECIALISTAS DE SEGURIDAD
Experiencia no menor a tres (03) años como especialista en soporte de Soluciones de Seguridad Informática y/o seguridad perimetral y/o seguridad gestionada.

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,*

[64] Absolución de Consultas y Observaciones N° 87, VERIFICACIÓN Y CONTROL DE DATOS SAC
[65] Absolución de Consultas y Observaciones N° 88, VERIFICACIÓN Y CONTROL DE DATOS SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

	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	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 4'000,000.00 (Cuatro millones 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. Se consideran servicios similares a los siguientes: - Servicio de Administración de Infraestructura de Seguridad y/o - Servicio de Implementación de Seguridad Perimetral y/o - Servicio de Gestión y/o soporte de seguridad informática y/o - Servicio de Seguridad Gestionada de Red de Datos y/o - Servicio de Gestión y/o Soporte de Firewall y/o - Servicio de Internet y Seguridad Gestionada y/o - Venta y/o Servicio de Firewall Perimetral y/o - Venta y/o Servicio de Firewall de Data center y/o - Venta y/o Servicio de Plataforma de Seguridad y/o - Venta y/o Servicio de Soluciones de Cibserseguridad (Firewalls, Antispam, Filtro Web, IPS, Análisis de Seguridad, Detección de Amenazas Avanzadas) y/o, - Venta y/o Servicio de Soluciones de Networking (Switches LAN) [66] [67] [68] 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

V°B° Ing. Ricardo Serras C. Gerente (e)

[66] Absolución de Consultas y Observaciones N° 9, IMPERIA SOLUCIONES TECNOLÓGICAS SAC
[67] Absolución de Consultas y Observaciones N° 114, VERIFICACIÓN Y CONTROL DE DATOS SAC
[68] Absolución de Consultas y Observaciones N° 131, INDRA PERÚ SAC

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

	documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[69], 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 solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. 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. 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 caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de una persona absorbida 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.

[69] 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".*

www.essalud.gob.pe
Jr. Domingo Cueto 120
Jesús María
Lima 11 - Perú
T.: 265-6000 / 265-7000

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 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 documentalmente, y no mediante declaración jurada.*

SUB GERENCIA DE COMUNICACIONES GP-GCTIC V°B° Ing. Ricardo Siancas C. Sub Gerente (e) ESSALUD