INVITACIÓN A LICITAR
PNUD/IAL-133/2018

"Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma"

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.

PERÚ

PROGRAMA DE LAS NACIONES UNIDAS PARA EL DESARROLLO

abril, 2018

SECCIÓN 1. CARTA DE INVITACIÓN

Lima, 03 de abril de 2018

De nuestra consideración:

REF.: Invitación a Licitar PNUD/IAL-133/2018 – "Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma"

El Programa de las Naciones Unidas para el Desarrollo (PNUD) tiene el gusto de invitarle a presentar una Oferta a la presente Invitación a Licitación (IaL) para la provisión de los bienes de la referencia.

La presente IaL está compuesta de los siguientes documentos:

Sección 1 Esta Carta de invitación
Sección 2 Instrucciones a los Licitantes (que incluyen la Hoja de Datos)
Sección 3 Lista de Requisitos y Especificaciones Técnicas
Sección 4 Formulario de Presentación de la Oferta
Sección 5 Documentos que avalan la elegibilidad y las calificaciones del Licitante
Sección 6 Formulario de Oferta Técnica
Sección 7 Formulario de Oferta Financiera
Sección 8 Formulario de Garantía de Oferta (No aplica)
Sección 9 Formulario de Garantía de Ejecución de Contrato
Seccion 10 Formulario de Garantía de Adelanto de Pago (No aplica)
Sección 11 Condiciones generales del PNUD aplicables a la Orden de Compra.
Sección 12 Resumen de Estados Financieros
Sección 13 Tabla de especificaciones técnicas mínimas requeridas
Sección 14 Declaración jurada de calidad de los bienes y garantía técnica
Sección 15: Declaración jurada de instalación, capacitación y mantenimiento

Su Oferta incluirá una Oferta Técnica y una Oferta Financiera, presentadas en un solo sobre y con arreglo a las indicaciones de la Sección 2, según el siguiente cronograma:

- Puesta a disposición de bases — Martes, 3 de abril de 2018
- Recepción de consultas — Lunes, 9° de abril de 2018 (por vía electrónica)
- Respuestas a consultas — jueves, 12 de abril de 2018 (vía web)
- Recepción de ofertas — jueves, 19 de abril de 2018, hasta las 13:00 horas (sin tolerancia)
- Apertura pública de ofertas — jueves, 19 de abril de 2018, a las 15:00 horas

Mucho agradeceremos, remitir una carta de interés dirigida a la siguiente dirección:

Programa de las Naciones Unidas para el Desarrollo (PNUD)
Av. Augusto Pérez Araníbar 750, Magdalena del Mar
Lima – Perú
Atención: Unidad de Adquisiciones
Email: adquisiciones.pe@undp.org

La carta deberá estar en posesión del PNUD a más tardar el 14 de abril de 2018 y en la misma se debe indicar si su empresa tiene intención de presentar una Oferta. Si no es posible, el PNUD agradecerá nos indique el motivo, para nuestra información.

Si usted ha recibido esta IaL a través de una invitación directa realizada por el PNUD, la transferencia de esta invitación a otra empresa requiere de su notificación por escrito al PNUD.

Si precisa cualquier aclaración adicional, le rogamos se ponga en comunicación con la persona de contacto que se indica en la Hoja de Datos adjunta, que coordina las consultas relativas a esta IaL.

El PNUD queda a la espera recibir su Oferta y le da las gracias de antemano por su interés en las oportunidades de adquisición que ofrece el PNUD.

Atentamente,

Unidad de Adquisiciones
Programa de las Naciones Unidas para el Desarrollo

Sección 2: Instrucciones a los Licitantes

Definiciones

a) *"Oferta"* se refiere a la respuesta del Licitante a la Invitación a Licitar, e incluirá el Formulario de Presentación de la Oferta, el Formulario de Oferta Técnica, el Formulario de Oferta Financiera y toda otra documentación pertinente que se requiera en la IaL.

b) *"Licitante"* se refiere a cualquier entidad legal que pueda presentar, o que haya presentado, una Oferta para el suministro de bienes y la provisión de servicios conexos solicitados por el PNUD.

c) *"Contrato"* se refiere al acuerdo que será firmado por y entre el PNUD y el Licitante elegido, y a todos los documentos adjuntos al mismo, entre otros los Términos y Condiciones Generales (TCG) y los Apéndices.

d) "*País*" se refiere al país indicado en la Hoja de Datos;

e) *"Hoja de Datos*" se refiere a la parte de las Instrucciones dadas a los Licitantes y se utilizan para reflejar las condiciones del proceso de licitación específicas para los requisitos de la IaL.

f) *"Día*" se refiere a día civil.

g) *"Bienes"* se refiere a cualquier producto, material prima, artículo, material, objeto, equipo, activo o mercancía que requiera el PNUD por la presente IaL.

h) *"Gobierno*" se refiere al Gobierno del país que ha de recibir los bienes o donde se han de prestar los servicios con arreglo a lo que se especifique en el contrato.

i) *"Instrucciones a los Licitantes"* se refiere a la serie completa de documentos que proporcionan a los Licitantes toda la información necesaria y los procedimientos que deben seguirse en el proceso de preparación de la Oferta.

j) *"IaL"* se refiere a la Invitación a Licitar, y consiste en las instrucciones y referencias preparadas por el PNUD a los efectos de seleccionar al mejor proveedor de servicios para el cumplimiento de los requisitos que se indican en el Lista de Requisitos y las Especificaciones Técnicas.

k) *"Carta de invitación (CdI)"* (Sección 1 de la IaL) se refiere a la Carta de Invitación que envía el PNUD a los Licitantes.

l) *"Desviación material*" se refiere a cualquier contenido o característica de la Oferta que sea significativamente diferente de un aspecto o requisito esencial de la IaL, y que: (i) altere sustancialmente el alcance y la calidad de los requisitos, (ii) limite los derechos del PNUD y/o las obligaciones del oferente, y (iii) afecte negativamente la equidad y los principios del proceso de adquisición, como por ejemplo poniendo en peligro la posición competitiva de otros oferentes.

m) *"Lista de Requisitos y Especificaciones Técnicas"* se refiere al documento incluido en la Sección 3 de esta IaL, en el que se recoge la relación de bienes solicitados por el PNUD, sus especificaciones, servicios y actividades conexos y las tareas que habrán de realizarse, junto a otras informaciones pertinentes relativas a la recepción y aceptación de los bienes por parte del PNUD.

n) *"Servicios*" se refiere a todo el conjunto de tareas relacionadas o accesorias a la finalización o la entrega de los bienes solicitados por el PNUD con arreglo a esta IaL.

o) "*Información Adicional a la IaL*" se refiere a una comunicación escrita transmitida por el PNUD a los posibles Licitantes, que incluye aclaraciones, respuestas a las consultas recibidas de los Licitantes potenciales o cambios que deban introducirse en la IaL, en cualquier momento después del lanzamiento de la IaL pero antes de la fecha límite para la presentación de las Ofertas.

A. ASPECTOS GENERALES

1. Por este medio, el PNUD solicita Ofertas en respuesta a la presente Invitación a Licitar (IaL). Los Licitantes deberán cumplir estrictamente todos los requisitos de esta IaL. No se autoriza la introducción de cambios, sustituciones u otras modificaciones a las normas y disposiciones estipuladas en esta IaL, a menos que lo ordene o apruebe por escrito el PNUD en forma de Información Adicional a la IaL.

2. La presentación de una Oferta se considerará como un reconocimiento por parte del Licitante de su obligación de aceptar todas las obligaciones estipuladas en esta IaL y, a menos que se especifique lo contrario, de que el Licitante ha leído, entendido y aceptado todas las instrucciones de esta Licitación.

3. Toda Oferta presentada será considerada como una Oferta del Licitante y no constituye ni implica la aceptación de la misma por el PNUD. El PNUD no tiene ninguna obligación de adjudicar un contrato a ningún Licitante, como resultado de esta IaL.

4. El PNUD mantiene una política de tolerancia cero ante las prácticas prohibidas, entre otras el fraude, la corrupción, la colusión, las prácticas contrarias a la ética y la obstrucción. El PNUD está decidido a prevenir, identificar y abordar todas las actividades y prácticas de fraude y corrupción contra el PNUD o contra terceros que participen en las actividades del PNUD. (Para una descripción completa de las políticas, véase http://www.undp.org/content/dam/undp/library/corporate/Transparency/UNDP_Anti-fraud_Policy-Spanish_FINAL.pdf y http://www.undp.org/content/undp/en/home/operations/procurement/protestandsanctions/

5. En sus respuestas a esta IaL, el PNUD insta a todos los Licitantes a comportarse de manera profesional, objetiva e imparcial, y a tener en todo momento presente en primer lugar los intereses primordiales del PNUD. Los Licitantes deberán evitar estrictamente los conflictos con otros trabajos asignados o con intereses propios, y actuar sin tener en cuenta trabajos futuros. Todo Licitante de quien se demuestre que tiene un conflicto de intereses será descalificado. Sin limitación de la generalidad de todo lo antes citado, se considerará que los Licitantes, y cualquiera de sus afiliados, tienen un conflicto de intereses con una o más partes en este proceso de licitación, si:

5.1 están o han estado asociados en el pasado, con una firma o cualquiera de sus filiales, que haya sido contratada por el PNUD para prestar servicios en la preparación del diseño, la lista de requisitos y las especificaciones técnicas, los análisis y estimaciones de costos, y otros documentos que se utilizarán en la adquisición de los bienes y servicios relacionados con este proceso de selección;
5.2 han participado en la preparación y/o el diseño del programa o proyecto relacionado con los bienes y servicios conexos solicitados en esta Licitación, o
5.3 se encuentran en conflicto por cualquier otra razón que pueda determinar el PNUD, a su discreción.

En caso de dudas de interpretación de lo que es, potencialmente, un conflicto de intereses, el Licitante deberá dar a conocer su situación al PNUD y pedir la confirmación de éste sobre si existe o no tal conflicto.

6. Del mismo modo, en su Oferta, los Licitantes deberán informar de lo siguiente:

6.1 Cuando los propietarios, copropietarios, oficiales, directores, accionistas mayoritarios o personal clave

sean familiares de personal del PNUD participante en las funciones de adquisición y/o el Gobierno del país, o cualquier asociado en la ejecución de recepción de los bienes y servicios conexos establecidos en esta IaL; y

6.2 Toda otra circunstancia que pudiera dar lugar a un conflicto de intereses, real o percibido como tal; colusión o prácticas de competencia improcedentes.

El ocultamiento de dicha información puede dar como resultado el rechazo de la Oferta.

7. La elegibilidad de los Licitantes que sean, total o parcialmente, propiedad del Gobierno estará sujeta a una posterior evaluación del PNUD y a la revisión de diversos factores, como por ejemplo que estén registrados como entidad independiente, alcance de la titularidad o participación estatal, percepción de subvenciones, mandato, acceso a información relacionada con esta IaL, y otros que pudieran permitirles gozar de una ventaja indebida frente a otros Licitantes, y al eventual rechazo de la Oferta.

8. Todos los Licitantes deberán respetar el Código de Conducta de Proveedores del PNUD, que se puede encontrar en este enlace: http://www.un.org/depts/ptd/pdf/conduct_english.pdf.

B. CONTENIDO DE LA OFERTA

9. Secciones de la IaL

Los Licitantes deberán completar, firmar y presentar los siguientes documentos:

9.1 Carta de acompañamiento al Formulario de Presentación de la Oferta (véase IaL, Sección 4);
9.2 Documentos que avalan la elegibilidad y calificaciones del Licitante (véase IaL, Sección 5);
9.3 Oferta Técnica (véase el formulario indicado en la IaL, Sección 6);
9.4 Oferta Financiera (véase el formulario indicado en la IaL Sección 7);
9.5 Garantía de Licitación, si procede (véase al respecto la HdD, nº 9 a 11; también, formulario prescrito en la Sección 8 de la IaL);
9.6 Anexos o apéndices a la Oferta (incluidos los que se especifican en la Hoja de Datos)

10. Aclaraciones a la licitación

10.1 Los Licitantes podrán solicitar aclaraciones sobre cualquiera de los documentos relativos a esta IaL a más tardar en el número de días indicados en la Hoja de Datos (HdD, nº 16) antes de la fecha de presentación de Ofertas. Toda solicitud de aclaración deberá ser enviada por escrito, por servicio de mensajería o por medios electrónicos a la dirección del PNUD que se indica en la Hoja de Datos (HdD, nº 17). El PNUD responderá por escrito y por medios electrónicos, y remitirá copias de la respuesta (incluyendo una explicación de la consulta pero sin identificar el origen de la misma) a todos los Licitantes que hayan confirmado su intención de presentar una Oferta.

10.2 El PNUD se compromete a dar respuesta a estas demandas de aclaración con rapidez, pero cualquier demora en la respuesta no implicará ninguna obligación por parte del PNUD de ampliar el plazo de presentación de Ofertas, a menos que el PNUD considere que dicha prórroga está justificada y es necesaria.

11. Modificación de la licitación

11.1 En cualquier momento antes de la fecha límite para la presentación de la Oferta, el PNUD podrá, por cualquier motivo –por ejemplo en respuesta a una aclaración solicitada por un Licitante– modificar la IaL, por medio de una Información Adicional a la IaL. Se informará por escrito a todos los posibles

Licitantes de todos los cambios o modificaciones y de las instrucciones adicionales a través de dicha Información Adicional a la IaL, por los medios que se especifican en la Hoja de Datos (HdD, nº 18).

11.2 Con el fin de proporcionar al potencial Licitante un plazo razonable para estudiar las enmiendas en la preparación de su Oferta, el PNUD podrá, de manera discrecional, prorrogar el plazo para la presentación de la Oferta, cuando la naturaleza de la enmienda a la IaL justifique dicha ampliación.

C. PREPARACIÓN DE LA OFERTA

12. Costos

El Licitante correrá con todos y cada uno de los costos relacionados con la preparación y/o presentación de la Oferta, independientemente de si ésta resulta seleccionada o no. El PNUD en ningún caso será responsable de dichos costos, independientemente de la modalidad o los efectos del proceso de contratación.

13. Idiomas

La Oferta, así como toda la correspondencia intercambiada entre el Licitante y el PNUD, se redactará en el o los idiomas que se especifiquen en la Hoja de Datos (HdD, nº 4). Todo material impreso proporcionado por el Licitante escrito en un idioma distinto del o de los que se indiquen en la Hoja de Datos, deberá ir acompañada de una traducción al idioma de preferencia indicado en la Hoja de Datos. A los efectos de interpretación de la Oferta, y en caso de discrepancia o incongruencia en el significado, la versión traducida al idioma de preferencia tendrá prioridad. Al concluir un contrato, el idioma del contrato regirá la relación entre el contratista y el PNUD.

14. Formulario de presentación de la Oferta

El Licitante deberá presentar su Oferta utilizando para ello el Formulario de Presentación de la Oferta que se adjunta en la Sección 4 de la presente IaL.

15. Formato y contenido de la Oferta técnica

A menos que se indique lo contrario en la Hoja de Datos (HdD, nº 28), el Licitante deberá estructurar la Oferta Técnica de la siguiente manera:

15.1 Experiencia de la Empresa u Organización: Esta sección proporcionará información detallada sobre la estructura de gestión de la empresa u organización; su capacidad y sus recursos organizativos y la experiencia de la empresa u organización; la lista de proyectos y contratos (tanto finalizados como en curso, tanto nacionales como internacionales) relacionados o de naturaleza similar a los requisitos de la IaL; la capacidad de producción de las instalaciones, cuando el Licitante sea también el fabricante; la autorización del fabricante de los bienes, cuando el Licitante no sea el fabricante, y la prueba de estabilidad financiera y suficiencia de recursos para completar los servicios requeridos por la IaL (véase la cláusula nº 18 de la IaL y la nº 26 de la HdD para más detalles). Otro tanto se aplicará a cualquier otra entidad participante en la IaL como empresa mixta o consorcio.

15.2 Especificaciones Técnicas y Plan de Implementación: En esta sección se deberá demostrar la respuesta del Licitante a la Lista de Requisitos y Especificaciones Técnicas, mediante la identificación de los componentes específicos propuestos, de cómo se abordarán los requisitos especificados, punto por punto; la inclusión de una descripción y especificación detallada de los bienes que se solicitan, y los planos y esquemas cuando proceda; las características esenciales de funcionamiento, con identificación de los trabajos o partes de ellos que se subcontraten; una relación de los principales subcontratistas y una explicación de cómo la Oferta cumple o supera las especificaciones al tiempo que garantiza la idoneidad de la aproximación a las condiciones locales y al resto del entorno operativo del proyecto durante toda la vida operativa de los bienes. Los detalles de la Oferta Técnica deberán ir acompañados y apoyados por un Calendario de Implementación, que especifique los plazos de transporte y entrega,

cuando proceda, en el marco de la duración del contrato según lo especificado en la Hoja de Datos (HdD, nº 29 y nº 30).

