GERENCIA CENTRAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

OFICINA DE SEGURIDAD INFORMÁTICA

TÉRMINOS DE REFERENCIA

CONTRATACIÓN DEL SERVICIO DE UNA MALLA DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI

Firmado digitalmente por RIEGA RIEGA Larry Edwin Anibal FAU 20131257750 soft
Motivo: Doy V° B°
Fecha: 11.12.2024 16:45:03 -05:00

Lima, 2024

CONTENIDO

1. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del Servicio de una Malla de Seguridad Informática e implementación del Sistema de Gestión de Seguridad de Información – SGSI

2. FINALIDAD PUBLICA

Proteger la red de datos institucional y los sistemas informáticos, la información y los datos evitando que se concreten los ataques o amenazas y vulnerabilidades, ya sean estos externos o internos, permitiendo contar con una solución de seguridad para la red de datos institucional, y así contar con un esquema de seguridad de la información adecuado que permitirá atender los requerimientos de los usuarios y proveedores de los servicios de ESSALUD; además, de proteger la información de la institución, manteniendo la seguridad en el intercambio de información interna con otras instituciones, entes externos y usuarios que hacen uso de la red de comunicaciones y de los sistemas de información de ESSALUD a través de internet, y así poder mantener la seguridad y operatividad de la red corporativa, la confidencialidad, la integridad y la disponibilidad de la información gestionada y de los servicios proporcionados por ESSALUD, para beneficio de los asegurados; y que sea la base para la implementación de un Sistema de Gestión de Seguridad de la Información – SGSI bajo el marco de la NTP ISO/IEC 27001:2022 para un proceso misional de ESSALUD.

3. ANTECEDENTES

Que, con fecha 08/JUN/2021, el Comité de Selección, adjudicó la buena pro del Concurso Público N° 006-2020-ESSALUD-1, para la CONTRATACIÓN DEL SERVICIO DE SEGURIDAD GESTIONADA PARA ESSALUD, al consorcio conformado por TELECOM BUSINESS SOLUTIONES SAC y VERIFICACIÓN Y CONTROL DE DATOS SAC, y con Contrato N° 4600055559 del 01/JUL/2021, por el cual se inicia la relación contractual con ESSALUD, por un periodo de tres (03) años, el cual inicio el 17/NOV/2021 y su fecha de vencimiento es el 16/NOV/2024. Es por ello que se hace necesario dotar de las herramientas tecnológicamente vigentes y de tipo corporativo que permitan realizar un adecuado control, protección y administración de las herramientas de seguridad de la información y protección de la red de datos de ESSALUD.

Que, la Ley N° 1412 Ley de Gobierno Digital tiene por objeto establecer el marco de gobernanza del gobierno digital para la *adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales* en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.

Que, el Decreto Supremo N° 029-2021-PCM, el cual aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo; dado que en el artículo 1. Objeto, del Decreto Supremo N° 029-2021-PCM, se estable: *regular las actividades de gobernanza y gestión de las tecnologías digitales en las entidades de la Administración Pública en materia de Gobierno Digital, que comprende la identidad digital, interoperabilidad, servicios digitales, datos, seguridad digital y arquitectura digital, así como establecer el marco jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales en los tres niveles de gobierno, conforme a lo señalado en el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital (en adelante la Ley), con observancia de los deberes y derechos fundamentales previstos en la Constitución Política del Perú y en los tratados internacionales de derechos humanos y otros tratados internacionales ratificados por el Perú.*

Que, en el artículo 8. Gestión de las tecnologías digitales, del Decreto Supremo N° 029-2021-PCM, se determina que: *las unidades de organización de tecnologías de la información o las que hagan sus veces en las entidades públicas son responsables de la planificación, implementación, ejecución y supervisión del uso y adopción de las tecnologías digitales como habilitantes de la implementación de la cadena de valor, soluciones de negocio, modelos de negocio o similares priorizadas en el marco de los instrumentos de gestión de la entidad, con el propósito de permitir alcanzar sus objetivos estratégicos, crear valor público y cumplir con lo establecido por el Comité de Gobierno Digital.*

Que, en el numeral 115.1 del artículo 115. Pruebas para evaluar vulnerabilidades, del Decreto Supremo N° 029-2021-PCM, se determina que: Las entidades públicas planifican y realizan pruebas para evaluar vulnerabilidades a los siguientes activos: *aplicativos informáticos, sistemas, infraestructura, datos y redes, que soportan los servicios digitales, procesos misionales o relevantes de la entidad; así también, en el numeral 115.2 se establece que: Los resultados de las pruebas realizadas constan como información documentada por la entidad. La Presidencia del Consejo de ministros, a través de la Secretaría de Gobierno Digital, solicita dichos resultados en el marco de sus funciones de supervisión o cuando lo considere necesario para la gestión de un incidente de seguridad digital.*

Que, actualmente los ataques, se caracterizan por el uso de tecnología que constantemente está escaneando redes a nivel mundial que son de interés de los atacantes los cuales se infiltran para robar información crítica, desestabilizar comunicaciones, robo y daño de las bases de datos, entre otras actividades dolosas e ilegales que pueden significar el

colapso de una red de datos, siendo estos ataques muchas veces anónimos y difíciles de determinar su autoría. Todas las tecnologías de infraestructura son explotadas por los atacantes, pudiendo transferir información con servidores criminales en Internet, denegación de servicios, ataques de fuerza bruta y comprometer servicios y archivos confidenciales, claves, o inclusive descargar malware adicional con resultados desastrosos en la red de datos institucional. El éxito de los ataques está directamente relacionado con la exposición de servicios de las entidades a Internet.

Que, en cumplimiento del Texto Actualizado y Concordado del Reglamento de Organización y Funciones del Seguro Social de Salud - ESSALUD aprobado por Resolución de Presidencia Ejecutiva Nº 686-PE-ESSALUD-2024. Referente a los presentes términos de referencia, se detallan las siguientes funciones descritas en el: *Artículo 115° Oficina de Seguridad Informática:*

b) Formular, implementar, controlar y evaluar las políticas de seguridad informática, control y administración de datos relativos a los sistemas de información, recursos informáticos y su entorno físico a fin de brindar una adecuada protección, con base en los planes aprobados.

j) Desarrollar las acciones para implementar el control interno y administrar los riesgos que correspondan en el ámbito de sus funciones, en el marco de las políticas y procedimientos establecidos.

Que, en el Decreto Legislativo N° 1412, en su Artículo 31.- Marco de Seguridad Digital del Estado Peruano, se determina que: *El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.*

Que, con fecha 08/ENE/2016, la Presidencia del Consejo de ministros emite la Resolución Ministerial N° 004-2016-PCM, que dispone el uso obligatorio de la *Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición (ahora: NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición*), el cual establece un plazo máximo de 02 años para su implementación en todas las entidades integrantes del sistema nacional de Informática.

4. OBJETIVOS DE LA CONTRATACIÓN

4.1. Objetivo General:

Proteger la Información de la Red de datos Institucional, contra ataques cibernéticos y otras amenazas avanzadas persistentes a fin de asegurar la continuidad operativa de los servicios, y protección de la información crítica de la entidad, así como asegurar la prestación segura y confiable de los servicios que se brinda a la población asegurada, en el marco de la norma ISO/IEC 27032, que proporciona orientación para mejorar el estado de la ciberseguridad, extrayendo los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad; en base a las prácticas básicas de seguridad para las partes interesadas en el ciberespacio, ofreciendo una visión general de la ciberseguridad y una definición de roles y tratamiento de riesgos; y para la implementación adecuada de un Sistema de Gestión de Seguridad de la Información – SGSI bajo el marco de la NTP ISO/IEC 27001:2022.

4.2. Objetivos Específicos:

a. Detener las amenazas en forma proactiva.

b. Contar con una arquitectura tecnológica de seguridad que garantice la continuidad operativa de **ESSALUD.**

c. Contar con reportes que permitan tomar decisiones adecuadas al personal de seguridad de la información.

d. Gestionar de forma eficiente las plataformas tecnológicas de seguridad bajo los criterios enmarcados en los dominios de seguridad de la información de las normas técnicas peruanas (NTP) vigentes.

e. Prevenir ataques cibernéticos como malware, phishing, ransomware y ataques de denegación de servicio.

f. Proteger la confidencialidad, integridad y disponibilidad de la información, garantizando que solo las personas autorizadas puedan acceder a ella, que no se modifique de manera no autorizada y que esté disponible cuando se necesite.

g. Reducir el riesgo de pérdida financiera, debido a la interrupción del negocio, el robo de datos o los daños a la reputación.

h. Mejorar la seguridad de los empleados, clientes y socios, protegiendo su información personal y confidencial.

i. Implementación del Sistema de Gestión de Seguridad de la Información – SGSI en los sistemas de información que dan soporte al proceso misional P.M1 Gestión del aseguramiento en salud y P.M2 Gestión de las prestaciones, del Seguro Social de Salud – **ESSALUD.**

5. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

El alcance de la presente contratación de servicio de la malla de seguridad e implementación del Sistema de Gestión de Seguridad de Información – SGSI, y es transversal a **ESSALUD.**

a. Descripción del servicio

El servicio consiste en contar con una malla de seguridad informática, la misma que debe ser íntegramente implementada por el contratista para su correcta operación.

ÍTEM	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN DEL SERVICIO
1	01	Servicio	Contratación del Servicio de una Malla de Seguridad Informática e implementación del Sistema de Gestión de Seguridad de Información – SGSI

b. Alcance del servicio

a. Implementar, configurar e instalar los equipos de seguridad informática para su operación.
b. Implementar el Sistema de Gestión de Seguridad de la Información – SGSI bajo el estándar NTP ISO/IEC 27001:2022.

A continuación, se detalla la descripción del equipamiento mínimo requerido para el servicio, el cual corresponde en su conjunto la Contratación del Servicio de una Malla de Seguridad Informática e implementación del Sistema de Gestión de Seguridad de Información – SGSI para ESSALUD.

5.1. Del equipamiento mínimo requerido para el Servicio de una Malla de Seguridad Informática e implementación del Sistema de Gestión de Seguridad de Información – SGSI

5.1.1. Equipamiento y funcionalidades del servicio requerido.

El presente servicio debe contemplar mínimamente los siguiente equipos y componentes.

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

EQUIPOS DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO I	
Cantidad	02 UNIDADES DE TIPO CORTAFUEGOS (01 CLÚSTER EN HA)
RENDIMIENTO MÍNIMO (POR CADA EQUIPO)	
Rendimiento en Prevención de Amenazas	Rendimiento (throughput) de 14 Gbps como mínimo (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, Antivirus, Anti-Bot o Antispyware y Emulación Malware día-cero.
Rendimiento en NGFW - Next Generation Firewall	Rendimiento (throughput) de 16 Gbps como mínimo (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones e IPS) o considerando las funcionalidades de firewall definidas por cada fabricante
Sesiones Concurrentes	11'000,000 conexiones o sesiones concurrentes; o 4'000,000 sesiones concurrentes como mínimo medidos en HTTP.
Conexiones por segundo	745,000 conexiones o sesiones por segundo; o 300,000 sesiones por segundo como mínimo medidos en HTTP.
Tamaño	Altura de 01 RU como mínimo, para ser instalado en gabinete de 19"
Interfaces de red	08 interfaces 10 GB SFP+ **(incluido transceiver)** Capacidad de soportar ampliación para 02 interfaces 40 GB QSFP+ 04 puertos de red 1GB (RJ45)
Fuentes Redundantes	02 fuentes de poder redundantes.
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO [1] [2]	
~~Consideraciones Generales~~	~~▪ El fabricante de la solución de seguridad debe estar presente en los últimos seis 06 reportes de Gartner (Magic Cuadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.~~
Alta Disponibilidad	▪ Los firewalls ofertados deben poder implementarse y operar en modalidad de Alta Disponibilidad en modo Activo-Activo y modo Activo-Pasivo. ▪ Debe soportar redundancia de hasta 04 enlaces ISP (Internet Service Provider) redundantes con capacidades de SD-WAN, considerando una licencia adicional o software/hardware de terceros de ser necesaria. ▪ Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster, así como contar con mecanismos de detección de fallas y detección de pérdida de enlaces.

[1] Absolución de consultas y observaciones Nº 24, 28,29 JAPAN COMPUTER SERVICE S.A.C.

[2] Absolución de consultas y observaciones Nº 83,84 NEXUSS ENTERPRISES S.A.C.

Funcionalidades de Red	▪ La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode). ▪ Deben soportar inspección del tráfico cifrado (SSL/HTTPS). ▪ Debe soportar enrutamiento con IPv4 e IPv6. ▪ Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación. ▪ Soporte de rutas estáticas, PBR (policy based routing) o PBF (Policy-Based Forwarding), LACP, OSPF (IPv4 e IPv6), RIP, BGP, IGMP, PIM, Ipsec Routing y Dual Stack IPv4 e IPv6 (NAT para comunicación iniciada por IPv4 e iniciada por IPv6), NAT64, NAT46 (NAT para comunicación iniciada por IPv4) y NAT66 o NPTv6. ▪ La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. ▪ El soporte a políticas de ruteo permite que, ante la presencia de dos enlaces, se pueda decidir por que enlace egresa tráfico determinado. ▪ La solución debe soportar políticas de ruteo estático en IPv6.
Gestión de políticas	▪ El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, direcciones de URL y aplicaciones. ▪ Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Deny o Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final; o similares. Las funcionalidades de ancho de banda y habilitación de autenticación podrán realizarse en políticas diferentes a las de seguridad. ▪ Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. ▪ Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando. ▪ Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora). ▪ Debe tener capacidad de crear reglas de firewall en base a objetos dinámicos o listas dinámicas externas, los cuales son basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos CSV o Json o archivo de texto, con la finalidad de automatizar las reglas de acceso, no siendo necesario publicar y/o compilar reglas en el firewall.
Otras funcionalidades	▪ Administración accesible a través de SSH y de interfaz Web segura (HTTPS). ▪ La comunicación entre los servidores de administración y el equipo de seguridad (firewall), debe ser cifrada y autenticada. ▪ Integración mediante API REST de Terceros. ▪ Los firewalls deben permitir manejo de ancho de banda de distintos protocolos y/o aplicaciones, permitiendo la definición de niveles de ancho de banda tanto para carga (upload) y descarga (download).
Geolocalización	▪ Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos. ▪ Debe posibilitar la visualización de los países de origen y destino en los logs de acceso. ▪ Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
Prevencion de Intrusos - IPS	▪ La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad. ▪ El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento. ▪ A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, SQL Injection, Command Injection e injection protecction para DN (Distinguished Names) y/o evasión de técnicas TLS para DN (Distinguished Names) ▪ Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, IMAP, DNS tunneling, FTP, SNMP, IMAP, SMB. ▪ Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos. ▪ Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound. ▪ Debe incluir capacidad de filtro DNS alimentada por un servicio de inteligencia de amenazas de la propia marca. ▪ La funcionalidad de IPS debe tener las siguientes capacidades: o Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos.

