Al servicio de las personas y las naciones

SOLICITUD DE COTIZACIÓN (SdC)

Señores Invitados al Proceso PNUD/SDC-229/2018 Presente. -	**FECHA**: 3 de julio de 2018 **REFERENCIA:** PNUD/SDC-229/2018 "Adquisición de Firewall"

De nuestra consideración:

El Programa de Naciones Unidas para el Desarrollo (PNUD), dentro del marco del Proyecto 00096804 – 00100712 - Fortalecimiento del Programa Nacional de Alimentación Escolar Qali Warma del Ministerio de Desarrollo e Inclusión Social (MIDIS) para mejorar la atención alimentaria de las niñas y niños de las instituciones educativas públicas del país, es grato dirigirnos a usted a fin de solicitarle la presentación de una cotización para la adquisición de los equipos indicados a continuación, según especificaciones técnicas detalladas en el Anexo 2 de esta Solicitud de Cotización (SdC):

DESCRIPCION	Unidad de Medida	CANTIDAD
FIREWALL SEGURIDAD PERIMETRAL	Unidad	2

Su cotización deberá ser presentada hasta el **9 de julio de 2018** vía correo electrónico a la siguiente dirección: **adquisiciones.pe@undp.org** o en sobre cerrado en la **Av. Augusto Pérez Araníbar 750, Magdalena del Mar**

Las cotizaciones que se reciban en el PNUD después del plazo indicado, por cualquier razón, no se tomarán en consideración a efectos de evaluación. Si usted envía su cotización por correo electrónico, le rogamos se asegure de que esta se encuentre firmada y sea remitida en formato pdf, libre de cualquier virus o archivo dañado, con un peso máximo de 4MB por envío.

Le rogamos tome nota de los siguientes requisitos y condiciones relativos al suministro de los bienes antes citados:

No.	Desripción	Detalle
1.	Plazo y lugar de entrega	El plazo de entrega: El Plazo máximo de entrega e instalación será de 60 días calendario, contados desde el día siguiente de la recepción de la Orden de Compra por parte del proveedor. Lugar de entrega: • Lugar de entrega: El PNUD comunicará al proveedor la entrega de los bienes en un almacen ubicado en Lima Metropolitana
2.	Moneda preferente de cotización	Soles, incluido impuestos. (Moneda para proveedodes nacionales) Dólares americanos incluido impuestos (Moneda para proveedores internacionales)
3.	Fecha límite de presentación de la cotización	**9 de julio de 2018** Las ofertas se recibirán por vía electrónica a la siguiente dirección: adquisiciones.pe@undp.org
4.	Documentos que deberán presentarse	1. Datos del Oferente conforme al formulario del Anexo 1 2. Especificaciones Técnicas detalladas en el Anexo2 3. Declaración Jurada de Bienes ofertados según Anexo 3. 4. Carta del fabricante autorizando al oferente a comercializar los equipos ofertados. 5. Declaración Jurada de Garantía de los bienes según lo establecido en las Especificaciones Técnicas. 6. Oferta económica conforme al Anexo 4.

No.	Desripción	Detalle
5.	Periodo de validez de la cotización, a partir de la fecha de presentación de ofertas	Noventa (90) días. En circunstancias excepcionales, el PNUD podrá pedir al proveedor que amplíe la vigencia de la cotización más allá del plazo inicialmente indicado en esta SdC. El proveedor confirmará entonces la ampliación por escrito, sin modificación alguna de los precios cotizados.
6.	Cotizaciones parciales	No permitidas
7.	Servicio Conexos	El o los Oferentes deberán considerar lo siguiente: • Todo el material utilizado en la instalación (cables, conectores, adaptadores, software, etc.) deberá ser suministrado por el proveedor y deberán ir alineadas con las características de los equipos.
8.	Condiciones de pago	100% dentro de los 15 días siguientes a la entrega de la factura, previa conformidad emitida. La factura deberá ser emitida a nombre del: Programa de las Naciones Unidas para el Desarrollo RUC: 20507728961 Dirección: Av. Del Ejército 750, Magdalena del Mar. En caso de existir algún error en la factura, se tomará contacto con el proveedor en el más breve plazo, de modo que éste proceda con la subsanación correspondiente. En este caso, el plazo que dure el trámite de pago se contabilizará a partir de la fecha en la que el documento corregido sea entregado. El plazo máximo para la emisión del Acta de Conformidad de Entrega por parte del adquiriente es de hasta seis (06) días calendario luego de haber sido recepcionado los equipos.
9.	Garantía contra defectos de fabricación	Mínimo dos (2) años
10.	Criterios de evaluación	☒Pleno cumplimiento de los requisitos y precio más bajo[1] ☒Plena aceptación de los Términos y Condiciones Generales de la Orden de compra
11.	El PNUD adjudicará el contrato a:	La adjudicación de la buena pro se otorgará a un proveedor que habiendo calificado técnicamente, presente la oferta económica más conveniente.
12.	Tipo de contrato que deberá firmarse	Orden de Compra
13.	Condiciones para la liberación del pago	- Presentación de la factura comercial correctamente emitida, por parte del proveedor. - Guia de remisión. - Garantías de los bienes entregados.
14.	Cronograma:	Puesta a Disposicion de bases: 3 de julio de 2018 (vía electrónica) Recepción de consultas: 5 de julio de 2018 (vía electrónica) Envío de respuestas: 6 de julio de 2018 (vía electrónica) Recepción de ofertas: 9 de julio de 2018 (vía electrónica)

No.	Desripción	Detalle
15.	Aclaraciones y confirmación de datos:	Durante el periodo de evaluación, el PNUD podrá solicitar a los oferentes las aclaraciones y confirmación de datos que considere pertinentes para la correcta interpretación de los documentos presentados. En ningún caso, estas aclaraciones podrán interpretarse como una opción para que las empresas participantes puedan completar documentación o información sustancial omitida o modificar la ya presentada. Las aclaraciones se realizarán a través del Correo electrónico: Adquisiciones.pe@undp.org únicamente consignando la en el asunto la siguiente referencia: PNUD/SDC-229/2018
16.	Penalidades:	Si por razones imputables al adjudicatario, éste no entregara los bienes en todo o en parte, dentro de los plazos especificados en la Orden de Compra, el PNUD, sin perjuicio de los demás recursos que tenga con arreglo a la Orden de Compra, aplicará una penalidad equivalente al 0.5% del monto total contratado por cada día de retraso, hasta un máximo equivalente al 10%. Una vez alcanzada esta cifra, se podrá considerar la resolución de la Orden de Compra.
17.	Intransferibilidad de la orden de compra	La Orden de Compra no podrá ser transferida total ni parcialmente a favor de terceros.
18.	a. Anexos a esta SdC	b. Formulario de Datos del Oferente (Anexo 1) c. Especificaciones Técnicas Mínimas requeridas (Anexo 2) d. Formulario de presentación de oferta económica (Anexo 3) e. Términos y Condiciones Generales/Condiciones Especiales (Anexo 4). La no aceptación de los Términos y Condiciones Generales será motivo de descalificación de este proceso de adquisición.
19.	Contacto para todo tipo de información (Preguntas por escrito únicamente)	Unidad de Adquisiciones: adquisiciones.pe@undp.org Cualquier retraso en la respuesta del PNUD no podrá ser esgrimido como motivo para ampliar el plazo de presentación, a menos que el PNUD decida que estima necesaria dicha ampliación y comunique un nuevo plazo límite a los solicitantes.

Se revisarán los bienes ofrecidos basándose en su integridad y en la conformidad de la cotización con especificaciones mínimas descritas supra y cualquier otro anexo que facilite detalles de los requisitos del PNUD.

Será seleccionada la cotización que cumpla con todos los términos de referencia y condiciones y ofrezca el precio más bajo. Cualquier oferta que no cumpla con los requisitos será rechazada.

En caso de discrepancia entre el precio unitario y el precio total (que se obtiene al multiplicar el precio unitario por la cantidad), el PNUD procederá a un nuevo cálculo, y el precio unitario prevalecerá y el precio total será corregido. Si el proveedor no aceptara el precio final sobre la base del nuevo cálculo del PNUD y su corrección de los errores, su oferta será rechazada.

En ningún momento durante la vigencia de la cotización, el PNUD aceptará una variación de precios debido a aumentos, inflación, fluctuación por tipos de cambio o cualquier otro factor de mercado, una vez haya recibido la oferta. En el momento de la adjudicación del Contrato, el PNUD se reserva el derecho de modificar (aumentar o disminuir) la cantidad de servicios y/o bienes, hasta un máximo equivalente al veinticinco por ciento (25%) de la oferta total, sin ningún cambio en el precio unitario o en los términos y condiciones.

Toda orden de compra resultante de esta SdC estará sujeta a los Términos y Condiciones Generales que se adjuntan a la presente. El mero acto de presentación de una oferta implica que el vendedor acepta sin cuestionamiento alguno los Términos y Condiciones Generales del PNUD que se adjuntan como Anexo 5.

El PNUD no está obligado a aceptar ninguna oferta, ni a adjudicar ningún contrato u orden de compra, ni se hace responsable por cualquier costo relacionado con la preparación y presentación de un presupuesto por parte de un suministrador, con independencia del resultado o la forma de llevar a cabo el proceso de selección.

Sírvase tener en cuenta que el procedimiento establecido por el PNUD para la recepción de reclamos de sus proveedores tiene por objeto ofrecer una oportunidad de apelación a las personas o empresas a las que no se haya adjudicado una orden de compra o un contrato en un proceso de contratación competitivo. En caso de que usted considere que no ha sido tratado(a) con equidad, puede encontrar información detallada sobre los procedimientos de reclamo por parte de los proveedores en el siguiente enlace: http://www.undp.org/procurement/protest.shtml.

El PNUD insta a todos los potenciales proveedores a evitar y prevenir los conflictos de intereses, informando al PNUD si ellos o cualquiera de sus afiliados o miembros de su personal han participado en la preparación de los requisitos, el diseño, las especificaciones, los presupuestos o cualquier otra información utilizada en esta SdC.

El PNUD practica una política de tolerancia cero ante el fraude y otras prácticas prohibidas, y está resuelto a identificar y abordar todos los actos y prácticas de este tipo contra el PNUD o contra terceros implicados en las actividades de PNUD. Asimismo, espera que sus proveedores se adhieran al Código de Conducta de los Contratistas de las Naciones Unidas, que se puede consultar en el siguiente enlace: http://www.un.org/depts/ptd/pdf/conduct_spanish.pdf.

Le agradecemos su atención y quedamos a la espera de recibir su cotización.