Los Licitantes deberán ser plenamente conscientes de que los bienes y servicios conexos que el PNUD solicita podrán ser transferidos, de inmediato o más adelante, por el PNUD a socios del Gobierno o a una entidad designada por éste, con arreglo a las políticas y los procedimientos del PNUD. Todos los Licitantes, por lo tanto deben presentar en sus Ofertas lo siguiente:

a) Una declaración que indique si es necesario algún tipo de licencia de importación o exportación en relación con los bienes adquiridos o servicios que han de ser prestados, incluyendo cualquier tipo de restricción en el país de origen, la naturaleza de uso o doble uso de los bienes o servicios y cualquier disposición relativa a los usuarios finales;
b) La confirmación de que el Licitante ha obtenido licencias de esta naturaleza en el pasado y tiene expectativas razonables de obtener todas las licencias necesarias, en caso de que su Oferta se considere la más adecuada, y
c) La documentación, información y declaración completas de las mercancías clasificadas, o que puedan serlo, como "mercancías peligrosas".

15.3 Estructura administrativa y personal clave: Esta sección debe incluir el currículo completo del personal clave asignado para apoyar la implementación de la Oferta Técnica, con una definición clara de sus funciones y responsabilidades. Los currículos deberán establecer su competencia y demostrar sus cualificaciones en los ámbitos relacionados con los requisitos de esta IaL.

En el cumplimiento de esta Sección, el Licitante asegurará y confirmará al PNUD que el personal nombrado estará disponible para cumplir con las exigencias del Contrato durante todo el período indicado. En caso de que alguna de las personas clave no esté disponible más adelante, salvo si ello es debido a motivos inevitables como fallecimiento o incapacidad médica, entre otros, el PNUD se reserva el derecho de declarar la Oferta inaceptable. Cualquier sustitución deliberada debida a razones de fuerza mayor, incluyendo el retraso en la implementación del proyecto de programa por causas ajenas a la Oferta, deberá hacerse sólo una vez que el PNUD haya aceptado la justificación de la sustitución y haya aprobado las calificaciones de la persona reemplazante, que deberá poseer unas credenciales iguales o superiores a las de la persona sustituida.

15.4 Cuando la Hoja de Datos requiera la presentación de una Garantía de Licitación, ésta se adjuntará a la Oferta Técnica. El PNUD podrá hacer efectiva la Garantía de Licitación y rechazar la Oferta cuando se den una o varias de las siguientes condiciones:

a) si el Licitante retira su Oferta durante el período de validez de la Oferta especificado en la Hoja de Datos (HdD, nº 11); o
b) si el importe de la Garantía de Licitación resulta ser inferior a lo requerido por el PNUD, tal como se indica en la Hoja de Datos (HdD, nº 9); o
c) en el caso de que el Licitante seleccionado no consiga:

   i. firmar el contrato después de la adjudicación por el PNUD;
   ii. cumplir con la variación de requisitos del PNUD, de acuerdo con la Cláusula 35 de la IaL; o
   iii. proporcionar la garantía de ejecución, los seguros u otros documentos que el PNUD pudiera exigir como condición para la prestación efectiva del contrato que pudiera ser adjudicado al Licitante.

16. Oferta financiera

La Oferta Financiera se preparará utilizando el formulario normalizado que se adjunta (Sección 7). Incluirá una relación de todos costos de los principales componentes vinculados a los bienes y servicios conexos, y el desglose detallado de dichos costos. Todos los bienes y servicios descritos en la Oferta Técnica deberán tener un precio

individual, en una correspondencia uno a uno. Todos los productos y las actividades descritas en la Oferta Técnica cuya cotización no figure en la Oferta Financiera se considerarán que se incluyen en los precios de otras actividades o productos, así como en el precio final total de la Oferta.

17. Monedas

Todos los precios serán cotizados en la moneda indicada en la Hoja de Datos (HdD, nº 15). Sin embargo, cuando las Ofertas se coticen en diferentes divisas, a efectos de comparación de todas las Ofertas:

17.1 el PNUD convertirá la moneda en que se cotice la Oferta en la moneda preferida del PNUD, de acuerdo con la tasa actual de cambio operacional de las Naciones Unidas en el último día de presentación de la Oferta, y

17.2 en caso de que la Oferta que resulte ser más aceptable según la IaL se cotice en otra moneda diferente de la moneda preferida como Hoja de Datos por (HdD, nº 15), el PNUD se reserva el derecho de adjudicar el contrato en la moneda de preferencia del PNUD, utilizando el método de conversión que se especifica más arriba.

18. Documentos que avalan la elegibilidad y las calificaciones del Licitante

18.1 El Licitante deberá proporcionar pruebas documentales de su condición de proveedor elegible y calificado, utilizando para ello los formularios previstos en la Sección 5, Documentos que avalan la elegibilidad y calificaciones del Licitante. A fin de adjudicar un contrato a un Licitante, sus calificaciones deberán estar documentadas de modo satisfactorio ante el PNUD. Dichas calificaciones incluirán, entre otros, lo siguiente:

a) que, en caso de que un Licitante, con arreglo al Contrato, ofrezca suministrar bienes que el Licitante no haya fabricado ni producido él mismo, el Licitante habrá sido debidamente autorizado por el fabricante o productor de la mercancía a suministrar los bienes al país de destino final;
b) que el Licitante posee la capacidad financiera, técnica y productiva necesarias para ejecutar el contrato, y
c) que, hasta donde el Licitante conozca, no está incluido en la Lista Consolidada 1267/1989 del Consejo de Seguridad de las Naciones Unidas, o en la lista de la División de Adquisiciones de las Naciones Unidas o en cualquier otra lista inelegible de proveedores del PNUD.

18.2 Las Ofertas presentadas por dos (2) o más Licitantes serán rechazadas por el PNUD si se comprueba que coinciden con alguna de las siguientes situaciones:

a) que tengan al menos un socio de control, director o accionista en común, o
b) que cualquiera de ellos reciba o haya recibido alguna subvención directa o indirecta de los demás,
c) que tengan el mismo representante legal a efectos de esta Licitación, o
d) que tengan una relación entre sí, directa o a través de terceros comunes, que les coloque en una posición de acceso a información relativa a la Oferta de otro Licitante o de influencia sobre dicha Oferta de otro Licitante, en el marco de este mismo proceso de IaL;
e) que sean subcontratistas entre sí, uno de la Oferta del otro y viceversa, o que un subcontratista de una Oferta también presente otra Oferta a su nombre como Licitante principal; o
f) que un experto que haya sido propuesto en la Oferta de un Licitante participe en más de una Oferta recibida en este proceso de IaL. Esta condición no se aplica a los subcontratistas que estén incluidos en más de una Oferta.

19. J*oint ventures*, consorcios, asociaciones

Si el Licitante es un grupo de personas jurídicas que vayan a formar o que hayan formado una Joint Venture, un

consorcio o una asociación, en el momento de la presentación de la Oferta, deberán confirmar en su Oferta que: (i) han designado a una de las partes a actuar como entidad líder, debidamente investida de autoridad para obligar legalmente a los miembros de la joint venture, consorcio o asociación, conjunta y solidariamente, lo que será debidamente demostrado mediante un acuerdo debidamente firmado ante notario entre dichas personas jurídicas, acuerdo que deberá presentarse junto con la Oferta, y (ii) si se le adjudica el contrato, el contrato podrá celebrarse por y entre el PNUD y la entidad líder designada, quien actuará en nombre y representación de todas las entidades asociadas que componen la empresa mixta.

Una vez que la Oferta haya sido presentada al PNUD, la entidad líder designada para representar a la joint venture, consorcio o asociación no podrá cambiar sin el consentimiento escrito previo del PNUD. Además, ni la entidad líder, ni las entidades asociadas de la joint venture, consorcio o asociación, podrán:

a) presentar una nueva Oferta, ni en representación propia ni
b) como entidad líder o entidad asociada de otra empresa mixta que presente otra Oferta.

La descripción de la organización de la empresa, el consorcio, la asociación deberá definir con claridad la función que se espera de cada una de las entidades de la empresa mixta en el cumplimiento de los requisitos de la IaL, tanto en la Oferta como en el Acuerdo de empresa mixta. Todas las entidades que forman la empresa mixta estarán sujetas a la evaluación de elegibilidad y calificación por parte del PNUD.

Cuando una empresa mixta presente su trayectoria y experiencia en compromisos similares a los que exige la IaL, deberá presentar la información de la siguiente manera:

a) los compromisos que hayan sido asumidos conjuntamente por la joint venture, consorcio asociación , y
b) los que hayan sido asumidos por las entidades individuales asociadas de la joint venture, consorcio asociación E que se supone que vayan a participar en la prestación de los servicios definidos en la IaL.

Los contratos anteriores suscritos por expertos individuales independientes que estén o hayan estado asociados de forma permanente con cualquiera de las empresas asociadas no podrán ser presentados como experiencia de la joint venture, consorcio o asociación o de sus asociadas, y únicamente podrán reivindicarlos los expertos individuales mismos en la presentación de sus credenciales individuales.

Si la Oferta de una joint venture, consorcio asociación es considerada por el PNUD como la más aceptable y la que ofrece la mejor relación calidad-precio, el PNUD adjudicará el contrato a esta la joint venture, consorcio o asociación, a nombre de su entidad líder designada, quien deberá firmar el contrato para todas las entidades asociadas y en nombre de éstas.

20. Ofertas alternativas

A menos que se especifique lo contrario en la Hoja de Datos (HdD, nº 5 y nº 6), no se tomarán en consideración las Ofertas alternativas. Cuando las condiciones de admisión se cumplan, o cuando las justificaciones se hayan establecido con claridad, el PNUD se reserva el derecho de adjudicar un contrato sobre la base de una Oferta alternativa.

21. Periodo de validez

21.1 La Oferta seguirá siendo válida durante el período que se especifique en la Hoja de Datos (HdD, nº 8), a partir de la fecha límite de presentación que también se indica en la Hoja de Datos (HdD, nº 21). Toda Oferta válida por un período más corto será inmediatamente rechazada por el PNUD y será automáticamente considerada no aceptable.

21.2 En circunstancias excepcionales, antes de la expiración del período de validez de la Oferta, el PNUD podrá

solicitar a los Licitantes la ampliación del periodo de validez de sus Ofertas. La solicitud y las respuestas se harán por escrito y se considerará que forman parte integrante de la Oferta.

22. Conferencia de Licitantes

Cuando sea conveniente, se llevará a cabo una conferencia de Licitantes en fecha, hora y lugar especificados en la Hoja de Datos (HdD, nº 7). Todos los Licitantes están invitados a asistir. La inasistencia, sin embargo, no dará lugar a la descalificación de un Licitante interesado. Las actas de la conferencia de Licitantes podrán ser expuestas en el sitio web del PNUD o difundidas a las empresas individuales que se hayan registrado o que hayan manifestado su interés en el contrato, hayan o no asistido a la conferencia. Ninguna declaración verbal hecha durante la conferencia podrá modificar los términos y condiciones de la IaL, a menos que dicha declaración sea específicamente inscrita en las actas de la conferencia o se emita/publique como modificación en forma de Información Complementaria a la IaL.

D. PRESENTACIÓN Y APERTURA DE LAS OFERTAS

23. Presentación

23.1 La Oferta Financiera y la Oferta Técnica deberán presentarse conjuntamente y bajo sello en un mismo y único sobre, y entregadas ya sea personalmente, por servicio de mensajería o por un medio electrónico de transmisión. Si la presentación no se realiza por medios electrónicos, la Oferta Técnica y la Oferta Financiera deberán ir juntas y bajo sello en un sobre cuya parte externa deberá:

a) llevar el nombre del Licitante;
b) estar dirigida al PNUD tal como se especifica en la Hoja de Datos (HdD, nº 20);
c) llevar una advertencia de no abrirlo antes de la hora y la fecha de apertura de la Oferta que se especifica en la Hoja de Datos (HdD, nº 24)

Si el sobre no está cerrado ni etiquetado de forma adecuada, el Licitante deberá asumir la responsabilidad por el extravío o la apertura prematura de la Oferta debidos al inadecuado sellado y etiquetado por parte del Licitante.

23.2 Los Licitantes deberán presentar sus Ofertas en la forma prevista en la Hoja de Datos (HdD. nº 22 y nº 23). Cuando se espere que la Oferta esté en tránsito más de 24 horas, el Licitante deberá asegurarse de prever un tiempo de entrega suficiente para cumplir con la fecha límite de presentación que haya establecido el PNUD. El PNUD indicará, para que quede constancia, que la fecha y hora oficiales recepción de la Oferta son la fecha y hora efectivas de la llegada física de dicha Oferta a las instalaciones del PNUD tal se indica en la Hoja de Datos (HdD, nº 20).

23.3 Los Licitantes que presenten Ofertas transmitidas por correo o entregadas personalmente deberán adjuntar el original y cada una de las copias de la Oferta en sobres cerrados y separados, debidamente identificados uno de los sobres como “Oferta original” y los otros como “Copia de la Oferta”. Los dos sobres, correspondientes al original y las copias, serán sellados y colocados en un sobre exterior. El número de copias necesarias se especificará en la Hoja de Datos (HdD, nº 19). En caso de discrepancia entre el contenido del sobre de la “Oferta original” y el de la “Copia de la Oferta”, el contenido del ejemplar marcado como original tendrá preferencia. El original de la Oferta deberá estar firmado o rubricado en cada página por el Licitante o por una persona debidamente facultada para representarlo. La autorización deberá ser comunicada mediante un documento acreditativo de la autorización, emitido por la máxima autoridad de la empresa o un poder notarial que acompañe a la Oferta.

23.4 Los Licitantes deberán tener en cuenta que el mero acto de presentación de una Oferta, en sí y por sí, implica que el Licitante acepta los Términos y Condiciones Generales de Contratación que se adjuntan en la Sección 11.

24. Plazo de presentación de la Oferta y ofertas de última hora

Las Ofertas deberán obrar en manos del PNUD en la dirección y, a más tardar, en la fecha y hora especificadas en la Hoja de Datos (HdD, nº 20 y nº 21).

El PNUD no tomará en consideración ninguna Oferta que llegue con posterioridad a la fecha y hora límites de presentación de las Ofertas. Toda Oferta recibida por el PNUD después de la fecha límite para la presentación de la Oferta será declarada tardía, y será rechazada y devuelta al Licitante sin abrir.

25. Retiro, sustitución y modificación de la Oferta

25.1 Será responsabilidad única de los Licitantes la adopción de las medidas necesarias para examinar cuidadosamente en detalle la plena coherencia de sus Ofertas con los requisitos de la IaL, teniendo en cuenta que las deficiencias materiales en el suministro de la información solicitada por el PNUD o la falta de claridad en la descripción de los bienes y servicios que se habrán de proporcionar podrían provocar el rechazo de la Oferta. El Licitante asumirá cualquier responsabilidad derivada de cualquier interpretación o conclusión errónea realizada por el Licitante en el curso de la comprensión de la IaL al margen del conjunto de información proporcionada por el PNUD.

25.2 El Licitante podrá retirar, sustituir o modificar su Oferta después de haber sido presentada, mediante el envío de una notificación por escrito, de conformidad con la Sección 23 de la IaL, debidamente firmada por un representante autorizado, y que deberá incluir una copia de la autorización (o un poder notarial) . La sustitución o modificación correspondientes de la Oferta deberán acompañar a la notificación respectiva por escrito. Todas las notificaciones deberán obrar en manos del PNUD antes de la fecha límite de presentación, y habrán sido presentadas de conformidad con la Sección 23 (salvo en lo que se refiere a las notificaciones de retiro, que no requieren copias). Los respectivos sobres deberán estar claramente rotulados con las palabras “RETIRO/RENUNCIA”, “SUSTITUCIÓN” o “MODIFICACIÓN”.

25.3 Las Ofertas cuya retirada se solicite, serán devueltas sin abrir a los Licitantes.

25.4 Ninguna Oferta podrá ser retirada, sustituida o modificada en el periodo que va de la fecha límite para la presentación de Ofertas hasta la expiración del período de validez de las Ofertas especificado por el Licitante en el Formulario de Presentación de la Oferta o cualquier prórroga del mismo.

26. Apertura de Ofertas

El PNUD abrirá las Ofertas en presencia de un comité especial establecido por el PNUD y compuesto de al menos dos (2) miembros. Si se autoriza la presentación electrónica, los procedimientos específicos de apertura de las Ofertas electrónicas serán los que se especifican en la Hoja de Datos (HdD, nº 23).

En el momento de la apertura, se darán a conocer los nombres, las modificaciones y los retiros de Licitantes; el estado de las etiquetas, los sobres y los sellos; el número de carpetas y archivos, y todo otro tipo de detalles que el PNUD estime oportuno. No se rechazará ninguna Oferta durante el procedimiento de apertura, excepto en los casos de presentación tardía, cuyas Ofertas serán devueltas sin abrir a los Licitantes.

27. Confidencialidad

La información relativa a la revisión, evaluación y comparación de las Ofertas, y la recomendación de adjudicación del contrato, no podrán ser reveladas a los Licitantes ni a ninguna otra persona que no participe oficialmente en dicho proceso, incluso después de la publicación de la adjudicación del contrato.

Cualquier intento por parte de un Licitante de influenciar al PNUD en la revisión, evaluación y comparación de las decisiones relativas a la Oferta o a la adjudicación del contrato podrá ser causa, por decisión del PNUD, del rechazo de su Oferta.