	○ Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial. ○ Detección y prevención de comunicaciones de malware salientes.
Anti-Bot o AntiSpyware	▪ La solución debe proveer una herramienta que haga descubrimiento de "bots" o host comprometidos dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados "bots" o host comprometidos hacia las redes de los atacantes en Internet (botnet) o command and control. ▪ La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL, direcciones IP y/o recursos DNS no identificados y/o no clasificados. ▪ La solución debe tener una capa de protección DNS, para protección contra ataques basados en Algoritmos de Generación de Dominio (DGA), así como protección fuga o exfiltración de información mediante DNS Tunneling. ▪ La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y/o los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).
VPN	▪ Debe soportar IPSec VPN Client-to-Site IPSec y VPN SSL con capacidad de usuarios ilimitada o hasta el máximo de usuarios que permita la capacidad del equipo. ▪ Debe soportar túneles VPN punto a punto Site-to-Site IPSEC con capacidad de usuarios ilimitada o hasta el máximo de usuarios que permita la capacidad del equipo. ▪ Para VPN IPSec deben ser soportados AES-128 y AES-256 para las fases I y II de IKE. ▪ Para VPN IPSec debe soportar integridad de datos con MD5 y SHA1, SHA-256, SHA-512 para las fases I y II de IKE. ▪ Para VPN IPSec debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Group19 (256-bit ECP) y Group20 (384-bit ECP). ▪ Debe incluir soporte a las topologías VPNs site-to-site: Todos a todos, Oficinas Remotas a Sitio Central (hub and spoke) y Sitio remoto a través del sitio central hacia otro sitio remoto (full mesh). ▪ Debe poder integrarse con Directorio Activo Microsoft u Open LDAP para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas y/o dispositivos, dirección IP y redes. ▪ Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN. ▪ El agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android e IOS. De ser requerido, se debe incluir el licenciamiento necesario para permitir esta capacidad. ▪ Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: Tokens (Ejemplo: SecureID), TACACS, RADIUS y Certificados Digitales. ▪ Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo. ▪ Se deberá incluir la autenticación de multi-factor para las cuentas VPN SSL mediante correo y/o token digital y/o físico y/o lógico (móvil, USB token). ▪ La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall, para comunicaciones VPN SSL. ▪ La solución deberá permitir el acceso remoto (VPN SSL) bajo identificación de usuario desde cualquier dispositivo móvil.
Control de aplicaciones y Filtro de Navegación (URLs)	▪ La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web. ▪ Se requiere que la detección de aplicaciones cuente con una base de datos (firmas) para la identificación de al menos 4,000 aplicaciones reconocidas. ▪ La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática. ▪ Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante. ▪ Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías y/o categorías similares para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Hacking, Artificial Intelligence (AI) y Spyware/ Malicious Sites. ▪ La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0 o aplicaciones SaaS, Widgets o aplicaciones de colaboración y base de datos de URL. ▪ Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.

	▪ Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos. ▪ Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios. ▪ La solución debe categorizar las aplicaciones y URLs por factor de riesgo. ▪ Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario. ▪ La solución debe proporcionar un mecanismo para limitar el uso de ancho de banda (tanto para carga (upload) y descarga (download)) por las aplicaciones, para controlar el consumo de ancho de banda por el tipo de aplicación y/o servicio de red definido. ▪ Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones. ▪ Debe ser capaz de analizar el tráfico cifrado para identificar amenazas, sin necesidad de descifrar el tráfico. ▪ Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2. ▪ Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).
Prevención de amenazas	▪ Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS. ▪ Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red. ▪ Los equipos deben tener integrada la detección y prevención de virus y amenazas (anti-malware). ▪ Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP. ▪ Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real. ▪ Debe soportar Inspección de tráfico cifrado/encriptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound). ▪ Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades: o Bloquear ataques en canal SSH. o Bloquea la transmisión de virus a través de los protocolos SCP y SFTP. o Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP. o Prevenir el reenvío de puertos SSH (Port Forwarding). ▪ Debe soportar el manejo personalizado (añadir, borrar o modificar) para la alimentación de IoC (Indicadores de Compromiso como IP, URL y dominios), en formato de archivo de texto y/o CSV y/o Structured Threat Information Expression (STIX XML). ▪ Debe tener capacidad de integración con fuente de IoC de terceros (External IoC como IP, URL y dominios) a través de direcciones web URL, con capacidades de detección y prevención. La aplicación y prevención de seguridad, en base a los IoC incluidos, debe ser de manera automática, sin interacción del usuario administrador.
Prevención de amenazas desconocidas o de día-cero	▪ La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables. ▪ La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática o a través de un equipo appliance o nube para la Emulación de Malware (SandBox) del propio fabricante. ▪ La solución debe proteger a los usuarios internos, de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados, si el archivo es benigno se entrega el archivo original al usuario y si el archivo el maligno se deniega su acceso o descarga, esto quiere decir la protección del paciente cero. ▪ La solución deberá poder emular archivos para la identificación de malware a través de un servicio de sandboxing del fabricante. ▪ La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (7Z, RAR y JAR), ejecutables (EXE, LNK, DLL, VBX o VBScript) y archivos de MacOS (APP o Mach-o, DMG, PKG). ▪ El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.

	▪ La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware. ▪ Tener habilitado la protección que al hacer una descarga por http/https, debe soportar modificar archivos (reconstruido durante su análisis) eliminando componentes riesgosos (código, link).
QoS	▪ Debe contar con un módulo integrado de Calidad de Servicio o QoS, que permita principalmente: o Priorización de tráfico crítico para el negocio, sobre el tráfico de menor prioridad (no critico). o Garantice el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia. o Otorgue acceso garantizado o prioritario a empleados específicos, incluso si acceden de forma remota a los recursos de la red. ▪ El QoS debe permitir la definición: o Porcentaje del ancho de banda disponible, basado en prioridad de regla. o Ancho de banda mínimo garantizado. o Ancho de banda máximo, basado en límites. ▪ Deberá permitir aplicar reglas de QoS para el tráfico cifrado de VPN. ▪ Debe tener capacidad de QoS Queuing para servicio de baja latencia (Low Latency) para poder definir clases especiales de servicio para aplicaciones "sensibles a demoras" como voz y video.
Identificación de usuarios	▪ La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como: o Sin agente, haciendo búsquedas al Directorio Activo Microsoft. o Con agente implementado en los servidores de Directorio Activo Microsoft. o Empleando un Portal Cautivo. o Empleando un Proveedor de Indentidad (IdP) basado en SAML. ▪ La solución debe integrarse con el Directorio Activo Microsoft sin la necesidad de instalar un agente en el Servidor de Dominio o en los equipos de los usuarios finales. ▪ La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall. ▪ La solución deberá permitir el acceso remoto bajo identificación de usuario desde cualquier dispositivo móvil, mediante VPN.

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

EQUIPO DE SEGURIDAD DE CORTAFUEGOS Y CONTROL DE NAVEGACIÓN WEB TIPO II	
Cantidad	02 unidades de tipo cortafuegos (01 clúster en HA)
RENDIMIENTO MÍNIMO (POR CADA EQUIPO)	
Rendimiento en Prevención de Amenazas	Rendimiento (throughput) de 24 Gbps como mínimo (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, Antivirus, Anti-Bot o Antispyware y Emulación Malware día-cero.
Rendimiento en NGFW - Next Generation Firewall	Rendimiento (throughput) de 25 Gbps como mínimo (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones e IPS) o considerando las funcionalidades de firewall definidas por cada fabricante
Sesiones Concurrentes	22'000,000 conexiones o sesiones concurrentes; o 10'000,000 sesiones concurrentes como mínimo medidos en HTTP.
Conexiones por segundo	950,000 conexiones o sesiones por segundo; o 450,000 sesiones por segundo como mínimo medidos en HTTP.
Tamaño	Altura de 01 RU como mínimo, para ser instalado en gabinete de 19"
Interfaces de red	08 interfaces 10 GB SFP+ **(incluido transceiver)** Capacidad de soportar ampliación para 02 interfaces 40 GB QSFP+ 04 puertos de red 1GB (RJ45)
Fuentes Redundantes	02 fuentes de poder redundantes.
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO[3] [4]	
~~Consideraciones Generales~~	~~▪ El fabricante de la solución de seguridad debe estar presente en los últimos seis 06 reportes de Gartner (Magic Cuadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.~~
Alta Disponibilidad	▪ Los firewalls ofertados deben poder implementarse y operar en modalidad de Alta Disponibilidad en modo Activo-Activo y modo Activo-Pasivo.

[3] Absolución de consultas y observaciones Nº 24, 28, 29 JAPAN COMPUTER SERVICE S.A.C.

[4] Absolución de consultas y observaciones Nº 83,84 NEXUSS ENTERPRISES S.A.C.

	▪ Debe soportar redundancia de hasta 04 enlaces ISP (Internet Service Provider) redundantes con capacidades de SD-WAN, considerando una licencia adicional o software/hardware de terceros de ser necesaria. ▪ Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster, así como contar con mecanismos de detección de fallas y detección de pérdida de enlaces.
Funcionalidades de Red	▪ La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode). ▪ Deben soportar inspección del tráfico cifrado (SSL/HTTPS). ▪ Debe soportar enrutamiento con IPv4 e IPv6. ▪ Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación. ▪ Soporte de rutas estáticas, PBR (policy based routing) o PBF (Policy-Based Forwarding), LACP, OSPF (IPv4 e IPv6), RIP, BGP, IGMP, PIM, Ipsec Routing y Dual Stack IPv4 e IPv6 (NAT para comunicación iniciada por IPv4 e iniciada por IPv6), NAT64, NAT46 (NAT para comunicación iniciada por IPv4) y NAT66 o NPTv6. ▪ La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. ▪ El soporte a políticas de ruteo permite que, ante la presencia de dos enlaces, se pueda decidir por que enlace egresa tráfico determinado. ▪ La solución debe soportar políticas de ruteo estático en IPv6.
Gestión de políticas	▪ El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, direcciones de URL y aplicaciones. ▪ Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Deny o Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final; o similares. Las funcionalidades de ancho de banda y habilitación de autenticación podrán realizarse en políticas diferentes a las de seguridad. ▪ Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. ▪ Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando. ▪ Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora). ▪ Debe tener capacidad de crear reglas de firewall en base a objetos dinámicos o listas dinámicas externas, los cuales son basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos CSV o Json o archivo de texto, con la finalidad de automatizar las reglas de acceso, no siendo necesario publicar y/o compilar reglas en el firewall.
Otras funcionalidades	▪ Administración accesible a través de SSH y de interfaz Web segura (HTTPS). ▪ La comunicación entre los servidores de administración y el equipo de seguridad (firewall), debe ser cifrada y autenticada. ▪ Integración mediante API REST de Terceros. ▪ Los firewalls deben permitir manejo de ancho de banda de distintos protocolos y/o aplicaciones, permitiendo la definición de niveles de ancho de banda tanto para carga (upload) y descarga (download).
Geolocalización	▪ Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos. ▪ Debe posibilitar la visualización de los países de origen y destino en los logs de acceso. ▪ Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
Prevencion de Intrusos - IPS	▪ La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad. ▪ El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento. ▪ A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, SQL Injection, Command Injection e injection protecction para DN (Distinguished Names) y/o evasión de técnicas TLS para DN (Distinguished Names) ▪ Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, IMAP, DNS tunneling, FTP, SNMP, IMAP, SMB.

	▪ Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos. ▪ Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound. ▪ Debe incluir capacidad de filtro DNS alimentada por un servicio de inteligencia de amenazas de la propia marca. ▪ La funcionalidad de IPS debe tener las siguientes capacidades: o Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos. o Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial. o Detección y prevención de comunicaciones de malware salientes.
Anti-Bot o AntiSpyware	▪ La solución debe proveer una herramienta que haga descubrimiento de "bots" o host comprometidos dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados "bots" o host comprometidos hacia las redes de los atacantes en Internet (botnet) o command and control. ▪ La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de URL, direcciones IP y/o recursos DNS no identificados y/o no clasificados. ▪ La solución debe tener una capa de protección DNS, para protección contra ataques basados en Algoritmos de Generación de Dominio (DGA), así como protección fuga o exfiltración de información mediante DNS Tunneling. ▪ La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y/o los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).
VPN	▪ Debe soportar IPSec VPN Client-to-Site IPSec y VPN SSL con capacidad de usuarios ilimitada o hasta el máximo de usuarios que permita la capacidad del equipo. ▪ Debe soportar túneles VPN punto a punto Site-to-Site IPSEC con capacidad de usuarios ilimitada o hasta el máximo de usuarios que permita la capacidad del equipo. ▪ Para VPN IPSec deben ser soportados AES-128 y AES-256 para las fases I y II de IKE. ▪ Para VPN IPSec debe soportar integridad de datos con MD5 y SHA1, SHA-256, SHA-512 para las fases I y II de IKE. ▪ Para VPN IPSec debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Group19 (256-bit ECP) y Group20 (384-bit ECP). ▪ Debe incluir soporte a las topologías VPNs site-to-site: Todos a todos, Oficinas Remotas a Sitio Central (hub and spoke) y Sitio remoto a través del sitio central hacia otro sitio remoto (full mesh). ▪ Debe poder integrarse con Directorio Activo Microsoft u Open LDAP para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas y/o dispositivos, dirección IP y redes. ▪ Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN. ▪ El agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android e IOS. De ser requerido, se debe incluir el licenciamiento necesario para permitir esta capacidad. ▪ Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: Tokens (Ejemplo: SecureID), TACACS, RADIUS y Certificados Digitales. ▪ Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo. ▪ Se deberá incluir la autenticación de multi-factor para las cuentas VPN SSL mediante correo y/o token digital y/o físico y/o lógico (móvil, USB token). ▪ La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall, para comunicaciones VPN SSL. ▪ La solución deberá permitir el acceso remoto (VPN SSL) bajo identificación de usuario desde cualquier dispositivo móvil.
Control de aplicaciones y Filtro de Navegación (URLs)	▪ La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web. ▪ Se requiere que la detección de aplicaciones cuente con una base de datos (firmas) para la identificación de al menos 4,000 aplicaciones reconocidas. ▪ La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.

	▪ Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante. ▪ Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías y/o categorías similares para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Hacking, Artificial Intelligence (AI) y Spyware/ Malicious Sites. ▪ La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0 o aplicaciones SaaS , Widgets o aplicaciones de colaboración y base de datos de URL. ▪ Debe alertar al usuario cuando una aplicación o página web fuera bloqueada. ▪ Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos. ▪ Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios. ▪ La solución debe categorizar las aplicaciones y URLs por factor de riesgo. ▪ Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario. ▪ La solución debe proporcionar un mecanismo para limitar el uso de ancho de banda (tanto para carga (upload) y descarga (download)) por las aplicaciones, para controlar el consumo de ancho de banda por el tipo de aplicación y/o servicio de red definido. ▪ Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones. ▪ Debe ser capaz de analizar el tráfico cifrado para identificar amenazas, sin necesidad de descifrar el tráfico. ▪ Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2. ▪ Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).
Prevención de amenazas	▪ Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS. ▪ Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red. ▪ Los equipos deben tener integrada la detección y prevención de virus y amenazas (anti-malware). ▪ Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP. ▪ Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real. ▪ Debe soportar Inspección de tráfico cifrado/encriptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound). ▪ Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades: o Bloquear ataques en canal SSH. o Bloquea la transmisión de virus a través de los protocolos SCP y SFTP. o Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP. o Prevenir el reenvío de puertos SSH (Port Forwarding). ▪ Debe soportar el manejo personalizado (añadir, borrar o modificar) para la alimentación de IoC (Indicadores de Compromiso como IP, URL y dominios), en formato de archivo de texto y/o CSV y/o Structured Threat Information Expression (STIX XML). ▪ Debe tener capacidad de integración con fuente de IoC de terceros (External IoC como IP, URL y dominios) a través de direcciones web URL, con capacidades de detección y prevención. La aplicación y prevención de seguridad, en base a los IoC incluidos, debe ser de manera automática, sin interacción del usuario administrador.
Prevención de amenazas desconocidas o de día-cero	▪ La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables. ▪ La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática o a través de un equipo appliance o nube para la Emulación de Malware (SandBox) del propio fabricante. ▪ La solución debe proteger a los usuarios internos, de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados, si el archivo es benigno se entrega el archivo original al usuario y si el archivo el maligno se

	deniega su acceso o descarga, esto quiere decir la protección del paciente cero. ▪ La solución deberá poder emular archivos para la identificación de malware a través de un servicio de sandboxing del fabricante. ▪ La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (7Z, RAR y JAR), ejecutables (EXE, LNK, DLL, VBX o VBScript) y archivos de MacOS (APP o Mach-o, DMG, PKG). ▪ El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema. ▪ La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware. ▪ Tener habilitado la protección que al hacer una descarga por http/https, debe soportar modificar archivos (reconstruido durante su análisis) eliminando componentes riesgosos (código, link).
QoS	▪ Debe contar con un módulo integrado de Calidad de Servicio o QoS, que permita principalmente: o Priorización de tráfico crítico para el negocio, sobre el tráfico de menor prioridad (no critico). o Garantice el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia. o Otorgue acceso garantizado o prioritario a empleados específicos, incluso si acceden de forma remota a los recursos de la red. ▪ El QoS debe permitir la definición: o Porcentaje del ancho de banda disponible, basado en prioridad de regla. o Ancho de banda mínimo garantizado. o Ancho de banda máximo, basado en límites. ▪ Deberá permitir aplicar reglas de QoS para el tráfico cifrado de VPN. ▪ Debe tener capacidad de QoS Queuing para servicio de baja latencia (Low Latency) para poder definir clases especiales de servicio para aplicaciones "sensibles a demoras" como voz y video.
Identificación de usuarios	▪ La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como: o Sin agente, haciendo búsquedas al Directorio Activo Microsoft. o Con agente implementado en los servidores de Directorio Activo Microsoft. o Empleando un Portal Cautivo. o Empleando un Proveedor de Indentidad (IdP) basado en SAML. ▪ La solución debe integrarse con el Directorio Activo Microsoft sin la necesidad de instalar un agente en el Servidor de Dominio o en los equipos de los usuarios finales. ▪ La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall. ▪ La solución deberá permitir el acceso remoto bajo identificación de usuario desde cualquier dispositivo móvil, mediante VPN.

