"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

Informe Técnico Previo de Evaluación de Software N° 006 -2019
Sustento Técnico para la Renovación de Licencias de Appliance de Seguridad Perimetral

1. NOMBRE DEL ÁREA

Oficina de Tecnología de la Información y la Comunicación - OTI

2. RESPONSABLE DE LA EVALUACIÓN

Nombre : Carlos Herr García
Cargo : Coordinador Unidad Funcional de Infraestructura

Nombre : Ray Daniel García Ramos.
Cargo : Analista de Redes

3. FECHA

17 de Mayo de 2019

4. JUSTIFICACIÓN

Actualmente el Servicio Nacional de Meteorología e Hidrología del Perú - SENAMHI, es un organismo público ejecutor adscrito al Ministerio del Ambiente, tiene como propósito generar y proveer información y conocimiento meteorológico, hidrológico y climático de manera confiable, oportuna y accesible en beneficio de la sociedad peruana, con el ánimo de difundir información confiable y de calidad, el SENAMHI opera, controla, organiza y mantiene la Red Nacional de más de 900 Estaciones Meteorológicas e Hidrológicas de conformidad con las normas técnicas de la Organización Meteorológica Mundial (OMM).

El Servicio Nacional de Meteorología e Hidrología del Perú (Senamhi) requiere contar con el servicio de renovación de suscripción de licencias para el equipo de la solución de seguridad perimetral y para la protección contra intentos de amenaza externa de última generación que intente ingresar a la red de la Entidad; manteniendo la operatividad de los sistemas informáticos en beneficio de los servicios brindados por la institución a usuarios internos y externos del SENAMHI.

Mantener actualizadas las firmas de ataques y el soporte de los equipos de la solución de seguridad perimetral, los cuales continuarán brindando la protección ante amenazas informáticas y accesos no autorizados externos a la red informática del SENAMHI.

Actualmente el Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI cuenta con dispositivos de Seguridad Perimetral Palo Alto (PA-850), los mismos que necesitan renovación de licencias para garantizar la continuidad de los servicios ofrecidos por el SENAMHI y seguirá permitiendo la seguridad de la red institucional.

Por lo expuesto y en el marco de la ley 28612 "Ley que norma el uso, adquisición y adecuación del software del a Administración Pública", se procede a evaluar la licencia para los equipos del SENAMHI.

5. ALTERNATIVAS DE EVALUACIÓN

En el mercado peruano existen variadas marcas propietarias de Appliance para Seguridad Perimetral, tales como Fortinet, WatchGuard, Sophos, Cisco, etc los cuales manejan licencias divergentes a los que requiere el SENAMHI por contar con equipos appliance PALO ALTO en la actualidad.

6. ANALISIS COMPARATIVO TÉCNICO

El análisis técnico ha sido realizado en conformidad con la metodología establecida en la "Guía Técnica sobre evaluación de software en la administración Pública RM 139-2004 - PCM".

Propósito de la Evaluación:

Seleccionar la licencia necesaria requerida por el dispositivo de Seguridad Perimetral (Firewall) del SENAMHI.

Identificador de tipo de producto:

Licencia para equipo de seguridad Perimetral PA-850 en HA

- Threat prevention subscription for device in an HA
- PAND URL Filtering subscription for device in an HA
- WildFire subscription for device in an HA
- Partner enable premium support PA-850.

Selección de Métricas:

Acorde a lo expuesto para este tipo de Licencias se elabora el siguiente análisis.

DESCRIPCIÓN	Next Generation Firewall (NGFW) en Alta Disponibilidad (2 equipos) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta. Debe estar presente en los últimos 3 reportes de Gartner, en el cuadrante de Líderes para Network Enterprise Firewalls.
GEO LOCALIZACIÓN	Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea bloqueado. Debe posibilitar la visualización de los países de origen y destino en los logs de acceso. Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.

CONTROL DE APLICACIONES	Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, mas no limitado a Yahoo Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, mas no limitado a la como partición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas; Debe Actualizar la base de firmas de aplicaciones automáticamente. Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios; Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano. Debe alertar al usuario cuando una aplicación fuera bloqueada. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como: ➢ Tecnología utilizada en las aplicaciones (Client-Server, Browser Based, Network Protocol, etc). ➢ Nivel de riesgo de las aplicaciones. ➢ Categoría y sub-categoría de aplicaciones. Aplicaciones que usen técnicas evasivas, utilizadas por malwares, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
PREVENCIÓN DE AMENAZAS	Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance de Firewall. Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware). Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante. Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo. Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Antivirus y Antispyware habilitadas simultáneamente. Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo.