Atentamente,

Unidad de Adquisiciones
PNUD/Oficina Perú

ANEXO 1

DATOS DEL OFERENTE

1. Nombre o Razón Social: _____

2. RUC:
   _____

3. Dirección Principal: _____

4. Teléfono No.: _____ Fax.:_____

5. Persona a contactar: _____

   Cargo:_____ E-mail: _____

6. Datos del Registro Mercantil de la Empresa: (Ejm: Nº Asiento, Foja, Tomo, Ficha, Partida Electrónica, etc. y/o algún otro dato:
   _____

   _____

7. Nombre del Representante Legal: _____

8. Documento de Identidad: _____

9. Número de cuenta bancaria en el BBVA Banco Continental en nuevos soles (20 dígitos):

   _____

10. En caso de no contar con cuenta en el BBVA Banco Continental, favor indicar el nombre de su banco y número de cuenta interbancaria (20 dígitos):
    _____

Fecha: _____

Nombre y firma del Representante Legal:
_____

ANEXO 2

ESPECIFICACIONES TÉCNICAS

1. DENOMINACIÓN DE LA ADQUISICIÓN DEL BIEN:

Adquisiciones equipos de seguridad perimetral para la Sede Central del Programa Nacional de Alimentación Escolar Qali Warma

2. ALCANCE Y DESCRIPCION DE LOS BIENES

El alcance comprende la provisión, instalación, configuración, soporte técnico y garantía del siguiente equipamiento:

I. CONSIDERACIONES GENERALES

Consideraciones de los productos esperados

- Provisión, Instalación, configuración y puesta en funcionamiento del equipamiento solicitado.
- Garantía y Soporte técnico por un periodo de dos (02) años de todo el equipamiento solicitado.
- La solución requerida es de tipo llave en mano; todos los componentes y/o subsistemas podrán ser de diferente marca y/o fabricante, siendo responsabilidad del proveedor realizar la integración de todos los componentes suministrados en el proyecto.
- Todos los equipos y componentes de la solución deben ser nuevos y de primera mano. La Entidad se reserva el derecho de consultar con el fabricante sobre la validación del modelo, los números de serie y la garantía ofertada por el Postor y la proporcionada por el fabricante.
- Instalación física de los equipos y ordenamiento de los cables.
- Diseño y/o rediseño de la Infraestructura de los equipos de seguridad perimetral.
- Definición de Listas de Control de Acceso y políticas de Seguridad
- Definición y Configuración de Políticas de Calidad de Servicio.
- Capacitación para dos (02) personas de la entidad, en configuración, operación, solución de problemas y mejoras de uso de los equipos de la Solución Ofertada, el mismo que deberá ser dictado por personal certificado en la marca del fabricante. Esta capacitación se realizará en la Sede Central del PNAEQW, sito en Av. Circunvalación Los Inkas N°208 Surco (Av. Javier Prado este) Piso 12 - Lima, durante la fase de implementación.
- Configuración y puesta en marcha de los equipos.
- El Contratista al finalizar el proyecto debe presentar los siguientes documentos:
  - ✓ El Informe de Implementación, el cual incluirá diagramas de diseño, diagramas de conectividad, diagramas lógicos, copias electrónicas de los archivos de configuración.
  - ✓ Un inventario de los equipos y aplicativos entregados al finalizar la implementación.

Condiciones de los productos esperados

- El Contratista será el responsable de realizar la instalación y configuración, brindar los componentes y accesorios necesarios para la puesta en marcha de los bienes que se entreguen como parte del presente proceso, para la cual debe proveer y detallar en su oferta todos los bienes y servicios necesarios para la puesta en funcionamiento de dichos dispositivos.
- El Plan de Trabajo del Proyecto deberá ser presentado, a los 15 días calendario como máximo, contados a partir del día siguiente de suscrito el contrato, estos días serán parte del plazo de la ejecución.
- El plan de trabajo deberá incluir un diagrama de Gantt con el cronograma final del proyecto.
- Se debe contemplar todos los materiales y herramientas necesarias para la correcta instalación de los equipos en el lugar que la Entidad destine para el efecto. Igualmente se debe asumir que los trabajos que impliquen la interrupción de las actividades de los usuarios de la Entidad, que suspendan la

continuidad de servicio deben realizarse los días laborables a partir de las 19:00 h. o en su defecto los fines de semana.

- Todos los equipos ofertados deberán ser nuevos e indicados vía carta del fabricante y tendrán instalada la última versión de sistema operativo propio del equipo que debe ser validada en la página web del fabricante.
- EL Contratista deberá realizar la actualización de firmware de los equipos a la última versión disponible por el fabricante por el periodo de dos (02) años a partir del acta entrega definitiva del proyecto, sin que esto genere costo alguno para la Entidad.
- Se deberá presentar un informe técnico final con toda la documentación necesaria del proyecto, en formato impreso y digital.
- Las licencias y garantías del Fabricante, de todo el bien ofertado; deberá figurar a nombre del Programa Nacional de Alimentación Escolar QALI WARMA y estos deberán presentarse en medio impreso y digital.
- Toda documentación y/o entregable deberá ser presentado y dirigido a la Unidad de Tecnologías de la Información del Programa Nacional de Alimentación Escolar Qali Warma - Ministerio de Desarrollo e Inclusión Social.

Pruebas de los productos esperados

- El Contratista deberá tomar las previsiones del caso, a fin de no perjudicar el inicio de las labores diarias en la Entidad en el momento de la implementación del equipamiento. La Entidad proporcionará las facilidades necesarias para realizar los trabajos dentro de sus instalaciones y en horarios fuera de oficina.
- Las pruebas de aceptación se realizarán en forma conjunta, entre el personal de la ENTIDAD y del Contratista, en base al protocolo de pruebas suministrado por el Contratista. Las pruebas tienen por finalidad verificar que los equipos son brindados de acuerdo a los requerimientos establecidos y deberán contener como mínimo lo siguiente:

  - ✓ Pruebas de Encendido y Apagado de Equipos luego de realizada la configuración.
  - ✓ Prueba de Funcionamiento de la Alta disponibilidad realizando el apagado de uno de los equipos.
  - ✓ Prueba de verificación de Políticas de Seguridad hacia los usuarios.
  - ✓ Prueba de funcionamiento de características de los equipos (IPS, Antivirus, Filtrado de URL, VPN, Control de Ancho de banda).
  - ✓ Verificación de Licencias Activas.
- Una vez finalizadas las pruebas de aceptación se firmará de manera conjunta entre el representante del Contratista y el representante de la Entidad, un Acta de Conformidad de la Instalación del Equipamiento.

II. ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS

EQUIPOS: FIREWALL SEGURIDAD PERIMETRAL
CANTIDAD: 02 Unidades

Especificaciones Técnicas	Descripción
Marca:	*indicar*
Modelo:	*Indicar*
Origen	*Indicar*
	Se deberá incluir todas las funcionalidades en un solo dispositivo del mismo fabricante.

Características del Firewall	El equipo no deberá degradar su performance cuando tenga habilitada todas sus funcionalidades en modo de producción. Esto será acreditado mediante una carta del fabricante señalando lo requerido
	El Firewall de seguridad perimetral debe tener la capacidad de operar en los modos de capa 2 (L2), capa 3 (L3). y modo transparente (brigde).
	La plataforma debe permitir el análisis de contenidos de aplicaciones en Capa 7.
	El software deberá ser ofrecido en su versión más estable y/o más avanzado.
	En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan anunciado su "End-of-life", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 5 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante.
	La solución de seguridad debe estar presente el en el cuadrante de Líderes para Network Enterprise Firewalls del reporte de Gartner 2017,
	El Firewall de seguridad perimetral debe estar instalado en un hardware del mismo fabricante, hardware diseñado exclusivamente para la función específica de seguridad, es decir, no se aceptarán equipos de propósito genérico (PC's o Servers).
	El Firewall de seguridad perimetral deberá estar implementado en Alta Disponibilidad, Activo- Pasivo
	Deberá contar con soporte para los siguientes servicios: Soporte de redes virtuales vlans 802.1q, Traducción de direcciones de red (NAT) por fuente y destino, por direcciones ip dinámicas y pool de puertos. PPPoE, bgp, ospf y rip2, dhcp server y dhcp relay. Protocolos de encriptación ike, 3des, aes, sha1 y md5. La identificación, control y visibilidad de aplicaciones deberá ser una funcionalidad de la solución Soporte de jumbo frames 9200 bytes como mínimo, En caso de protocolos desconocidos, se podrán asignar firmas propias Descripción y control de tráfico sshv2 Control de tráfico ipv4 e ipv6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y control de contenido ipv6 debe ser soportado en interfaces trabajando en L2 y L3
	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 funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente.
	Throughput de al menos 1.5 Gbps para la función de Firewall y control de aplicaciones, lo cual debe ser acreditado mediante documentación técnica del fabricante (Brochures, Datasheet, manuales técnicos). La propuesta debe incluir todas las licencias correspondientes para cumplir al 100% la necesidad propuesta.
	Throughput de al menos 750 Mbps con las siguientes funcionalidades habilitadas simultáneamente, para todas las firmas que la plataforma de seguridad posea, debidamente activadas y actuando: Firewall, control de aplicaciones, IPS, Antivirus.
	Se tomará en consideración solamente mediciones de throughput tomadas con 100% de tráfico http o tráfico real, no se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242. Esta medición debe ser acreditado en la propuesta técnica a través de folletos, manuales, catálogos, brochures, datasheet u otros documentos técnicos similares emitidos por el fabricante.
	Throughput mínimo de 500 Mbps para la función de VPN IPSec. La propuesta debe incluir todas las licencias correspondientes para cumplir al 100% la necesidad propuesta.
	Debe incluir integración completa con el Active Directory y LDAP

	Debe permitir crear controles de acceso basados en aplicaciones/ servicios/ protocolos predefinidos.
	Soportar un mínimo de 190,000 conexiones.
	Soportar 9500 nuevas conexiones por segundo como mínimo.
	Capacidad de disco como mínimo de 220 GB o mayor.
	Deberá contar con fuente de poder redundante.
	Deberá incluir cuatro (04) interfaces de cobre 10/100/1000 como mínimo por cada equipo
	Deberá incluir cuatro (04) interfaces SFP como mínimo por cada equipo, se deberá realizar la provisión e instalación de todos los Transceivers.
	Deberá incluir cuatro (04) interfaces SFP+ como mínimo por cada equipo, se deberá realizar la provisión e instalación de todos los Transceiver.
	Conexiones tipo red privada virtual (vpn ipsec y ssl), el módulo de vpn ipsec debe soportar al menos 1000 túneles.
	Deberá contar con un software cliente de vpn-ssl para los sistemas operativos, vista (32 y 64 bits) y Windows 7 (32 y 64 bits), Windows 8, a su vez deberá permitir crear políticas para tráfico vpn-ssl.
	Deberán poder dar servicio al menos 100 usuarios concurrentes vía ssl.
	Soporte para autenticación de vpn ssl, secure id y base de datos propia
	La actualización de la base de datos debe ser automática con opción a hacerla manual vía tftp
	Debe permitir hasta 1500 políticas
	Debe permitir la creación de un mínimo de 40 zonas de seguridad
Control de Aplicaciones y Administración de ancho de banda (QoS)	Reconocer por lo menos 2000 aplicaciones diferentes, incluyendo, mas no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail.
	Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo.
	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
	Reconocer aplicaciones diferentes: el trafico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail. Se entiende por aplicación un determinado programa informático considerando todas sus versiones, ejemplo: Una aplicación será Skype para todas sus versiones. No se aceptará soluciones que considere cada versión de una determinada aplicación como una aplicación distinta.
	Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, Skype, Facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, Oracle, active Directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, como mínimo.
	Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado.
	Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones criptografiadas, tales como Skype y ataques mediante el puerto 443.
	Para tráfico encriptado (SSL y SSH), debe desencriptar paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante.
	Debe Actualizar la base de firmas de aplicaciones automáticamente.
	Debe Reconocer aplicaciones en IPv6.
	Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD.