C. EQUIPO DE SEGURIDAD ADMINISTRACIÓN CENTRALIZADA DE CORTAFUEGOS

EQUIPO DE SEGURIDAD ADMINISTRACIÓN CENTRALIZADA DE CORTAFUEGOS	
Cantidad	01 unidad
Factor de forma	Tipo Rack (Para gabinete 19") 1 RU como mínimo
Almacenamiento	04 TB RAID-1
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
Descripción	▪ Una consola de gestión centralizada, con capacidad de gestión de mínimo 04 Firewalls. ▪ La consola debe tener un hardware (servidor) de propósito específico para los fines de gestión y configuración de políticas de seguridad.
Consideraciones generales	▪ Hardware y el software de gestión del propio fabricante de la solución de firewall ofertado. ▪ La consola centralizada debe permitir el despliegue de actualizaciones y parches de seguridad en los firewalls gestionados. ▪ La consola centralizada debe permitir revisar los cambios históricos en las políticas de seguridad, quien realizo los cambios y revertir los cambios a una versión especifica. ▪ La herramienta debe integrar en una única consola gráfica segmentando el estado general de todos los dispositivos administrados, la configuración de la política de seguridad, los logs registrados y el monitoreo de toda la plataforma.

	▪ Debe incluir una herramienta que administre centralizadamente la licencia de todos los equipos, controlados desde la estación de administración. ▪ La herramienta debe permitir sesiones concurrentes de diferentes usuarios o dispositivos para los cambios de políticas. ▪ La herramienta debe permitir la creación de perfiles de administradores, basados en roles, que accedan a secciones parciales de administración o a la totalidad, indicando también si los perfiles son de solo lectura o lectura/escritura. ▪ La herramienta debe permitir el acceso concurrente de administradores, la modificación de la política de seguridad, la publicación de los cambios realizados antes de aplicarlos y la segregación de funciones según el administrador. ▪ Capacidad de automatización mediante API, para organizar los flujos de trabajo, en los procesos de seguridad de TI. ▪ Se debe poder adicionar una capa adicional de seguridad, adicional a los tipos de autenticación indicados anteriormente, mediante el uso de certificado digital. ▪ Debe tener una herramienta o capacidad de: gestión de certificados de usuario final (ICA) o similares, crear certificados, recrear CRL (listas de revocación) y remover los certificados expirados.

D. SEGURIDAD GESTOR DE LOG Y CORRELACIÓN DE EVENTOS FIREWALL

EQUIPO DE SEGURIDAD GESTOR DE LOG Y CORRELACIÓN DE EVENTOS FIREWALL	
Cantidad	**01 unidad**
Factor de forma	Tipo Rack (Para gabinete 19") 1 RU como mínimo
Almacenamiento	24 TB utilizables RAID-1 o superior
Capacidad	19,500 logs por segundo o ~~600~~ 60 Gb por día de log [5][6][7]
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
Descripción	▪ Una consola centralizada para el almacenamiento de logs (registros), correlación de eventos de seguridad y reportes, con capacidad de 04 Firewalls. ▪ La consola debe tener un hardware de propósito específico para los fines de almacenamiento de logs (registros) y correlación de eventos. ▪ El software de correlación de eventos y reportes debe ser del propio fabricante de la solución de firewall ofertado.
Capacidad de Correlación de Eventos y reportes	▪ Solución unificada de análisis y gestión de eventos de seguridad que permitan obtener información gráfica de gestión de amenazas. ▪ Solución que permite consolidar miles de millones de registros y mostrarlos como eventos de seguridad prioritarios para que se pueda responder ante los incidentes de seguridad y realizar las acciones necesarias para evitar más ataques. ▪ Debe permitir profundizar directamente desde el evento que se está viendo hasta la regla inmediata en la política de seguridad. ▪ Debe permitir el análisis de datos en tiempo real o casi en tiempo real y los registros de eventos de manera personalizada, también notificación inmediata a los administradores para permitir una acción rápida y/o remediación. ▪ Capacidad de habilitar un "horario laboral" para detectar intentos no autorizados de accesos a sistemas protegidos y otras operaciones prohibidas fuera del horario laboral, el cual podrá ser cumplido a través de filtros de atributos personalizables ▪ Capacidad de realizar excepciones y parametrizar los umbrales para evitar "falsos positivos" en las acciones de mitigación o respuesta automática. ▪ Debe contar con un catálogo propio de vistas interactivas y reportes, para poder explotar la información en periodos personalizados. ▪ Debe poder crear vistas y reportes propios (custom) empleando tablas y/o charts

[5] Absolución de consultas y observaciones N° 10 DANAE CONTRATISTAS GENERALES EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADO - DANAE CONTRATISTAS GEN.

[6] Absolución de consultas y observaciones N° 30 JAPAN COMPUTER SERVICE S.A.C..

[7] Absolución de consultas y observaciones Nº 85 TELEFÓNICA TECH PERÚ S.A.C.

	▪ Debe soportar como tipos de eventos por lo menos: ataques de denegación de servicio, anomalías de red, actividad basada en host y/o rastreos no autorizados y/o logins no autorizados. ▪ Posibilidad de calendarizar reportes predefinidos o customizados, para su entrega automática vía correo electrónico. ▪ Debe permitir exportar en formato XLSX o PDF los reportes generados.

E. EQUIPO DE SEGURIDAD EMULACIÓN DE MALWARE (SANDBOX)

EQUIPO DE SEGURIDAD EMULACIÓN DE MALWARE (SANDBOX)	
Cantidad	▪ Servicio debe incluir 01 equipo
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
Tipo	▪ Equipo de seguridad de propósito especifico. ▪ La solución debe integrarse y operar con los firewalls de seguridad de TIPO I.
Emulación	Debe realizar la emulación de malware a nivel de CPU o memoria RAM y a nivel de Sistema Operativo
Protocolos	HTTP, HTTPS para inspección de descargas de Internet, capacidad de inspección tráfico cifrado SSL/TLS.
	SMTP, IMAP, POP3 para inspección de archivos adjuntos en correos electrónicos.
Tipo de archivos	▪ Deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (7Z, RAR y JAR), ejecutables (EXE, LNK, DLL, VBX o VBScript) y archivos de MacOS (APP o Mach-o, DMG, PKG). ▪ Análisis de malware en archivos comprimidos
Capacidades	8,000 archivos por hora, el cual no deberá estar basado en firmas, ni prefiltros, sino en emulación completa.
	10 máquinas virtuales de emulación (capacidad habilitada y licenciada) por cada equipo o se debe garantizar la máxima capacidad soportada por cada FW propuesto.
	Debe contar con un motor de análisis basado en Machine Learning (ML) o Deep Learning (DL) para detectar malware desconocido y ransomware de manera rápida.
	Debe contar con mecanismos para prevenir el uso de técnicas de evasión por parte del malware o soportar "bare metal analysis".
	Debe mostrar las técnicas de ataque utilizadas por el malware según la matriz del MITRE ATT&CK
Almacenamiento	900 GB SSD ~~en caso la solución sea~~ on premise[8]
Interfaces de Red y Puertos	04 puertos de red de cobre

F. SOLUCIÓN DE SEGURIDAD PARA CORREO ELECTRONICO

SOLUCIÓN DE SEGURIDAD PARA CORREO ELECTRONICO	
Cantidad	01 unidad
Factor de forma	Tipo Rack (Para gabinete 19") 1 RU como mínimo
Almacenamiento	02 TB RAID-1
FUNCIONALIDADES MÍNIMAS REQUERIDAS POR EQUIPO	
Descripción	• El equipo de seguridad para correo electrónico deberá ser nuevo sin uso en su integridad. Debe basarse en aplliance de propósito especifico y dedicado.
Consideraciones generales	• La solución debe tener características antispam, antivirus, anti-spyware y anti-phishing. • La solución debe permitir la notificación de alertas de antivirus y anti-spyware. • La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente. • 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 solución debe ser capaz de programar el envío de informes de cuarentena. • La solución debe ser compatible con el enrutamiento en IPv4 y IPv6.

[8] Absolución de consultas y observaciones Nº 12 DANAE CONTRATISTAS GENERALES EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADO - DANAE CONTRATISTAS GEN.

	• La solución debe ser capaz de realizar la inspección del correo de Internet entrante y saliente. • 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. • La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing. • La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS). • 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. • La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog). • La solución debe generar y enviar informes en formato PDF o HTML. • La solución debe permitir añadir un "descargo de responsabilidad" o disclaimer a los correos entrantes y salientes. El disclaimer podrá ser personalizado tanto en contenido, idioma y ubicación (al inicio del mensaje o al final del mensaje). • Soportar crear al menos 300 políticas por recipiente por dominio. • Soportar crear al menos 1000 políticas por recipiente por sistema. • Soportar enrutar al menos 600,000 mensajes por hora. • Soportar como mínimo 400,000 mensajes por hora con el análisis de antispam y antivirus habilitados.
Funcionalidades de Antispam y Antimalware	• La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam. • La solución puede detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante. • La solución puede detectar si un correo es spam revisando las URLs que esta contenga, comparándolas con la base de datos de reputación suministrada por el fabricante. • La revisión de URLs debe permitir seleccionar las categorías URL que serán permitidas o no en los correos analizados. Esta base de datos de categorías será actualizada por el fabricante. • La solución debe ser capaz de realizar análisis heurístico y definir umbrales máximos de acuerdo al comportamiento del correo y así determinar si un correo es spam. • La solución debe ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter). • La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words). • La solución debe contar con Diccionarios predefinidos de palabras que pueden ser escaneados en el correo electrónico. • La solución debe permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal y archivar • La solución debe ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6. • La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail. • La solución debe ser capaz de ejecutar el análisis antivirus / antispyware en archivos comprimidos como ZIP y RAR • La solución debe contar con una base de datos de malware suministrada por el fabricante y Terceros aliados, la cual puede ser actualizada recurrentemente. • La solución debe contar con capacidades de evaluar, retener y/o bloquear correos que cuenten con amenazas avanzadas, Dia-Zero mediante el análisis de archivos con herramientas de Sandboxing. • Debe permitir el análisis de sandboxing con soluciones on-premise o en la nube, sea del fabricante o de terceros. • Deberá incluir el licenciamiento para enviar archivos adjuntos a la herramienta de Sandboxing. • La solución debe permitir el desarmado y reconstrucción del contenido (CDR) para prevenir la infección de los equipos finales debido a correos con archivos adjuntos, hipervínculos, javascript y macros, sin afectar la integridad del contenido. • La solución debe analizar el contenido y adjuntos de un mensaje en busca de palabras que indiquen que el correo deba ser puesto en cuarentena, Cifrado, Archivado, Bloqueado, Taggeado, sobrescrito o reenviado a otro host.

G. CONMUTADOR DMZ

CONMUTADOR DMZ	
Cantidad	02 unidades
REQUERIMIENTOS MÍNIMOS POR EQUIPO	
Tipo	Rack 1RU
Estándar de gabinete	19" deberá incluir todos los accesorios de fabricante para fijación en gabinete de servidores
Puertos	48x10GbE SFP+ / 2x40GbE QSFP+ / 4x100GbE QSFP28
Patch cord / transceiver	▪ Debe incluir 48 transceiver a 10GbE SFP+ y debe incluir 20 transceiver a 1 GbE de Cobre para cada Switchs ▪ Debe incluir 48 patch cord de fibra multimodo 50/125µm (LSZH) min 3m / 10GbE SFP+ El dispositivo conmutador DMZ deberá soportar al menos los siguientes protocolos en capa 2 y capa 3. En capa 2 (enlace de datos): • Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) y Multiple Spanning Tree Protocol (MSTP) • Link Aggregation Control Protocol (LACP) • VLAN (Virtual Local Area Network) • Protocolo de Resolución de Direcciones (ARP) En capa 3 (red): • Enrutamiento estático y dinámico • Inter-VLAN Routing • VRRP[9]
Garantía del equipo	03 (tres) años garantía + RMA (Return Merchandise Authorization) con reemplazo a 04 horas del fabricante de la marca ofertada
Integridad	▪ Anclajes del mismo fabricante del conmutador ethernet de administración para instalación en gabinete (19")
Instalación	La implementación a realizar por EL PROVEEDOR, incluye labores de cableado estructurado (datos y eléctrico) bajo fibra óptica y cobre (en gabinete y líneas troncales), instalación de equipos en gabinete de servidores, conexión a gabinete de comunicaciones de los servicios a atender y aterramientos. Los puntos de conectividad de red deberán estar certificados y debidamente etiquetados.

5.1.2. Garantía de servicio. (Backup)

En caso que alguno de los componentes de la solución presente desperfectos, fallas o averías, consecutivas en un mes durante el periodo de vigencia de la garantía, **EL PROVEEDOR** deberá tener un componente Backup, con las mismas características ofertadas que lo reemplace y garantice la continuidad operativa del servicio.

5.1.3. Periodo de garantía de los equipos contemplados en el servicio: La Garantía será por un periodo no menor a los tres (03) años, los cuales se contabilizarán a partir del día siguiente de la firma del *Acta de* ***Conformidad de Puesta en Producción*** de los equipos y componentes implementados parte del servicio en el Centro de Datos de la Sede Central de **ESSALUD,** ubicado en Av. Arenales 1402 – Piso 6, Jesús María, Lima.

Se precisa que la garantía de los equipos contemplados en el servicio, incluyen las licencias de software de solución.

5.1.4. Devolución de equipamiento.

Culminado el plazo de ejecución del servicio, según lo descrito en el numeral 5.12.2, los equipos descritos en numeral 5.1.1. del presente Términos de Referencia, serán retirados de ESSALUD por el Proveedor, en un plazo de treinta (30) días hábiles.

Previa a la devolución del equipamiento, ESSALUD en coordinación con el PROVEEDOR, ejecutaran un procedimiento de borrado seguro, para garantizar la eliminación definitiva de los datos e información de propiedad de ESSALUD almacenada o tratada por el PROVEEDOR.