En el caso de que un Licitante no tenga éxito, podrá solicitar celebrar una reunión de información con el PNUD. El objetivo de dicha reunión es discutir los puntos fuertes y las debilidades de la presentación del Licitante, a fin de ayudar éste a mejorar las Ofertas que presente al PNUD. En estas reuniones, no se discutirá con el Licitante el contenido de otras Ofertas, ni se compararán éstas con la Oferta presentada por el Licitante.

E. EVALUACIÓN DE LA OFERTA

28. Examen preliminar de la Oferta

El PNUD examinará las Oferta para determinar si está completa con respecto a los requisitos documentales mínimos, si los documentos han sido debidamente firmados, si el Licitante figura o no en la Lista 1267/1989 del Consejo de Seguridad de la ONU como terroristas o financiadores del terrorismo, o en lista del PNUD de proveedores inelegibles o retirados, y si la Oferta está en general conforme, entre otros indicadores que puedan utilizarse en esta etapa. El PNUD podrá rechazar cualquier Oferta en esta etapa.

29. Evaluación de la Oferta

29.1 El PNUD examinará la Oferta para confirmar que todos los términos y condiciones, con arreglo a los Términos y Condiciones Generales y las Condiciones Generales del PNUD, han sido aceptadas por el Licitante sin desviaciones ni reservas.

29.2 El equipo de evaluación revisará y evaluará las Ofertas sobre la base de su capacidad de respuesta a la Lista de Requisitos y Especificaciones Técnicas y demás documentación prevista, aplicando el procedimiento indicado en la Hoja de Datos (HdD, nº 25). El PNUD no podrá en absoluto hacer cambios en los criterios una vez que todas las Ofertas hayan sido recibidas.

29.3 El PNUD se reserva el derecho a realizar un ejercicio posterior a la calificación, con el objetivo de determinar a su plena satisfacción la validez de la información proporcionada por el Licitante. Este ejercicio de calificación deberá estar plenamente documentado y, entre los que se pueden enumerar en la Hoja de Datos (HdD, nº 33), podrá incluir, entre otros, una combinación de todos o alguno de los pasos siguientes:

a) Verificación de la exactitud, veracidad y autenticidad de la información proporcionada por el Licitante en los documentos legales, técnicos y financieros presentados;
b) Validación del grado de cumplimiento de los requisitos y criterios de evaluación de la IaL, sobre la base de lo que hasta ahora haya podido hallar el equipo de evaluación;
c) Investigación y verificación de referencias con las entidades gubernamentales con jurisdicción sobre el Licitante, o con cualquier otra entidad que pueda haber hecho negocios con el Licitante;
d) Investigación y verificación de referencias con otros clientes anteriores sobre la calidad del cumplimiento de los contratos en curso o ya terminados;
e) Inspección física de las instalaciones del Licitante, fábrica, oficinas u otras instalaciones– donde se realiza el negocio, con o sin previo aviso al Licitante;
f) Pruebas y muestreos de los productos terminados similares a los requisitos del PNUD, si están disponibles, y

g) Otros medios que el PNUD estime necesarios en cualquier momento dentro del proceso de selección previo a la adjudicación del contrato.

F. ADJUDICACIÓN DEL CONTRATO

30. Derecho a aceptar, rechazar o considerar no aceptable cualquiera o todas las Ofertas

30.1 El PNUD se reserva el derecho de aceptar o rechazar cualquier Oferta, declarar una o todas las Ofertas no aceptables, y rechazar todas las Ofertas en cualquier momento antes de la adjudicación del contrato, sin incurrir en ninguna responsabilidad u obligación de informar a los Licitantes afectados de los motivos de la decisión del PNUD. Además, el PNUD no está obligado a adjudicar el contrato a la Oferta de precio más bajo.

30.2 El PNUD verificará y rechazará asimismo de inmediato las Ofertas correspondientes a Licitantes que figuren en la Lista Consolidada de las Naciones Unidas de Personas y Entidades Vinculadas con Organizaciones Terroristas, en la lista de proveedores suspendidos o retirados de la lista de proveedores de la División de Adquisiciones de la Secretaría de las Naciones Unidas, en la lista de proveedores inelegibles de las Naciones Unidas, y en otras listas de este tipo que puedan ser establecidas o reconocidas en la política del PNUD respecto a sanciones de los proveedores (Véase http://www.undp.org/content/undp/en/home/operations/procurement/protestandsanctions/)

31. Criterios de adjudicación

Antes del vencimiento del período de validez de la Oferta, el PNUD adjudicará el contrato al Licitante calificado y elegible que se estime responda a las exigencias de la Lista de Requisitos y Especificaciones Técnicas, y haya ofrecido el precio más bajo (Ver HdD, nº 32).

32. Derecho a modificar los requisitos en el momento de la adjudicación

En el momento de la adjudicación del Contrato, el PNUD se reserva el derecho a modificar la cantidad de bienes y/o servicios, hasta un máximo del veinticinco por ciento (25%) de la Oferta total, sin cambios en el precio por unidad o en otros términos y condiciones.

33. Firma del contrato

En el curso de quince (15) días a contar desde la fecha de recepción del Contrato, el Licitante que haya recibido la adjudicación firmará y pondrá fecha al Contrato y lo devolverá al PNUD.

Si el Licitante no consigue cumplir con el requisito de la Sección F.3 de la IaL y si esta disposición es motivo suficiente para la anulación de la adjudicación y la pérdida de la Garantía de Ejecución, si procede, el PNUD podrá adjudicar el contrato al Licitante que cuya Oferta haya obtenido la segunda más alta calificación o convocar nueva licitación.

34. Garantía de Ejecución

Si se considera necesaria, se facilitará una Garantía de Ejecución, en la cantidad y la forma prevista en la Sección 9 y por el plazo indicado en la Hoja de Datos (HdD, nº 14), según proceda. Cuando se exija una garantía de ejecución, se deberá presentar dicho documento y la confirmación de su aceptación por el PNUD como condición de efectividad del contrato que vaya a ser suscrito entre el Licitante y el PNUD.

35. Garantía bancaria de pagos anticipados

Excepto cuando los intereses de PNUD así lo requieran, el PNUD prefiere no hacer ningún pago por adelantado sobre los contratos (es decir, pagos sin haber recibido ningún producto). En caso de que el Licitante requiera un pago anticipado a la firma del contrato, y si dicha solicitud es aceptada debidamente por el PNUD, y cuando dicho pago anticipado exceda del 20% del valor de la Oferta total o exceda de 30.000 dólares EE.UU., el PNUD solicitará al Licitante que presente una garantía bancaria por el mismo importe del pago anticipado. La garantía bancaria de pago anticipado se presentará utilizando el formulario previsto al efecto en la Sección nº 10.

36. Reclamaciones de los proveedores

El procedimiento que establece el PNUD de reclamación para sus proveedores ofrece una oportunidad de apelación a aquellas personas o empresas a las que no se haya adjudicado una orden de compra o un contrato a través de un proceso de licitación competitiva. En caso de que un Licitante considere que no ha sido tratado de manera justa, podrá hallar en el siguiente enlace más detalles sobre el procedimiento de reclamación de los proveedores del PNUD:
http://www.undp.org/content/undp/en/home/operations/procurement/protestandsanctions/

Instrucciones a los Licitantes
HOJA DE DATOS

Los datos que se indican a continuación relacionados con el suministro de bienes y servicios conexos serán complementarios a las disposiciones de las Instrucciones a los Licitantes. En caso de conflicto entre las Instrucciones a los Licitantes y la Hoja de Datos, las disposiciones de la Hoja de Datos tendrán carácter preferente.

HdD, nº	Ref. a instrucciones	Datos	Instrucciones/Requisitos específicos
1		Título del proyecto:	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.
2		Título de los trabajos o servicios:	"Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma"
3		País:	Perú
4	C.13	Idioma de la Oferta:	☒ Español
5	C.20	Condiciones de presentación de Ofertas alternativas para partes o subpartes de los requisitos totales	☒ No Permitidas
6	C.20	Condiciones de presentación de Ofertas alternativas	☒ No serán tenidas en cuenta
7	C.21	Periodo de validez de la Oferta a partir de la fecha de presentación de ofertas	☒ 120 días calendario
8	B.9.5 C.15.4 b)	Garantía de Oferta	☒ No Aplica
9	B.9.5	Formas aceptables de Garantía de Oferta	☒ No Aplica
10	B.9.5 C.15.4 a)	Validez de la Garantía de Oferta	☒ No Aplica
11		Pago por adelantado a la firma del contrato	Permitido hasta un máximo de 20% del contrato Si el pago por adelantado solicitado por el Licitante excede de un total de 30.000 dólares

			EE.UU, el Licitante deberá presentar una Garantía de Pago por Adelantado por el mismo monto del pago por adelantado, utilizando para ello la plantilla y el contenido del documento que se halla en la Sección 10. ***El licitante deberá indicar en su oferta si hará uso de este beneficio completando el Formulario de la sección 10***
12		Penalidades	Si por razones imputables al adjudicatario, éste no entregara los bienes requeridos dentro de los plazos especificados en el Contrato, el PNUD, podrá aplicar una penalidad equivalente al 2% por semana o fracción del precio de los bienes o servicios demorados, hasta un máximo equivalente al 10% del monto contratado. Una vez alcanzada esta cifra se podrá resolver el contrato y ejecutar la garantía de ejecución sin reclamo por parte del contratista.
13	F.37	Garantía de Ejecución	☒ No aplica
14	C.17, C.17 b)	Moneda preferida de la Oferta y método de conversión de moneda	☒ Nuevos soles
15	B.10.1	Fecha límite para la presentación de consultas y preguntas aclaratorias	• Recepción de consultas: Hasta el **9 de abril de 2018** (por vía electrónica a: adquisiciones.pe@undp.org • Respuesta a consultas: Hasta el **12 de abril de 2018** (por vía electrónica y publicación vía web). Las consultas deberán ser remitidas, haciendo referencia al proceso PNUD/IAL-133/2018 – Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma.
16	B.10.1	Detalles de contacto para la presentación de aclaraciones y preguntas	Unidad de Adquisiciones Email: adquisiciones.pe@undp.org Los licitantes deberán indicar en el asunto el número de la referencia del proceso: PNUD/IAL-133/2018 – Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma.

17	B.11.1	Medio de transmisión de la Información Adicional a la IaL, y respuestas y aclaraciones a las demandas de información	☒ Comunicación directa con los potenciales Licitantes por correo electrónico y publicada en el sitio internet: http://www.pe.undp.org/content/peru/es/home/operations/procurement.html
18	D.23.3	Nº obligatorio de copias de la Oferta que habrán de presentarse.	Original: Uno (1) física (Debidamente foliada y rubricada) Copias: Uno (1) Digital
19	D.23.1 D.23.2 D.24	Dirección de presentación de la Oferta	Oficinas del PNUD sito en: Av. Augusto Pérez Araníbar No. 750 Magdalena del Mar Lima – Perú
20	C.21 D.24	Fecha límite de presentación de ofertas	Fecha: Hasta el **19 de abril de 2018** Hora: 13:00 horas (sin tolerancia)
21	D.23.2	Forma aceptable de presentar la Oferta	☒Mensajería/Entrega en mano ☒ Correo/Entrega en mano Las ofertas deberán presentarse en un (01) sobre AB conteniendo la Oferta Técnica y Económica en un (1) original y una (1) copia con todas las páginas que contengan información numerada en forma correlativa, sellada y rubricada por el Representante Legal del Licitante. La propuesta deberá incluir un Indice y encontrarse debidamente Foliada. **Los postores deberán adjuntar a su propuesta una copia digital de su propuesta en Formato WORD (CD, DVD y/o USB).**
			Los sobres estarán dirigidos al PNUD y deberán identificarse de la siguiente manera:

			(*) Fecha y hora de la apertura de propuestas según lo indicado en las Instrucciones a los Proponentes, Notas Aclaratorias y/o Enmiendas. Nombre y dirección del Oferente Programa de las Naciones Unidas para el Desarrollo Av. Augusto Pérez Araníbar No. 750, Magdalena del Mar /Lima - Perú Atención: Unidad de Adquisiciones *SOBRE "AB" - PROPUESTA TÉCNICA Y ECONÓMICA* Invitación a Licitar PNUD/IAL-133/2018 "Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma" No de Item(s):_____ NO ABRIR ANTES DE: _____
22	D.23.2 D.26	Condiciones y procedimientos de presentación y apertura electrónicas, si procede	☒ No aplica
23	D.23.1 c)	Fecha, hora y lugar de apertura de las Ofertas	Fecha: **19 de abril de 2018** Hora: 15:00 horas Lugar: Oficinas del PNUD
24		Método de evaluación utilizado en la selección de la Oferta más aceptable	☒ Precio más bajo Ofertado de una Oferta calificada/aceptable técnicamente.
25	C.15.1	Documentos de presentación obligatoria para establecer la calificación de los Licitantes	**a. Documentación General** a.1 Formulario de Presentación de la Oferta (Sección 4). a.2 Formulario de información del Licitante (Sección 5). a.3 Formulario de Información sobre Socios de un Joint Venture aplicable para el caso de licitantes que se presenten asociación o consorcio, incluido Contrato de consorcio, según lo indicado en el numeral 27 (Sección 5). a.4 Reporte de Calificacion crediticia expedida por Inforcorp/ Sentinel **b. Documentación Legal**

			b.1 Copia simple de la constitución social vigente de la empresa o Copia Literal, inscrita en los Registros Públicos. b.2 Copia del Poder Legal vigente otorgado por escritura pública o Vigencia de Poder al Representante Legal del Licitante identificado en el Formulario de Presentación de Oferta, para firmar la oferta y la orden de compra, si corresponde. b.3 En caso aplique, Carta de Intención de suscribir un Contrato o Compromiso de Asociación en Participación o Consorcio, según lo indicado en el numeral 27 de esta Sección, incluido copia simple de los poderes legales vigentes de los representantes de las empresas que integran la asociación o consorcio. La presente Carta deberá contener como mínimo la presente información: a. Empresas que conforman el Joint Venture o Consorcio. b. Designación del Representante Legal común y domicilio fijado por el Joint Venture o Consorcio. c. Designación de uno de los integrantes como Representante Líder, el cual deberá contar con facultades para contraer obligaciones y recibir instrucciones para y en nombre de todos y cada uno de los integrantes del Joint Venture o Consorcio. La ejecución de la totalidad del contrato, incluyendo los pagos, se manejará exclusivamente con el integrante designado como Representante Común. d. Actividades que cada integrante del Joint Venture o Consorcio realizará (indicando además porcentaje en costo y ejecución de la prestación). e. Declaración expresa que todos los integrantes serán responsables mancomunada y solidariamente por el cumplimiento del Contrato de acuerdo con los términos del mismo Se incentiva la presentación de las empresas en Consorcio a fin de fomentar la participación de la micro y pequeña empresa (Mypes). **c. <u>Documentación Financiera</u>** c.1 Presentación de los últimos dos (2) estados

			financieros auditados (estado de resultados y balance general), debidamente firmados por un Contador Público Colegiado o el que haga sus veces en el país de origen, para el caso de proveedores locales esta información podrá ser reemplazada por los Reportes de los Estados Financieros presentados a la Superintendencia de Administración Tributaria-SUNAT durante los periodos (2015-2016). c.2 Resumen de Estados Financieros, certificado por un Contador Público Colegiado (o el que haga sus veces en el país de origen). **Deberá presentarse en el Formato establecido en la Sección 12.** **d. <u>Documentación Técnica – Sección 6</u>** La documentación técnica dependerá del No. del Item o de los Items al que se presentará el postor. Los postores serán responsables de presentar de manera clara y ordenada la documentación, a fin de que la Comisión Evaluadora pueda realizar la evaluación adecuada de la propuesta. d.1 Proporcione información relativa a la experiencia empresarial, en adquisición y prestacion del servicio objeto de la convocatoria, realizada en los últimos cinco (5) años, por un monto facturado acumulado no menor a tres veces el monto de su oferta. Dicha información deberá estar acompañada con copia simple de contratos, órdenes de compra y/o facturas canceladas, incluidas las correspondientes constancias de conformidad, emitidas por el cliente al cual se le brindó el servicio. En caso de los consorcios, la experiencia será evaluada de manera acumulada entre los partipantes del mismo. d.2 Tabla de especificaciones técnicas mínimas requeridas (Sección 13). d.3 Los licitantes deberán presentar un cronograma detallado (diagrama tipo Gantt) conteniendo el plan de entregas propuesto que podrá incluir entregas parciales, y el cual no podrá exceder de 60 dias calendario. d.4 Declaración Jurada de Calidad de bienes y Garantía Técnica, según lo establecido en las especificaciones técnicas. Dicho plazo