	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.
	Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas.
	Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas.
	Permitir la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias, con o sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano.
	Debe ser posible la creación de grupos estáticos y dinámicos de aplicaciones basados en las características de las aplicaciones.
	Deberá permitir el monitoreo del uso que hacen las aplicaciones por bytes, sesiones y por usuario, Así mismo disponer de estadísticas Real Time para clases de QoS.
	Como la finalidad de controlar aplicaciones y trafico cuyo consumo pueda ser excesivo, (como YouTube, upstream, 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 aplicaciones. 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.
Protección contra amenazas	Deberá incluir un módulo de protección contra amenazas de red, bloqueo de virus, spyware, control de transferencia de archivos, control de la navegación en internet y bloqueo de archivos por tipo, integrados en el propio appliance de Firewall
	Debe sincronizar las firmas de IPS, Antivirus, entre otros cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo.
	Cuando se utilicen las funciones de IPS, Antivirus, el equipamiento debe entregar el mismo performance (no degradar) entre tener algunas firmas de IPS habilitada o tener todas las firmas de IPS, Anti-Virus habilitadas simultáneamente.
	Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
	Protección contra descargas involuntarias usando http de archivos ejecutables maliciosos
	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3.
	Posea firmas específicas para la mitigación de ataques DoS;
	Deberá permitir la inspección en archivos comprimidos que usan algoritmo deflate (Zip, gzip, etc).
	Deberá permitir la adaptación de firmas de software espía y explotación de vulnerabilidades.
	Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables maliciosos.
	Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antivirus.

	Debe permitir que en la captura de paquetes por firmas de IPS y Antivirus, podra definirse el número de paquetes a ser capturados.
	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.).
	La actualización de firmas de ataques deberá ser diaria, semanal y de emergencia.
	El módulo de protección contra amenazas de virus, malware y spyware (módulo de IPS) deberá tener un rendimiento de al menos 750 Mbps de throughput.
	Incluya los siguientes mecanismos de IPS basados en: Análisis de patrones de estado Análisis de decodificación de protocolo Análisis para detección de anomalías de protocolo Análisis heurístico o comportamiento (de aplicaciones) IP desfragmentación (Fragmentación de IP) Re ensamblado de paquetes de tcp Permita el diseño de firmas de vulnerabilidades Identificación de botnet por comportamiento Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, scan.
	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.
	Exenciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma a firma.
Emulación de Archivos	La solución debe ofrecer una capa de protección contra amenazas desconocidas mediante emulación de archivos (sandboxing).
	Debe ofrecer el servicio de emulación basado en la nube para la solución ofertada.
	Debe prevenir archivos maliciosos antes de que lleguen a la red interna.
	Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7.
	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/o 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).
	El sistema automático de análisis debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware.

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.
Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), binarios de Mac OS, flash y archivos java en el ambiente controlado.
Permitir el envió de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.
Debe proteger de ataques dirigidos a sistemas operativos Windows en múltiples versiones.
Debe identificar malware desconocido escondido en documentos de office (Microsoft Office), archivos Adobe PDF, archivos ejecutables y archivos compresos.
Debe soportar emular archivos que están siendo transferidos en una comunicación cifrada SSL o TLS.
Emulación al monitorear: actividad y comportamiento del sistema de archivos, sistema de registro, procesos y actividad de red que provoca el archivo inspeccionado en múltiples sistemas operativos y versiones de office.
Debe generar reportes detallados de la emulación que incluya: detalles de los cambios realizados por el archivo malicioso, mostrado por diferentes sistemas operativos. O que incluya:detalles de la actividad anormal y tomas de pantalla reales del resultado de la emulación del archivo.
La solución de emulación debe soportar: emulación a nivel de sistema operativo (OS-Level Sandboxing)
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.
Para verificar que la red de la entidad se encuentre libre de malware antes de la instalación del firewall se deberá realizar un análisis de amenazas de malware en la red, a partir del cual se deben inspeccionar todo el tráfico entrante y saliente con el fin de encontrar todo tipo de amenaza cibernética que quiera ingresar a la red o detectar él envió de información que las maquinas ya infectadas estén realizando hacia el atacante. Esta tarea se realizará en modo de monitoreo, por lo cual no se deberá de bloquear el tráfico entrante o saliente, pero deberá tener la capacidad de ponerse in-line ante necesidad de la Entidad, generando un bloqueo en modo automático y tiempo real Análisis en base a tráfico no menos a 250 Mbps y despliegue en modalidad SPAN/TAP o INLINE El análisis se debe realizar en el appliance que realiza el análisis de malware y no debe ser realizado a través de enviar la información para análisis externa (a la nube) para inspección. Deberá emular sistemas operativos Windows y Mac. Las máquinas virtuales del equipo que realiza el análisis de malware deberán ser propietarias, y no de entorno público o comercial. Debe actuar en tiempo real (en el instante en que la amenaza intenta afectar a la red interna). De modo que informe por consola y por correo electrónico acerca de la presencia del malware moderno y/o avanzado en la red interna, a nivel de usuario por IP y por hostname. Indicar si hubiera malware descocido, debiendo proporcionar la siguiente Información: MD5, Tipo de archivo, protocolo usado, cantidad de ocurrencias, ejecutable del malware. El servicio a través del appliance instalado, debe ser capaz de ejecutar el código sospechoso, URL's y diversos tipos de archivos en un entorno virtual de inspección dentro del mismo dispositivo. Para ello realizara tanto análisis estático como dinámico en el sistema

	Para realizar las funciones indicadas preferentemente no debe requerir conectarse a otro dispositivo en la red que tenga como función proporcionar firmas de malware o depender de una tecnología (herramientas de seguridad)) para poder operar. El servicio deberá incluir un sistema que utilice técnicas avanzadas de sandboxing (virtualización del entorno infectado) y remisión de reportes y resultados en formato de presentación forense dentro del mismo appliance. La herramienta a utilizar deberá tener la capacidad de revisar todo el tráfico de datos con lo que actualmente cuenta la entidad, con capacidad superior a 1000 usuarios concurrentes en navegación web. Debe soportar la ejecución e inspección de los siguientes tipos de archivos: 3gp, asf, avi, bat, chm, cmd, com, csv, dll, doc, docx, exe, flv, gif, hop, hml, htm, hwp, ico, jar, jpg, js, lnk, midi, mov, mp3, mp4, mpg, pdf, png, ppsx, ppt, pptx, qt, rm, rmi, rtf, swf, tiff, url, vbs, vcf, vcs, wav, wma, wsf, xls, xlsx, xml. Debe tener la capacidad de emular entornos x.86 y x.64 localmente. El análisis de amenazas de malware en la red deberá tener una duración de 15 días calendario.
	Para verificar que la red de la entidad se encuentre libre de vulnerabilidades antes de la instalación del firewall se deberá realizar un escáner de análisis de vulnerabilidades. Esta consiste en efectuar una búsqueda basada en un software que puede escanear vulnerabilidades que funcionan sobre distintas plataformas informáticas o diversos Sistemas Operativos (Windows - Linux - Mac - Solaris, etc...), y que permitirá encontrar errores de configuraciones, ya sean por falta de actualización del S.O, puertos que pueden llevar a sesiones, procesos Web o fallos en softwares instalados (Apache, Mysql, etc) además, brindando reportes personalizados que permitan a la entidad definir medidas para salvaguardar la información interna. Esto será desarrollado para 15 direcciones Ips internas. Debe permitir realizar escaneos sin agentes, para una fácil instalación y mantenimiento. El software deberá realizar las siguientes tareas como mínimo: Debe permitir crear fácilmente políticas usando una variedad de asistentes. Debe permitir programar análisis, para ejecutarse una vez o de forma recurrente. Debe permitir clasificar los riesgos en 5 niveles de gravedad: Crítica, Alta, Media, Baja e Informativo. Debe permitir realizar informes flexibles, que puedan ser personalizados para ser ordenados por tipos vulnerabilidad o host, crear un resumen ejecutivo o comparar los resultados del análisis para destacar los cambios. Debe permitir generar reportes en formatos: XML, PDF, CSV, HTML. Debe permitir notificaciones vía email de los resultados, remediación y las recomendaciones y mejoras del escaneo de vulnerabilidades. Debe permitir escaneos de vulnerabilidades de redes IPV4, IPV6 e hibridas. Debe permitir realizar la detección de configuraciones erróneas en el sistema y parches faltantes. Debe permitir detectar virus, malware, backdoors, hosts que se comunican con los sistemas infectados por botnets, procesos conocidos / desconocidos, servicios web con enlaces a contenidos maliciosos. Debe cumplir con los requisitos del PCI DSS, a través de una auditoría de configuración y escaneo de aplicaciones web. El sistema permitirá realizar escaneos de vulnerabilidades que cubran las siguientes normativas: FFIEC, FISMA, CyberScope Reporting Protocol, GLBA, HIPAA/HITECH, NERC, PCI, SCAP, SOX, que permitan al IRTP realizar mejora continua de la seguridad interna.

	La auditoría de las configuraciones considerará las buenas prácticas y procesos de TI definidos por: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, IBM iSeries, ISO, NIST, NSA.
Identificación de Usuarios	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está usando qué aplicaciones, a través de la integración con servicios de directorio. Autenticación vía ldap, directorio activo 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.
	Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo. Así como también deberá incluir la capacidad de creación de políticas basadas en el control por usuario, grupos de usuarios o dirección ip.
	Deberá incluir la capacidad de creación de políticas basadas en “traffic shaping” por aplicación, usuario, fuente, destino, túnel vpn-ipsec-ssl.
	Deberá permitir el control, sin instalación de cliente de software, en equipos que soliciten salida a internet para que antes de iniciar la navegación, se despliegue un portal de autenticación residente en el firewall (captive portal) con soporte a autenticación por client certificate.
Filtro de Datos	Permite la creación de filtros para archivos y datos predefinidos;
	Los archivos deben ser identificados por extensión y firmas;
	Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc.) identificados sobre aplicaciones (P2P, Instant Messaging, SMB, entre otros.
	Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;
	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, más no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular;
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 via LDAP, Active 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 soportar una cacheé 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 accede a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de “continuar” para permitirle seguir a ese site).
	Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios.
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.
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
	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 y 256 (Advanced Encryption Standard) Autenticación vía certificado IKE PKI.
	Debe poseer interoperabilidad con los siguientes fabricantes: Cisco; Checkpoint; Juniper; Palo Alto Networks; Fortinet; Sonic Wall;
	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 una opción en el cliente remoto de escoger manualmente el gatteway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles.
	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.
Reportes y Administración	Debe tener un módulo de reportes y administración incluido dentro del mismo equipo sin necesidad de licenciamiento adicional
	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.

	Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados: Resumen gráfico de las aplicaciones utilizadas; Principales aplicaciones por utilización de ancho de banda de entrada y salida; Principales aplicaciones por tasa de transferencia en bytes; Principales hosts por número de amenazas identificadas; Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico; Debe permitir la creación de reportes personalizado.

III. GARANTÍA COMERCIAL

Se deberá proveer una garantía comercial contra defectos de diseño y/o fabricación, averías, por mal funcionamiento o pérdida total de los bienes derivados de desperfectos o fallas ajenas al uso normal o habitual de los bienes, los cuales no fueron detectados en el momento que se otorgó la conformidad, por un periodo de veinticuatro (24) meses.

IV. UBICACIÓN/SEDE

La Provisión, Instalación y Configuración del equipamiento se realizará en sede principal del Programa Nacional de Alimentación Escolar QALI WARMA, sito en Av. Circunvalación Los Inkas N°208 Surco (Av. Javier Prado este) - Lima

V. PERFIL CARACTERÍSTICO DEL PROVEEDOR Y/O SU PERSONAL A CONTRATAR - CALIFICACIONES Y EXPERIENCIA

Del Proveedor:

Los requisitos que deben ser cumplidos por el proveedor son:

a) El proveedor deberá asegurar que el equipamiento a ofertar no cuente a la fecha de presentación de propuestas con anuncio de Fin de Ciclo Vital (Fin de Vida) del fabricante con el fin de asegurar una mayor vigencia tecnológica de los equipos a adquirir. Esta deberá ser sustentada con información de referencia pública (páginas de internet) o mediante Carta del Fabricante.
b) El proveedor deberá contar con los perfiles profesionales correspondientes para la implementación. Es preciso indicar que todos los certificados deben estar en vigencia al momento de la firma del contrato. Estos se acreditarán con una declaración jurada
c) El proveedor deberá proporcionar todos los equipos, cables y accesorios necesarios para la interconexión entre los distintos componentes.
d) El proveedor deberá presentar documentación tales como catálogos, brochures, datasheet, hojas de datos, fichas técnicas, que sustenten el cumplimiento de las especificaciones técnicas minimas, solicitadas del equipamiento propuesto.

Del personal:
(01) Jefe de Proyecto:
a. Educación:

- Ingeniero o bachiller como mínimo en una de las siguientes carreras profesionales: Ingeniería Electrónica, Telecomunicaciones, Sistemas, Informática, Industrial, Cómputo o afines.
- Certificación vigente en PMP o en estudios como especialista en gerencia de proyectos.
- Con Certificación Técnica en la marca o producto ofertado.
- Con conocimiento demostrable en ISO 27001.
- Capacidades de coordinación, comunicación y trabajo en equipo.

b. Experiencia profesional:

- Experiencia profesional mínima de dos (2) años como jefe de proyecto

- Experiencia en gestión de proyectos de tecnologías de la información o proyectos relacionados al objeto de la convocatoria.

(01) Especialista en Seguridad Perimetral

a. Educación:

- Iingeniero o bachiller o técnico como mínimo en una de las siguientes carreras profesionales: Ingeniería Electrónica, Telecomunicaciones, Sistemas, Informática, Industrial, Cómputo o afines.
- Certificación de nivel técnico emitida por el fabricante de la Solución de Seguridad Perimetral ofertada.

b. Experiencia profesional:

- Experiencia profesional mínima de dos (2) años como implementado

VI. DEL MANTENIMIENTO PREVENTIVO, SOPORTE TECNICO, SEGURIDAD GESTIONADA Y CAPACITACION

Mantenimiento Preventivo

Se deberán realizar dos (02) mantenimientos preventivos, durante el periodo de garantía, el primero al finalizar el primer año de garantía y el segundo un mes antes de finalizar el segundo año de garantía, el mantenimiento consiste en lo siguiente:

- Limpieza de los equipos en caso sea necesario.
- Actualizaciones de Software y/o firmware de los equipos, a la versión más reciente y estable disponible al momento de realizar los respectivos mantenimientos.

Soporte Técnico y Seguridad Gestionada:

Soporte Técnico:

En lo relacionado al soporte técnico y la seguridad gestionada el contratista deberá tener en cuenta lo siguiente:

a) El servicio de soporte técnico debe ser bajo la modalidad 24x7x365 y tener la misma duración que el tiempo de garantía de los equipos especificado en el punto anterior. Asimismo, debe incluir cambio de partes, actualizaciones del software.
b) Los tiempos de atención deben cumplir lo siguiente:
   - ✓ Respuesta telefónica menor a sesenta (60) minutos confirmando la recepción del reporte de incidencia.
   - ✓ Respuesta de atención de dos (02) horas como máximo a cargo de técnico especializado.
   - ✓ Tiempo de resolución máxima de cuatro (04) horas luego de reportado el problema, en caso se requiera el reemplazo del hardware (RMA).
c) El Contratista debe poseer un Centro de Control, ubicado en el Perú, que emplee las buenas prácticas de gestión de servicios.
d) El Contratista debe poseer una línea directa fija, además de líneas celulares de soporte. El Contratista deberá facilitar el detalle de los números telefónicos para su verificación por parte de la entidad.
e) El Contratista debe proporcionar los niveles de escalamiento para los casos de avería, registro de incidencias y soporte.
f) El Contratista como empresa integradora de soluciones de tecnología será la responsable de todas las coordinaciones ante el fabricante, en caso sea requerido.
g) Los daños ocasionados por el Contratista durante la ejecución de los trabajos, sobre propiedad de terceros, será cubierto por este, sin perjuicio de la Entidad.

Seguridad Informática Gestionada:

En cuanto a la seguridad gestionada de los equipos a ofertar, el Contratista deberá cumplir lo siguiente:

a) Contar con una mesa de control o SOC (Security Operation Center), ubicado geográficamente dentro del país y donde se cuente con personal experto, certificado y dedicado para la gestión del servicio. El cual debe contemplar las siguientes actividades:
   - ✓ Disponibilidad de monitoreo y control de la seguridad en las redes y en Internet bajo la modalidad 24x7x365 deberá estar disponible durante la ejecución de la garantía, siendo la

Entidad quien solicitará al proveedor la intervención necesaria durante este periodo. Este monitoreo debe incluir la evaluación de la performance, disponibilidad, uso de interfaces y estatus de procesamiento de las funcionalidades de los equipos.

- ✓ El control sobre las actividades de los administradores de la solución, es decir; "quién" hizo, "qué" cambios, "cuándo" y "por qué".
- ✓ La notificación de los eventos de seguridad, caída de equipos y comportamiento anómalo a los responsables de la Entidad. Es preciso indicar que la comunicación de estos incidentes se realizará en base al nivel de escalamiento que establecerá la entidad.
- ✓ El apoyo en la respuesta a incidentes y en la neutralización de ataques relacionados a la seguridad de la información.
- ✓ La gestión y administración de los equipos propuestos deberán ser de manera compartida con la Entidad. Es preciso indicar que todo cambio planificado o ejecutado por el SOC debe ser autorizado de manera formal por los responsables de la Entidad, según el procedimiento de gestión de cambios. Los cambios que requiera la Entidad serán comunicados con un mínimo de seis (06) horas de anticipación.
- ✓ Designar a una persona del SOC para la atención de reportes a solicitud de la Entidad. Este responsable debe contar con los conocimientos y experiencia en el manejo y generación de reportes en los equipos propuestos. Los reportes serán enviados a la Entidad de manera mensual indicando los incidentes ocurridos, así también se considerarán reportes a demanda cuando la Entidad así lo requiera (los tiempos de entrega serán de un máximo de 24 horas). Algunos de reportes requeridos serán los siguientes:
  - ➢ Cambios de políticas en los cortafuegos, fecha y hora de cambio, usuario, IP origen, política, detalles de cambios, etc. Este reporte será requerido en los cortafuegos perimetrales e interno.
  - ➢ Cambios en el módulo de acceso web (filtro web), fecha y hora, usuario, IP origen, detalles de cambio, etc.
  - ➢ Conexiones establecidas por usuarios VPN (SSL, IPSEC, SITE to SITE, etc.). Estos reportes deberán contener información de fecha y hora de conexión, usuarios, IP origen, IP destino, aplicaciones, puertos, tráfico, etc.
  - ➢ Creación de usuarios VPN (SSL, IPSEC, SITE to SITE, etc.). Estos reportes deberán contener información de fecha y hora de conexión, usuarios, IP origen, IP destino, aplicaciones, puertos, tráfico, etc.
  - ➢ Cambios y/o modificaciones en los usuarios VPN (SSL, IPSEC, SITE to SITE, etc.).
  - ➢ Y otros reportes que la Entidad pudiera necesitar en el transcurso de la vigencia del servicio del SOC.

b) Contar con los recursos técnicos, software y herramientas propietarias que le permitan generar los reportes solicitados por la Entidad.

c) Contar con políticas de seguridad de la información, debidamente implementadas en el SOC

Capacitación:

Se deberá brindar una Capacitación a dos (02) profesionales de la Unidad de Tecnologías del Programa Nacional de Alimentación Escolar Qali Warma - Ministerio de Desarrollo e Inclusión Social, en configuración, operación, solución de problemas y mejoras de uso de los equipos de la Solución Ofertada según lo siguiente:

Para los equipos de Seguridad Perimetral.

- Tipo de Capacitación: Deberá seguir el modelo curricular del curso Oficial o curricula similar a la indicada por el fabricante
- Número de Horas: 16 Horas
- Perfil del Capacitador.
  - ✓ Ingeniero de las escuelas profesionales de Ingeniería de Sistemas o Informática o Electrónica o Computación o afines
  - ✓ Experiencia mínima de dos (02) años como capacitador soluciones de seguridad
  - ✓ El Expositor deberá contar con la certificación técnica oficial de la marca ofertada, en su grado de especialización más alto.

La capacitación se realizará en la Sede Central sito en la Av. Circunvalación Los Inkas N°208 Surco (Av. Javier Prado este) Piso 12 - Lima, durante la fase de implementación.

Deberá realizarse la entrega de Certificado por parte del Contratista

ISO 27001 (acorde a la NTP ISO/IEC 27001):

Se deberá brindar una Capacitación para tres (03) profesionales de la Unidad de Tecnologías de la Informacion del Programa Nacional de Alimentación Escolar Qali Warma - Ministerio de Desarrollo e Inclusión Social, en la norma ISO 27001, considerando los siguientes objetivos finales:

- Identificar las razones para adoptar un Sistema de Gestión de Seguridad de la Información.
- Conocer los requerimientos de la Norma ISO 27001.
- Identificar usos y controles de un Sistema de Gestión de Seguridad de la Información.
- Comprender el Diseño de un Sistema de Gestión de Seguridad de la Información.