5.2. Actividades a desarrollar

5.2.1. Acondicionamiento, montaje e instalación

5.2.1.1. **EL PROVEEDOR** deberá presentar el Plan de Trabajo para Instalación vía por la mesa de partes digital a **través** del enlace: https://mpv.essalud.gob.pe/Login/Index; o a través de la mesa de partes física

[9] Absolución de consultas y observaciones Nº 46 JAPAN COMPUTER SERVICE S.A.C.

ubicada en la Av. Arenales N° 1402, Jesús María, Piso 2), en un plazo no mayor a los cinco (05) días calendarios posteriores a la suscripción del contrato, el cual será aprobado por el Jefe de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones, en un plazo no mayor de un (01) día calendario, emitiendo el *Acta de Conformidad al Plan de Trabajo para Instalación,* u observación del Plan de Trabajo, que deberá ser subsanada en un plazo no mayor de un (1) día por el **PROVEEDOR** para que se pueda continuar con cada una de las etapas indicadas e iniciar los trabajos de instalación de los componentes de la solución de la malla de seguridad propuesta.

El plan de trabajo deberá contemplar mínimamente las siguientes etapas: planeación, diseño, evaluación y operación de los equipos instalados.

5.2.1.2. **EL PROVEEDOR** implementará los componentes de la solución propuesta bajo los parámetros y normativas aprobadas por ESSALUD y bajo lo establecido en la NTP en materia de seguridad de la información.

5.2.1.3. **EL PROVEEDOR** deberá ingresar el equipamiento (el cual debe ser nuevo de primer uso) para el desarrollo del servicio, en un plazo no mayor a ~~treinta (30)~~ cuarenta y cinco (45)[10] días calendarios, contabilizado a partir del día siguiente de aprobado el **Plan de Trabajo**, por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones. La recepción de estos será en el Centro de Datos de la Sede Central de ESSALUD, ubicado en la Av. Arenales 1402, piso 6 en el Distrito de Jesús María, el cual será aprobado por el jefe de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones

5.2.1.4. **LA ENTIDAD** a través de la Oficina de Seguridad Informática de la Gerencia Central de tecnologías de Información y Comunicaciones, deberá verificar el equipamiento para el desarrollo del servicio, en un (01) día calendario, contabilizado a partir del día siguiente de ingresados a la Gerencia Central de Tecnologías de Información y comunicantes ubicado en Av. Arenales 1402 – Piso 6, Jesús María, Lima.

5.2.1.5. **EL PROVEEDOR** deberá instalar los componentes de la solución de la malla de seguridad propuesta, en el (los) gabinete(s) de la entidad, luego procederá con la instalación, configuración y puesta en marcha, estas actividades tendrán un plazo no mayor a diez (10) días calendarios (contados a partir de la culminación de la actividad precedente), pudiendo ampliarse este periodo hasta un máximo de veinte (20) días, previo sustento que justifique el motivo de ampliación por parte del proveedor. Finalizada la actividad, la Oficina de Seguridad Informática de la Gerencia Central de tecnologías de Información y Comunicaciones brindará conformidad a la Instalación.

5.2.1.6. Una **vez** notificada dicha conformidad, **EL PROVEEDOR** deberá dar inicio a la operatividad de la solución de la malla de seguridad propuesta (desconectar la solución actual para el inicio de la implementación adquirida por **ESSALUD**), esta actividad contará con una ventana de tiempo de máximo una (01) hora para contar con la operatividad del 100% de la solución de malla de seguridad propuesta y se emitirá un ***Acta de Conformidad de Puesta en Producción*** el cual será aprobado por el Jefe de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.

5.2.2. Capacitación en el Sistema de Gestión de Seguridad de la Información – SGSI

a. **EL PROVEEDOR** deberá presentar un cronograma de capacitación una vez culminada la implementación de la malla de seguridad informática (emitida el acta de conformidad de puesta en producción) en un plazo no mayor de tres (3) días calendarios, bajo las siguientes consideraciones:
   - Un (01) curso de Interpretación y Formación de Auditor Interno del Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001 con una duración de veinticuatro (24) horas, para un mínimo de veinte (20) participantes para cada uno de los procesos definidos.
   - Un (01) curso de Seguridad de la Información, ciberseguridad y protección de la privacidad – controles de seguridad de la información basado en el estándar ISO/IEC 27002 con una duración de veinticuatro (24) horas, para un mínimo de veinte (20) participantes por cada uno de los procesos definidos.
   - Un (01) curso de Evaluación de Riesgos basado en el estándar ISO 31000 con una duración de veinticuatro (24) horas, para un mínimo de veinte (20) participantes por cada proceso definido.

[10] Absolución de consultas y observaciones Nº 94TELEFÓNICA TECH PERÚ S.A.C.

- Una charla de sensibilización a la Alta Dirección sobre seguridad de la información con una (01) hora de duración, siendo la cantidad de personas definida por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.
- Un curso de Identificación y tratamiento de incidentes de seguridad de la información con una duración de dieciséis (16) horas, para un mínimo de veinte (20) participantes por cada proceso definido.
- Un (01) Taller de Capacitación de Tratamiento de No Conformidades con una duración de cuatro (04) horas, para un mínimo de veinte (20) participantes por cada proceso definido.

b. **EL PROVEEDOR** deberá entregar por cada curso, taller y/o capacitación realizada los certificados correspondientes.
c. Los cursos, capacitaciones y/o talleres deberán ser impartidas por un profesional certificado en ISO/IEC 27001 y/o ISO/IEC 27002 y/o ISO 31000.
d. Será de manera virtual y en horario laboral; la programación (fecha y hora) será acordada con **ESSALUD.**
e. **EL PROVEEDOR** deberá proveer la infraestructura tecnológica necesaria y grabación de la capacitación
f. La capacitación tendrá **un plazo máximo de ejecución** de 180 días calendario contados desde el día siguiente de firmado el *acta de conformidad de puesta en producción* hasta completar el periodo total de días antes mencionado, así mismo, el contratista al inicio de cada capacitación deberá entregar a cada participante los materiales necesarios.

g. Al finalizar las actividades descritas en el literal a. del numeral 5.2.2, **EL PROVEEDOR** deberá presentar un informe que contenga el syllabus de los temas tratados, los certificados para cada uno de los asistentes, el listado de asistencia firmado por los asistentes y el instructor y una copia de los materiales entregados en formato digital.

h. Los documentos deberán ser entregados a través de la Mesa de Partes de EsSalud ubicado en Av. Arenales N° 1402 Jesús María o en su defecto a través de la Mesa de Partes virtual de **ESSALUD** (https://mpv.EsSalud.gob.pe/Login), en un plazo no mayor de tres (3) días de culminado el plazo máximo de ejecución, el informe debe contener: el syllabus de los temas tratados, los certificados de los asistentes con la cantidad de horas dictadas, el listado de asistencia debidamente firmado por el personal designado y el instructor y una copia de los manuales y/o instructivos entregados a cada personal capacitado tanto en físico como en digital.

5.2.3. Desarrollo del servicio.

Una vez culminada la implementación de la malla de seguridad informática (emitida el acta de conformidad de puesta en producción) el proveedor deberá realizar lo siguiente:

5.2.3.1. Del servicio de Malla de Seguridad Informática.

- Soporte de la solución / servicio 24x7 por tres (03) años.
- Elaboración de informes ejecutivos, de gestión y reportes técnicos.
- Atenciones de mitigación de riesgos y vulnerabilidades y configuración de políticas de seguridad
- Bloqueos preventivos y a demanda.
- Gestión de funcionabilidades de comunicación de la malla de seguridad.
- Mantener la operatividad de la solución por toda la integración.
- Operación de las funcionalidades de administración centralizada.
- Operación de las funcionalidades de reportes y generadores de eventos.

5.2.3.2. Implementación del Sistema de Gestión de Seguridad de la Información bajo la NTP ISO/IEC 27001:2022

a. El alcance del Sistema de Gestión de Seguridad de la Información contempla como alcance los procesos misionales: P.M1 Gestión del Aseguramiento en salud y P.M2 Gestión de las Prestaciones, del Seguro Social de Salud – EsSalud, ubicados en la Sede Central y Complejo Arenales.

b. **EL PROVEEDOR** deberá elaborar la estructura del Sistema de Gestión de Seguridad de la Información – SGSI, conformado por las políticas, procedimientos y, base documental asociada dentro del alcance definido por **ESSALUD,** así como con los registros necesarios para asegurar el cumplimiento de los objetivos específicos de Seguridad de la Información.

<u>Etapa 1</u>: Planificación del Proyecto

En esta etapa **EL PROVEEDOR** deberá:

a. Elaborar y presentar del Acta de Constitución del Proyecto,
b. Elaborar el cronograma de actividades del proyecto,

c. Elaborar la matriz de identificación de documentos de cumplimiento de la norma ISO/IEC 27001:2022,
d. Elaborar la estructura documental que permita desarrollar los procesos o procedimientos del SGSI.
e. Elaborar la metodología detallada para la implementación del SGSI. Esta metodología debe incluir la identificación de todos los documentos y registros que el proveedor deberá elaborar y que permitan cumplir con los requisitos establecidos en la norma ISO/IEC 27001:2022 y el anexo de controles NTP ISO/IEC 27002:2022.
f. Hacer un diagnóstico de estado situacional para determinar el estado de cumplimiento de los requisitos de la NTP ISO/IEC 27001:2022 (análisis de brecha).

Etapa 2: Establecimiento del SGSI

En esta etapa **EL PROVEEDOR** deberá:

a. Presentar todo documento formato o registro establecido en la metodología detallada para la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.
b. Desarrollar talleres multidisciplinarios siguiendo lo establecido en la metodología y procedimiento para la gestión de riesgos de seguridad de la información y oportunidades del SGSI para elaborar las matrices de riesgo de seguridad de la información.
c. Identificar los activos de información a proteger en base a su identificación, clasificación y valorización.
d. Realizar la gestión de riesgos que permita identificar, analizar y valorar las potenciales amenazas asociados a los procesos definidos en el alcance del SGSI y a la información administrada o custodiada por las Áreas involucradas, su vulnerabilidad, la probabilidad de ocurrencia, su posible impacto y los controles que serán necesarios incorporar.
e. Para la gestión de riesgos tener en cuenta lo siguiente:
   - Definición y Aplicación de Riesgos, a los que están expuestos los activos identificados, los cuales deben:
     - o Establecer criterios de aceptación de riesgo de seguridad de la información.
     - o Identificar los riesgos de la seguridad de información y definir propietarios de estos.
     - o Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.
     - o Identificar las amenazas para aquellos activos.
     - o Identificar las vulnerabilidades que podrían ser explotados por las amenazas.
     - o Identificar los impactos que pueden tener, las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.
     - o Identificar propietarios de los riesgos

   - Analizar los Riesgos de seguridad de la información.
     - o Determinar riesgos en base a un análisis de consecuencias y probabilidad.
     - o Valorizar y ponderar las amenazas identificadas en el análisis de riesgos, con la finalidad de definir el alcance de aplicación de la NTP ISO/IEC 27001-2022, en coordinación con el Oficial de Seguridad y Confianza Digital (OSCD).

   - Evaluar los Riesgos de seguridad de la información y realizar priorizaciones.
     - o Seleccionar controles y objetivos de control.
     - o Establecer la Declaración de Aplicabilidad (SoA) para el tratamiento de riesgos tomando como referencia mínima, lo establecido en la norma NTP ISO/IEC 27001-2022:
       - Seleccionar controles
       - Producir la declaración de aplicabilidad
       - Formular el plan de seguridad de la información.

Etapa 3: Elaborar el Plan de Seguridad Digital

En esta etapa **EL PROVEEDOR** deberá:

a. Elaborar el Plan de Seguridad de la Información considerando los riesgos identificados y las brechas en temas de seguridad. En base a este plan se definirán e implementarán los controles necesarios que aseguren la reducción de los riesgos identificados, según lo definido en el plan de tratamiento de riesgos.
b. Elaborar las políticas, prácticas, estándares, procedimientos y toda información complementaria, que conformen las actividades del Plan de Seguridad de la Información que conduzcan a la implementación del SGSI.
c. Definir los controles y políticas para la seguridad de la información en la gestión de continuidad de negocio, que incluyan:
   - Planificación de continuidad de seguridad de la información.
   - Implementación de continuidad de seguridad de la información.

- Verificación, revisión y evaluación de continuidad de la seguridad de la información.
- Definir controles.

Etapa 4: Auditoría Interna

En esta etapa **EL PROVEEDOR** deberá:

a. Contratar un equipo de auditores internos para que realicen la auditoría interna al SGSI implementado en EsSalud.
b. Acompañar como observador durante la auditoría interna, deberá brindar soporte a las preguntas planteadas por el equipo de auditoría interna. Al finalizar el proceso de auditoría deberá analizar los hallazgos (no conformidades u oportunidades de mejora), de ser el caso analizar la causa raíz y proponer acciones correctivas o de mejora, las mismas que debe sustentar ante EsSalud para obtener la conformidad.
c. Elaborar y proponer, un plan de revisión periódica de la política y alcance del SGSI, así como de su eficacia. Asimismo, proponer un cronograma de revisiones de los niveles de riesgos residuales y riesgos aceptables.
d. Evaluar después de la implementación efectuada el nivel de cumplimiento entre los procedimientos y normas definidas (los cuales conforman el SGSI) para identificar falencias y mejoras posibles a las prácticas de seguridad definidas inicialmente.