			empezará a regir a partir de la instalación y funcionamiento de los bienes (Lima Metropolitana). (Sección 15). d.2 Declaración Jurada emitida por el fabricante autorizando la comercialización de los bienes y representación de la marca (Sección 14). d.3 Declaración Jurada emitida por el Licitante indicando las fechas de instalación, capacitación y mantenimiento de los bienes suministrados (Sección 15). *Sin perjuicio de lo detallado de manera precedente, los postores deberán presentar toda la información requerida en la SECCIÓN 6*. **e. <u>Documentación Económica</u>** **Los postores deberán presentar el Formulario de acuerdo al Item que postulan. En la sección 7 se establecen los formatos según cada Item.** e.1 Formulario de Oferta Financiera (ver Sección 7).
26		Otros documentos que se puedan presentar para establecer la elegibilidad	En el caso que el ganador de la buena pro sea un Joint Venture o Consorcio, para la etapa de suscripción del contrato, deberá presentar el Contrato o Compromiso de Joint Venture o Consorcio con vigencia hasta 30 días calendario posteriores a la culminación de todas las obligaciones ante el PNUD, el mismo que deberá estar legalizado ante Notario Público (o la autoridad competente en el país de origen) y que contendrá por lo menos los siguientes aspectos: i. Empresas que conforman el Joint Venture o Consorcio. ii. Designación mediante un documento notarial del Representante Legal común y domicilio fijado por el Joint Venture o Consorcio. iii. Designación de uno de los integrantes como Representante Común, el cual deberá contar con facultades para contraer obligaciones y recibir instrucciones para y en nombre de todos y cada uno de los integrantes del Joint Venture o Consorcio. La ejecución de la totalidad del contrato, incluyendo los pagos, se manejará exclusivamente con el integrante designado

			como Representante Común. iv. Actividades que cada integrante del Joint Venture o Consorcio realizará (indicando además porcentaje en costo y ejecución de la prestación). v. Declaración expresa que todos los integrantes serán responsables mancomunada y solidariamente por el cumplimiento del Contrato de acuerdo con los términos del mismo; vi. Declaración expresa del compromiso formal de no modificar los términos del documento de asociación hasta que el total de los servicios hayan sido prestados a satisfacción y concluyan sus obligaciones, contractuales, en caso de adjudicársele el Contrato. vii. Asimismo se precisa que ninguna empresa participante podrá formar parte de más de un Joint Venture o Consorcio.
27	C.15	Estructura de la Oferta Técnica y lista de documentos que habrán de presentarse	☒ Favor remitirse a lo indicado en el numeral 26 de esta Sección.
28	C.15.2	Última fecha prevista para el inicio del Contrato	mayo 2018
29	C.15.2	Duración máxima prevista del Contrato	El plazo máximo para la entrega de los bienes, instalación y capacitación es de **cuarenta y cinco (45) días calendario**.
30		El PNUD adjudicará el Contrato a:	☒ **Un Item por licitante o Ambos Itemes a un licitante** La buena pro será adjudicada, al postor que cumpla con las especificaciones técnicas y sobre la base del precio más bajo.
31	F.34	Criterios para la adjudicación del Contrato y la evaluación de Ofertas	**<u>CRITERIOS DE EVALUACIÓN DE LA OFERTA</u>** **1. EXAMEN PRELIMINAR** **1.1. Verificación de la presentación de la documentación general, legal, financiera y técnica** La evaluación consistirá en verificar que los documentos presentados por las empresas licitantes, estén de acuerdo a lo solicitado en el numeral 26 de la presente Sección, aplicando como criterio de evaluación, Presenta / No Presenta.

			Asimismo, se verificará la presencia de los postores dentro de la Lista 1267/1989. Serán inhabilitadas las ofertas que no cumplan con los requisitos de carácter técnico y/o que presenten serios incumplimientos en los requisitos establecidos en las bases. **2. OFERTA TÉCNICA** **2.1. Evaluación Técnica** 2.1.1. Evaluación de la experiencia del licitante 2.1.2. Evaluación de cumplimiento de especificaciones técnicas mínimas. 2.1.3. Evaluación Financiera Se evaluará la situación financiera de las empresas a través de la verificación de los siguientes índices financieros correspondientes al promedio de los últimos tres ejercicios fiscales, como sigue: ▪ Índice de Liquidez (Activo Corriente/Pasivo Corriente) Mayor a 1.00 en promedio ▪ Índice de Endeudamiento (Pasivo Total / Activo Total) Menor que 1.00 en promedio En caso el Licitante sea un Joint Venture o Consorcio, la evaluación se realizará en forma individual para cada una de las empresas que conforman el mismo. El ratio correspondiente al Consorcio será el resultado del promedio de los resultados individuales obtenido por cada uno de los miembros de la Asociación. **3. OFERTA ECONÓMICA** **3.1 Evaluación Económica** La evaluación económica de las ofertas habilitadas se realizará de acuerdo al siguiente procedimiento: 4. En caso se encontrarán errores aritméticos en las ofertas económicas, éstos serán

			corregidos y los nuevos valores se tomarán en cuenta para evaluar las ofertas. 5. Ante discrepancias entre el precio unitario ofertado y el monto total resultante de multiplicar el precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido en la magnitud correspondiente.
32	E.29.	Medidas posteriores a la adjudicación	☒ Facultad de Verificar de la exactitud, veracidad y autenticidad de la información proporcionada por el Licitante en los documentos legales, técnicos y financieros presentados
33		Condiciones para determinar la efectividad del contrato	☒ En el caso de licitantes que se presenten en asociación o consorcio y resulten adjudicados con la buena pro, deberán presentar el documento de formalización jurídica de la referida asociación. ☒ Facultad de solicitar la presentación de documentación adicional (certificados, permisos, autorizaciones, licencias, entre otros) que se requiera para la adecuada ejecución del contrato.
34	F.33	Otras informaciones relativas a la IaL	**(No aplica)**

CRITERIOS DE EVALUACIÓN

El **PNUD** efectuará la evaluación de las ofertas presentadas teniendo en consideración los siguientes aspectos:

CONCEPTOS DE EVALUACIÓN	CRITERIO
1. 1. EXAMEN PRELIMINAR	
1.1. Presentación de la Documentación General	Presenta / No Presenta
1.2. Presentación de la Documentación Legal	Presenta / No Presenta
1.3. Presentación de la Documentación Financiera	Presenta / No Presenta
1.4. Verificación de Lista 1267/1989	Se encuentra/No se encuentra
2. OFERTA TÉCNICA – SECCIÓN "A"	
2.2. Evaluación Técnica	
2.2.1. Evaluación de la experiencia del licitante	Cumple / No cumple
2.2.2. Evaluación de cumplimiento de especificaciones técnicas mínimas.	Cumple / No cumple
2.2.3. Evaluación Financiera	Cumple / No cumple
3. OFERTA ECONÓMICA – SECCIÓN "B"	
3.1. Evaluación Económica	
3.1.1. Evaluación Económica	El que cumpla y presente la oferta más baja
EVALUACIÓN FINAL	Comparación de Precios

Sección 3: Lista de Requisitos y Especificaciones Técnicas

I. ANTECEDENTES

El Programa Nacional de Alimentación Escolar Qali Warma (PNAE QW) es un programa social del Ministerio de Desarrollo e Inclusión Social fue creado de acuerdo con el Decreto Supremo N°008-2012-MIDIS, con el propósito de brindar un servicio alimentario de calidad, adecuado a los hábitos de consumo locales, cogestionado con la comunidad para niñas y niños del nivel de educación inicial a partir de los tres años de edad y del nivel de educación primaria de la Educación Básica en Instituciones Educativas Públicas. Asimismo, mediante Decreto Supremo N° 006-2014-MIDIS se modificó el Decreto Supremo N° 008-2012-MIDIS indicando que la vulnerabilidad de la población escolar abarca además de niñas y niños de educación inicial y primario a los adolescentes de educación secundaria regular en las Instituciones Educativas Públicas localizadas en los pueblos indígenas que se ubican en la Amazonia Peruana, comprendidos en la Base de Datos Oficial de Pueblos Indígenas, listados en la Resolución Ministerial N° 321-2014-MC del Ministerio de Cultura, o la que la reemplace o actualice.

Los objetivos del PNAE Qali Warma son:
Garantizar el servicio alimentario durante todos los días del año escolar a los usuarios del Programa de acuerdo a sus características y las zonas donde viven.
Contribuir a mejorar la atención de los usuarios del Programa en clases, favoreciendo su asistencia y permanencia.
Promover mejores hábitos de alimentación en los usuarios del Programa.

El 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"; busca prestar asistencia técnica al PNAE Qali Warma para fortalecer sus capacidades para la provisión de un servicio alimentario adecuado, considerando los factores económicos, sociales y culturales de cada territorio. Al respecto, en el plan de trabajo 2017 se está considerando desarrollar la adquisición de switches de fibra óptica para la infraestructura de red de alta disponibilidad orientada a la Interconexión a una mayor velocidad a nivel nacional 02 switches de core y 02 switches de distribución; así como la adquisición de los equipos de seguridad perimetral para la Sede Central tiene por finalidad brindar la alta disponibilidad y seguridad de los equipos de infraestructura de TI de la Sede Central, con la finalidad de mantener la disponibilidad de los servicios informáticos que son brindados a nivel nacional.

II. AREA USUARIA

Unidad de Tecnologías de la Información del Programa Nacional de Alimentación Escolar Qali Warma - Ministerio de Desarrollo e Inclusión Social.

III. OBJETO DE LA CONTRATACIÓN

ITEM No. 1: SWITCHES DE CORE Y DISTRIBUCION

La adquisición de switches de fibra óptica para la infraestructura de red de alta disponibilidad está orientada a la Interconexión a una mayor velocidad a nivel nacional 02 switches de core y 02 switches de distribución

ITEM No. 2: FIREWALL DE SEGURIDAD PERIMETRAL

La adquisición de los equipos de seguridad perimetral para la Sede Central tiene por finalidad brindar la alta disponibilidad y seguridad de los equipos de infraestructura de TI de la Sede Central, con la finalidad de mantener la disponibilidad de los servicios informáticos que son brindados a nivel nacional.

IV. DETALLE DE LA ADQUISICIÓN DE LOS BIENES:

NO DE ITEM	DESCRIPCIÓN	CANTIDAD
ITEM No. 1	**SWITCHES DE CORE Y DISTRIBUCION**	**4**
Sub Item 1.1	SWITCHES TIPO 1: Switches de core para centro de datos	2
Sub Item 1.2	SWITCHES TIPO 2: Switches de Distribución	2
ITEM No. 2	**FIREWALL DE SEGURIDAD PERIMETRAL**	**2**
Sub item 2.1	Firewall de seguridad perimetral	2

V. ALCANCE Y DESCRIPCION DE LOS BIENES

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

a) 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.

b) 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.

c) UBICACIÓN/SEDE

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

VI. ITEM No. 1 - ESPECIFICACIONES TÉCNICAS: ADQUISICION DE SWITCHES DE CORE Y DISTRIBUCION

A. SUB - ITEM No. 1.1: SWITCH TIPO 1 - SWITCHES DE CORE PARA CENTRO DE DATOS

Especificaciones Técnicas	Descripción
Marca:	*Indicar*
Modelo:	*Indicar*
Origen	*Indicar*
Cantidad	*2 unidades*
Alta Disponibilidad	Con la finalidad de garantizar la alta disponibilidad de la red para los servidores del Centro de Datos, los Switches para servidores deberán ser interconectados y configurados de tal manera que los servidores que tengan múltiples interfaces de red, puedan conectarse a estos equipos teniendo activas estas conexiones de manera simultánea. Los switches para servidores deberán interconectarse entre sí mediante dos (02) puertos de 10GB en cada equipo configurando un trunk de 20GB entre ellos, como mínimo
Hardware	Switches multicapa diseñados específicamente para centro de datos.
	Cada switch deberá ser del mismo modelo y familia. Año de fabricación 2017 o más reciente.
	Los switches para Centro de Datos deberán permitir que los servidores que cuenten con múltiples interfaces de red puedan conectarse a ambos switches utilizando agregación de puertos sin que se ocasionen loops o que se tengan puertos bloqueados. Es decir, las conexiones deberán operar en modo activo/activomstsc.
	Incluir al menos 48 puertos fixed SPF+ port (1 o 10Gbpa)
	El equipo ofertado deberá trabajar en capa 2, con una tasa de envió mínima de 960 Gbps.
	El equipo deberá soportar la inserción en caliente de fuentes de poder y módulos ventiladores.
	El equipo deberá contar con una redundancia de fuentes de poder N+1 y N+N
	El equipo deberá contar con una redundancia de módulo de ventilador de N+1
	Capaz de consolidar tráfico Ethernet proveniente de la red LAN.
	Cada switch Centro de Datos deberá incluir al menos treinta y dos (32) puertos 10 GE, capaces de soportar transceiver de 1 GE (SFP) o 10 GE (SFP+), con soporte de capa 2 (L2). Se deberá incluir por cada equipo veinte (20) tranceivers para puertos UTP de 1GE, ocho (08) Tranceiver del tipo 10GBASE-SR además de los conectores que permitan unir ambos equipos utilizando como mínimo dos (02) puertos 10 Gigabit.
	El equipo ofertado deberá cumplir con un diseño que provea latencia de tráfico predecible y consistente a pesar del tamaño del paquete, patrón de tráfico o características habilitadas en las interfaces correspondientes.
	El equipo ofertado deberá cumplir con la misma tasa de transferencia en todos los puertos.
	Los dos Switches de Centro de datos se conectarán entre sí mediante dos enlaces de 10 Gbps como mínimo. Estas conexiones pueden ser mediante cobre o fibra y los módulos son adicionales a los 10GBASE-SR ya solicitados.
	Cada switch de Centro de Datos no deberá exceder de 1 RU de altura.
	Fuentes de Poder y ventiladores redundantes hot swap.
	Los dispositivos a ofertar no deberán contar a la fecha de presentación de propuestas con anuncio de Fin de Ciclo de Vida (Fin de Vida) del fabricante con el fin de asegurar una mayor vigencia tecnológica de los equipos a adquirir. Esto deberá ser sustentado con documentación del fabricante.
Software	Capacidad de Operación a nivel 2 y nivel 3 del Modelo OSI.
	El switch solicitado tiene que tener habilitado el enrutamiento en capa 3, que soporte los protocolos (RIPv2, EIGRPv2, OSPFv2,)
	Soporte de calidad de servicio 802.1p
	Soporte de QoS, con 8 colas de prioridad por puerto 10GE.
	El equipo ofertado deberá soportar la configuración de QoS por puerto.
	El equipo ofertado deberá soportar clasificación QoS basada en listas de acceso (Capas 2, 3 y 4)
	Soporte de tramas gigantes (giants) en todos los puertos (hasta 9216 bytes)

	Manejo de 4 000 VLANs y 60 000 MAC address.
	Manejo de VLANs por puerto y 802.1q (trunking).
	Soporte del estándar IEEE 802.1AB (LLDP - Link Layer Discovery Protocol) o mecanismo similar para intercambio de información de dispositivos.
	Soporte de protocolos NTP y DNS.
	Soporte de DHCP relay.
	Enrutamiento unicast, multicast basado en hardware.
	Soporte del protocolo VRRP
	Deberá incluir protocolos de enrutamiento IPv4 estático y dinámico.
	Tráfico Multicast IGMPv2 y v3 snooping. Soporte de tráfico Multicast IGMPv3.
	Soportar enrutamiento multicast basado en hardware para IPv4 e IPv6. PIM-SM instalado y operativo.
	El equipo deberá cumplir con ACLs de entrada (estandar y extendido) en Ethernet y puertos Ethernet virtuales.
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad. Se deberá asegurar que se pueda realizar la agregación en al menos dos puertos ubicados en módulos distintos
	Soporte de los siguientes estándares: IEEE 802.3ab 1000BASE-T, Gigabit sobre cobre IEEE 802.3z 1000BASE-X, Gigabit sobre fibra IEEE 802.1d, Spanning Tree Protocol IEEE 802.1s, MSTP IEEE 802.1w, RSTP IEEE 802.1p, CoS Priorización de tráfico IEEE 802.1q, VLAN tagging IEEE 802.3ad, LACP IEEE 802.3x, Control de flujo IEEE 802.3ae, 10 Gigabit Ethernet RMON
Gestión y monitoreo	Deberá combinar la gestión de Ethernet y redes de almacenamiento en un único panel de control.
	Gestión por consola y puerto independiente para gestión fuera de banda.
	Permitir la administración segura protocolo SSHv2.
	Permitir múltiples sesiones simultáneas de administración
	Incluir el soporte de SNMP v2c y v3.
	Incluir los MIBs de los Switches considerados.
	Registro de eventos vía Syslog.
	Soporte de protocolos de transferencia de archivos TFTP, FTP y/o sFTP.
	Soporte de protocolos RCP y/o SCP y/o SFTP.
	Deseable que cuente con herramientas que permitan la captura de tráfico para su análisis y decodificación a nivel de paquetes.
	Deseable mecanismo de detección de fallas en cables de cobre y de fibra óptica.
	Incluir procesos de debug para el análisis detallado de fallas.
	Deberá contar con licencia para LAN.
	Brindar la funcionalidad de "puerto espejo" o funcionalidad similar, por puerto o grupo de puertos y por VLAN.
Mecanismos de seguridad	Filtrado basado en parámetros de capas 2, 3 y 4. Estos filtros deben ser aplicables por puerto y por VLAN.
	Seguridad por puerto, en base a la dirección MAC.
	Supresión y limitación de tormentas de broadcast, multicast y/o unicast.
	Control de acceso centralizado mediante RADIUS y/o TACACS+
	Incluir el manejo de protocolos SSHv2 y/o SSL.
	Permitir mínimo 4 niveles de privilegios de acceso para administración por consola, telnet y ssh.
	Permitir la restricción del acceso mediante SSH y SNMP desde múltiples direcciones IP.
	La versión del sistema operativo no debe poseer vulnerabilidades DoS conocidas a la fecha de publicación de las bases.