Generalidades:

- Estructura: Deberá seguir el siguiente modelo curricular:
  - .1.1.1..1. Conceptos y fundamentos de seguridad de la información
  - .1.1.1..2. Terminología
  - .1.1.1..3. Familia de normas ISO/IEC 27000
  - .1.1.1..4. Importancia del SGSI en la organización
  - .1.1.1..5. La estructura de la norma 27001
  - .1.1.1..6. Identificación de requisitos
  - .1.1.1..7. El sistema de gestión
  - .1.1.1..8. Los controles del anexo A
  - .1.1.1..9. El proceso de auditoría y certificación
- Número de Horas: 08 Horas
- Perfil del Capacitador.
  - ✓ Ingeniero de las escuelas profesionales de Ingeniería de Sistemas o Informática o Electrónica o Computación o afines
  - ✓ Experiencia mínima de cinco (05) años como capacitador en ISO 27001.
  - ✓ Deberá ser Lead Auditor ISO/IEC 27001
  - ✓ El Expositor deberá contar con la certificación técnica oficial de la marca ofertada para la seguridad perimetral.

La capacitación se realizará en la Sede Central sito en la Av. Circunvalación Los Inkas N°208 Surco (Av. Javier Prado este) Piso 12 - Lima, durante la fase de implementación.

Deberá realizarse la entrega de Certificado por parte del Contratista

VII. ENTREGABLES

Al finalizar la Instalación y configuración del equipamiento solicitado se deberá presentar un informe final el cual debe contener la siguiente documentación, los mismos que deberán entregarse en dos (02) juegos en formato impreso y digital:

- Diagrama de conexión de los Equipos de Seguridad Perimetral
- Procedimiento detallado de la instalación y configuración de los equipos de seguridad perimetral.
- Archivos conteniendo el Backup de los equipos de seguridad perimetral.
- Instructivos y/o manuales de configuración de los equipos de seguridad perimetral.
- Documento en donde se pueda verificar el periodo de Garantía del fabricante del Equipamiento propuesto.

VIII. PLAZO DE ENTREGA

El Plazo de entrega será de 60 días calendario, contados desde el día siguiente de la recepción de la Orden de Compra por parte del proveedor.

ANEXO 3

DECLARACION JURADA DE BIENES OFERTADOS

El que suscribe _____ (nombre del representante legal de la empresa) DECLARA que los bienes ofertados son nuevos y sin uso.
Los detalles del cumplimiento de las Especificaciones Técnicas se encuentran según el siguiente cuadro:

A. Cumplimiento de Expecificaciones Técnicas

Especificaciones Técnicas	Descripción	Detalle de Especificaciones Propuestas	Numero de Folio de la Cotización
Marca:	*(consignar)*	*(consignar)*	*(consignar)*
Modelo:	*(consignar)*	*(consignar)*	*(consignar)*
Origen	*(consignar)*	*(consignar)*	*(consignar)*
Características del Firewall	Se deberá incluir todas las funcionalidades en un solo dispositivo del mismo fabricante.	*(consignar)*	*(consignar)*
	El equipo no deberá degradar su performance cuando tenga habilitada todas sus funcionalidades en modo de producción. Esto será acreditado mediante una carta del fabricante señalando lo requerido	*(consignar)*	*(consignar)*
	El Firewall de seguridad perimetral debe tener la capacidad de operar en los modos de capa 2 (L2), capa 3 (L3). y modo transparente (brigde).	*(consignar)*	*(consignar)*
	La plataforma debe permitir el análisis de contenidos de aplicaciones en Capa 7.	*(consignar)*	*(consignar)*
	El software deberá ser ofrecido en su versión más estable y/o más avanzado.	*(consignar)*	*(consignar)*
	En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan anunciado su “End-of-life”, o dejen de ser fabricadas, comercializadas y/o soportadas durante los 5 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante.	*(consignar)*	*(consignar)*
	La solución de seguridad debe estar presente el en el cuadrante de Líderes para Network Enterprise Firewalls del reporte de Gartner 2017,	*(consignar)*	*(consignar)*
	El Firewall de seguridad perimetral debe estar instalado en un hardware del mismo fabricante, hardware diseñado exclusivamente para la función específica de seguridad, es decir, no se aceptarán equipos de propósito genérico (PC’s o Servers).	*(consignar)*	*(consignar)*
	El Firewall de seguridad perimetral deberá estar implementado en Alta Disponibilidad, Activo- Pasivo	*(consignar)*	*(consignar)*
	Deberá contar con soporte para los siguientes servicios: Soporte de redes virtuales vlans 802.1q, Traducción de direcciones de red (NAT) por fuente y destino, por direcciones ip dinámicas y pool de puertos. PPPoE, bgp, ospf y rip2, dhcp server y dhcp relay. Protocolos de encriptación ike, 3des, aes, sha1 y md5. La identificación, control y visibilidad de aplicaciones deberá ser una funcionalidad de la solución Soporte de jumbo frames 9200 bytes como mínimo, En caso de protocolos desconocidos, se podrán asignar firmas propias Descripción y control de tráfico sshv2 Control de tráfico ipv4 e ipv6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y control de contenido ipv6 debe ser soportado en interfaces trabajando en L2 y L3	*(consignar)*	*(consignar)*

	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	*(consignar)*	*(consignar)*
	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente.	*(consignar)*	*(consignar)*
	Throughput de al menos 1.5 Gbps para la función de Firewall y control de aplicaciones, lo cual debe ser acreditado mediante documentación técnica del fabricante (Brochures, Datasheet, manuales técnicos). La propuesta debe incluir todas las licencias correspondientes para cumplir al 100% la necesidad propuesta.	*(consignar)*	*(consignar)*
	Throughput de al menos 750 Mbps con las siguientes funcionalidades habilitadas simultáneamente, para todas las firmas que la plataforma de seguridad posea, debidamente activadas y actuando: Firewall, control de aplicaciones, IPS, Antivirus.	*(consignar)*	*(consignar)*
	Se tomará en consideración solamente mediciones de throughput tomadas con 100% de tráfico http o tráfico real, no se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242. Esta medición debe ser acreditado en la propuesta técnica a través de folletos, manuales, catálogos, brochures, datasheet u otros documentos técnicos similares emitidos por el fabricante.	*(consignar)*	*(consignar)*
	Throughput mínimo de 500 Mbps para la función de VPN IPSec. La propuesta debe incluir todas las licencias correspondientes para cumplir al 100% la necesidad propuesta.	*(consignar)*	*(consignar)*
	Debe incluir integración completa con el Active Directory y LDAP	*(consignar)*	*(consignar)*
	Debe permitir crear controles de acceso basados en aplicaciones/ servicios/ protocolos predefinidos.	*(consignar)*	*(consignar)*
	Soportar un mínimo de 190,000 conexiones.	*(consignar)*	*(consignar)*
	Soportar 9500 nuevas conexiones por segundo como mínimo.	*(consignar)*	*(consignar)*
	Capacidad de disco como mínimo de 220 GB o mayor.	*(consignar)*	*(consignar)*
	Deberá contar con fuente de poder redundante.	*(consignar)*	*(consignar)*
	Deberá incluir cuatro (04) interfaces de cobre 10/100/1000 como mínimo por cada equipo	*(consignar)*	*(consignar)*
	Deberá incluir cuatro (04) interfaces SFP como mínimo por cada equipo, se deberá realizar la provisión e instalación de todos los Transceivers.	*(consignar)*	*(consignar)*
	Deberá incluir cuatro (04) interfaces SFP+ como mínimo por cada equipo, se deberá realizar la provisión e instalación de todos los Transceiver.	*(consignar)*	*(consignar)*
	Conexiones tipo red privada virtual (vpn ipsec y ssl), el módulo de vpn ipsec debe soportar al menos 1000 túneles.	*(consignar)*	*(consignar)*
	Deberá contar con un software cliente de vpn-ssl para los sistemas operativos, vista (32 y 64 bits) y Windows 7 (32 y 64 bits), Windows 8, a su vez deberá permitir crear políticas para tráfico vpn-ssl.	*(consignar)*	*(consignar)*
	Deberán poder dar servicio al menos 100 usuarios concurrentes vía ssl.	*(consignar)*	*(consignar)*
	Soporte para autenticación de vpn ssl, secure id y base de datos propia	*(consignar)*	*(consignar)*
	La actualización de la base de datos debe ser automática con opción a hacerla manual vía tftp	*(consignar)*	*(consignar)*
	Debe permitir hasta 1500 políticas	*(consignar)*	*(consignar)*
	Debe permitir la creación de un mínimo de 40 zonas de seguridad	*(consignar)*	*(consignar)*
Control de Aplicaciones y Administración de ancho de banda (QoS)	Reconocer por lo menos 2000 aplicaciones diferentes, incluyendo, mas no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail.	*(consignar)*	*(consignar)*
	Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo.	*(consignar)*	*(consignar)*

	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.	*(consignar)*	*(consignar)*
	Reconocer aplicaciones diferentes: el trafico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail. Se entiende por aplicación un determinado programa informático considerando todas sus versiones, ejemplo: Una aplicación será Skype para todas sus versiones. No se aceptará soluciones que considere cada versión de una determinada aplicación como una aplicación distinta.	*(consignar)*	*(consignar)*
	Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, Skype, Facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, Oracle, active Directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, como mínimo.	*(consignar)*	*(consignar)*
	Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado.	*(consignar)*	*(consignar)*
	Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones criptografiadas, tales como Skype y ataques mediante el puerto 443.	*(consignar)*	*(consignar)*
	Para tráfico encriptado (SSL y SSH), debe desencriptar paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante.	*(consignar)*	*(consignar)*
	Debe Actualizar la base de firmas de aplicaciones automáticamente.	*(consignar)*	*(consignar)*
	Debe Reconocer aplicaciones en IPv6.	*(consignar)*	*(consignar)*
	Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD.	*(consignar)*	*(consignar)*
	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.	*(consignar)*	*(consignar)*
	Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas.	*(consignar)*	*(consignar)*
	Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas.	*(consignar)*	*(consignar)*
	Permitir la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias, con o sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano.	*(consignar)*	*(consignar)*
	Debe ser posible la creación de grupos estáticos y dinámicos de aplicaciones basados en las características de las aplicaciones.	*(consignar)*	*(consignar)*
	Deberá permitir el monitoreo del uso que hacen las aplicaciones por bytes, sesiones y por usuario, Así mismo disponer de estadísticas Real Time para clases de QoS.	*(consignar)*	*(consignar)*
	Como la finalidad de controlar aplicaciones y trafico cuyo consumo pueda ser excesivo, (como YouTube, upstream, 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.	*(consignar)*	*(consignar)*