El plazo máximo para la implementación del Sistema de Gestión de Seguridad de la Información, será de 240 días calendario, una vez otorgada el acta de conformidad de puesta en producción

5.2.3.3. Procedimiento de continuidad operativa permanente durante el periodo de servicio de las herramientas de seguridad soportadas

- Solicitudes ante la necesidad de corte de servicio solo se podrá programar con una ventana no mayor a una (01) hora de indisponibilidad, siendo este evento coordinado directamente con el Coordinador del Proyecto de la Oficina de Seguridad Informática y autorizado por esta, debiendo considerar que las actividades se realicen fuera del horario de oficina; toda coordinación adicional se deberá realizar a través del Coordinador del Proyecto de la Oficina de Seguridad Informática.
- El procedimiento de migración parte del servicio deberá considerar un corte no mayor a 60 minutos de inoperatividad, serán indicadas por el jefe de la Oficina de Seguridad Informática al momento de la firma del acuerdo de confidencialidad posterior a la firma del contrato del servicio entre el **PROVEEDOR** y **ESSALUD.**

5.2.3.4. Condiciones de operación del servicio

a. **EL PROVEEDOR** deberá garantizar que la solución de la malla de seguridad propuesta soportará labores de misión crítica. Opcionalmente, sus componentes tendrán escalabilidad tanto interna (agregar memoria, mayor potencia de procesador, adicionar más discos tipo SSD, adicionar tarjetas PCI, entre otros.) como externa (adicionar módulos para discos, equipos de similar configuración para nuevos clústeres, conexión a equipos de comunicaciones, entre otros). En caso de proponer equipamiento dedicado este deberá contar con un escalamiento vertical y horizontal, siempre y cuando aplique.
b. **EL PROVEEDOR** deberá realizar la actualización lógica diaria de la plataforma y/o en base a incidentes, eventos fortuitos que involucren a los componentes de la solución de la malla de seguridad propuesta y/o actualizaciones periódicas del fabricante.
c. **EL PROVEEDOR,** deberá realizar labores de seguimiento de la solución, programando reuniones trimestrales para los procesos de soporte técnico, a fin de:
   - c.1. Mantener el soporte técnico alineado a los requerimientos y necesidades de **ESSALUD,** siendo supervisado por el Coordinador de la Oficina de Seguridad Informática de **ESSALUD**.
   - c.2. Informar a la Oficina de Seguridad Informática de **ESSALUD,** a través de un (01) informe técnico (ingresado por la mesa de partes digital por el enlace: https://mpv.essalud.gob.pe/Login/Index; o a través de la mesa de partes física ubicada en la Av. Arenales 1402, Jesús María, Piso 2), la información complementaria y/o de valor que se pueda generar a partir de actualizaciones, modificaciones, incidentes y eventos de ciberseguridad; y de los cambios realizados en las plataformas de seguridad que comprenden las mejoras realizadas por **EL PROVEEDOR,** para la toma de decisiones estratégicas para una retroalimentación constante.
d. En el caso de que **EL PROVEEDOR**, requiera realizar un corte de servicio, éste deberá ser programado con al menos veinticuatro (24) horas de anticipación vía correo electrónico y deberá contar necesariamente con la aprobación respectiva de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de

ESSALUD, debiendo considerar que las actividades se realicen fuera del horario de oficina. Este tiempo no deberá superar el límite de una (01) hora de indisponibilidad programada.

e. **EL PROVEEDOR** será el único responsable ante **ESSALUD** de cumplir con la prestación contratada, no pudiendo transferir dicha responsabilidad a terceros, es decir, **EL PROVEEDOR** no podrá subcontratar las actividades generadas por la prestación del servicio.
f. **EL PROVEEDOR** deberá cumplir con las disposiciones y normativas nacionales e internas de seguridad de la información de **ESSALUD**, detalladas en el numeral 5.5. y 5.28., de los presentes términos de referencia.
g. **EL PROVEEDOR** deberá contar con una política de niveles de atención de servicio de requerimientos.
h. **EL PROVEEDOR,** no podrá realizar cambios del personal asignado al proyecto sin conocimiento y previa comunicación y aprobación de **ESSALUD.**
i. Los daños ocasionados por **EL PROVEEDOR** durante la ejecución de los procedimientos de instalación sobre la propiedad de **ESSALUD** ajenas, serán cubiertos en su totalidad por éste, sin perjuicio de **ESSALUD.**
j. **EL PROVEEDOR** deberá proporcionar el soporte técnico (en sitio y/o remoto), a toda la solución de acuerdo con las normas utilizadas en el Centro de Datos de **ESSALUD**, por el periodo de vigencia de la garantía.
k. **EL PROVEEDOR** deberá mantener la actualización diaria de la plataforma y/o en base a incidentes, eventos fortuitos que involucren a la solución y/o actualizaciones periódicas del fabricante.
l. **EL PROVEEDOR** deberá identificar el grado de madurez de seguridad, respecto al modelo de gestión basado en: procesos, tecnología y personas.
m. **EL PROVEEDOR** deberá identificar, analizar y evaluar periódicamente los riesgos de los procesos y activos de información: servicios y proyectos de TI.
n. **EL PROVEEDOR** deberá gestionar los riesgos de seguridad, estableciendo métricas e indicadores de cumplimiento.
o. **EL PROVEEDOR** deberá contar con un proceso de atención de requerimientos para:
   - **Requerimientos de cambio de configuración**: Implica efectuar cambios al servicio o a los dispositivos administrados por el servicio.
   - **Requerimientos de investigación de seguridad:** Implica indagar en los eventos generados para buscar una evidencia de una situación de riesgo específica.

5.2.3.5. **Supervisión de los equipos del servicio de la malla de seguridad**

EL PROVEEDOR deberá operar bajo solicitud de **ESSALUD**, con cobertura 24x7 los tres (03) años de garantía, el correcto funcionamiento de todos los componentes que forman parte de la solución de seguridad.

5.3. **Recursos a ser provistos por EL PROVEEDOR, para el servicio de malla de seguridad informática.**

EL PROVEEDOR brindará una solución de hardware, software, licencias, insumos, periféricos, accesorios, servicios de reparación y soporte técnico del equipamiento y otros componentes necesarios (solución integral) para la instalación, configuración, pruebas necesarias para el correcto funcionamiento y puesta en operación del equipamiento parte del servicio de implementación de la solución de la malla de seguridad informática para **ESSALUD;** siendo que este servicio deberán de tener en cuenta las siguientes consideraciones:

a. **EL PROVEEDOR** será el responsable de la implementación del equipamiento, instalación, configuración física y lógica, integración y optimización de todos los componentes, mantenimientos y transferencia del conocimiento.
b. **EL PROVEEDOR** deberá incluir la autenticación de multi-factor para las cuentas VPN SSL mediante correo y/o token digital y/o físico y/o lógico (móvil, USB token).
c. **EL PROVEEDOR** deberá contar con un Centro de Operaciones de Seguridad con una mesa de ayuda de 24x7x3 años, con atención inmediata vía telefónica y por correo electrónico.
d. **EL PROVEEDOR** deberá brindar el soporte técnico a la solución de la malla de seguridad propuesta de 24x7x3 años, donde deberá incluir todos los recursos entre otros que sean necesarias para la correcta ejecución de los mismos.
e. **EL PROVEEDOR** deberá brindar la implementación del servicio de ciberseguridad, incluye labores de cableado de datos y eléctrico de los equipos ofertados, bajo fibra óptica y cobre, instalación de equipos en gabinete de servidores, conexión a gabinete de comunicaciones de los equipos, aterramientos, instalaciones de software y puesta en producción.

5.4. **Recursos y facilidades a ser provistos por ESSALUD**

La entidad brindará las facilidades al **PROVEEDOR** para el desarrollo de sus funciones:

a. Acceso a las instalaciones de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones, para coordinaciones solicitadas y determinadas por la Oficina de Seguridad Informática, si el servicio lo requiere.
b. Acceso por VPN institucional para realizar las actividades inherentes a la presente contratación, si el servicio lo requiere.
c. La entidad brindará a través de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones, un coordinador que supervisará el desarrollo del servicio y será el nexo de comunicación entre la **ESSALUD** y **EL PROVEEDOR.**
d. Todo cambio interno de arquitectura tecnológica será comunicado con veinticuatro (24) horas antes al **PROVEEDOR** del servicio para la realización de actividades previas.
e. **ESSALUD,** a través de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de **ESSALUD,** una vez iniciado el periodo del servicio, se reserva el derecho de evaluar en todo momento el desarrollo y cumplimiento de lo contratado del servicio, y podrá solicitar el cambio del personal (jefe del proyecto, personal implementador y residente) asignado por **EL PROVEEDOR,** para la ejecución de la presente contratación.

5.5. Normas técnicas

a. NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición.
b. NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición.
c. NTP-ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición.
d. NTP-ISO 31000:2018: Gestión del Riesgo. Directrices. 2ª Edición.
e. ISO/IEC 27032:2023: Directrices para la Ciberseguridad.
f. Código Nacional de Electricidad vigente.

5.6. Impacto ambiental

Esta contratación para la implementación de una malla de seguridad informática para **ESSALUD,** no tiene impacto ambiental, dado que los equipamientos serán instalados en un ambiente controlado, seguro y que utiliza estándares tecnológicos en su operación y el servicio se ejecuta sobre estos de manera lógica.

5.7. Seguros

EL PROVEEDOR, deberá presentar como requisito para la suscripción del contrato los documentos que acrediten que todo el personal que realizará los trabajos cuenta con **"Seguro Complementario de Trabajo de Riesgo (SCTR)"** vigente, con cobertura de salud y pensiones por accidente de trabajo y enfermedad profesional.

EL PROVEEDOR, será el único responsable del seguro de los componentes de la solución de seguridad hasta su instalación final en el Centro de Datos de la Sede Central de **ESSALUD,** ubicado en Av. Arenales 1402 – Piso 6, Jesús María, Lima, sin que esto genere costos adicionales para **ESSALUD.**

5.8. Soporte técnico

EL PROVEEDOR deberá contar con un servicio de soporte técnico para la solución de seguridad ofertada, el cual deberá cumplir con el siguiente procedimiento en caso se presente un desperfecto, falla o avería:

a. El plazo de contratación es de tres (03) años en lo que respecta a la garantía de soporte por la solución de seguridad ofertada.
b. Una vez registrado el ticket de atención, **EL PROVEEDOR** deberá atender de forma inmediata y no podrá exceder el tiempo de solución según lo indicado en numeral 5.10.1., de solucionarse el desperfecto, falla o avería, se procederá a cerrar el ticket, previa conformidad por correo electrónico del Coordinador de la Oficina de Seguridad Informática de **ESSALUD;** se generará el *Reporte de Servicio Técnico* por parte de **EL PROVEEDOR** y se enviará por correo electrónico, el respectivo reporte y se deberá entregar una copia física al Jefe de la Oficina de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de **ESSALUD.**
c. Si el desperfecto, falla o avería no puede ser resuelto, se deberá de realizar la atención de forma presencial en un tiempo no mayor a dos (02) horas en las instalaciones de **ESSALUD,** en caso **EL PROVEEDOR** no pueda solucionar dicho desperfecto, falla o avería, deberá escalarlo al fabricante de (los) componente(s), para esto, la solicitud deberá ser vía correo electrónico con copia al Coordinador de la Oficina de Seguridad Informática de **ESSALUD** y no deberá exceder el plazo máximo de solución definitiva de cuatro (04) horas, siendo este proceso, exclusivo de **EL PROVEEDOR,** de solucionarse el desperfecto, falla o avería, se procederá a cerrar el ticket, previa conformidad del Coordinador de la Oficina de Seguridad Informática de **ESSALUD;** se generará el *Reporte de Servicio Técnico* por parte de **EL PROVEEDOR** y se enviará por correo electrónico, el respectivo reporte y se deberá entregar una copia física al Jefe de la Oficina de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de **ESSALUD.**

d. El soporte técnico es en modalidad en sitio y/o remoto por parte de **EL PROVEEDOR,** para todos los componentes de la solución de seguridad, por el periodo de vigencia de la garantía, además, se deberá tener en consideración que todos los componentes, partes y/o piezas, cables, accesorios, etc. deberán ser originales y nuevos (sin uso) del fabricante del equipo ofertado, garantizando compatibilidad y operatividad al 100%.

e. En caso de ser necesario el soporte en sitio, **EL PROVEEDOR** deberá presentar al personal técnico debidamente identificado con fotocheck, herramientas e insumos necesarios para cumplir con su trabajo, además, deberán contar con el Seguro Complementario de Trabajo de Riesgo por cada personal asignado por **EL PROVEEDOR** para la atención.

f. En caso de ser necesario trasladar el equipo para la revisión, los costos del envío y/o retorno serán por cuenta de **EL PROVEEDOR,** debiendo reemplazarlo por un equipo de igual o mejores características de manera INMEDIATA, siendo que esta actividad no deberá generar costos para **ESSALUD** y sobrepasar el máximo de cuatro (04) hora para realizar el procedimiento de reemplazo y reinicio de la operatividad.

g. **EL PROVEEDOR** deberá operar la solución desde su Centro de Operaciones de Seguridad, de manera remota y deberá comprender lo siguiente:

g.1. Participación en la resolución de incidentes de seguridad: El personal del Centro de Operaciones de Seguridad, deberá de ser el primer nivel de atención ante desperfectos, fallas o averías en coordinación con el Coordinador de la Oficina de Seguridad Informática de **ESSALUD** hasta la solución de la misma.

g.2. Identificación y análisis de:

g.2.1. Eventos.

g.2.2. Preventivo – (Inteligencia de Procedimientos de Seguridad).

g.2.3. Brechas de Seguridad de la Información, de acuerdo con los indicadores de compromiso.

g.3. Planificación y ejecución de cambios: Contempla el estudio y realización de los cambios sobre los elementos operados que solicite **ESSALUD** y que sean recomendados en base a las mejores prácticas, recomendaciones o normativas estandarizadas. Se deberán contemplar los cambios que no impliquen una modificación de la arquitectura/funcionalidad de los dispositivos de seguridad operados. En caso de que los cambios supongan una modificación sustancial, se deberán de programar con el Coordinador de la Oficina de Seguridad Informática de **ESSALUD**.

g.4. Resolución de solicitudes realizadas: Contempla la realización de las tareas de operación solicitadas por **ESSALUD** y tipificadas dentro del numeral 5.10.

g.5. Supervisar el correcto funcionamiento de los componentes de la solución de seguridad: Contempla la realización de tareas de vigilancia, acciones predictivas y correctivas, generación de reportes, definición de riesgos e inteligencia de seguridad predefinidas por el Centro de Operaciones de Seguridad para comprobar el correcto funcionamiento y disponibilidad de los dispositivos de seguridad administrados.

g.6. Mantenimiento y actualización de la política de seguridad: Según se establezca en el manual de administración de cada dispositivo, **EL PROVEEDOR** deberá de apoyarse en el documento de criterios pre-autorizados / denegados facilitado por **ESSALUD**.

g.7. Actualización de parches y firmwares: Las políticas de parchado y actualización de los equipos operados son responsabilidad de **EL PROVEEDOR.** Las actualizaciones se realizarán dentro de las ventanas de mantenimiento que se hayan definido, coordinado y aprobado por la Oficina de Seguridad Informática.

g.8. Identificación proactiva de riesgos, análisis de riesgos a proyectos de seguridad y de plataforma tecnológica, gestión de riesgos de seguridad de la información, activación de logs de aplicaciones, gestión de vulnerabilidades y análisis de riegos a aplicaciones: **EL PROVEEDOR** deberá gestionar, analizar e informar de forma proactiva a **ESSALUD** si en el ejercicio de las funciones y nuevas implementaciones, los operadores detectaran riesgos evidentes para la seguridad de la información y aplicaciones, se deberán ejecutar los logs necesarios para determinar los eventos o incidentes de seguridad proactivamente, analizando y mitigando las brechas de seguridad y vulnerabilidades en las plataformas tecnológicas y aplicaciones de **ESSALUD.**

g.9. Detección, ejecución y corrección del ciclo de vida de las vulnerabilidades: **EL PROVEEDOR** participará en la realización de los cambios necesarios para subsanar vulnerabilidades encontradas.

g.10. Registro y control de las peticiones: Todas las peticiones se recogerán vía llamada telefónica y/o correo electrónico.

g.11. Configuración, gestión y monitoreo de las VPN IPsec con terceros (empresas externas que ofrezcan servicios y tengan contrato vigente con ESSALUD): Independientemente si los usuarios de este servicio son internos o externos, **EL PROVEEDOR** deberá realizar permanentemente la revisión y monitoreo de accesos remotos VPN SSL.

g.12. Gestión: **EL PROVEEDOR** es responsable de recibir, revisar y responder proactiva, inmediata y eficientemente a informes, eventos, incidentes y cualquier otra actividad que pueda vulnerar la seguridad en la red de **ESSALUD.**

g.13. Revisión de controles de seguridad: **EL PROVEEDOR** deberá realizar el soporte de acuerdo con lo establecido en las normas técnicas peruanas vigentes y/o modificatorias para el cumplimiento de los controles de seguridad en los procedimientos de gestión de las soluciones de seguridad implementadas a nivel de plataforma tecnológica.