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 oficin
	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. ✓ 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.

B. SUB - ITEM 1.2: SWITCH TIPO 2 - SWITCHES PARA DISTRIBUCIÓN

Especificaciones Técnicas	Descripción
Marca:	*Indicar*
Modelo:	*Indicar*
Origen	*Indicar*
Cantidades	*2 unidades*
Alta Disponibilidad	Para garantizar la alta disponibilidad de la red para los switches de acceso a usuarios, se deberá contar con switches de distribución, cada uno de los cuales tendrá habilitado un enlace a velocidad 10 Gigabit a cada gabinete de piso. Estos switches de distribución deberán interconectarse entre sí mediante dos (02) puertos de 10GB en cada equipo configurando un trunk de 20GB entre ellos, como mínimo.
Hardware	Switches de distribución multicapa, de operación en L2 y L3 del modelo OSI y diseñados como equipos de agregación o distribución LAN.
	Cada switch deberá ser del mismo modelo y familia. Año de fabricación 2017 o más reciente.
	Los dos switches de distribución deberán trabajar en alta disponibilidad operando como una unidad lógica virtualizada, para lo cual se debera provisionar los componentes necesarios.
	Capacidad mínima de conmutación de 640 Gbps por cada equipo.
	Cada switch de distribución deberá incluir como mínimo Dieciséis (16) Puertos SFP+ y ser escalable hasta 24 Puertos SFP+. Deberán soportar transceivers de 1 GE (SFP) o 10 GE (SFP+), con soporte de capa 2 (L2) y capa 3 (L3). Se deberá tener equipados por cada equipo: ocho (08) Tranceivers ópticos 10GBASE-SR para fibra multimodo.
	Se deberá incluir por cada equipo cuatro (04) tranceivers para puertos UTP de 1GE.
	Los dos Switches de distribución se conectarán entre sí mediante dos enlaces de 10 Gbps como mínimo, esta conexión podrá ser mediante fibra o cobre, se deberán incluir los componentes necesarios para habilitar esta conexión redundante.
	Cada switch de distribución no deberá exceder de 1 RU de altura.
	Los módulos de fuente de poder y ventiladores deben ser hot-swap.
	Cada switch deberá contar con una tasa de reenvío en hardware de 400 Mpps como mínimo.
	Deben contar con fuentes de poder redundantes con voltaje de entrada de 200-240 VAC, 60 Hz, en una configuración N+1 y ventiladores con flujo de aire desde el frente hacia atrás como mínimo.
	Los dispositivos a ofertar no deberán contar a la fecha de presentación de propuestas con anuncio de Fin de Ciclo de Vida (Fin de Vida) del fabricante con el fin de asegurar una mayor vigencia tecnológica de los equipos a adquirir. Esto deberá ser sustentado con documentación del fabricante.
	El equipo deberá incluir memoria DRAM como mínimo 4GB
	El equipo deberá incluir memoria FLASH como mínimo 4GB
Software	Capacidad de Operación a nivel 2, nivel 3 y nivel 4 del Modelo OSI.
	Soporte de calidad de servicio 802.1p y DSCP
	Soporte de QoS, con 8 colas de prioridad por puerto como mínimo.
	Manejo de 1000 VLANs, 4000 VLAN IDs y 30 000 MAC address como mínimo.
	Manejo de VLANs por puerto y 802.1q (trunking).
	Soporte del estándar IEEE 802.1AB (LLDP - Link Layer Discovery Protocol) o similar para intercambio de información de dispositivos.
	Soporte de protocolos SNTP o NTP y o DNS.
	Soporte de DHCP relay.
	Enrutamiento unicast, multicast basado en hardware.
	Deberá incluir protocolos de enrutamiento IPv4 estático y dinámico (RIPv2, OSPFv2 y BGP como mínimo) con soporte de OSPF y BGP en IPv6 mediante upgrade de software.
	Tráfico Multicast IGMPv2 y v3 snooping. Soporte de tráfico Multicast IGMPv3.
	Soportar enrutamiento multicast basado en hardware para IPv4 e IPv6. PIM-SM instalado y operativo.

	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad. Se deberá asegurar que se pueda realizar la agregación en al menos dos puertos ubicados en módulos distintos.
	Soporte de los siguientes estándares: IEEE 802.3ab 1000BASE-T, Gigabit sobre cobre IEEE 802.3z 1000BASE-X, Gigabit sobre fibra IEEE 802.1d, Spanning Tree Protocol IEEE 802.1s, MSTP IEEE 802.1w, RSTP IEEE 802.1p, CoS Priorización de tráfico IEEE 802.1q, VLAN tagging IEEE 802.3ad, LACP IEEE 802.3x, Control de flujo
Gestión y monitoreo	Gestión por consola y puerto independiente para gestión fuera de banda.
	Permitir la administración utilizando protocolo SSH.
	Permitir múltiples sesiones simultáneas de administración
	Incluir el soporte de SNMP v2c y v3.
	Se deben Incluir los MIBs de los Switches considerados.
	Registro de eventos vía Syslog.
	Soporte de protocolos de transferencia de archivos TFTP, y/o FTP y/o sFTP.
	Soporte de Sflow, Netflow o protocolo similar instalado y operativo.
	Es deseable que incluyan mecanismos de detección de fallas en cables de cobre y de fibra óptica.
	Incluir procesos de debug para el análisis detallado de fallas.
	Brindar la funcionalidad de “puerto espejo” o funcionalidad similar, por puerto o grupo de puertos y por VLAN.
	Permitir configurar múltiples sesiones de “puerto espejo” o funcionalidad similar, deseable soporte de "puerto espejo" remoto o funcionalidad similar. Se requiere soportar al menos dos (02) sesiones simultáneas.
Mecanismos de seguridad	Filtrado basado en parámetros de capas 2, 3 y 4. Estos filtros deben ser aplicables por puerto y por VLAN.
	Seguridad por puerto, en base a la dirección MAC.
	Supresión y limitación de tormentas de broadcast, multicast y unicast.
	Control de acceso centralizado mediante RADIUS y/o TACACS+
	Incluir el manejo de protocolos SSH.
	Permitir al menos 4 niveles de privilegios de acceso para administración por consola, telnet y ssh.
	Permitir la restricción del acceso mediante SSH y SNMP desde múltiples direcciones IP.
	Soporte de DHCP Snooping o mecanismo similar.
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 oficin
	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. ✓ 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.

A. 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, broshures, datasheet, hojas de datos, fichas técnicas, que sustenten el cumplimiento de las especificaciones solicitadas del equipamiento propuesto.

Del personal:

(01) Jefe de Proyecto:

a. Educación:

- Ingeniero colegiado 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 y/o gestión de proyectos
- Con conocimientos demostrables en ISO 27001,
- Deberá tener ITIL Foundation como mínimo, o certificación en gestión de servicios de TI.
- Capacidades de coordinación, comunicación y trabajo en equipo.

b. Experiencia profesional:

- No menor a dos (02) años de experiencia en Tecnologías de la Información.
- Experiencia en Gestión de proyectos de Tecnologías de la Información.

(02) Especialistas en Equipos de Comunicación

a. Educación:

- Ingeniero o bachiller 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 equipos de comunicación ofertada.

b. Experiencia profesional:

- Experiencia profesional mínima de dos (02) años como implementador

B. DEL MANTENIMIENTO PREVENTIVO, SOPORTE TECNICO 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

En lo relacionado al soporte técnico 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 quince (15) 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.

Capacitación

Se deberá brindar una Capacitación para dos (02) profesionales de la Unidad de Tecnologías de la Información 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 comunicación

- Tipo de Capacitación: Deberá seguir el modelo curricular del curso Oficial o curricula similar a la indicada por el fabricante
- Número de Horas: 24 Horas
- Perfil del Capacitador:
  - ✓ Mínimo Grado de Bachiller de las escuelas profesionales de Ingeniería de Sistemas, Informática, Electrónica, Computación o afines
  - ✓ Experiencia mínima de dos (02) años como capacitador de soluciones de seguridad
  - ✓ El Expositor deberá contar con certificación oficial de la marca ofertada.

La capacitación se realizará en la Sede Central del PNAEQW sito en en 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

C. ENTREGABLES

- Al finalizar la Instalación y configuración del equipamiento solicitado se deberá presentar un informe final, el cual deberá entregarse en dos (02) juegos en formato impreso y digital, conteniendo la siguiente información:
  - Diagrama de conexión de los equipos de comunicaciones
  - Procedimiento detallado de la Instalación de los equipos de comunicaciones.
  - Archivos conteniendo los Backups de los equipos de comunicaciones.
  - Instructivos y/o manuales de configuración de los equipos de comunicaciones.
  - Documento en donde se pueda verificar el periodo de Garantía del fabricante del Equipamiento propuesto.

D. PLAZO DE ENTREGA DE LOS BIENES

- El Plazo de entrega será de 45 días calendario, contados desde el día siguiente de la recepción de la Orden de Compra por parte del proveedor.

E. FORMA DE PAGO

- El pago se efectuará a la aprobación de la conformidad técnica de los bienes y capacitación del uso de los bienes incluido informe final: El pago del 100% del precio de los bienes, se realizará dentro de los 30 días calendario siguientes a la verificación del total de los bienes y del cumplimiento técnico de los mismos, así como la capacitación sobre el uso de los bienes a través de la presentación del informe final. En caso se haya otorgado el pago por adelantado no mayor al 20% del total de los bienes, solicitado por el Licitante, este será descontado del pago de las entregas realizadas.

VII. ITEM 2: ESPECIFICACIONES TÉCNICAS: ADQUISICION DE FIREWALL DE SEGURIDAD PERIMETRAL

ITEM 2.1: ADQUISICION DE FIREWALL DE SEGURIDAD

EQUIPOS: FIREWALL SEGURIDAD PERIMETRAL

Especificaciones Técnicas	Descripción
Marca:	*indicar*
Modelo:	*Indicar*
Origen:	*Indicar*
Cantidad:	02 Unidades
Características del Firewall	Se deberá incluir todas las funcionalidades en un solo dispositivo del mismo fabricante.
	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 ser optimizada para análisis de contenido 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 en los últimos 3 reportes de Gartner, en el cuadrante de Líderes para Network Enterprise Firewalls.
	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, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
	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 e Antispyware;
	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.
	Deberá incluir cuatro (04) interfaces SFP+ como mínimo por cada equipo.
	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 un máximo de 1500 políticas
	Debe permitir 40 zonas de seguridad y 05 routers virtuales
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, vozIP, 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 nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano.
	Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
	Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, como mínimo).
	Nivel de riesgo de las aplicaciones.
	Categoría y sub-categoría de aplicaciones.
	Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
	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
	Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
	Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo.
	Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener algunas firmas de IPS habilitada o tener todas las firmas de IPS, Anti-Virus y Antispyware 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 Antispyware.
	Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes.
	Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos.
	Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP,
	SMB, SMTP e POP3.
	Los eventos deben identificar el país de donde partió la amenaza.
	Debe incluir seguridad contra virus en contenido HTML y javascript, software espía (spyware) y worms.
	Seguridad contra descargas involuntarias usando HTTP de archivos ejecutables Maliciosos.
	Rastreo de virus en PDFs.
	Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.).

	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.
	El fabricante debe ser considerado como un Lider en el reporte de evaluación de Forrester Wave Automated Malware Analysis, Q2 2016
	Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Mac OSX y Android
	Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB
	El sistema de análisis debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red).
	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, apk y archivos java en el ambiente controlado.
	Poseer SLA de, como máximo, 10 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado.
	Permitir el 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 certifícate.
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;
	Permitir listar el número de aplicaciones soportadas para control de datos;
	Permitir listar el número de tipos de archivos soportados para el control de datos.
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, E-Directory y base de datos local.
	Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio.
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.
	Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función.
	Debe soportar una 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 e 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;
	El portal de VPN debe enviar al cliente remoto la lista de Gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente
	Debe haber una opción en el cliente remoto de escoger manualmente el gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.
	Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa.
Reportes y Administración	Debe tener un módulo de reportes y administración incluido dentro del mismo equipo sin necesidad de licenciamiento ideal
	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.
Pruebas de los productos esperados	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.
	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.
	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.

A. 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:

e) 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.

f) 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

g) El proveedor deberá proporcionar todos los equipos, cables y accesorios necesarios para la interconexión entre los distintos componentes.

h) 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
-

B. 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:

h) 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.
i) 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).
j) El Contratista debe poseer un Centro de Control, ubicado en el Perú, que emplee las buenas prácticas

de gestión de servicios.

k) 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.
l) El Contratista debe proporcionar los niveles de escalamiento para los casos de avería, registro de incidencias y soporte.
m) El Contratista como empresa integradora de soluciones de tecnología será la responsable de todas las coordinaciones ante el fabricante, en caso sea requerido.
n) 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:
  - Conceptos y fundamentos de seguridad de la información
  - Terminología
  - Familia de normas ISO/IEC 27000
  - Importancia del SGSI en la organización
  - La estructura de la norma 27001
  - Identificación de requisitos
  - El sistema de gestión
  - Los controles del anexo A
  - 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

C. 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.

D. PLAZO DE ENTREGA

- El Plazo de entrega será de 45 días calendario, contados desde el día siguiente de la recepción de la Orden de Compra por parte del proveedor.

E. FORMA DE PAGO

- El pago se efectuará a la aprobación de la conformidad técnica de los bienes y capacitación del uso de los bienes incluido informe final: El pago del 100% del precio de los bienes, se realizará dentro de los 30 días calendario siguientes a la verificación del total de los bienes y del cumplimiento técnico de los mismos, así como la capacitación sobre el uso de los bienes a través de la presentación del informes final. En caso se haya otorgado el pago por adelantado no mayor al 20% del total de los bienes, solicitado por el Licitante, este será descontado del pago de las entregas realizadas.

Sección 4: Formulario de presentación de la Oferta[1]

(Este documento deberá presentarse en papel membretado del Licitante. Salvo en los campos que se indican, no se podrán introducir cambios en este modelo.)

[Indíquese: lugar, fecha]

A: Centro de Servicios
Programa de las Naciones Unidas para el Desarrollo
PNUD/Perú

Estimados señores:

Los abajo firmantes tenemos el placer de dirigirnos a ustedes para ofrecer al PNUD los bienes y servicios conexos *[indíquese el nombre de los bienes y servicios tal como figura en la IaL]* conforme a los requisitos que se establecen en la Invitación a Licitación PNUD/IAL-133/2018. De igual manera, remitimos nuestra oferta, que incluye la Oferta Técnica y Financiera.

Por la presente declaramos que:

a) Toda la información y las afirmaciones realizadas en esta Oferta son verdaderas, y aceptamos que cualquier malinterpretación contenida en ella pueda conducir a nuestra descalificación;
b) No estamos incluidos actualmente en la lista de proveedores suspendidos o retirados de la ONU u otro tipo de agencia de la ONU, ni estamos asociados con ninguna empresa o individuo que aparezca en la Lista 1267/1989 del Consejo de Seguridad de la ONU;
c) No estamos en situación de bancarrota pendiente, o litigios pendientes o ninguna otra acción legal que pudiera poner en peligro nuestra operación como empresa en funcionamiento, y
d) No utilizamos ni tenemos previsto emplear a ninguna persona que esté o haya estado empleada recientemente por la ONU o el PNUD.

Confirmamos que hemos leído y entendido, y por consiguiente aceptamos plenamente la Lista de Requisitos y Especificaciones Técnicas que describe los deberes y responsabilidades que se requieren de nosotros en esta IaL, así como los Términos y Condiciones Generales de Contratación del PNUD.

Asimismo, manifestamos nuestro compromiso de respetar la presente Oferta durante 120 días calendario.
En caso de aceptación de nuestra Oferta, nos comprometemos a iniciar los suministros de bienes y la provisión de servicios a más tardar en la fecha indicada en la Hoja de Datos.

Estamos plenamente conscientes y reconocemos que el PNUD no tiene la obligación de aceptar esta Oferta, que nos corresponde a nosotros asumir todos los costos relacionados con su preparación y presentación, y que en ningún caso será el PNUD responsable o estará vinculado a dichos costos, con independencia del desarrollo y resultado de la evaluación.

Atentamente les saluda,

Firma autorizada [*firma completa e inicial*]: _____
Nombre y cargo del firmante: _____
Nombre de la empresa: _____
Información de contacto: _____ *[Sírvanse sellar esta carta con el sello de su empresa, si lo tuvieren]*

1 No se hará ninguna modificación ni supresión a este formulario. Cualquier modificación o supresión puede llevar al rechazo de la Oferta.