	Soportar la creación de políticas de QoS por: Dirección de origen Dirección de destino Por usuario y grupo de LDAP/AD. Por aplicaciones. Por puerto. El QoS debe permitir la definición de clases por: Ancho de Banda garantizado Ancho de Banda Máximo Cola de prioridad	*(consignar)*	*(consignar)*
	Soportar priorización Real Time de protocolos de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.	*(consignar)*	*(consignar)*
Protección contra amenazas	Deberá incluir un módulo de protección contra amenazas de red, bloqueo de virus, spyware, control de transferencia de archivos, control de la navegación en internet y bloqueo de archivos por tipo, integrados en el propio appliance de Firewall	*(consignar)*	*(consignar)*
	Debe sincronizar las firmas de IPS, Antivirus, entre otros cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo.	*(consignar)*	*(consignar)*
	Cuando se utilicen las funciones de IPS, Antivirus, el equipamiento debe entregar el mismo performance (no degradar) entre tener algunas firmas de IPS habilitada o tener todas las firmas de IPS, Anti-Virus habilitadas simultáneamente.	*(consignar)*	*(consignar)*
	Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.	*(consignar)*	*(consignar)*
	Protección contra descargas involuntarias usando http de archivos ejecutables maliciosos	*(consignar)*	*(consignar)*
	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3.	*(consignar)*	*(consignar)*
	Posea firmas específicas para la mitigación de ataques DoS;	*(consignar)*	*(consignar)*
	Deberá permitir la inspección en archivos comprimidos que usan algoritmo deflate (Zip, gzip, etc).	*(consignar)*	*(consignar)*
	Deberá permitir la adaptación de firmas de software espía y explotación de vulnerabilidades.	*(consignar)*	*(consignar)*
	Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables maliciosos.	*(consignar)*	*(consignar)*
	Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antivirus.	*(consignar)*	*(consignar)*
	Debe permitir que en la captura de paquetes por firmas de IPS y Antivirus, podra definirse el número de paquetes a ser capturados.	*(consignar)*	*(consignar)*
	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.	*(consignar)*	*(consignar)*
	Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP,	*(consignar)*	*(consignar)*
	SMB, SMTP e POP3.	*(consignar)*	*(consignar)*
	Los eventos deben identificar el país de donde partió la amenaza.	*(consignar)*	*(consignar)*
	Debe incluir seguridad contra virus en contenido HTML y javascript, software espía (spyware) y worms.	*(consignar)*	*(consignar)*
	Seguridad contra descargas involuntarias usando HTTP de archivos ejecutables Maliciosos.	*(consignar)*	*(consignar)*
	Rastreo de virus en PDFs.	*(consignar)*	*(consignar)*
	Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.).	*(consignar)*	*(consignar)*
	La actualización de firmas de ataques deberá ser diaria, semanal y de emergencia.	*(consignar)*	*(consignar)*
	El módulo de protección contra amenazas de virus, malware y spyware (módulo de IPS) deberá tener un rendimiento de al menos 750 Mbps de throughput.	*(consignar)*	*(consignar)*

	Incluya los siguientes mecanismos de IPS basados en: Análisis de patrones de estado Análisis de decodificación de protocolo Análisis para detección de anomalías de protocolo Análisis heurístico o comportamiento (de aplicaciones) IP desfragmentación (Fragmentación de IP) Re ensamblado de paquetes de tcp Permita el diseño de firmas de vulnerabilidades Identificación de botnet por comportamiento Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, scan.	*(consignar)*	*(consignar)*
	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.	*(consignar)*	*(consignar)*
	Exenciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma a firma.	*(consignar)*	*(consignar)*
Emulación de Archivos	La solución debe ofrecer una capa de protección contra amenazas desconocidas mediante emulación de archivos (sandboxing).	*(consignar)*	*(consignar)*
	Debe ofrecer el servicio de emulación basado en la nube para la solución ofertada.	*(consignar)*	*(consignar)*
	Debe prevenir archivos maliciosos antes de que lleguen a la red interna.	*(consignar)*	*(consignar)*
	Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7.	*(consignar)*	*(consignar)*
	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	*(consignar)*	*(consignar)*
	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/o 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).	*(consignar)*	*(consignar)*
	El sistema automático de análisis debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware.	*(consignar)*	*(consignar)*
	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.	*(consignar)*	*(consignar)*
	Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración.	*(consignar)*	*(consignar)*
	Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), binarios de Mac OS, flash y archivos java en el ambiente controlado.	*(consignar)*	*(consignar)*
	Permitir el envió de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.	*(consignar)*	*(consignar)*
	Debe proteger de ataques dirigidos a sistemas operativos Windows en múltiples versiones.	*(consignar)*	*(consignar)*
	Debe identificar malware desconocido escondido en documentos de office (Microsoft Office), archivos Adobe PDF, archivos ejecutables y archivos compresos.	*(consignar)*	*(consignar)*
	Debe soportar emular archivos que están siendo transferidos en una comunicación cifrada SSL o TLS.	*(consignar)*	*(consignar)*
	Emulación al monitorear: actividad y comportamiento del sistema de archivos, sistema de registro, procesos y actividad de red que provoca el archivo inspeccionado en múltiples sistemas operativos y versiones de office.	*(consignar)*	*(consignar)*

Debe generar reportes detallados de la emulación que incluya: detalles de los cambios realizados por el archivo malicioso, mostrado por diferentes sistemas operativos. O que incluya:detalles de la actividad anormal y tomas de pantalla reales del resultado de la emulación del archivo.	*(consignar)*	*(consignar)*
La solución de emulación debe soportar: emulación a nivel de sistema operativo (OS-Level Sandboxing)	*(consignar)*	*(consignar)*
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.	*(consignar)*	*(consignar)*
Para verificar que la red de la entidad se encuentre libre de malware antes de la instalación del firewall se deberá realizar un análisis de amenazas de malware en la red, a partir del cual se deben inspeccionar todo el tráfico entrante y saliente con el fin de encontrar todo tipo de amenaza cibernética que quiera ingresar a la red o detectar él envió de información que las maquinas ya infectadas estén realizando hacia el atacante. Esta tarea se realizará en modo de monitoreo, por lo cual no se deberá de bloquear el tráfico entrante o saliente, pero deberá tener la capacidad de ponerse in-line ante necesidad de la Entidad, generando un bloqueo en modo automático y tiempo real Análisis en base a tráfico no menos a 250 Mbps y despliegue en modalidad SPAN/TAP o INLINE El análisis se debe realizar en el appliance que realiza el análisis de malware y no debe ser realizado a través de enviar la información para análisis externa (a la nube) para inspección. Deberá emular sistemas operativos Windows y Mac. Las máquinas virtuales del equipo que realiza el análisis de malware deberán ser propietarias, y no de entorno público o comercial. Debe actuar en tiempo real (en el instante en que la amenaza intenta afectar a la red interna). De modo que informe por consola y por correo electrónico acerca de la presencia del malware moderno y/o avanzado en la red interna, a nivel de usuario por IP y por hostname. Indicar si hubiera malware descocido, debiendo proporcionar la siguiente Información: MD5, Tipo de archivo, protocolo usado, cantidad de ocurrencias, ejecutable del malware. El servicio a través del appliance instalado, debe ser capaz de ejecutar el código sospechoso, URL's y diversos tipos de archivos en un entorno virtual de inspección dentro del mismo dispositivo. Para ello realizara tanto análisis estático como dinámico en el sistema Para realizar las funciones indicadas preferentemente no debe requerir conectarse a otro dispositivo en la red que tenga como función proporcionar firmas de malware o depender de una tecnología (herramientas de seguridad)) para poder operar. El servicio deberá incluir un sistema que utilice técnicas avanzadas de sandboxing (virtualización del entorno infectado) y remisión de reportes y resultados en formato de presentación forense dentro del mismo appliance. La herramienta a utilizar deberá tener la capacidad de revisar todo el tráfico de datos con lo que actualmente cuenta la entidad, con capacidad superior a 1000 usuarios concurrentes en navegación web. Debe soportar la ejecución e inspección de los siguientes tipos de archivos: 3gp, asf, avi, bat, chm, cmd, com, csv, dll, doc, docx, exe, flv, gif, hop, hml, htm, hwp, ico, jar, jpg, js, lnk, midi, mov, mp3, mp4, mpg, pdf, png, ppsx, ppt, pptx, qt, rm, rmi, rtf, swf, tiff, url, vbs, vcf, vcs, wav, wma, wsf, xls, xlsx, xml. Debe tener la capacidad de emular entornos x.86 y x.64 localmente.	*(consignar)*	*(consignar)*

	El análisis de amenazas de malware en la red deberá tener una duración de 15 días calendario.		
	Para verificar que la red de la entidad se encuentre libre de vulnerabilidades antes de la instalación del firewall se deberá realizar un escáner de análisis de vulnerabilidades. Esta consiste en efectuar una búsqueda basada en un software que puede escanear vulnerabilidades que funcionan sobre distintas plataformas informáticas o diversos Sistemas Operativos (Windows - Linux - Mac - Solaris, etc...), y que permitirá encontrar errores de configuraciones, ya sean por falta de actualización del S.O, puertos que pueden llevar a sesiones, procesos Web o fallos en softwares instalados (Apache, Mysql, etc) además, brindando reportes personalizados que permitan a la entidad definir medidas para salvaguardar la información interna. Esto será desarrollado para 15 direcciones Ips internas. Debe permitir realizar escaneos sin agentes, para una fácil instalación y mantenimiento. El software deberá realizar las siguientes tareas como mínimo: Debe permitir crear fácilmente políticas usando una variedad de asistentes. Debe permitir programar análisis, para ejecutarse una vez o de forma recurrente. Debe permitir clasificar los riesgos en 5 niveles de gravedad: Crítica, Alta, Media, Baja e Informativo. Debe permitir realizar informes flexibles, que puedan ser personalizados para ser ordenados por tipos vulnerabilidad o host, crear un resumen ejecutivo o comparar los resultados del análisis para destacar los cambios. Debe permitir generar reportes en formatos: XML, PDF, CSV, HTML. Debe permitir notificaciones vía email de los resultados, remediación y las recomendaciones y mejoras del escaneo de vulnerabilidades. Debe permitir escaneos de vulnerabilidades de redes IPV4, IPV6 e hibridas. Debe permitir realizar la detección de configuraciones erróneas en el sistema y parches faltantes. Debe permitir detectar virus, malware, backdoors, hosts que se comunican con los sistemas infectados por botnets, procesos conocidos / desconocidos, servicios web con enlaces a contenidos maliciosos. Debe cumplir con los requisitos del PCI DSS, a través de una auditoría de configuración y escaneo de aplicaciones web. El sistema permitirá realizar escaneos de vulnerabilidades que cubran las siguientes normativas: FFIEC, FISMA, CyberScope Reporting Protocol, GLBA, HIPAA/HITECH, NERC, PCI, SCAP, SOX, que permitan al IRTP realizar mejora continua de la seguridad interna.	*(consignar)*	*(consignar)*