5.9. Centro de Operaciones de Seguridad

Deberá contar con un Centro de Operaciones de Seguridad (SOC), asimismo el precitado SOC, de preferencia certificado con ISO 27001 y deberá contar con personal certificado en ISO 27001, al menos CINCO personas certificadas. Debiendo estar vigente al inicio de operaciones de la malla de seguridad implementada, siendo que, esta certificación deberá ser presentada ante la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones, previo al inicio de operaciones.

a. **EL PROVEEDOR** deberá contar con un Centro de Operaciones de Seguridad (SOC), que tenga como mínimo cinco (05) años de experiencia en operación de servicios y atenciones de soporte técnico 24x7 dentro del territorio nacional.
   a.1. El Centro de Operaciones de Seguridad (SOC), de **EL PROVEEDOR** deberá contar con un organigrama de gestión de la operación de soporte técnico, el cual deberá ser presentado al Coordinador de la Oficina de Seguridad Informática de **ESSALUD,** como adjunto al Plan de trabajo de instalación, configuración e implementación de los equipos de seguridad.
b. El periodo de operación por parte del Centro de Operaciones de Seguridad (SOC), de la solución implementada será por tres (03) años, contabilizados a partir del día siguiente de suscrita el ***Acta de Conformidad de Puesta en Producción de la Solución.***
c. El Centro de Operaciones de Seguridad (SOC) deberá garantizar un *canal de comunicación permanente,* debiendo contar con una única central telefónica (0800) y/o único canal de comunicación permanente,[11] para reporte de requerimientos e incidentes y una cuenta de correo electrónico dedicado a **ESSALUD,** y para ambos casos la cobertura de atención será de 24x7 durante el periodo de vigencia del servicio de soporte técnico (tres 03 años). Se utilizarán estos canales como medio de contacto, permitiendo control, gestión y seguimiento de los requerimientos presentados.
d. El Centro de Operaciones de Seguridad (SOC) deberá garantizar el *monitoreo permanente de la solución implementada,*[12] ~~con declaración jurada (presentada en la propuesta técnica)~~ para la labor de monitoreo de la solución de seguridad integral; durante la vigencia del periodo de operación, mantenimiento y soporte, el Centro de Operaciones de Seguridad (SOC) deberá mantener el monitoreo 24x7 durante el periodo de vigencia del servicio (tres 03 años), en modo remoto, y de ser necesario para incidentes críticos a demanda de **ESSALUD** el monitoreo se podrá realizar de forma presencial; con la finalidad de anticipar y reportar constantemente en tiempo real cualquier tipo de ataque y/o vulnerabilidad para la toma de decisiones y precisar acciones que conlleven a afrontar cualquier afectación a la seguridad y la continuidad operativa de forma preventiva.

5.10. Mesa de Ayuda

Deberá garantizar los siguientes requerimientos de tiempo de atención a fallas durante la vigencia del periodo de la garantía:

a. TIEMPO DE RESPUESTA Mesa de Ayuda (Call Center): Si el reporte se realizara vía telefónica, la atención será en un plazo de atención no mayor a cinco 05 minutos, aun si el reporte de atención es vía correo electrónico, debiéndose generar inmediatamente el ticket de atención correspondiente. La mesa de ayuda deberá atender a la solución de la malla de seguridad propuesta implementada en su conjunto.
b. TIEMPO DE RESPUESTA En-Sitio: Se brindará de acuerdo con el nivel de atención conforme a lo descrito en el presente documento dentro del periodo de garantía, en un máximo de dos (02) horas para resolver el desperfecto, falla o avería vía telefónica.
c. TIEMPO DE RESPUESTA EN EL Centro de Operaciones de Seguridad: Se brindará de acuerdo con el nivel de atención conforme a lo descrito en el inciso **a** del numeral 5.10.1
d. TIEMPO DE SOLUCIÓN DEFINITIVA: De acuerdo con lo indicado conforme a lo descrito en el numeral 5.10.1, a partir del momento en que el personal del Centro de Operaciones de Seguridad toma conocimiento del desperfecto, falla o avería y genera el ticket de atención respectivo para determinar la atención del incidente.

5.10.1. **Acuerdos de Niveles de Servicios (SLA) de requerimientos ante desperfectos, fallas o averías de la solución de seguridad en sitio:** El cumplimiento es obligatorio de los procedimientos y se encuentra debidamente detallado y dependerá de las repercusiones que tenga en los requerimientos que **EL PROVEEDOR** presta a **ESSALUD,** a demanda:

[11] Absolución de consultas y observaciones Nº 40 JAPAN COMPUTER SERVICE S.A.C.

[12] Absolución de consultas y observaciones Nº 41 JAPAN COMPUTER SERVICE S.A.C.

TIEMPOS DE SOLUCIÓN

a. Tiempo de solución SOC: Una vez reportado un desperfecto, falla o avería **EL PROVEEDOR** dispondrá del tiempo relacionado en el siguiente cuadro, donde el tiempo de respuesta hace referencia a la cantidad de tiempo que transcurre desde que se reporta el desperfecto, falla o avería hasta que se da respuesta; la resolución temporal es una acción urgente para salir del incidente pudiendo encontrarse la operación en condiciones inferiores al nivel pactado y la resolución definitiva es restablecer las condiciones normales del servicio y haber solucionado de manera definitiva el problema. A continuación, se detallan los niveles de servicios para la atención ante desperfectos, fallas o averías, y su cumplimiento es obligatorio:

ATENCIÓN EN EL CENTRO DE OPERACIONES DE SEGURIDAD – SOC			
Nivel de atención	Tiempo de contacto	Solución temporal	Tiempo de respuesta
Nivel 1	05 minutos	10 minutos	30 minutos
Nivel 2	05 minutos	20 minutos	45 minutos
Nivel 3	05 minutos	30 minutos	01 hora
Nivel 4	05 minutos	40 minutos	01 hora

a.1. En caso de que la atención deba ser escalada al fabricante el tiempo para la SOLUCIÓN DEFINITIVA no deberá excederse en más de cuatro (04) horas de respuesta, de no cumplirse el tiempo de respuesta se aplicará la penalidad correspondiente, la cual se encuentra detallada en el numeral 5.25., esta atención deberá ser comunicado y autorizada por el Coordinador de la Oficina de Seguridad Informática de **ESSALUD,** previo informe técnico inmediato elaborado por **EL PROVEEDOR** donde se describa la avería o incidente.

b. Tiempo de solución residentes.

Una vez reportado o identificado un desperfecto, falla o avería **EL PROVEEDOR** dispondrá del tiempo relacionado en el siguiente cuadro, donde el tiempo de respuesta hace referencia a la cantidad de tiempo que transcurre desde que se reporta el desperfecto, falla o avería hasta que se da respuesta; la resolución temporal es una acción urgente para salir del incidente pudiendo encontrarse la operación en condiciones inferiores al nivel pactado y la resolución definitiva es restablecer las condiciones normales del servicio y haber solucionado de manera definitiva el problema. A continuación, se detallan los niveles de servicios para la atención ante desperfectos, fallas o averías, y su cumplimiento es obligatorio:

ATENCIÓN EN SITIO (RESIDENTES)			
Nivel de atención	Tiempo de contacto	Solución temporal	Tiempo de respuesta
Nivel 1	05 minutos	10 minutos	30 minutos
Nivel 2	05 minutos	20 minutos	45 minutos
Nivel 3	05 minutos	30 minutos	01 hora
Nivel 4	05 minutos	40 minutos	01 hora

b.1 En caso de que la atención deba ser escalada al fabricante el tiempo para la SOLUCIÓN DEFINITIVA no deberá excederse en más de cuatro (04) horas de respuesta, de no cumplirse el tiempo de respuesta se aplicará la penalidad correspondiente, la cual se encuentra detallada en el numeral 5.25, esta atención deberá ser comunicado y autorizada por el Coordinador de la Oficina de Seguridad Informática de **ESSALUD,** previo informe técnico inmediato elaborado por **EL PROVEEDOR** donde se describa la avería o incidente.

DETALLE DE LOS NIVELES DE ATENCIÓN

c.1. **Nivel de atención 1:** Son aquellos desperfectos, fallas o averías que afectan algunas funcionalidades, pero no el funcionamiento básico de la solución de seguridad contratada o aquellos casos en los que existe un riesgo de degradación e incumplimiento de requerimientos, entre los cuales se encuentran:

c.1.1. Requerimientos de configuraciones que no implican corte de servicios de **ESSALUD,** continuidad operativa, pérdidas financieras o afecten la imagen institucional.

c.1.2. En caso de que no se pueda solucionar el desperfecto, falla o avería, se deberá realizar la visita para concluir la solución; este tiempo no podrá ser mayor a cuatro (04) hora, luego de ser reportado al Coordinador de la Oficina de Seguridad Informática de **ESSALUD.**

C.2. **Nivel de atención 2:** Son aquellos desperfectos, fallas o averías que afectan el normal funcionamiento de la solución de seguridad contratada o aquellos que afectan la operación o la continuidad operativa. Entre los cuales se encuentran:

c.2.1. Desperfectos, fallas o averías de alguno de los componentes (hardware o software) de la solución de seguridad contratada, que requieran ser re-configurados para la continuidad operativa de la solución.

c.2.2. En caso de que no se pueda solucionar el desperfecto, falla o avería, se deberá realizar la visita para concluir la solución; este tiempo no podrá ser mayor a cuatro (04) hora, luego de ser reportado al Coordinador de la Oficina de Seguridad Informática de ESSALUD.

c.3. **Nivel de atención 3:** Son aquellos desperfectos, fallas o averías que afectan el normal funcionamiento de la solución de seguridad contratada o aquellos que afectan la operación, la continuidad operativa o causan pérdidas financieras. Entre los cuales se encuentran:

c.3.1. Parchado frente a vulnerabilidades críticas de alguno de los componentes (hardware o software) de la solución de seguridad contratada.

c.3.2. Desperfectos, fallas o averías de alguno de los componentes (hardware o software) de la solución de seguridad contratada, que lo deje inoperativo temporalmente.

c.3.3. Configuraciones de emergencia frente a un ataque en ejecución o anunciado cualquiera que este sea y que puede sobrepasar las funcionalidades normales de alguno de los componentes (hardware o software) de la solución de seguridad contratada.

c.3.4. En caso de que no se pueda solucionar el desperfecto, falla o avería, se deberá realizar la visita para concluir la solución; este tiempo no podrá ser mayor a cuatro (04) hora, luego de ser reportado al Coordinador de la Oficina de Seguridad Informática de ESSALUD.

c.4. **Nivel de atención 4:** Son aquellos desperfectos, fallas o averías que afectan críticamente el funcionamiento de la solución de seguridad contratada o aquellos que afectan la operación o causan pérdidas financieras, continuidad operativa o de imagen a ESSALUD. Entre los cuales se encuentran:

c.4.1. Inoperatividad de alguno de los componentes (hardware o software) de la solución de seguridad contratada, software que lo deje inoperativo permanentemente.

c.4.2. En caso de que no se pueda solucionar el desperfecto, falla o avería, se deberá realizar la visita para concluir la solución; este tiempo no podrá ser mayor a cuatro (04) hora, luego de ser reportado al Coordinador de la Oficina de Seguridad Informática de ESSALUD.

c.4.3. Corresponde a EL PROVEEDOR la realización de requerimientos de atención por incidentes que afecten o no afectan a la funcionalidad de alguno de los componentes (hardware o software) de la solución de seguridad contratada, aun si se deba escalar al fabricante. Pudiendo ESSALUD escalar al fabricante en caso de tener complicaciones con EL PROVEEDOR.

5.11. Requisitos de EL PROVEEDOR y su personal

5.11.1. Requisitos de EL PROVEEDOR

EL PROVEEDOR deberá contar con Registro Nacional de Proveedores vigente y no estar sancionado e impedido para contratar con el Estado.

5.11.2. Personal Clave

EL POSTOR deberá designar como parte del proyecto al siguiente personal clave, el cual deberá de contar con las siguientes características.

5.11.2.1. <u>01 jefe del Proyecto para la malla de seguridad informática:</u>

- Titulado en Ingeniería: de Sistemas y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática.
- Experiencia como mínimo de siete (07) años como: jefe de proyecto o Gerente de proyectos o líder de proyecto o gestor de proyecto, en gestión de tecnología de información y/o en proyectos de seguridad de la información y/o ciberseguridad y/o informático.[13]

<u>Funciones</u>:

[13] Absolución de consultas y observaciones Nº 10 GRUPO RADICAL S.A.C.

- Deberá elaborar toda la documentación de gestión del proyecto, como las actas de inicio/cierre de proyecto, las mismas que deberá presentar como parte del informe final de la implementación de la solución ofertada (informes ejecutivos e informes técnicos).
- Definir y optimizar las configuraciones del equipamiento para la gestión eficiente de incidentes de Seguridad de Información.
- Liderar el proceso de implementación y el equipo multidisciplinario que formara parte de la implementación, coordinando con las áreas involucradas, otorgando las pautas necesarias.
- Elaboración del plan de migración y planes de acción ante posibles cortes de operatividad.
- Deberá establecer la estrategia y liderar la implementación y mejora continua en los procesos y procedimientos de administración de servicios de seguridad para lograr una administración eficiente de incidentes y operaciones.
- Definir, monitorear y optimizar la gestión de incidentes de Seguridad de Información.
- Liderar el proceso de gestión y el equipo multidisciplinario de respuesta a incidentes de seguridad, coordinando con las áreas involucradas, otorgando las pautas necesarias y ejecutando un plan de acción.
- Analizar de manera integral las operaciones de seguridad, tanto en procesos, servicios y plataformas tecnológicas a fin de garantizar la seguridad de manera unificada.
- Definir y optimizar las configuraciones del equipamiento para la gestión eficiente de incidentes de Seguridad de Información.
- Deberá liderar la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.
- Toda información elaborada como parte de las prestaciones del servicio, deberá ser presentada de acuerdo a las actividades programas y a solicitud de la Oficina de Seguridad Informática, esta información es considerada de propiedad del Seguro Social de Salud – **ESSALUD** y deberá ser presentada a nombre del mismo.

Coordinaciones:
Tendrá como función principal, ser el contacto permanente entre **EL PROVEEDOR** y **ESSALUD,** a través del jefe de la Oficina de Seguridad Informática.

Certificaciones: deberá tener al menos dos (2) las siguientes certificaciones.
- Certificación en PMP o Prince2 Pactitioner
- Certificado CRISC (Certified in Risk and Information Systems Control) y/o ISO 27005 Lead Risk Manager
- Certificado en ISO 27002 Information Security Foundations
- Certificado en Ciberseguridad como Lead Cybersecurity Manager y/o Lead CyberSecurity Professional
- Certificado como ITIL 4 Foundation
- Certificado ISO/IEC 27001 Auditor

NOTA: A continuación, se detallan las consideraciones obligatorias:
- Los profesionales requeridos por ESSALUD, no podrán ocupar ningún rol adicional en la implementación o como residentes.
- Las certificaciones requeridas, deberán presentarse en copia como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.

5.11.2.2. 01 jefe del Proyecto para el Sistema de Gestión de Seguridad de la información:

- Titulado en Ingeniería: de Sistemas y/o Industrial y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes.
- La experiencia requerida no podrá ser menor de cuatro (04) años como: jefe o analista, o supervisor o consultor o implementador o auditor, en seguridad de la información y/o seguridad informática y/o ciberseguridad y/o especialista en seguridad de la información y/o continuidad de negocio.

Funciones:
Gestiona la implementación del Sistema de Gestión de Seguridad de Información – SGSI, del proceso definido por **ESSALUD.**

Coordina:
Tendrán como función principal, la implementación del Sistema de Gestión de Seguridad de la Información - SGSI la solución de la malla de seguridad y estarán en comunicación constante con el jefe del Proyecto.

Certificaciones: deberá tener al menos dos (2) las siguientes certificaciones.

- Certificado de ISO/IEC 27001 Lead Auditor
- Certificado de ISO/IEC 27001 Lead Implementer
- Certificación de ISO 22301 Lead Implementer
- Certificación de ISO 31000
- Certificado CRISC (Certified in Risk and Information Systems Control) y/o ISO 27005 Lead Risk Manager
- Certificado en Ciberseguridad como Lead Cybersecurity Manager y/o Lead CyberSecurity Professional

NOTA: Las certificaciones requeridas, para el jefe del Proyecto para el Sistema de Gestión de Seguridad de la información deberán presentarse en copia como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.