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA – REPÚBLICA DEL PERÚ

	Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma a firma. Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems. Debe permitir el bloqueo de vulnerabilidades. Debe permitir el bloqueo de exploits conocidos. Debe incluir seguridad contra ataques de negación de servicios. Deberá poseer los siguientes mecanismos de inspección de IPS: ➢ Análisis de patrones de estado de conexiones; ➢ Análisis de decodificación de protocolo; ➢ Análisis para detección de anomalías de protocolo; ➢ Análisis heurístico; ➢ IP Defragmentation; ➢ Re ensamblado de paquetes de TCP; Bloqueo de paquetes malformados. Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc. Detectar y bloquear el origen de portscans. Identificar y prevenir ataques de phishing al limitar los sitios a los que los usuarios pueden enviar credenciales Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones. Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re ensamblado de paquetes de TCP y bloqueo de paquetes malformados. Posea firmas específicas para la mitigación de ataques DoS. Posea firmas para bloqueo de ataques de buffer overflow. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto. Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3. Soportar bloqueo de archivos por tipo. Identificar y bloquear comunicaciones como botnets. Bloquear comunicaciones de comando y control

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA REPÚBLICA DEL PERÚ

	Las firmas deben basarse en patrones del payload del paquete y no en el hash del archivo malicioso. Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos). Debe soportar referencia cruzada como CVE. Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antispyware. Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos. Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3. Los eventos deben identificar el país de donde partió la amenaza. Debe incluir seguridad contra virus en contenido HTML y javascript, software espía (spyware) y worms. Seguridad contra descargas involuntarias usando HTTP de archivos ejecutables. Maliciosos. Rastreo de virus en PDFs. Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.). Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad, etc., o sea, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por Usuarios, Grupos de usuario, origen, destino, zonas de seguridad.
PREVENCIÓN DE AMENAZAS DESCONOCIDAS	Poseer la capacidad de análisis de amenazas no conocidas. Debido a los Malware hoy en día hay que ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada debe poseer funcionalidades para análisis de Malwares no conocidos incluidas en la propia herramienta o verificar a través de servicio Cloud. El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA – REPÚBLICA DEL PERÚ

	automática para análisis en la nube donde el archivo será ejecutado y simulado en un ambiente controlado o sandboxing. Seleccionar a través de la política de Firewall que tipos de archivos sufrirá este análisis o ser enviados a ambiente de sandboxing para ser analizados. El fabricante debe ser considerado como un Lider en el reporte de evaluación de Forrester Wave Automated Malware Analysis, Q2 2016. Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Mac OSX y Android. Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB. El sistema de análisis debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red). Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración. Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración. Debe permitir visualizar los resultados de los análisis de malware de día cero en los diferentes sistemas operacionales soportados. Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración. Soportar el análisis de archivos ejecutables (EXE), DLLs, ZIP y criptografiados en SSL en el ambiente controlado. Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), binarios de Mac OS, flash, apk y archivos java en el ambiente controlado. Poseer SLA de, como máximo, 10 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado. Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API La solución debe ser capaz de observar procesos que busquen inyectar código malicioso y explotar vulnerabilidades por medio de heap spray.

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA

	La solución debe detectar programas de auto-arranque, mutexes y actividades sospechosas en los servicios de Windows. La solución debe analizar todo el tráfico producido por el archive a analizar, debe detector la creación de backdoors, descargas posteriores de malware y conexiones a dominios de baja reputación. La solución de sandboxing debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor, infección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host. La solución debe enviar amenazas evasivas a un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales. La solución de sandboxing debe ser capaz de detectar e interrumpir la comunicación de comando y control saliente a través de firmas específicas de DNS y comando y control.
FILTRO URL	La plataforma de seguridad de debe poseer las siguientes funcionalidades de filtro de URL. Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora). Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local. Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función. Debe soportar una caché local de URL en el appliance, evitando el delay de comunicación/validación de las URLs. Debe poseer al menos 60 categorías de URLs. Debe soportar la creación de categorías URL custom. Debe soportar la exclusión de URLs del bloqueo por categoría. Debe permitir la customización de la página de bloqueo. Debe permitir o bloquear y continuar (habilitando que el usuario accese a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de "continuar" para permitirle seguir a ese site).

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA Y SEGURIDAD — REPÚBLICA DEL PERÚ

	Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios.
IDENTIFICACIÓN DE USUARIOS	Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local. Debe poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios. Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios. Debe posea integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Soporte a autenticación Kerberos. Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios. Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows
QOS	Como la finalidad de controlar aplicaciones y trafico cuyo consumo pueda ser excesivo, (como youtube, stream, etc) y tener un alto consumo de ancho de banda, se requiere que la solución, a la ves de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming. Soportar la creación de políticas de QoS por: ➢ Dirección de origen ➢ Dirección de destino ➢ Por usuario y grupo de LDAP/AD. Por puerto. El QoS debe permitir la definición de clases por: ➢ Ancho de Banda garantizado ➢ Ancho de Banda Máximo Cola de prioridad. Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. Disponer de estadísticas Real Time para clases de QoS.