	La auditoría de las configuraciones considerará las buenas prácticas y procesos de TI definidos por: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, IBM iSeries, ISO, NIST, NSA.		
Identificación de Usuarios	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está usando qué aplicaciones, a través de la integración con servicios de directorio. Autenticación vía ldap, directorio activo y base de datos local.	*(consignar)*	*(consignar)*
	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.	*(consignar)*	*(consignar)*
	Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo. Así como también deberá incluir la capacidad de creación de políticas basadas en el control por usuario, grupos de usuarios o dirección ip.	*(consignar)*	*(consignar)*
	Deberá incluir la capacidad de creación de políticas basadas en "traffic shaping" por aplicación, usuario, fuente, destino, túnel vpn-ipsec-ssl.	*(consignar)*	*(consignar)*
	Deberá permitir el control, sin instalación de cliente de software, en equipos que soliciten salida a internet para que antes de iniciar la navegación, se despliegue un portal de autenticación residente en el firewall (captive portal) con soporte a autenticación por client certifícate.	*(consignar)*	*(consignar)*
Filtro de Datos	Permite la creación de filtros para archivos y datos predefinidos;	*(consignar)*	*(consignar)*
	Los archivos deben ser identificados por extensión y firmas;	*(consignar)*	*(consignar)*
	Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc.) identificados sobre aplicaciones (P2P, Instant Messaging, SMB, entre otros.	*(consignar)*	*(consignar)*
	Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;	*(consignar)*	*(consignar)*
	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, más no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular;	*(consignar)*	*(consignar)*
Filtro URL	La plataforma de seguridad de debe poseer las siguientes funcionalidades de filtro de URL.	*(consignar)*	*(consignar)*
	Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora).	*(consignar)*	*(consignar)*
	Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad.	*(consignar)*	*(consignar)*
	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 via LDAP, Active Directory y base de datos local.	*(consignar)*	*(consignar)*
	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.	*(consignar)*	*(consignar)*
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.	*(consignar)*	*(consignar)*
	Debe soportar una cacheé local de URL en el appliance, evitando el delay de comunicación/validación de las URLs.	*(consignar)*	*(consignar)*
	Debe poseer al menos 60 categorías de URLs.	*(consignar)*	*(consignar)*
	Debe soportar la creación de categorías URL custom.	*(consignar)*	*(consignar)*
	Debe soportar la exclusión de URLs del bloqueo por categoría.	*(consignar)*	*(consignar)*
	Debe permitir la customización de la página de bloqueo.	*(consignar)*	*(consignar)*
	Debe permitir o bloquear y continuar (habilitando que el usuario accede a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de "continuar" para permitirle seguir a ese site).	*(consignar)*	*(consignar)*
	Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios.	*(consignar)*	*(consignar)*

Geo-localización	Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea bloqueado.	*(consignar)*	*(consignar)*
	Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.	*(consignar)*	*(consignar)*
	Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.	*(consignar)*	*(consignar)*
VPN	Soportar VPN Site-to-Site y Cliente-To-Site.	*(consignar)*	*(consignar)*
	Soportar IPSec VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo.	*(consignar)*	*(consignar)*
	Soportar SSL VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo	*(consignar)*	*(consignar)*
	Soportar VPN Site-to-Site y Cliente-To-Site.	*(consignar)*	*(consignar)*
	Soportar IPSec VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo.	*(consignar)*	*(consignar)*
	Soportar SSL VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo.	*(consignar)*	*(consignar)*
	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 y 256 (Advanced Encryption Standard) Autenticación vía certificado IKE PKI.	*(consignar)*	*(consignar)*
	Debe poseer interoperabilidad con los siguientes fabricantes: Cisco; Checkpoint; Juniper; Palo Alto Networks; Fortinet; Sonic Wall;	*(consignar)*	*(consignar)*
	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;	*(consignar)*	*(consignar)*
	Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente:	*(consignar)*	*(consignar)*
	La asignación de dirección IP en los clientes remotos de VPN;		
	La asignación de DNS en los clientes remotos de VPN;		
	Debe haber una opción en el cliente remoto de escoger manualmente el gatteway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles.	*(consignar)*	*(consignar)*
	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.	*(consignar)*	*(consignar)*
	Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa.	*(consignar)*	*(consignar)*
Reportes y Administración	Debe tener un módulo de reportes y administración incluido dentro del mismo equipo sin necesidad de licenciamiento adicional	*(consignar)*	*(consignar)*
	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).	*(consignar)*	*(consignar)*
	La solución de seguridad debe permitir al administrador del sistema autenticarse vía usuario/contraseña o vía certificados digitales.	*(consignar)*	*(consignar)*
	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)	*(consignar)*	*(consignar)*

	La solución debe permitir a los administradores conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o https.	*(consignar)*	*(consignar)*
	La solución de seguridad cuenta con soporte de SNMP versión 3	*(consignar)*	*(consignar)*
	La solución de seguridad permite integrar al menos 3 servidores syslog.	*(consignar)*	*(consignar)*
	Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados: Resumen gráfico de las aplicaciones utilizadas; Principales aplicaciones por utilización de ancho de banda de entrada y salida; Principales aplicaciones por tasa de transferencia en bytes; Principales hosts por número de amenazas identificadas; Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico; Debe permitir la creación de reportes personalizado.	*(consignar)*	*(consignar)*

B. Otras Consideraciones

Servicios	Descripción	Detalle de Especificaciones Propuestas	Numero de Folio de la Cotización
Servicios Complementarios	GARANTÍA COMERCIAL	*(consignar)*	*(consignar)*
	PLAZO DE ENTREGA	*(consignar)*	*(consignar)*
	PERSONAL A CONTRATAR - CALIFICACIONES Y EXPERIENCIA	*(consignar)*	*(consignar)*
	MANTENIMIENTO PREVENTIVO, SOPORTE TECNICO Y CAPACITACION	*(consignar)*	*(consignar)*

Los abajo firmantes aceptamos en su totalidad los Términos y Condiciones Generales del PNUD, y por la presente nos ofrecemos a suministrar los elementos que se enumeran a continuación, de conformidad con las especificaciones y requisitos del PNUD con arreglo a la SdC con el número de referencia PNUD/SDC-229/2018.

Toda otra información que no hayamos facilitado automáticamente implica nuestra plena aceptación de los requisitos, términos y condiciones de la Solicitud de Cotización.

[Firma y nombre del Representante Legal]
[Fecha]

Al servicio de las personas y las naciones

ANEXO 4

FORMULARIO DE PRESENTACIÓN DE COTIZACIÓN
POR PARTE DE LOS PROVEEDORES
(La presentación de este formulario se realizará únicamente en papel de carta con el membrete oficial del suministrador)

Los abajo firmantes aceptamos en su totalidad los Términos y Condiciones Generales del PNUD, y por la presente nos ofrecemos los servicios/bienes de los elementos que se enumeran a continuación, de conformidad con los términos referencia y requisitos del PNUD con arreglo a la SdC con el número de referencia PNUD/SDC-229/2018:

A. Desglose de costos (todo incluido)

No.	**DESCRIPCIÓN**	**CANT.**	**P.UNITARIO** ***(indicar moneda)***	**P.TOTAL** **(*indicar moneda)***
1	FIREWALL SEGURIDAD PERIMETRAL	2		
	Subtotal			
	IGV (18%)			
	MONTO TOTAL OFERTADO INCLUIDO IGV			

B. Desglose de Costos por Componente

No.	**DESCRIPCIÓN**	**CANT.**	**P.UNITARIO** ***(indicar moneda)***	**P.TOTAL** **(*indicar moneda)***
1	**FIREWALL SEGURIDAD PERIMETRAL**	2		
2	**MANTENIMIENTO PREVENTIVO**	2		
3	**SOPORTE TECNICO**	Según Especificaciones Técnicas		
4	**PERSONAL**	Según Especificaciones Técnicas		
5	**CAPACITACION**	Según Especificaciones Técnicas		
	Subtotal			
	IGV (18%)			
	MONTO TOTAL OFERTADO INCLUIDO IGV			

Toda otra información que no hayamos facilitado automáticamente implica nuestra plena aceptación de los requisitos, términos y condiciones de la Solicitud de Cotización.

Son: _____ (indicar en números y letras)
Firma y nombre: _____ (Representante Legal)
Fecha: _____

ANEXO 5

TÉRMINOS Y CONDICIONES GENERALES

1. ACEPTACIÓN DE LA ORDEN DE COMPRA

Esta Orden de Compra sólo podrá ser aceptada una vez que el Proveedor haya firmado y devuelto una copia como acuse de recibo, o tras la entrega oportuna de las mercancías de conformidad con los términos de esta Orden de Compra, según se especifica aquí. La aceptación de esta Orden de Compra constituirá un contrato entre las Partes en virtud del cual los derechos y obligaciones de las Partes se regirán exclusivamente por los términos y condiciones de la presente Orden de Compra, incluyendo las presentes Condiciones Generales. Ninguna cláusula adicional o incompatible que propusiere el Proveedor obligará al PNUD, salvo que dé su acuerdo por escrito un funcionario debidamente autorizado del PNUD.

2. PAGO

2.1 El PNUD deberá, en cumplimiento de las condiciones de entrega y salvo disposición en contra en la presente Orden de Compra, efectuar el pago en los 30 días siguientes a la recepción de la factura del Proveedor por los bienes y copias de los documentos de embarque especificados en la presente Orden de Compra.

2.2 El pago de la factura mencionada supra reflejará cualquier descuento indicado en las condiciones de pago de la presente Orden de Compra, siempre y cuando el pago se efectúe en el plazo estipulado en dichas condiciones.

2.3 Salvo que fuera autorizado por el PNUD, el Proveedor deberá presentar una factura en relación con la presente Orden de Compra y en dicha factura se consignará el número de identificación de la citada Orden.

2.4 Los precios indicados en esta Orden de Compra no podrán aumentarse, salvo acuerdo expreso y por escrito del PNUD.

3. EXENCION TRIBUTARIA

3.1 El Artículo 7 de la Convención sobre Privilegios e Inmunidades de las Naciones Unidas dispone, entre otras cosas, que las Naciones Unidas, incluidos sus órganos subsidiarios, quedarán exentas del pago de todo tipo de impuestos directos, salvo las tasas por servicios públicos; además, se exime a las Naciones Unidas de pagar derechos aduaneros e impuestos similares en relación con los artículos importados o exportados de uso oficial. Si alguna autoridad gubernamental se negase a reconocer la exención impositiva de las Naciones Unidas en relación con dichos impuestos, derechos o gravámenes, el Proveedor consultará de inmediato al PNUD a fin de determinar un procedimiento que resulte aceptable para ambas partes.

3.2. De igual modo, el Proveedor autoriza al PNUD a deducir de la facturación del Proveedor cualquier monto en concepto de dichos impuestos, derechos o gravámenes, salvo que el Proveedor haya consultado al PNUD antes de abonarlos y que el PNUD, en cada caso, haya autorizado específicamente al Proveedor el pago de los impuestos, derechos o gravámenes en cuestión, bajo protesto. En este caso, el Proveedor entregará al PNUD los comprobantes por escrito de que el pago de los impuestos, derechos o gravámenes se haya realizado y haya sido debidamente autorizado.