Sección 5: Documentos que avalan la elegibilidad y las calificaciones del Licitante

Formulario de Información del Licitante[2]

Fecha: *[indíquese la fecha (día, mes y año) de presentación de la Oferta]*
REF.: IAL N°: PNUD/IAL-133/2018

Página _____ de_____ páginas

1. Nombre legal del Licitante [indíquese el nombre legal del Licitante]		
2. Si se trata de un Joint Venture, nombre legal de cada una de las partes: *[indíquese el nombre legal de cada una de las partes del Joint Venture]*		
3. País o países actuales o previstos para el registro/operación: *[indíquese el país de registro actual o previsto]*		
4. Año de registro en dicho lugar: *[indíquese el año de registro del Licitante]*		
5. Países donde opera	6. N° de empleados en cada país	7. Años de operación en cada país
8. Dirección o direcciones legal(es) de registro/operación: *[indíquese la dirección legal del Licitante en el país de registro]*		
9. Monto y descripción de los cinco (5) contratos mayores realizados durante el periodo comprendido entre los años 2011-2014		
10. Última calificación crediticia (con puntuación y fuente, si las hay)		
11. Breve descripción de la historia judicial (litigios, arbitrajes, reclamaciones, etc.), con indicación de la situación actual y los resultados, en los casos ya resueltos.		
12. Información sobre el representante autorizado del Licitante Nombre: *[indíquese el nombre del representante autorizado del Licitante]* Dirección: *[indíquese la dirección del representante autorizado del Licitante]* Teléfono/Fax: *[indíquese los números de teléfono y fax del representante autorizado del Licitante]* Dirección de correo electrónico: *[indíquese la dirección electrónica del representante autorizado del Licitante]*		
13. ¿Está usted incluido en la Lista Consolidada 1267/1989 de las Naciones Unidas? (Sí / No)		
14. Número de cuenta bancaria en el BBVA Banco Continental en la moneda en la que presenta su cotización (20 dígitos):_____		

[2] *El Licitante completará este formulario siguiendo las instrucciones. Además de proporcionar información adicional, no se permitirá realizar ninguna modificación del formulario ni se aceptarán sustituciones.*

15. En caso de no contar con cuenta en el BBVA Banco Continental, favor indicar su número de cuenta Interbancaria (20 dígitos): _____
16. Para el caso de bancos en el exterior indicar adicionalmente, el nombre del banco, dirección, ABA/ ACH Rounting Number/swift, IBAN, etc.: Nombre del banco: _____ Dirección: _____ Número de ABA/ACH/Swift/ IBAN: _____ Datos del banco intermediario _____ (en caso aplique):
17. Se adjuntan copias de los documentos originales siguientes: ☐ Todos los requisitos documentales que se establecen en la Hoja de Datos ☐ Si se trata de un Joint Venture/Consorcio, copia del memorando de entendimiento o carta de intenciones para la creación de un la JV/consorcio, o registro de JV/consorcio, si lo hay ☐ Si se trata de una corporación pública o una entidad controlada o propiedad del Estado, documentos que establecen la autonomía financiera y legal y el cumplimiento del derecho mercantil.

Nombre del representante legal: _____

Lugar y fecha: _____

Formulario de Información sobre socios de un Joint Venture (Si se encuentra registrado)[3]

Fecha: *[indíquese la fecha (día, mes y año) de presentación de la Oferta]*
IAL N°: PNUD/IAL-133/2018

Página _____ de_____ páginas

1. Nombre legal del Licitante *[indíquese el nombre legal del Licitante]*		
2. Nombre legal del asociado al JV: *[indíquese el nombre legal de asociado]*		
3. País de registro del JV: *[indíquese el país de registro de la empresa mixta]*		
4. Año de registro: *[indíquese el año de registro del asociado]*		
5. Países donde opera	6. N° de empleados en cada país	7. Años de operación en cada país
8. Dirección o direcciones legal(es) de registro/operación: *[indíquese la dirección legal del asociado en el país de registro]*		
9. Valor y descripción de los cinco (5) contratos mayores realizados durante los últimos cinco (5) años		
10. Última calificación crediticia (si la hay)		
11. Breve descripción de la historia judicial (litigios, arbitrajes, reclamaciones, etc.), con indicación de la situación actual y los resultados en los casos ya resueltos.(Por cada uno de los participantes)		
12. Información sobre el representante autorizado del asociado al JV Nombre: *[indíquese el nombre del representante autorizado del asociado alJoint venture]* Dirección: *[indíquese la dirección del representante autorizado del asociado alJoint Venture]* Teléfono/Fax: *[indíquese el teléfono/fax del representante autorizado del asociado al Joint Venture]* Dirección de correo electrónico: *[indíquese la dirección electrónica del representante autorizado del asociado al Joint Venture]*		
14. Se adjuntan copias de los documentos originales siguientes: *[márquense el cuadro o los cuadros de los documentos originales que se adjuntan]* ☐Todos los requisitos documentales que se establecen en la Hoja de Datos ☐Artículos de la incorporación o Registro de la empresa citada en el punto 2 supra. ☐Cuando se trate de una entidad de propiedad pública, los documentos que establecen su autonomía financiera y legal y sujeción al Derecho Comercial.		

[3] *El Licitante completará este formulario siguiendo las instrucciones. Además de proporcionar información adicional, no se permitirá realizar ninguna modificación del formulario ni se aceptarán sustituciones.*

Sección 6: Formulario de Oferta Técnica[4]

Este formulario deberá ser presentado por el licitante de acuerdo al Item o ítems a los cuales postule.

PNUD/IAL-133/2018 – "Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma"

Nombre de la empresa u organización licitantes:	
País de registro:	
Nombre del Representante Legal	
Número de cuenta bancaria en la moneda en la que presenta su cotización (20 dígitos):	
Nombre de la persona de contacto para esta Oferta:	
Dirección:	
Teléfono / Fax:	
Correo electrónico:	

SECCIÓN 1: EXPERIENCIA DE LA EMPRESA U ORGANIZACION

En esta Sección se debe explicar, en su totalidad, los recursos del Licitante en términos de personal e instalaciones necesarias para la realización de este encargo.

1.1. Breve descripción del Licitante como entidad: Proporcionen una breve descripción de la empresa u organización que presenta la Oferta, sus mandatos legales y actividades de negocios autorizadas, el año y el país de constitución, los tipos de actividades llevadas a cabo, el presupuesto anual aproximado, etc. Incluyan referencias a su buena reputación o cualquier antecedente de litigios / arbitrajes en que haya estado implicada la empresa u organización y que pudiera afectar negativamente o tener repercusión en la ejecución de los servicios, con indicación de la situación o el resultado de este litigio / arbitraje durante los últimos 5 años.

1.2. Proporcionen los dos (2) últimos estados financieros auditados (estado de resultados y balance general), debidamente firmados por un Contador Público Colegiado o el que haga sus veces en el país de origen, para el caso de proveedores locales esta información podrá ser reemplazada por los Reportes de los Estados Financieros presentados a la Superintendencia de Administración Tributaria-SUNAT durante los periodos (2015-2016). (liquidez, líneas de créditos standby, etc.) del licitante para contratar. Se deberá incluir cualquier indicación de la calificación de crédito, calificación de la industria, etc. Esta información deberá estar acompañada del Resumen indicado en la Sección 13.

1.3. Trayectoria y experiencias: Proporcione información relativa a la experiencia empresarial, en la Distribucion, fabricación y/o comercialización de Swicht y/o firewall de seguridad perimetral, realizada en los últimos cinco (5) años, por un monto facturado acumulado no menor a tres veces el monto de su oferta.

No.	*Cliente*	*Descripción de Bienes entregados*	*Cantidad de Bienes suministrados*	*Valor del contrato*	*Fecha de inicio y fecha de término*	*Referencias del Cliente*		
						Nombre de contacto	*teléfono*	*correo electrónico*

[4] *Las Ofertas Técnicas que no sean presentadas en este formato podrán ser rechazadas.*

SECCION 2 - ÁMBITO DEL SUMINISTRO, ESPECIFICACIONES TÉCNICAS Y SERVICIOS CONEXOS

En esta Sección se debe demostrar la aceptabilidad del Licitante ante las especificaciones identificando los componentes específicos propuestos, abordando los requisitos, según se especifique, punto por punto; proporcionando una descripción detalla de las características de ejecución esenciales propuestas; y demostrando de qué modo esta Oferta prevé cumplir con las especificaciones o superarlas.

2.1 Ámbito del suministro: Proporcione una descripción detallada de los bienes a suministrar, indicando claramente la forma en que cumplen con las especificaciones técnicas establecidas en esta IaL (véase Anexo 1); y describan de qué modo suministrará la organización/empresa los bienes y servicios conexos, teniendo en cuenta la adecuación a las condiciones locales y el medio ambiente del proyecto.

2.2 Mecanismos de garantía de calidad técnica: La Oferta también incluirá detalles de los mecanismos internos del Licitante en materia de revisión técnica y garantía de calidad, todos los certificados de calidad correspondientes, licencias de exportación y otros documentos que atestigüen la superioridad de la calidad de los productos y tecnologías que serán suministrados.

2.3 Informes y monitoreo: Sírvanse proporcionar una breve descripción de los mecanismos propuestos en este proyecto destinados a informar al PNUD y sus socios, incluyendo un calendario de informes.

2.4 Subcontratación: Expliquen si prevén subcontratar algún trabajo, a quién, qué porcentaje de la obra, la razón de ser de la subcontratación y las funciones de los subcontratistas propuestos. Se debe prestar especial atención a proporcionar una descripción clara de la función de cada entidad y cómo cada una va a funcionar como un equipo.

2.5 Riesgos y medidas de mitigación: Sírvanse describir los riesgos potenciales para la implementación de este proyecto que puedan afectar el logro de los resultados esperados y su terminación oportuna, así como su calidad. Describir las medidas que se pondrán en marcha para mitigar estos riesgos.

2.6 Plazos para la Implementación: El Licitante deberá presentar un cronograma en el que se indicará la secuencia detallada de las actividades que se llevarán a cabo, sus plazos correspondientes y el número de unidades a entregar.

2.7. Asociaciones (opcional): Expliquen las asociaciones con organizaciones locales, internacionales o de otro tipo que se hayan previsto para la ejecución del proyecto. Se debe prestar especial atención a proporcionar una imagen clara de la función de cada entidad y cómo cada uno va a funcionar como un equipo. Se ruega el envío de las cartas de compromiso de los socios así como indicaciones de si algunos o todos han trabajado conjuntamente en otros proyectos anteriores.

2.8. Estrategia de lucha contra la corrupción (opcional): Definan la estrategia de lucha contra la corrupción que se aplicará a este proyecto para prevenir el uso indebido de los fondos; describan asimismo los controles financieros que se instaurarán.

2.9 Declaración de divulgación total: Con ella se pretende conocer cualquier posible conflicto, de acuerdo con la definición de "Conflicto" que se hace en la Sección 4 de este documento, si procede.

2.10 Capacidad de Producción: Se deberá detallar cuál es la capacidad de producción semanal y mensual del fabricante, indicando la capacidad comprometida y la capacidad de libre disponibilidad.

2.11 Otros: Otros comentarios o informaciones sobre la Oferta y su ejecución.

SECCION 3: PERSONAL		
3.1 Estructura de gestión: Describan el enfoque de gestión global en relación con la planificación e implementación del contrato. Incluyan un organigrama de la gestión del contrato, si el contrato les fuera adjudicado. 3.2 Cuadro horario del personal: Sírvanse proporcionar una hoja de cálculo que muestre las actividades de cada miembro del personal y el tiempo asignado para su participación. Dada la importancia crítica de la preparación del personal para el éxito del Contrato, el PNUD no permitirá realizar sustituciones de personal cuyas calificaciones hayan sido examinadas y aprobadas durante el proceso de licitación. (Si la sustitución de dicho personal es inevitable, el o los reemplazantes estarán sujetos a la aprobación del PNUD. No podrá derivarse ningún aumento de costos como resultado de una sustitución). 3.3 Calificaciones del personal clave: Sírvanse proporcionar currículos del personal clave disponibles en la ejecución de este proyecto. Los currículos deben demostrar las calificaciones en ámbitos relevantes para el Contrato. Rogamos utilicen el siguiente formulario:		
Nombre:		
Cargo en relación con este Contrato:		
Nacionalidad:		
Información de contacto:		
Países en los que ha adquirido su experiencia de trabajo:		
Conocimientos lingüísticos:		
Calificaciones educativas y otras:		
Resumen de experiencia: *Destáquese la experiencia en la región y en proyectos similares.*		
Periodo: De – A	**Nombre de la actividad / proyecto / organización de financiación, si procede:**	**Nombre del empleo y las actividades desarrolladas / descripción de la función desarrollada:**
p.ej. julio 2004-enero 2005		
Etc.		
Etc.		
Referencias (mín. 3):	*Nombre* *Cargo* *Organización* *Información de contacto – Dirección; teléfono; Correo electrónico; etc.*	
Declaración: Por la presente, confirmo mi intención de servir en el puesto indicado, así como mi disponibilidad actual para servir durante el periodo del contrato propuesto. También entiendo que cualquier declaración intencionalmente falsa de los datos descritos anteriormente puede conducir a mi inhabilitación, antes de mi entrada en funciones o durante las mismas. _____ _____ Firma del Jefe de Equipo/Miembro designado Fecha		

Sección 7: Formulario de Oferta Financiera[5]

El Licitante está obligado a presentar su Oferta Financiera según se indica en las Instrucciones a los Licitantes.

PNUD/IAL-133/2018 – "Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma"

A. Cuadro Resumen de precios ofertados por ITEM (2)

NO DE ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO TOTAL Incluido impuestos
ITEM No. 1	**SWITCHES DE CORE Y DISTRIBUCION**	**4**	
ITEM No. 2	**FIREWALL DE SEGURIDAD PERIMETRAL**	**2**	

B. Cuadro Resumen de precios ofertados por componente (2)

NO DE ITEM	DESCRIPCIÓN	CANTIDAD	Precio Unitario	Precio Total
ITEM No. 1	**SWITCHES DE CORE Y DISTRIBUCION**			
Sub Item 1.1	SWITCHES TIPO 1: Switches de core para centro de datos	2		
Sub Item 1.2	SWITCHES TIPO 2: Switches de Distribución	2		
	Servicio de instalación,	4		
	Servicio de capacitación	4		
	Servicio de mantenimiento	4		
Monto total incluido impuestos				

[5] *No podrá realizarse ninguna supresión o modificación en este formulario. Toda supresión o modificación puede conducir al rechazo de la Oferta.*

NO DE ITEM	*DESCRIPCIÓN*	CANTIDAD	Precio Unitario	Precio Total
ITEM No. 2	**FIREWALL DE SEGURIDAD PERIMETRAL**			
Sub item 2.1	Firewall de seguridad perimetral	2		
	Servicio de instalación,	2		
	Servicio de capacitación	2		
	Servicio de mantenimiento	2		
Monto total incluido impuestos				

Los precios ofertados deberán incluir todos los gastos e impuestos hasta su entrega DDP, instalación, capacitacion y mantenimiento en las instalaciones del Programa Nacional de Alimentacion Escolar Qali Warmaubicada en Lima Metropolitana, de acuerdo a un cronograma de entregas aprobado por PNUD.

Son: _____ (indicar importe en números y en letras, y Moneda)

Nombre y firma del Representante Legal: _____

Lugar y fecha: _____

Sección 8: Formulario de Garantía de la Oferta (No aplica)

(Este documento se finalizará utilizando el encabezamiento oficial del banco emisor. Excepto en los campos indicados, no podrán introducirse cambios a este formulario)

A: PNUD
[indicar la información de contacto que figura en la Hoja de Datos]

POR CUANTO [*nombre y dirección del Contratista*] (en lo sucesivo denominado "el Licitante") ha presentado una Oferta al PNUD en fecha ……. para el suministro de bienes y la ejecución de servicios correspondiente a la Invitación a Licitar PNUD/IAL-133/2018 (en lo sucesivo denominado "la Oferta");

Y POR CUANTO han estipulado ustedes que el Licitante proporcione una Garantía Bancaria de un banco reconocido por la suma especificada en la IaL como garantía en el caso de que el Licitante:

a) no llegue a firmar el contrato después de la adjudicación de éste por el PNUD;
a) retire su Oferta después de la fecha de apertura de las Ofertas;
b) no cumpla con las modificaciones de requisitos del PNUD, según se indica en la Sección F.3 de la IaL;
c) no aporte la Garantía de Ejecución, los seguros o los restantes documentos que el PNUD pueda exigir como condición para la efectividad del contrato;

Acordamos otorgarle al Licitante esta Garantía Bancaria a favor de ustedes en forma solidaria, incondicional, irrevocable, sin beneficio de excusión y de realización automática, a su solo requerimiento, por la suma de _____ (*expresar en número y letras*) nuevos soles/dólares de los Estados Unidos de América (USD o S/.), a fin de garantizar la Oferta presentada por nuestro cliente, de conformidad con las Bases de la Licitación Pública Internacional PNUD/IAL-133/2018 – Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma.

Fecha de vencimiento: _____ (*esta fecha no podrá ser menor a la estipulada en las Bases de la Licitación).*

Esta garantía será válida por un periodo mínimo de 120 días contados a partir de la fecha de presentación de ofertas.

FIRMA Y SELLO DEL BANCO PROVEEDOR DE LA GARANTÍA

Fecha .....

Nombre del Banco .....

Dirección .....