5.11.2.3. 01 especialista en Normatividad de Seguridad de la Información:

- Titulado en Ingeniería: de Sistemas y/o de Computación y Sistema y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes y/o Telecomunicaciones.
- La experiencia requerida no podrá ser menor de cinco (05) años como: jefe o analista o supervisor o consultor o implementador o auditor, en seguridad de la información y/o seguridad informática y/o ciberseguridad.

Funciones:
Implementar el Sistema de Gestión de Seguridad de Información – SGSI, del proceso definido por ESSALUD.

Coordina:
Tendrán como función principal, la implementación del Sistema de Gestión de Seguridad de la Información - SGSI la solución de la malla de seguridad y estarán en comunicación constante con el Ingeniero Especialista en Consultoría de Seguridad de la Información.

Temporalidad:
Personal asignado por EL PROVEEDOR, para la implementación del Sistema de Gestión de Seguridad de la Información - SGSI.

Certificaciones: deberá tener al menos una (1) de las siguientes certificaciones:

- Certificado de ISO/IEC 27001 Fundamento
- Certificado de ISO/IEC 27001 Lead Implementer
- Certificado en Lead CyberSecurity Professional

NOTA: Las certificaciones requeridas, para el Especialista en Normatividad de Seguridad de la Información deberán presentarse en copia como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.

5.11.2.4. 01 ingeniero Especialista:

- Titulado en Ingeniería: de Sistemas y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes.
- La experiencia requerida no podrá ser menor de Tres (03) años como: auditor o implementador o especialista o analista o supervisor o consultor, en implementación de equipamiento de seguridad de la marca del equipamiento ofertados.

Funciones:

- Identificar el grado de madurez de seguridad, respecto al modelo de gestión basado en: procesos, tecnología y personas.
- Identificar, analizar y evaluar periódicamente los riesgos de los procesos y activos de información: servicios y proyectos de TI.
- Gestionar los riesgos, estableciendo métricas e indicadores de cumplimiento de la plataforma tecnológica de la institución y de la plataforma de seguridad implementada.
- Definir bases objetivas, a través del análisis de la información, indicadores, incidentes, para tener un nivel adecuado para la administración de riesgos.
- Colaborar con la retroalimentación con las áreas de tecnologías de la información a nivel transversal ESSALUD.

- Identificar vulnerabilidades y tráficos anómalos que puedan generar brechas de seguridad.
- Utilizar procedimientos de hardnering, mitigación y mejora constante de las tecnologías perimetrales implementadas.
- Gestionar los componentes de la solución de seguridad implementada.
- Evidenciar los posibles incidentes externos e internos y elaborar las tareas de mitigación.
- Se requiere que el personal se encuentre disponible 24x7x365 días del año.

Coordina:
Tendrán como función principal, la implementación de la solución de la malla de seguridad y estarán en comunicación constante con el jefe del Proyecto.

Certificaciones: deberá tener al menos dos (2) de las siguientes certificaciones:
- Certificación oficial del fabricante de la marca ofertada en Next Generation Firewall.
- CCNA – routing and switching y/o Curso Oficial en routing and switching
- Certificado en Lead CyberSecurity Professional

NOTA: Las certificaciones requeridas, para el Ingeniero Especialista deberán presentarse en copia como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.

5.11.2.5. 02 Residente de Operación:
- Titulado o Bachiller[14] [15] en Ingeniería: de Sistemas y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes.
- La experiencia requerida no menor de un (01) año como: jefe o analista o supervisor, o consultor o implementador o auditor, en operación de equipamiento de seguridad de la marca del equipamiento ofertado.

Funciones:
- Identificar el grado de madurez de seguridad, respecto al modelo de gestión basado en: procesos, tecnología y personas.
- Identificar, analizar y evaluar periódicamente los riesgos de los procesos y activos de información: servicios y proyectos de TI.
- Gestionar los riesgos, estableciendo métricas e indicadores de cumplimiento de la plataforma tecnológica de la institución y de la plataforma de seguridad implementada.
- Definir bases objetivas, a través del análisis de la información, indicadores, incidentes, para tener un nivel adecuado para la administración de riesgos.
- Colaborar con la retroalimentación con las áreas de tecnologías de la información a nivel transversal ESSALUD.
- Identificar vulnerabilidades y tráficos anómalos que puedan generar brechas de seguridad.
- Utilizar procedimientos de hardnering, mitigación y mejora constante de las tecnologías perimetrales implementadas.
- Gestionar los componentes de la solución de seguridad implementada.
- Evidenciar los posibles incidentes externos e internos y elaborar las tareas de mitigación.
- ~~Se requiere que el personal se encuentre disponible 24x7x365 días del año.~~
- Se requiere que el personal se encuentre disponible 24x7x365 días del año; de lunes a viernes en horario de 08:00 hasta las 20:00 horas en la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de EsSalud y resto de tiempo y días en remoto.[16] [17]

Coordina:
Tendrá como función principal, la operación por parte de ESSALUD, y estarán en comunicación constante el jefe del Proyecto y las áreas de tecnologías de la información de ESSALUD a nivel nacional.

Certificaciones: facultativo
- Certificación oficial del fabricante de la marca ofertada en Next Generation Firewall.
- CCNA – routing and switching y/o Curso Oficial en routing and switching

[14] Absolución de consultas y observaciones Nº 55 JAPAN COMPUTER SERVICE S.A.C.
[15] Absolución de consultas y observaciones Nº 68 GRUPO RADICAL S.A.C.
[16] Absolución de consultas y observaciones Nº 64 GRUPO RADICAL S.A.C.
[17] Absolución de consultas y observaciones Nº 99 TELEFÓNICA TECH PERÚ S.A.C.

NOTA: De contar con las certificaciones requeridas, para los Residentes de Operación, deberán presentarse en copia como requisito para la suscripción del contrato, las mismas que deberán estar vigentes durante la ejecución de la prestación y serán verificadas por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones.

IMPORTANTE:

- **ESSALUD,** a través Oficina de Seguridad Informática de la Gerencia Central de Tecnología de Información y Comunicaciones, una vez iniciado el periodo del servicio y del soporte, se reserva el derecho de evaluar, en todo momento, y de solicitar el cambio del personal asignado a la atención de requerimientos y gestión del proyecto cuantas veces se crea necesario.
- **EL PROVEEDOR** no podrá realizar cambios del personal asignado al proyecto sin previa comunicación y aprobación de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de **ESSALUD.**

5.12. Lugar y plazo de ejecución de la prestación del servicio

5.12.1. Lugar:

La *prestación del servicio* se ejecutará en el Jr. Domingo Cueto # 120, Piso 6, Jesús María – Lima.

5.12.2. Plazo de ejecución del servicio

El plazo de ejecución del servicio será de un mil noventa y cinco (1,095) días calendario, los cuales serán contabilizados a partir del día siguiente de firmada el *Acta de Conformidad de Puesta en producción* de los componentes implementados.

5.13. Entregables

PARA EL PRIMER ENTREGABLE

1. **EL PROVEEDOR** deberá presentar el informe técnico inicial correspondiente, donde describirá la metodología que utilizará para la configuración de los componentes de la solución de seguridad que se está proponiendo y la cual será adecuada a la necesidad operacional de **ESSALUD.**
2. Acta de conformidad de puesta en producción.
3. Presentación del informe detallado sobre las labores de implantación y migración.
4. Se deberán presentar informes técnicos indicando los incidentes presentados y requerimientos atendidos durante el periodo de 30 días, y las actividades de soporte realizadas, estos informes se entregarán mensualmente, y el periodo de inicio se contabilizará desde el día siguiente de suscrito el contrato; Estos informes deberán ser entregados en formato digital, vía la mesa de partes institucional (virtual: https://mpv.essalud.gob.pe/Login/Index).
5. En caso de que se presente algún incidente dentro del periodo del entregable en relación a la atención de requerimientos, se deberá generar el informe técnico correspondiente de la incidencia en cualquier momento en que se presente y/o a demanda de ESSALUD; este informe técnico deberá indicar al menos lo siguiente:
   - Incidentes presentados durante el periodo de la implementación y servicio.
   - Actividades realizadas para la resolución del incidente.
   - El informe técnico se entregará en formato digital, adjuntando anexos para obtener la mayor cantidad de información de los incidentes ocurridos vía la mesa de partes virtual (https://mpv.essalud.gob.pe/Login/Index) de **ESSALUD**, inmediatamente después de solucionada la incidencia.
   - Así mismo, el Informe Técnico deberá estar dirigido al jefe de la Oficina de Seguridad Informática, indicando detalladamente las actividades realizadas según los tiempos establecidos en el numeral 5.10.1., los mismos que deberán ser requisito indispensable para las conformidades mensuales de atención de requerimientos y el pago de los mismos.
6. Informe de Implementación del Sistema de Gestión de Seguridad de la Información – SGSI, en cumplimiento de lo establecido en la etapa Nº1 del numeral 5.2.3.2 del presente termino de referencia.
7. Informe de Capacitación, que contenga el syllabus de los temas tratados, los certificados para cada uno de los asistentes, el listado de asistencia firmado por los asistentes y el instructor y una copia de los materiales entregados en formato digital, dentro del plazo establecido en el numeral 5.2.2. literal f.

A PARTIR DEL SEGUNDO ENTREGABLE

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

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

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

5.14. Otras obligaciones del contratista

a. **EL PROVEEDOR** es el único responsable ante **ESSALUD** de cumplir con el servicio, no pudiendo transferir dicha responsabilidad a terceros, es decir, **EL PROVEEDOR** no podrá subcontratar las actividades generadas del presente servicio.

b. En el caso de que **EL PROVEEDOR** requiera realizar un corte en el servicio, éste deberá ser programado y deberá contar necesariamente con la aprobación y autorización de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de **ESSALUD,** debiendo considerar que las actividades se realicen fuera del horario de oficina. Este tiempo no deberá superar el límite de una (01) hora de indisponibilidad de los servicios de **ESSALUD.**

c. **EL PROVEEDOR** deberá identificar las brechas de seguridad a través de la evaluación de vulnerabilidades a los servicios críticos de TI de **ESSALUD.**

d. **EL PROVEEDOR** deberá establecer los criterios de valoración de los activos analizados cualitativamente. Los aspectos de seguridad que se tendrán en cuenta a la hora de valorar el riesgo son la confidencialidad, integridad y disponibilidad de la información.

e. **EL PROVEEDOR** deberá tomar los resultados del análisis de vulnerabilidades, añadiendo nuevas fuentes de amenazas relevantes a los activos de información evaluados, calculando la probabilidad de que estas amenazas se puedan materializar.

f. **EL PROVEEDOR** deberá cuantificar la probabilidad de ocurrencia respecto a la posible materialización de amenazas.

g. **EL PROVEEDOR** deberá determinar los niveles de impacto (consecuencias) frente amenazas e incidentes que pudieran causar daño sobre los activos de información.

5.14.1. Lugar de presentación de Entregables y conformidad.

5.14.1.1. Lugar

EL PROVEEDOR deberá ingresar por mesa de partes institucional (virtual: https://mpv.essalud.gob.pe/Login/Index, o presencial: Av. Arenales N° 1402, Jesús María, Lima), cualquier tipo de comunicación, envío de documentos y medios de almacenamiento de ser el caso correspondiente al objeto de la contratación, la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de **ESSALUD,** no recibirá documentos que no hayan sido registrados por mesa de partes institucional (virtual: https://mpv.essalud.gob.pe/Login/Index), o presencial: Av. Arenales N°

1402, Jesús María, Lima) y que no hayan sido derivados vía el Sistema de Gestión Documental – SGD.

Toda documentación presentada a **ESSALUD**, deberá estar firmada digitalmente por el jefe del Proyecto.

5.14.1.2. Conformidad

La **conformidad** por cada entregable será otorgada por la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de la Información y Comunicaciones, previa presentación y según evaluación de los entregables y actividades descritas en el numeral 5.13.[18]

5.15. Otras obligaciones de la Entidad

5.15.1. Durante la implementación:

a. Comunicación y coordinación con **EL PROVEEDOR** del servicio, a través del Coordinador de la Oficina de Seguridad Informática de **ESSALUD**, quien será el nexo de coordinación entre **EL PROVEEDOR** con el personal responsable de las comunicaciones internas.

b. **ESSALUD** indicará al **PROVEEDOR** la arquitectura lógica y física de las plataformas de seguridad que deberán ser implementadas, las condiciones iniciales de bloqueos estándar, listas negras, listas blancas; así como, el espacio físico en el Centro de Datos institucional para el equipamiento, acometidas de energía estabilizada y de datos, así como, los tiempos de migración y corte para el inicio de operaciones.

5.15.2. Durante el periodo contractual:

a. Los mantenimientos internos programados por otras unidades orgánicas que puedan afectar a las plataformas de seguridad implementadas serán advertidos y coordinados previamente con **EL PROVEEDOR** por un tiempo no menor de veinticuatro (24) horas antes de iniciar estas labores.

b. Todo cambio interno de la arquitectura tecnológica de comunicaciones o de plataformas críticas de servicio que puedan afectar a la plataforma de seguridad implementada será advertido y comunicado previamente a **EL PROVEEDOR** con un tiempo no menor de veinticuatro (24) horas antes de iniciar estas labores.

5.16. Adelantos

Este proceso de contratación del servicio de implementación de la malla de seguridad no contempla adelantos de ninguna índole durante el periodo contractual.

5.17. Subcontratación

EL PROVEEDOR, es el único responsable ante **ESSALUD** del cumplimiento de lo contenido en los presentes términos de referencia y de lo establecido en los presentes términos de referencia. **EL PROVEEDOR** no podrá transferir la responsabilidad total o parcial del cumplimiento de la implementación de la solución de seguridad, mantenimientos y soporte técnico de la misma, sobre la elaboración de los informes técnicos o de cualquier otra incidencia sucedida derivada de la prestación de servicio, a otras entidades o a terceros por subcontratación.

5.18. Confidencialidad

EL PROVEEDOR deberá guardar confidencialidad y reserva sobre toda la información que llegue a conocer en desarrollo del contrato. En consecuencia, no podrá reproducir todo o parte, ni suministrar esta información a terceras personas, ni usarlas con fines distintos al propósito del objetivo del concurso y se encargará de mantener la confidencialidad de la información, la cual es extensiva a las personas a su cargo, siendo responsables frente a **ESSALUD,** por los daños y perjuicios que se generen en caso de que la misma no sea respetada. Así mismo, se obliga a la conservación, cuidado y manejo de información de hasta cinco (05) años posteriores a la última conformidad otorgada por **ESSALUD.**

EL PROVEEDOR se compromete a no revelar ni permitir la revelación de cualquier detalle a los medios de comunicación (digital, televisiva, radio, prensa escrita, entre otros de difusión) o a terceros, y a no usar el nombre de **ESSALUD** en cualquier promoción, publicidad o anuncio, sin previa autorización escrita de **ESSALUD,** de acuerdo con lo establecido en el Acuerdo de Confidencialidad que **EL PROVEEDOR** firmará con **ESSALUD,** a la firma del contrato.

5.19. Propiedad intelectual

Los documentos, archivos y en general cualquier información o conocimiento generados digital o físicamente, durante la prestación del servicio, serán de propiedad única y exclusiva de **ESSALUD,** quedando prohibido su uso para cualquier tipo de explotación de la misma, por parte **EL PROVEEDOR,** salvo que cuente con autorización expresa por parte del Seguro Social de Salud – **ESSALUD.** Así mismo, queda prohibido cualquier tipo de reproducción, publicación, disertación o divulgación pública o con terceros, por cualquier medio verbal y/o escrito.

[18] Absolución de consultas y observaciones N° 74 BIGSECURE S.A.C.