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA

	Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario
VPN	Soportar VPN Site-to-Site y Cliente-To-Site. Soportar IPSec VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo. Soportar SSL VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo. VPNs IPSec debe soportar: ➢ 3DES; ➢ Autenticación MD5 e SHA-1; ➢ Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14; ➢ Algoritmo Internet Key Exchange (IKE); ➢ AES 128, 192 e 256 (Advanced Encryption Standard) Autenticación vía certificado IKE PKI. Debe poseer interoperabilidad con los siguientes fabricantes: ➢ Cisco ➢ Checkpoint ➢ Juniper ➢ Palo Alto Networks ➢ Fortinet Las VPN SSL deben permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB. Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente: ➢ La asignación de dirección IP en los clientes remotos de VPN; ➢ La asignación de DNS en los clientes remotos de VPN; Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario. El portal de VPN debe enviar al cliente remoto la lista de Gateway VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente. Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los Gateways disponibles con base al más rápido. Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa.
ADMINISTRACIÓN	La administración de las políticas de seguridad debe realizarse sobre los mismos applainces de seguridad, sin necesidad de un servidor o appliance aparte. La solución debe contar con Interface gráfica de usuario (GUI), vía Web por HTTP y/o HTTPS compatible al menos con, Windows, Linux y Mac OS.

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA

	La administración de la solución debe posibilitar un conjunto de estadísticas de todo el tráfico que pasa por los equipos de la plataforma de seguridad. La solución debe contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación. La solución debe contar con una interface gráfica de usuario (GUI) la cual se podrá elegir al menos entre los idiomas inglés y español. La solución debe poseer una Interface basada en línea de comando (CLI) para administración de la solución. La solución debe poseer puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. La solución de seguridad debe poseer comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet). La solución de seguridad debe permitir al administrador del sistema autenticarse vía usuario/contraseña o vía certificados digitales. La solución cuenta con la capacidad de asignar un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. (RBAC) La solución debe permitir a los administradores conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o https. La solución de seguridad cuenta con soporte de SNMP versión 3. La solución de seguridad permite integrar al menos 3 servidores syslog. Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. La solución de seguridad debe permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. La gestión de los firewalls debe realizarse por puertos Ethernet dedicados. Los equipos deben soportar administración fuera de línea (Out of band management). El software de administración debe proveer un medio de ver, filtrar y gestionar las trazas de tráfico registradas (logs). Los registros (logs) del firewall deben contener información de la regla que está gatillando el mismo. Estos registros (logs) no deben ser modificables.

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA
REPÚBLICA DEL PERÚ

	El sistema de gestión debe proveer estadísticas en tiempo real del estatus de la "salud" de los módulos del firewall en el dashboard de monitoreo, considerando parámetros como utilización de CPU y número total de sesiones concurrentes.

7. ANALISIS DE COSTO BENEFICIO

No se ha realizado un análisis comparativo de Costo – Beneficio, por cuanto en el presente Informe Técnico Previo de Evaluación de Licencia, solo se desea establecer la licencia más adecuada técnicamente.

La evaluación formal del análisis de costos se realizará durante el proceso de selección.

Licenciamiento:
A continuación se hace referencia a las condiciones del licenciamiento:

Auth Code	Part Number	Descripcion
63615292	PAN-PA-85-TP-HA2	Threat prevention subscription for device in an HA
39328703	PAN-PA-85-TP-HA2	Threat prevention subscription for device in an HA
72566218	PAN-PA-85-URL4-HA2	PAND URL Filtering subscription for device in an HA
76098099	PAN-PA-85-URL4-HA2	PAND URL Filtering subscription for device in an HA
78743258	PAN-PA-85-WF-HA2	WildFire subscription for device in an HA
62078780	PAN-PA-85-WF-HA2	WildFire subscription for device in an HA
16144651	PAN-SVC-BKLN-850	Partner enable premium support PA-850
33902031	PAN-SVC-BKLN-850	Partner enable premium support PA-850

Hardware necesario para su funcionamiento:
El SENAMHI cuenta en la actualidad con equipos Palo Alto de la seria 850 (PA-850) en alta disponibilidad (HA).

Soporte y Mantenimiento externo:
El soporte será por el periodo que dure la licencia (365 días).

El mantenimiento preventivo deberá darse por lo menos una (01) vez durante el período de garantía, y previa coordinación con la Oficina de Tecnologías de la Información - OTI.

Capacitaciones:
En todos los casos es necesaria la capacitación para el personal de TI, con un mínimo de 8 horas por parte del Contratista, la misma que se brindará en los ambientes de la institución sito en la Sede Principal de SENAMHI Jr. Cahuide 785, Jesús María - Lima, para un mínimo de cuatro (04) personas.

8. CONCLUSIONES

En base al análisis de la evaluación técnica y el análisis costo beneficio, se precisa que por los motivos ya señalados, se solicita la adquisición de Licencias para los equipos PA-850 en HA.

9. FIRMAS

Carlos Herr García Coordinador de la Oficina de Tecnologías de la Información y la Comunicación - OTI	
Ray Daniel García Ramos Analista de Redes Oficina de Tecnologías de la Información y la Comunicación - OTI	

UNIDAD FUNCIONAL OPERATIVA DE INFRAESTRUCTURA TECNOLÓGICA
REPÚBLICA DEL PERÚ