Sección 9: Formulario de garantía de ejecución de contrato (No aplica)[6]

(Este documento se finalizará utilizando el encabezamiento oficial del banco emisor. Excepto en los campos indicados, no podrán introducirse cambios a este formulario)

A: PNUD
[indicar la información de contacto que figura en la Hoja de Datos]

POR CUANTO [*nombre y dirección del Contratista*] (en lo sucesivo denominado "el Contratista") ha aceptado, en cumplimiento del Contrato nº … de fecha …, ejecutar los servicios … (en adelante "el Contrato");

Y POR CUANTO ha sido estipulado por ustedes en dicho Contrato que el Contratista proveerá una garantía bancaria de un banco reconocido por la suma especificada en él como garantía del cumplimiento de sus obligaciones con arreglo al Contrato;

Y POR CUANTO hemos acordado conceder al Contratista dicha Garantía Bancaria;

POR LO TANTO afirmamos por la presente que somos Garantes y responsables ante ustedes, en nombre del contratista, en forma solidaria, incondicional, irrevocable, sin beneficio de excusión en nombre de nuestro cliente, hasta un total hasta un total de *[monto de la garantía] [en letras y cifras]*, que constituye la suma pagadera, en los tipos y proporciones de monedas en que se pague el precio del Contrato, y que nos comprometemos a pagar contra su primera solicitud por escrito y sin argumentaciones ni objeciones cualquier suma o sumas dentro de los límites de *[monto de la garantía arriba indicado*] sin necesidad de que se prueben o acrediten los motivos o las razones de su demanda, en la suma especificada en la misma.

Esta garantía será válida hasta una fecha a 30 días desde la fecha de expedición por el PNUD de un certificado de desempeño satisfactorio y la finalización completa de servicios por el Contratista.

FIRMA Y SELLO DEL BANCO PROVEEDOR DE LA GARANTÍA
Fecha .....
Nombre del Banco .....
Dirección .....

[6] Si en la IaL se requiere la presentación de una garantía de ejecución como condición para la firma y efectividad del Contrato, la garantía de ejecución que emita el banco del Licitante se ajustará al contenido de este formulario.

Sección 10: Formulario de Garantía de Pago por Adelantado

(Este documento se finalizará utilizando el encabezamiento oficial del banco emisor. Excepto en los campos indicados, no podrán introducirse cambios a este formulario)

_____ *[Nombre del banco y dirección de la sucursal u oficina emisora]*
Beneficiario: _____ *[Nombre y dirección del PNUD]*
Fecha: _____
GARANTÍA DE PAGO POR ADELANTADO NO.: _____

Se nos ha informado que *[nombre de la Empresa]* (en adelante denominado "el Contratista") ha celebrado el Contrato no. *[número de referencia del contrato]* de fecha *[indíquese la fecha]* con ustedes para el suministro de *[breve descripción de los servicios]* (en lo sucesivo denominado "el Contrato").

Por otra parte, entendemos que, de acuerdo con las condiciones del contrato, se habrá de realizar un pago anticipado por la suma de *[monto en letras]* (*[monto en cifras]*) contra una Garantía de Pago por Adelantado.

A petición del Contratista, nosotros *[nombre del banco]* por la presente nos comprometemos con carácter irrevocable a pagarles a ustedes cualquier suma o sumas que no excedan en total de la cantidad de *[monto de la garantía] [en letras y cifras])*[7] a la recepción por nuestra parte de su primera demanda por escrito acompañada de una declaración escrita que indique que el Contratista ha incumplido sus obligaciones en virtud del Contrato por cuanto el Contratista ha utilizado el anticipo para otros fines diferentes de la prestación de los servicios y entrega de bienes que estipula el Contrato.

Es condición para cualquier reclamo y pago con arreglo a esta Garantía que el pago por adelantado a que se hace referencia más arriba haya sido recibido por el Contratista en su cuenta número _____ de *[nombre y dirección del Banco]*.

El importe máximo de esta garantía será reducido progresivamente en función del importe del anticipo reembolsado por el Contratista, tal como se indique en las copias certificadas de los estados de cuenta mensuales que se nos presenten. Esta garantía expirará, a más tardar, a nuestra recepción del certificado de pago mensual que indique que los Consultores han procedido a la devolución total del importe del anticipo, o el día __ de _____ de ___, lo que ocurra primero. Consecuentemente, cualquier solicitud de pago con arreglo a esta Garantía deberá ser recibida por nosotros en esta oficina en o antes de la fecha citada.

Esta garantía está sujeta a las *Reglas uniformes de la CCI relativas a las garantías a primer requerimiento* (*ICC* Uniform Rules for Demand Guarantees). (Folleto nº *458*).

_____
[firma(s)]

Nota: Las indicaciones que figuran en cursiva tienen solamente carácter indicativo, y tienen por objeto ayudar a la preparación de este formulario; serán suprimidas de la Oferta final.

[7] *El banco que extienda la Garantía establecerá una cantidad que represente el monto total del pago por adelantado, denominada en cualquier moneda en que se especifique en el Contrato que se ha realizado el pago por adelantado.*

Sección 11: - CONDICIONES GENERALES DEL PNUD APLICABLES A LAS ORDENES DE COMPRA

A. ACEPTACION DE LA ORDEN DE COMPRA

La presente orden de compra se considerará aceptada únicamente cuando el Proveedor hubiere firmado y devuelto la Copia de Acceptación de ésta, o hubiere efectuado la entrega puntual de la mercancía de conformidad con los términos de la presente orden de compra, según las especificaciones en ella consignadas. La aceptación de la presente orden de compra constituirá un contrato entre las partes, cuyos derechos y obligaciones se regirán exclusivamente por las condiciones establecidas en la presente orden de compra, incluidas las presentes Condiciones Generales. Ninguna cláusula adicional o incompatible que hubiere propuesto el Proveedor obligará al PNUD si no hubiere sido aceptada por escrito por el funcionario debidamente autorizado del PNUD.

B. PAGO

1. Una vez cumplidas las condiciones de entrega, y salvo disposición en contrario en la presente orden de compra, el PNUD efectuará el pago en un plazo de 30 días a contar de la fecha de recepción de la factura del Proveedor y de las copias de los documentos de embarque especificados en la presente orden de compra.
2. El pago de la factura mencionada supra reflejará cualquier descuento indicado en las condiciones de pago de la presente orden de compra, siempre que tal pago se hiciere en el plazo estipulado en dichas condiciones.
3. Salvo cuando el PNUD hubiere autorizado otra cosa, el Proveedor deberá presentar una sola factura por la presente orden de compra y en dicha factura se consignará el número de identificación de la presente orden de compra.
4. El Proveedor no podrá aumentar los precios consignados en la presente orden de compra, a menos que el PNUD lo hubiere autorizado expresamente por escrito.

C. EXENCION TRIBUTARIA

1. La sección 7 de la Convención sobre Privilegios e Inmunidades de la Organización de las Naciones Unidas dispone, entre otras cosas, que la Organización de las Naciones Unidas, incluidos sus órganos subsidiarios, está exenta de todo impuesto directo, salvo por los cargos correspondientes a servicios públicos, así como de derechos de aduana y gravámenes de naturaleza similar respecto de
los artículos que importare o exportare para su uso oficial. Cuando una autoridad gubernamental se negare a reconocer la exención del PNUD respecto de estos impuestos, derechos o gravámenes, el Proveedor consultará inmediatamente al PNUD para determinar la forma de actuar que resulte mutuamente aceptable.
2. En consecuencia, el Proveedor autoriza al PNUD a deducir de sus facturas toda suma que corresponda a esos impuestos, derechos o gravámenes, salvo cuando hubiere consultado al PNUD antes de efectuar esos pagos y el PNUD, en cada caso, le hubiere autorizado específicamente a pagar esos impuestos, derechos o gravámenes en protesto. En ese caso, el Proveedor presentará al PNUD prueba por escrito de que ha pagado estos impuestos, derechos o gravámenes y de que ese pago ha sido debidamente autorizado.

D. RIESGO DE PERDIDA

Salvo que las partes hayan acordado otra cosa en la presente orden de compra, el riesgo de pérdida, daño o destrucción de la mercancía se regirá por el DDU INCOTERM 1990.

E. LICENCIAS DE EXPORTACION

Con independencia de cualquier INCOTERM utilizado en la presente orden de compra, el Proveedor tendrá la obligación de obtener las licencias de exportación que fueren requeridas para la mercancía.

F. CONFORMIDAD DE LA MERCANCIA Y SU EMBALAJE

El Proveedor garantiza que la mercancía, incluido su embalaje, es conforme con las especificaciones de la mercancía solicitada en virtud de la presente orden de compra y que es apta para el uso al que normalmente se destina y para los fines expresamente comunicados por el PNUD al Proveedor; asimismo, el Proveedor garantiza que la mercancía

no adolece de defectos ni en los materiales ni en su fabricación. El Proveedor garantiza también que la mercancía está embalada de la forma más adecuada para su protección.

G. INSPECCION
1. El PNUD tendrá un plazo razonable después de la entrega de la mercancía para inspeccionarla y rechazar y rehusar su aceptación si no es conforme a lo indicado en la presente orden de compra; el pago de la mercancía en virtud de la presente orden de compra no se entenderá que constituye aceptación de la mercancía.
2. La inspección anterior al embarque no exonerará al Proveedor de ninguna de sus obligaciones contractuales.

H. VIOLACION DE DERECHOS DE PROPIEDAD INTELECTUAL
El Proveedor garantiza que el uso o suministro por el PNUD de la mercancía vendida conforme a la presente orden de compra no viola ninguna patente, derecho de autor, nombre comercial o marca registrada o cualquier otro derecho de propiedad industrial o intelectual. Además, el Proveedor, en virtud de la presente garantía, indemnizará y defenderá a su costa al PNUD y a la Organización de las Naciones Unidas por cualquier acción o reclamación que se entablare contra el PNUD o la Organización de las Naciones Unidas en relación con la presunta violación de cualquiera de los derechos mencionados supra en relación con la mercancía vendida en virtud de la presente orden de compra.

I. DERECHOS DEL PNUD
Si el Proveedor no cumpliere sus obligaciones conforme a los términos y condiciones de la presente orden de compra, incluido, sin carácter limitativo, el incumplimiento de la obligación de obtener las licencias de exportación necesarias o de la obligación de efectuar la entrega, total o parcial, de la mercancía en la fecha o fechas convenidas, el PNUD, previo emplazamiento al Proveedor, con razonable antelación, de que cumpla su obligación y sin perjuicio de otros derechos o recursos, podrá ejercer uno o más de los derechos que se mencionan infra: 2

A. Adquirir la mercancía, en todo o en parte, de otros proveedores, en cuyo caso el PNUD podrá exigir que el Proveedor le compense por cualquier aumento de los costos en que hubiere incurrido.
B. Rehusar la mercancía, en todo o en parte.
C. Rescindir la presente orden de compra sin responsabilidad alguna por cargos de rescisión o ninguna otra responsabilidad.

J. ENTREGA TARDIA
Sin perjuicio de los derechos u obligaciones de las partes, si el Proveedor no pudiere efectuar la entrega de la mercancía en la fecha o fechas estipuladas en la presente orden de compra, (i) consultará inmediatamente al PNUD para determinar la manera más expeditiva de efectuar la entrega de la mercancía y (ii) utilizar un medio rápido de entrega, a su costa (salvo cuando la demora se debiere a fuerza mayor), si asi lo solicita razonablemente el PNUD.

K. CESION E INSOLVENCIA
1. Salvo cuando el PNUD le hubiere previamente autorizado por escrito, el Proveedor no podrá ceder, transferir o disponer de la presente orden de compra o de cualquiera de sus partes o de cualquiera de los derechos u obligaciones que le correspondieren en virtud de la presente orden de compra.
2. Si el Proveedor cayera en insolvencia o perdiera el control de su empresa por causa de insolvencia, el PNUD podrá, sin perjuicio de cualquier otro derecho o recurso que pudiera corresponderle, rescindir inmediatamente la presente orden de compra mediante aviso por escrito al Proveedor.

L. USO DEL NOMBRE Y EMBLEMA DEL PNUD Y DE LA ORGANIZACION DE LAS NACIONES UNIDAS
El Proveedor no utilizará en ninguna forma el nombre, el emblema o el sello oficial del PNUD o de la Organización de las Naciones Unidas.

M. PROHIBICION DE PUBLICIDAD
El Proveedor no anunciará ni hará público el hecho de que es un proveedor del PNUD sin la autorización específica del PNUD en cada caso.

N. DERECHOS DEL NIÑO

1. El Proveedor declara y garantiza que ni él ni ninguna de sus filiales realiza ninguna práctica que sea incompatible con los derechos estipulados en la Convención sobre los Derechos del Niño, incluido su artículo 32 que, entre otras disposiciones, reconoce el derecho del niño a estar protegido contra el desempeño de cualquier trabajo que pueda ser peligroso o entorpecer su educación, o que sea nocivo para su salud o para su desarrollo físico, mental, espiritual, moral o social.
2. Todo incumplimiento de esta declaración y garantía dará derecho al PNUD a rescindir la presente orden de compra inmediatamente mediante notificación al Proveedor, sin costo alguno para el PNUD.

O. MINAS

1. El Contratista declara y garantiza que ni él ni ninguna de sus filiales está directa y activamente involucrado en patentes, desarrollo, ensamblaje, producción, comercio o manufacturación de minas o de componentes utilizados principalmente en la fabricación de minas. El término "minas" se refiere a aquellos artefactos definidos en el artículo 2, párrafos 1, 4 y 5 del Protocolo II de la Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que pueden considerarse excesivamente nocivas o de efectos indiscriminados, de 1980.
2. Todo incumplimiento de esta declaración y garantía dará derecho al PNUD a rescindir el presente Contrato inmediatamente mediante notificación al Contratista, sin costo alguno para el PNUD.

P. SOLUCION DE CONTROVERSIAS

Arreglo amigable

Las partes harán todo lo posible por solucionar de manera amigable toda disputa, controversia o reclamación derivada de la presente orden de compra o su incumplimiento, rescisión o invalidez. Cuando las partes desearen llegar a un arreglo amigable mediante la conciliación, ésta se regirá por el Reglamento de Conciliación de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional que estuviera vigente en esa oportunidad o de conformidad con cualquier otro procedimiento en el que las partes que pudieren convenir.

Arbitraje

A menos que la disputa, controversia o reclamación entre las partes mencionada supra se pueda resolver amigablemente conforme a lo dispuesto en el párrafo precedente del presente artículo dentro de los sesenta (60) días de que una de las partes hubiere recibido de la otra una petición de arreglo amigable, dicha disputa, controversia o reclamación será sometida a arbitraje por cualquiera de las partes de conformidad con el Reglamento de Arbitraje de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional que estuviera vigente en esa oportunidad, incluidas las disposiciones sobre ley aplicable. El tribunal arbitral no podrá conceder indemnizaciones punitivas. Además, a menos expresamente convenido en la presente orden de compra, el tribunal arbitral no podrá conceder intereses [EN CASOS ESPECIALES, PREVIA CONSULTA CON OLA, SE PODRA AÑADIR: “QUE EXCEDAN .....%, Y SIEMPRE QUE SEAN INTERESES SIMPLES] El laudo arbitral que se pronuncie como resultado de ese arbitraje será la resolución definitiva y vinculante de la controversia, reclamación o disputa entre las partes.

Q. PRIVILEGIOS E INMUNIDADES

Ninguna disposición de las presentes Condiciones Generales o de la presente orden de compra podrá interpretarse que constituye una renuncia de cualquiera de los privilegios e inmunidades de la Organización de las Naciones Unidas, incluidos sus órganos subsidiarios.