5.20. Medidas de control durante la ejecución contractual

5.20.1. Áreas que coordinarán con EL PROVEEDOR:

La **Oficina de Seguridad Informática** dependiente de la Gerencia Central de Tecnologías de Información y Comunicaciones, se encargará de coordinar con **EL PROVEEDOR** las labores de implementación y puesta en operación de la plataforma de seguridad y será el nexo para las coordinaciones con otras unidades orgánicas de corresponder.

5.20.2. Áreas responsables de las medidas de control:

La **Oficina de Seguridad Informática** dependiente de la Gerencia Central de Tecnologías de Información y Comunicaciones, se encargará de establecer e informar al **PROVEEDOR** sobre las medidas de control necesarias para el monitoreo, seguimiento y cumplimiento de lo establecido en los términos de referencia motivo de la presente contratación.

5.21. Modalidad de contratación:

No corresponde

5.22. Sistema de contratación:

El sistema de contratación será a SUMA ALZADA

5.23. Forma de pago

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

N° DE ENTREGABLE	VALOR DEL MONTO CONTRATADO	FECHA DE PAGO
01	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
02	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
03	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
04	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
05	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
06	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
07	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
08	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
09	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
10	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
11	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
12	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
13	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
14	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
15	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
16	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
17	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
18	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
19	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
20	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable

21	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
22	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
23	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
24	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
25	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
26	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
27	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
28	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
29	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
30	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
31	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
32	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
33	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
34	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
35	2.77 % del monto contratado	Se efectuará a la entrega y conformidad del entregable
36	3.05 % del monto contratado	Se efectuará a la entrega y conformidad del entregable

Importante: Los documentos parte de la descripción deberán ser presentados a través de la mesa de partes digital de **ESSALUD** (https://mpv.essalud.gob.pe/Login/Index), en formato digital.

5.24. Penalidades

En caso de retraso injustificado del proveedor en la ejecución de la prestación objeto de la contratación, se le aplicará automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

Penalidad diaria = 0.10 x monto
F x plazo en días

Donde F tiene los siguientes valores;

a. Para plazos menores o iguales a sesenta (90) días, para bienes, servicios en general y consultorías: F=0.40.
b. Para plazos mayores a sesenta (60) días, para bienes, servicios en general y consultorías: F = 0.25.

Tanto el monto como el plazo se refieren, según corresponda, al contrato o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica, a la prestación parcial que fuera en materia de retraso.

Para efectos del cálculo de la penalidad diaria se considera el monto del contrato vigente.

El proveedor incurre en aplicación de penalidades, cuando:

a. No cumpla con entregar el bien, prestar el servicio o presentar el entregable, según corresponda, en el plazo previsto en la orden de servicio y/o compra.
b. Cuando se hubiera otorgado un plazo de ampliación y este no se hubiera cumplido.

Se considera justificado el retraso, cuando el proveedor acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. Esta calificación de la conformidad.

5.25. Otras penalidades aplicables

Teniendo en consideración las condiciones generales referidas a otras penalidades y de acuerdo a lo establecido en el artículo 134, del reglamento de la **Ley N° 30225: LEY DE CONTRATACIONES DEL ESTADO Y SU REGLAMENTO,** vigente, al **PROVEEDOR** se le aplicará las penalidades según el siguiente detalle:

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CALCULO	PROCEDIMIENTO[19]
01	Por la incorrecta aplicación o la no aplicación de los procedimientos o requisitos establecidos por **ESSALUD y** bajo lo establecido en la NTP vigente: NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición. Según lo descrito en el numeral 5.2.1.2	Cinco (05) UIT	Informe Técnico de la Oficina de Seguridad Informática.
02	Por no presentar el Plan de Trabajo para Instalación, dentro del plazo descrito en el numeral 5.2.1.1.	Cuatro (04) UIT por cada día.	Informe Técnico de la Oficina de Seguridad Informática.
03	Por no ingresar el equipamiento requerido, dentro del plazo descrito en el numeral 5.2.1.3.	Cinco (05) UIT por cada día.	Informe Técnico de la Oficina de Seguridad Informática.
04	Por exceder el tiempo de instalación, configuración y puesta en marcha de los componentes requerido, según lo descrito en el numeral 5.2.1.5.	Diez (10) UIT por cada día.	Informe Técnico de la Oficina de Seguridad Informática.
05	Por exceder el tiempo máximo de inoperatividad en la implementación de la solución de la malla de seguridad propuesta, según lo descrito en el numeral 5.2.1.6.	Cinco (05) UIT por hora.	Informe Técnico de la Oficina de Seguridad Informática.
06	Por no presentar un cronograma de capacitación, según lo establecido en el numeral 5.2.2.	Cuatro (04) UIT por día.	Informe Técnico de la Oficina de Seguridad Informática.
07	Por carecer de licencias originales de los productos de software utilizados para brindar el servicio.	Díez (10) UIT	Informe Técnico de la Oficina de Seguridad Informática.
08	Por cambio del personal denominado: residente de operación, asignado al proyecto sin previa comunicación y aprobación de **ESSALUD.**	Cinco (05) UIT	Informe Técnico de la Oficina de Seguridad Informática.
09	Por corte del servicio por soporte, sin justificación y no informado a la Oficina de Seguridad Informática de **ESSALUD.**	Cinco (05) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
10	En caso de no cumplirse el tiempo de respuesta del Nivel 1 por la Atención en el Centro de Operaciones de Seguridad – SOC. Descrito en el inciso a. del numeral 5.10.1.	Cinco (05) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
11	En caso de no cumplirse el tiempo de respuesta del Nivel 2 por la Atención en el Centro de Operaciones de Seguridad – SOC. Descrito en el inciso a. del numeral 5.10.1	Cinco (05) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
12	En caso de no cumplirse el tiempo de respuesta del Nivel 3 por la Atención en el Centro de Operaciones de Seguridad – SOC. Descrito en el inciso a. del numeral 5.10.1.	Cinco (05) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
13	En caso de no cumplirse el tiempo de respuesta del Nivel 4 por la Atención en el Centro de Operaciones de Seguridad – SOC. Descrito en el inciso a. del numeral 5.10.1.	Cinco (05) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
14	En caso de no cumplirse el tiempo de respuesta máximo para la **SOLUCIÓN DEFINITIVA;** por **la Atención en el Centro de Operaciones de Seguridad – SOC**. Descrito en el subíndice **a.1** del inciso **a** del numeral 5.10.1.	Seis (06) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
15	En caso de no cumplirse el tiempo de respuesta del Nivel 1 por la Atención en Sitio (Residentes). Descrito en el inciso b. del numeral 5.10.1.	Cinco (5) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
16	En caso de no cumplirse el tiempo de respuesta del Nivel 2 por la Atención en Sitio (Residentes). Descrito en el inciso b. del numeral 5.10.1.	Cinco (5) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
17	En caso de no cumplirse el tiempo de respuesta del Nivel 3 por la Atención en Sitio (Residentes). Descrito en el inciso b. del numeral 5.10.1.	Cinco (5) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
18	En caso de no cumplirse el tiempo de respuesta del Nivel 4 por la Atención en Sitio (Residentes). Descrito en el inciso b. del numeral 5.10.1.	Cinco (5) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
19	En caso de no cumplirse el tiempo de respuesta máximo para la **SOLUCIÓN DEFINITIVA**; por la **Atención en Sitio** (Residentes). Descrito en el subíndice **a.1** del inciso **a** del numeral 5.10.1.	Seis (06) UIT por cada evento	Informe Técnico de la Oficina de Seguridad Informática.
20	Por el incumplimiento de la garantía en cuanto al equipamiento y licencias de software solución, según lo descrito en el numeral 5.1.2.	Diez (10) UIT	Informe Técnico de la Oficina de Seguridad Informática.

5.26. Responsabilidad por vicios ocultos

[19] Absolución de consultas y observaciones Nº 72 BIGSECURE S.A.C.

EL PROVEEDOR es el responsable por la calidad ofrecida de la prestación del servicio ofertado por un plazo de tres (03) años contados a partir de la conformidad otorgada por la ESSALUD.

5.27. Cláusula anticorrupción

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

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

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

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

5.28. Normativa específica

a. Ley N° 29733: Ley de Protección de Datos Personales.
b. Ley N° 28858: Ley que complementa la Ley N° 16053, Ley que autoriza a los Colegios de Arquitectos del Perú y al Colegio de Ingenieros del Perú para supervisar a los profesionales de Arquitectura e Ingeniería de la República y su Reglamento (Decreto Supremo N° 016-2008-VIVIENDA).
c. Ley N° 30225, Ley de Contrataciones del Estado.
d. Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado.
e. Ley N° 30999, Ley de Ciberdefensa.
f. Decreto de Urgencia N° 006-2020: Que crea el Sistema Nacional de Transformación Digital.
g. Decreto Supremo N° 017-2024-PCM.: Que aprueba el Reglamento de la Ley N° 30999, Ley de Ciberdefensa.
h. Decreto Supremo N° 003-2013-JUS: Que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos personales, y sus modificatorias.
i. Decreto Supremo N° 029-2021-PCM, Que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
j. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

ANEXO A

ACTA DE CONFORMIDAD DE PUESTA EN PRODUCCIÓN

Siendo las..... horas del día....., se procede a redactar la presente Acta sobre la Instalación, Configuración y Puesta en Producción de la solución ofertada del proceso

CONTRATACIÓN DEL SERVICIO DE UNA MALLA DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI.

Por la presente Acta, el jefe de la Oficina de Seguridad Informática, otorga la conformidad a las pruebas de puesta en producción realizadas por el proveedor de manera satisfactoria, de acuerdo al numeral 5.2.1.6.de los términos de referencia del servicio precitado.

Firman dando fe de lo anterior.

.....
Lugar y Fecha

.....	.....
SELLO Y FIRMA Representante Legal Contratista	SELLO Y FIRMA Jefe de la Oficina de Seguridad Informática

ANEXO B

ACTA DE CONFORMIDAD AL PLAN DE TRABAJO PARA INSTALACIÓN.

Siendo las..... horas del día....., se procede a redactar la presente Acta sobre la conformidad al plan de trabajo para Instalación del proceso *CONTRATACIÓN DEL SERVICIO DE UNA*

MALLA DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI.

Por la presente Acta, el jefe de la Oficina de Seguridad Informática, otorga la conformidad al plan de trabajo de instalación del proveedor, de acuerdo al numeral 5.2.1.1.de los términos de referencia del servicio precitado.

Firman dando fe de lo anterior.

.....
Lugar y Fecha

.....	.....
SELLO Y FIRMA Representante Legal Contratista	SELLO Y FIRMA Jefe de la Oficina de Seguridad Informática

ANEXO C

ACTA DE CONSTITUCIÓN DEL PROYECTO

Siendo las..... horas del día....., se procede a redactar la presente Acta de constitución del proyecto de implementación del Sistema de Gestión de Seguridad de la Información – SGSI, del proceso de *CONTRATACIÓN DEL SERVICIO DE UNA MALLA DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI.*

Por la presente Acta, el jefe de la Oficina de Seguridad Informática, otorga la conformidad al acta de constitución del proyecto, de acuerdo al numeral 5.2.3.2 .de los términos de referencia del servicio precitado.

Firman dando fe de lo anterior.

.....
Lugar y Fecha

.....	.....
SELLO Y FIRMA Representante Legal Contratista	SELLO Y FIRMA Jefe de la Oficina de Seguridad Informática

REQUISITOS DE CALIFICACIÓN

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA

	6. 01 Jefe del Proyecto para la malla de seguridad informática: Titulado en Ingeniería: de Sistemas y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática. ▪ 01 jefe del Proyecto para el Sistema de Gestión de Seguridad de la información Titulado en Ingeniería: de Sistemas y/o Industrial y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes. ▪ 01 especialista en Normatividad de Seguridad de la Información: Titulado en Ingeniería: de Sistemas y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes y/o Telecomunicaciones. ▪ 01 ingenieros Especialistas: Titulado en Ingeniería: de Sistemas y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes. ▪ 02 residente de Operación: Titulado o bachiller en Ingeniería: de Sistemas y/o de Computación y Sistemas y/o de Sistemas e Informática y/o Informática y/o Electrónica y/o de Redes. Acreditación: El Título Profesional 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: https://titulosinstitutos.minedu.gob.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 Título Profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
B.4	EXPERIENCIA DEL PERSONAL CLAVE
	Requisitos: 01 jefe de Proyecto para la malla de seguridad informática Experiencia profesional no menor a siete (07) años como: jefe de proyecto o Gerente de proyectos o líder de proyecto o gestor de proyecto, en gestión de tecnología de información y/o, en proyectos de seguridad de la información y/o ciberseguridad. 01 jefe del Proyecto para el Sistema de Gestión de Seguridad de la información Experiencia profesional no menor a cuatro (04) años como: jefe o analista o supervisor o consultor o implementador o auditor, en seguridad de la información y/o seguridad informática y/o ciberseguridad y/o especialista en seguridad de la información y/o continuidad de negocio.[20] 01 ingeniero Especialista en Normatividad de Seguridad de la Información: Experiencia profesional no menor a cinco (05) años como: jefe o analista o supervisor o consultor o implementador o auditor, en seguridad de la información y/o seguridad informática y/o ciberseguridad. 01 ingenieros Especialistas: Experiencia profesional no menor a tres (03) años como: auditor o implementador o especialista o analista o supervisor o consultor, en implementación de equipamiento de seguridad de la marca del equipamiento ofertados. 02 residente de Operación: Experiencia profesional no menor a un (1) años como: jefe o analista o supervisor o consultor o implementador o auditor, en operación de equipamiento de seguridad de la marca del equipamiento ofertado.

[20] Absolución de consultas y observaciones Nº 67 GRUPO RADICAL S.A.C.

	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 de prestaciones de servicios o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. **Importante** • *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.* • *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.* • *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.* • *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.*

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD[21] [22] [23]
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/. 10'000,000.00 (Diez 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 y/o implementación de equipamiento de seguridad de información y/o - Seguridad gestionada y/o - Administración de herramientas de seguridad informática y/o - Ciberseguridad y/o - Recolección de eventos y/o - Implementación de cableado de datos especializado a centro de datos y/o - Implementación de sistemas de gestión de seguridad de la información – SGSI y/o - Aplicación e implementación de normativas (ISO, NTPS, Normativas Nacionales, entre otras) y/o - Servicios de solución de respuesta, automatización y orquestación de seguridad, alineadas a: Seguridad de la información y/o Seguridad informática y/o Ciberseguridad. y/o - Servicio de Firewall Perimetral y/o - Servicio de Firewalls de Data Center y/o - Servicio de Plataforma de Seguridad y/o - Servicio de Soluciones de Ciberseguridad (Firewalls, Antispam, Filtro web, IS, Análisis de seguridad, Detección de Amenazas Avanzadas) y/o - Servicio de Soluciones de Networking (Switches LAN) y/o - Servicio de Licenciamiento y/o soporte y/o mantenimiento de Soluciones de Seguridad Perimetral y/o - Servicio de Renovación y/o suscripción de Licencias de Seguridad Perimetral y/o Ciberseguridad - Servicio de seguridad de la información y seguridad informática gestionada y/o - Solución de ciberseguridad para la gestión de seguridad de TI **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

[21] Absolución de consultas y observaciones Nº 44, 58 JAPAN COMPUTER SERVICE S.A.C.

[22] Absolución de consultas y observaciones Nº 70 GRUPO RADICAL S.A.C.

[23] Absolución de consultas y observaciones Nº 104 TELEFÓNICA TECH PERÚ S.A.C.

cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago13, 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 otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.

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

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo 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 las Especificaciones Técnicas 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 las características y/o requisitos funcionales. 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.*