4. RIESGO DE PÉRDIDA

El riesgo de pérdida, daño o destrucción de los bienes se regirá de conformidad con Incoterms 2010, a menos que haya sido acordado lo contrario por las Partes en la parte frontal de esta Orden de Compra.

5. LICENCIAS DE EXPORTACIÓN

Con independencia del Incoterm 2010 que se utilice en esta Orden de Compra, el Proveedor obtendrá todas las licencias de exportación que requieran los bienes.

6. BUEN ESTADO DE LOS BIENES Y SU EMBALAJE

El Proveedor garantizará que los bienes, incluido su embalaje, cumplen con las especificaciones establecidas en la presente Orden de Compra y que aptos para los fines a que suelen destinarse dichos bienes y para los fines que el PNUD comunicó expresamente al Proveedor, y que están libres de defectos de materiales y fabricación. El Proveedor garantizará también que las mercancías estén envasadas o embaladas adecuadamente para proteger los bienes.

7. INSPECCIÓN

7.1 El PNUD dispondrá de un plazo razonable después de la entrega de la mercancía para inspeccionarla y rechazar y rehusar su aceptación si no cumplen con lo indicado en la presente Orden de Compra, el pago de los bienes de conformidad con la presente Orden de Compra no se considerará una aceptación de la mercancía.

7.2 La inspección anterior al embarque no exonerará al Proveedor de ninguna de sus obligaciones contractuales.

8. VIOLACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

El Proveedor garantiza que el uso o suministro por el PNUD de la mercancía vendida en virtud de la presente orden de compra no viola ninguna patente, diseño, nombre comercial o marca registrada. Además, el Proveedor, de conformidad con esta garantía, indemnizará, defenderá y mantendrá al PNUD y a las Naciones Unidas a salvo de cualquier acción o reclamo interpuesto contra el PNUD o las Naciones Unidas relativa a una supuesta infracción de patente, diseño, nombre comercial o marca en relación con los productos vendidos bajo esta Orden de Compra.

9. DERECHOS DEL PNUD

En caso de incumplimiento por parte del proveedor de sus obligaciones en virtud de los términos y condiciones de esta Orden de Compra, incluyendo pero no limitado a la imposibilidad de obtener las licencias de exportación necesarias o de hacer entrega de todo o parte de los bienes en la fecha o fechas de entrega acordada, el PNUD podrá, después de dar al Proveedor un aviso razonable para que cumpla su obligación y sin perjuicio de cualesquiera otros derechos o recursos, ejercer uno o más de los siguientes derechos:

9.1 Adquirir la totalidad o parte de los productos de otros proveedores, en cuyo caso el PNUD podrá exigir al proveedor la responsabilidad por cualquier aumento de los costos en que hubiese incurrido.

9.2 Negarse a aceptar la entrega de todos o parte de los bienes.

9.3 Rescindir la presente Orden de Compra sin responsabilidad alguna por los gastos de rescisión u otra responsabilidad de cualquier tipo del PNUD.

10. RETRASO EN LA ENTREGA

Sin perjuicio de cualesquiera otros derechos u obligaciones de las partes que constan en el presente, si el Proveedor no pudiera entregar los bienes en la(s) fecha(s) de entrega(s) prevista(s) en esta Orden de Compra, el Proveedor, (i) consultará inmediatamente al PNUD para establecer los medios más rápidos para suministrar la mercancía, y (ii) utilizará un medio rápido de entrega, a su costa (a menos que el retraso se deba a un caso de fuerza mayor), si así lo solicita razonablemente el PNUD.

11. CESION Y QUIEBRA

11.1 El Proveedor no podrá, excepto después de haber obtenido el consentimiento por escrito del PNUD, ceder, transferir, dar en prenda o disponer de otro modo de la presente Orden de Compra, o parte de ella, o cualquiera de los derechos u obligaciones del Proveedor en virtud de la presente Orden de Compra.

11.2 Si el Proveedor cayera en insolvencia o perdiera el control de la empresa por causa de insolvencia, el PNUD podrá, sin perjuicio de cualesquiera otros derechos o recursos, rescindir inmediatamente la presente Orden de Compra emplazando al Proveedor mediante aviso escrito de terminación.

12. UTILIZACIÓN DEL NOMBRE O, EMBLEMA DEL PNUD O DE LAS NACIONES UNIDAS

El Contratista no utilizará en modo alguno el nombre, el emblema o el sello oficial del PNUD o de las Naciones Unidas con ninguna finalidad.

13. PROHIBICIÓN DE PUBLICIDAD

El Proveedor no anunciará ni hará público el hecho de que es un proveedor del PNUD, sin contar antes con la autorización específica del PNUD en cada caso.

14. TRABAJO INFANTIL

El Proveedor declara y garantiza que ni él mismo ni ninguno de sus filiales realiza prácticas que violen los derechos establecidos en la Convención sobre los Derechos del Niño, en particular el Artículo 32 de la misma que, entre otras cosas, requiere que se proteja a los menores del desempeño de trabajos peligrosos que entorpezcan su educación o sean nocivos para

su salud o para su desarrollo físico, mental, espiritual, moral o social.

Cualquier violación de esta declaración y estas garantías autorizará al PNUD a rescindir la presente Orden de Compra de inmediato, mediante la debida notificación al proveedor y sin responsabilidadalguna para el PNUD por costos de rescisión u otro tipo de responsabilidad.

15. MINAS

El Proveedor declara y garantiza que ni él mismo ni ninguna de sus filiales se encuentra activa y directamente comprometidos en actividades de patente, desarrollo, ensamblado, producción, comercialización o fabricación de minas, o en actividades conexas relacionadas con los componentes utilizados en la fabricación de minas. El término "minas" se refiere a aquellos dispositivos definidos en el Artículo 2, Párrafos 1, 4 y 5 del Protocolo II anexo a la Convención de 1980 sobre Armas Convencionales Excesivamente Nocivas o de Efectos Indiscriminados.

Cualquier violación de esta declaración o garantías autorizará al PNUD a rescindir el presente Contrato en forma inmediata, mediante la debida notificación al Proveedor, sin que esto implique responsabilidad alguna por los gastos de rescisión o cualquier otra responsabilidad para el PNUD.

16.0 RESOLUCION DE CONFLICTOS

16.1 Resolución de mutuo acuerdo: Las Partes realizarán todos los esfuerzos posibles para resolver de mutuo acuerdo cualquier conflicto, controversia o reclamo que surgiese en relación con la presente Orden de Compra o con algún incumplimiento, rescisión o invalidez relacionados con éste. En caso de que las Partes desearan buscar una solución de mutuo acuerdo mediante un proceso de conciliación, éste tendrá lugar con arreglo a las Reglas de Conciliación de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) vigentes en ese momento, o con arreglo a cualquier otro procedimiento que puedan acordar las Partes.

16.2 Arbitraje:Si el conflicto, controversia o reclamo que pudiera surgir entre las Partes en relación con esta Orden de Compra, o con su incumplimiento, rescisión o invalidez no, se resolviera de mutuo acuerdo con arreglo a lo estipulado en el Artículo 16.1 supra dentro de los sesenta (60) días a partir de la recepción por una de las Partes de la solicitud de resolución de mutuo acuerdo de la otra Parte , dicha disputa, controversia o reclamo podrá ser sometida por cualquiera de las Partes a un proceso de arbitraje según el Reglamento de Arbitraje de la CNUDMI vigente en ese momento, incluidas sus disposiciones sobre las leyes aplicables. El tribunal arbitral no tendrá autoridad para imponer sanciones punitivas. Las Partes estarán vinculadas por el fallo del tribunal arbitral resultante del citado proceso de arbitraje, a modo de resolución final de toda controversia, reclamo o disputa.

17. PRIVILEGIOS E INMUNIDADES

Nada de lo estipulado en estos Términos y Condiciones Generales o en esta Orden de Compra se considerará como renuncia a los privilegios e inmunidades de las Naciones Unidas, incluidos sus órganos subsidiarios.

18. EXPLOTACIÓN SEXUAL

18.1 El Contratista deberá tomar todas las medidas necesarias para impedir la explotación o el abuso sexual de cualquier persona por parte del Contratista, de sus empleados o de cualquier otra persona que pueda ser contratada por el Contratista para prestar cualquier servicio en virtud del presente Contrato. Para estos efectos, todo intercambio sexual con cualquier persona menor de dieciocho años, con independencia de cualesquiera leyes relativas al consentimiento, constituirá un caso de explotación y abuso sexual de dicha persona. Además, el Contratista se abstendrá, y tomará todas las medidas adecuadas para prohibirque lo hagan sus empleados u otras personas contratadas por él, intercambien dinero, bienes, servicios, ofertas de empleo u otros artículos de valor por favores o actividades sexuales, o entablar relaciones sexuales que constituyan una explotación o degradación de cualquier persona. El Contratista reconoce y acuerda que estas disposiciones del presente Contrato constituyen una condición esencial del mismo, y que cualquier incumplimiento de esta representación y garantía autorizará al PNUD a rescindir el Contrato de inmediato mediante notificación

al Contratista, sin obligación alguna relativa a gastos de rescisión o responsabilidad de ningún otro tipo.

18.2 El PNUD no aplicará la norma que antecede relativa a la edad en ningún caso en que el personal del Contratista o cualquier otra persona contratada por éste para prestar cualquier servicio en virtud del presente Contrato esté casado(a) con la persona menor de dieciocho años con quien haya mantenido dicho intercambio sexual y cuyo matrimonio sea reconocido como válido ante la ley del país de ciudadanía de las personas involucradas contratadas por el Contratista o de cualquier otra persona que pueda contratar el Contratista para realizar alguno de los servicios que incluye este Contrato.

19. LOS FUNCIONARIOS NO SE BENEFICIARÁN

El Contratista garantizará que ningún funcionario del PNUD o de las Naciones Unidas haya recibido o vaya a recibir beneficio alguno, directo o indirecto, como resultado del presente Contrato o de su adjudicación. El Contratista tendrá presente que la violación de esta disposición constituye un incumplimiento de una cláusula esencial del presente Contrato.

20. FACULTAD PARA INTRODUCIR MODIFICACIONES

Con arreglo al Reglamento Financiero y a las normas del PNUD, únicamente el Funcionario Autorizado del PNUD posee la autoridad para aceptar en nombre del PNUD cualquier modificación o cambio del presente Contrato, o renunciar a cualquiera de sus disposiciones o a cualquier relación contractual adicional de cualquier tipo con el Contratista. Del mismo modo, ninguna modificación o cambio introducidos en el presente Contrato tendrá validez y será aplicable contra el PNUD, a menos que se incluya en una enmienda al presente Contrato debidamente firmada por el Funcionario Autorizado del PNUD y por el Contratista.