Sección 12: Resumen de estados financieros

(a ser presentado en papel membretado del licitante)

Nombre del Licitante: _____

Proceso: PNUD/IAL-133/2018 – "Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma"

	DESCRIPCIÓN	BALANCE 2015	BALANCE 2016
1.	Volumen de Ventas (según lo indicado en el Estado de Ganancias y Pérdidas)		
2.	Capital Social (suscrito) de la empresa (US$.)		
3.	Patrimonio Neto de la Empresa (S/.)		
4.	Índice de Liquidez (razón corriente): IL = AC/PC AC = Activo Corriente (indiar monto por cada año) PC = Pasivo Corriente (indicar monto por cada año)		
5.	Índice de Endeudamiento: IE = PT/AT PT = Pasivo Total (indicar monto por cada año) AT = Activo Total (indicar monto por cada año)		
6.	Capital Neto de Trabajo: CT = AC-PC AC = Activo Corriente (indicar monto por cada año) PC = Pasivo Corriente ((indicar monto por cada año)		

Firma del Representante Legal : _____

Firma de Contador Público Colegiado: _____

Lugar, día y fecha: _____

Sección 13: Tabla de Especificaciones Técnicas Mínimas Requeridas

– "Adquisición de Switches para centro de Datos, Switches de Distribucion y Firewall de Seguridad Perimetrall para el Programa Nacional de Alimentación Escolar Qali Warma"

ESPECIFICACIONES TÉCNICAS: ADQUISICIÓN DE SWITCHES PARA CENTRO DE DATOS, SWITCHES DE DISTRIBUCION

ITEM No. 1.1: SWITCH TIPO 1 - SWITCHES DE CORE PARA CENTRO DE DATOS

Especificaciones Técnicas	Descripción	Detalle de Especificaciones Propuestas	Observación / No. Folio
Marca:	*Indicar*		
Modelo:	*Indicar*		
Origen	*Indicar*		
Cantidad	*2 unidades*		
Alta Disponibilidad	Con la finalidad de garantizar la alta disponibilidad de la red para los servidores del Centro de Datos, los Switches para servidores deberán ser interconectados y configurados de tal manera que los servidores que tengan múltiples interfaces de red, puedan conectarse a estos equipos teniendo activas estas conexiones de manera simultánea. Los switches para servidores deberán interconectarse entre sí mediante dos (02) puertos de 10GB en cada equipo configurando un trunk de 20GB entre ellos, como mínimo		
Hardware	Switches multicapa diseñados específicamente para centro de datos.		
	Cada switch deberá ser del mismo modelo y familia. Año de fabricación 2017 o más reciente.		
	Los switches para Centro de Datos deberán permitir que los servidores que cuenten con múltiples interfaces de red puedan conectarse a ambos switches utilizando agregación de puertos sin que se ocasionen loops o que se tengan puertos bloqueados. Es decir, las conexiones deberán operar en modo activo/activomstsc.		
	Incluir al menos 48 puertos fixed SPF+ port (1 o 10Gbpa)		
	El equipo ofertado deberá trabajar en capa 2, con una tasa de envió mínima de 960 Gbps.		
	El equipo deberá soportar la inserción en caliente de fuentes de poder y módulos ventiladores.		
	El equipo deberá contar con una redundancia de fuentes de poder N+1 y N+N		
	El equipo deberá contar con una redundancia de módulo de ventilador de N+1		
	Capaz de consolidar tráfico Ethernet proveniente de la red LAN.		
	Cada switch Centro de Datos deberá incluir al menos treinta y dos (32) puertos 10 GE, capaces de soportar transceiver de 1 GE (SFP) o 10 GE (SFP+), con soporte de capa 2 (L2). Se deberá incluir por cada equipo veinte (20) tranceivers para puertos UTP de 1GE, ocho (08) Tranceiver del tipo 10GBASE-SR además de los conectores que permitan unir ambos equipos utilizando como mínimo dos (02) puertos 10 Gigabit.		
	El equipo ofertado deberá cumplir con un diseño que provea latencia de tráfico predecible y consistente a pesar del tamaño del paquete, patrón de tráfico o características habilitadas en las interfaces correspondientes.		

	El equipo ofertado deberá cumplir con la misma tasa de transferencia en todos los puertos.		
	Los dos Switches de Centro de datos se conectarán entre sí mediante dos enlaces de 10 Gbps como mínimo. Estas conexiones pueden ser mediante cobre o fibra y los módulos son adicionales a los 10GBASE-SR ya solicitados.		
	Cada switch de Centro de Datos no deberá exceder de 1 RU de altura.		
	Fuentes de Poder y ventiladores redundantes hot swap.		
	Los dispositivos a ofertar no deberán contar a la fecha de presentación de propuestas con anuncio de Fin de Ciclo de Vida (Fin de Vida) del fabricante con el fin de asegurar una mayor vigencia tecnológica de los equipos a adquirir. Esto deberá ser sustentado con documentación del fabricante.		
Software	Capacidad de Operación a nivel 2 y nivel 3 del Modelo OSI.		
	El switch solicitado tiene que tener habilitado el enrutamiento en capa 3, que soporte los protocolos (RIPv2, EIGRPv2, OSPFv2,)		
	Soporte de calidad de servicio 802.1p		
	Soporte de QoS, con 8 colas de prioridad por puerto 10GE.		
	El equipo ofertado deberá soportar la configuración de QoS por puerto.		
	El equipo ofertado deberá soportar clasificación QoS basada en listas de acceso (Capas 2, 3 y 4)		
	Soporte de tramas gigantes (giants) en todos los puertos (hasta 9216 bytes)		
	Manejo de 4 000 VLANs y 60 000 MAC address.		
	Manejo de VLANs por puerto y 802.1q (trunking).		
	Soporte del estándar IEEE 802.1AB (LLDP - Link Layer Discovery Protocol) o mecanismo similar para intercambio de información de dispositivos.		
	Soporte de protocolos NTP y DNS.		
	Soporte de DHCP relay.		
	Enrutamiento unicast, multicast basado en hardware.		
	Soporte del protocolo VRRP		
	Deberá incluir protocolos de enrutamiento IPv4 estático y dinámico.		
	Tráfico Multicast IGMPv2 y v3 snooping. Soporte de tráfico Multicast IGMPv3.		
	Soportar enrutamiento multicast basado en hardware para IPv4 e IPv6. PIM-SM instalado y operativo.		
	El equipo deberá cumplir con ACLs de entrada (estandar y extendido) en Ethernet y puertos Ethernet virtuales.		
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad. Se deberá asegurar que se pueda realizar la agregación en al menos dos puertos ubicados en módulos distintos		
	Soporte de los siguientes estándares: IEEE 802.3ab 1000BASE-T, Gigabit sobre cobre IEEE 802.3z 1000BASE-X, Gigabit sobre fibra IEEE 802.1d, Spanning Tree Protocol IEEE 802.1s, MSTP IEEE 802.1w, RSTP IEEE 802.1p, CoS Priorización de tráfico IEEE 802.1q, VLAN tagging IEEE 802.3ad, LACP IEEE 802.3x, Control de flujo IEEE 802.3ae, 10 Gigabit Ethernet		

	RMON		
Gestión y monitoreo	Deberá combinar la gestión de Ethernet y redes de almacenamiento en un único panel de control.		
	Gestión por consola y puerto independiente para gestión fuera de banda.		
	Permitir la administración segura protocolo SSHv2.		
	Permitir múltiples sesiones simultáneas de administración		
	Incluir el soporte de SNMP v2c y v3.		
	Incluir los MIBs de los Switches considerados.		
	Registro de eventos vía Syslog.		
	Soporte de protocolos de transferencia de archivos TFTP, FTP y/o sFTP.		
	Soporte de protocolos RCP y/o SCP y/o SFTP.		
	Deseable que cuente con herramientas que permitan la captura de tráfico para su análisis y decodificación a nivel de paquetes.		
	Deseable mecanismo de detección de fallas en cables de cobre y de fibra óptica.		
	Incluir procesos de debug para el análisis detallado de fallas.		
	Deberá contar con licencia para LAN.		
	Brindar la funcionalidad de "puerto espejo" o funcionalidad similar, por puerto o grupo de puertos y por VLAN.		
Mecanismos de seguridad	Filtrado basado en parámetros de capas 2, 3 y 4. Estos filtros deben ser aplicables por puerto y por VLAN.		
	Seguridad por puerto, en base a la dirección MAC.		
	Supresión y limitación de tormentas de broadcast, multicast y/o unicast.		
	Control de acceso centralizado mediante RADIUS y/o TACACS+		
	Incluir el manejo de protocolos SSHv2 y/o SSL.		
	Permitir mínimo 4 niveles de privilegios de acceso para administración por consola, telnet y ssh.		
	Permitir la restricción del acceso mediante SSH y SNMP desde múltiples direcciones IP.		
	La versión del sistema operativo no debe poseer vulnerabilidades DoS conocidas a la fecha de publicación de las bases.		
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 oficin		
	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. ✓ 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.		

ITEM 1.2: SWITCH TIPO 2 - SWITCHES PARA DISTRIBUCIÓN

Especificaciones Técnicas	Descripción	Detalle de Especificaciones Propuestas	Observación / No. Folio
Marca:	*Indicar*		
Modelo:	*Indicar*		
Origen	*Indicar*		
Cantidades	*2 unidades*		
Alta Disponibilidad	Para garantizar la alta disponibilidad de la red para los switches de acceso a usuarios, se deberá contar con switches de distribución, cada uno de los cuales tendrá habilitado un enlace a velocidad 10 Gigabit a cada gabinete de piso. Estos switches de distribución deberán interconectarse entre sí mediante dos (02) puertos de 10GB en cada equipo configurando un trunk de 20GB entre ellos, como mínimo.		
Hardware	Switches de distribución multicapa, de operación en L2 y L3 del modelo OSI y diseñados como equipos de agregación o distribución LAN.		
	Cada switch deberá ser del mismo modelo y familia. Año de fabricación 2017 o más reciente.		
	Los dos switches de distribución deberán trabajar en alta disponibilidad operando como una unidad lógica virtualizada, para lo cual se debera provisionar los componentes necesarios.		
	Capacidad mínima de conmutación de 640 Gbps por cada equipo.		
	Cada switch de distribución deberá incluir como mínimo Dieciséis (16) Puertos SFP+ y ser escalable hasta 24 Puertos SFP+. Deberán soportar transceivers de 1 GE (SFP) o 10 GE (SFP+), con soporte de capa 2 (L2) y capa 3 (L3). Se deberá tener equipados por cada equipo: ocho (08) Tranceivers ópticos 10GBASE-SR para fibra multimodo.		
	Se deberá incluir por cada equipo cuatro (04) tranceivers para puertos UTP de 1GE.		
	Los dos Switches de distribución se conectarán entre sí mediante dos enlaces de 10 Gbps como mínimo, esta conexión podrá ser mediante fibra o cobre, se deberán incluir los componentes necesarios para habilitar esta conexión redundante.		
	Cada switch de distribución no deberá exceder de 1 RU de altura.		
	Los módulos de fuente de poder y ventiladores deben ser hot-swap.		
	Cada switch deberá contar con una tasa de reenvío en hardware de 400 Mpps como mínimo.		
	Deben contar con fuentes de poder redundantes con voltaje de entrada de 200-240 VAC, 60 Hz, en una configuración N+1 y ventiladores con flujo de aire desde el frente hacia atrás como mínimo.		
	Los dispositivos a ofertar no deberán contar a la fecha de presentación de propuestas con anuncio de Fin de Ciclo de Vida (Fin de Vida) del fabricante con el fin de asegurar una mayor vigencia tecnológica de los equipos a adquirir. Esto deberá ser sustentado con documentación del fabricante.		
	El equipo deberá incluir memoria DRAM como mínimo 4GB		
	El equipo deberá incluir memoria FLASH como mínimo 4GB		
Software	Capacidad de Operación a nivel 2, nivel 3 y nivel 4 del Modelo OSI.		
	Soporte de calidad de servicio 802.1p y DSCP		
	Soporte de QoS, con 8 colas de prioridad por puerto como mínimo.		
	Manejo de 1000 VLANs, 4000 VLAN IDs y 30 000 MAC address como mínimo.		
	Manejo de VLANs por puerto y 802.1q (trunking).		
	Soporte del estándar IEEE 802.1AB (LLDP - Link Layer Discovery Protocol)		

	o similar para intercambio de información de dispositivos.		
	Soporte de protocolos SNTP o NTP ~~y~~ o DNS.		
	Soporte de DHCP relay.		
	Enrutamiento unicast, multicast basado en hardware.		
	Deberá incluir protocolos de enrutamiento IPv4 estático y dinámico (RIPv2, OSPFv2 y BGP como mínimo) con soporte de OSPF y BGP en IPv6 mediante upgrade de software.		
	Tráfico Multicast IGMPv2 y v3 snooping. Soporte de tráfico Multicast IGMPv3.		
	Soportar enrutamiento multicast basado en hardware para IPv4 e IPv6. PIM-SM instalado y operativo.		
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad. Se deberá asegurar que se pueda realizar la agregación en al menos dos puertos ubicados en módulos distintos.		
	Soporte de los siguientes estándares: IEEE 802.3ab 1000BASE-T, Gigabit sobre cobre IEEE 802.3z 1000BASE-X, Gigabit sobre fibra IEEE 802.1d, Spanning Tree Protocol IEEE 802.1s, MSTP IEEE 802.1w, RSTP IEEE 802.1p, CoS Priorización de tráfico IEEE 802.1q, VLAN tagging IEEE 802.3ad, LACP IEEE 802.3x, Control de flujo		
Gestión y monitoreo	Gestión por consola y puerto independiente para gestión fuera de banda.		
	Permitir la administración utilizando protocolo-SSH~~.~~		
	Permitir múltiples sesiones simultáneas de administración		
	Incluir el soporte de SNMP v2c y v3.		
	Se deben Incluir los MIBs de los Switches considerados.		
	Registro de eventos vía Syslog.		
	Soporte de protocolos de transferencia de archivos TFTP~~,~~ y/o FTP y/o sFTP.		
	Soporte de Sflow, Netflow o protocolo similar instalado y operativo.		
	Es deseable que incluyan mecanismos de detección de fallas en cables de cobre y de fibra óptica.		
	Incluir procesos de debug para el análisis detallado de fallas.		
	Brindar la funcionalidad de “puerto espejo” o funcionalidad similar, por puerto o grupo de puertos y por VLAN.		
	Permitir configurar múltiples sesiones de “puerto espejo” o funcionalidad similar, deseable soporte de "puerto espejo" remoto o funcionalidad similar. Se requiere soportar al menos dos (02) sesiones simultáneas.		
Mecanismos de seguridad	Filtrado basado en parámetros de capas 2, 3 y 4. Estos filtros deben ser aplicables por puerto y por VLAN.		
	Seguridad por puerto, en base a la dirección MAC.		
	Supresión y limitación de tormentas de broadcast, multicast y unicast.		
	Control de acceso centralizado mediante RADIUS y/o TACACS+		
	Incluir el manejo de protocolos SSH~~.~~		
	Permitir al menos 4 niveles de privilegios de acceso para administración por consola, telnet y ssh.		
	Permitir la restricción del acceso mediante SSH y SNMP desde múltiples direcciones IP.		
	Soporte de DHCP Snooping o mecanismo similar.		

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 oficin		
	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. ✓ 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.		

ESPECIFICACIONES TÉCNICAS: ADQUISICION DE FIREWALL DE SEGURIDAD PERIMETRAL

ITEM 2: ADQUISICION DE FIREWALL DE SEGURIDAD

ITEM 2.1: ADQUISICION DE FIREWALL DE SEGURIDAD

Especificaciones Técnicas	Descripción	Detalle de Especificaciones Propuestas	Observación / No. Folio
Marca:	*indicar*		
Modelo:	*Indicar*		
Origen:	*Indicar*		
Cantidad:	02 Unidades		
Características del Firewall	Se deberá incluir todas las funcionalidades en un solo dispositivo del mismo fabricante.		
	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 ser optimizada para análisis de contenido 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 en los últimos 3 reportes de Gartner, en el cuadrante de Líderes para Network Enterprise Firewalls.		
	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, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.		
	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 e Antispyware;		
	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.		
	Deberá incluir cuatro (04) interfaces SFP+ como mínimo por cada equipo.		
	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 un máximo de 1500 políticas		
	Debe permitir 40 zonas de seguridad y 05 routers virtuales		
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, vozIP, 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 nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano.		
	Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:		
	Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, como mínimo).		
	Nivel de riesgo de las aplicaciones.		
	Categoría y sub-categoría de aplicaciones.		
	Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.		
	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		
	Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.		
	Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo.		
	Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener algunas firmas de IPS habilitada o tener todas las firmas de IPS, Anti-Virus y Antispyware 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 Antispyware.		
	Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes.		
	Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos.		
	Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP,		
	SMB, SMTP e POP3.		
	Los eventos deben identificar el país de donde partió la amenaza.		
	Debe incluir seguridad contra virus en contenido HTML y javascript, software espía (spyware) y worms.		
	Seguridad contra descargas involuntarias usando HTTP de archivos ejecutables Maliciosos.		
	Rastreo de virus en PDFs.		
	Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.).		
	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.		
	El fabricante debe ser considerado como un Lider en el reporte de evaluación de Forrester Wave Automated Malware Analysis, Q2 2016		
	Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Mac OSX y Android		
	Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB		
	El sistema de análisis debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red).		
	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, apk y archivos java en el ambiente controlado.		
	Poseer SLA de, como máximo, 10 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado.		
	Permitir el 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 certifícate.		
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;		
	Permitir listar el número de aplicaciones soportadas para control de datos;		
	Permitir listar el número de tipos de archivos soportados para el control de datos.		
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, E-Directory y base de datos local.		
	Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio.		
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.		

	Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función.		
	Debe soportar una 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 e 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;		
	El portal de VPN debe enviar al cliente remoto la lista de Gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente		
	Debe haber una opción en el cliente remoto de escoger manualmente el gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.		
	Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa.		
Reportes y Administración	Debe tener un módulo de reportes y administración incluido dentro del mismo equipo sin necesidad de licenciamiento ideal		
	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.		
Pruebas de los productos esperados	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.		

	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.		
	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.		

Sección 14: Declaración jurada de calidad de los bienes y garantía técnica

(a ser presentado en papel membretado del licitante)

Señores
Programa de las Naciones Unidas para el Desarrollo
Proyecto 00100712
Presente

REF.: Invitación a Licitar PNUD/IAL-133/2018
En relación con los bienes propuestos para la Invitación a Licitar PNUD/IAL-133/2018, el fabricante que suscribe declara lo siguiente:

Que los bienes ofertados son nuevos, sin uso, fabricados a partir del año 2017/2018, con insumos de alta calidad, totalmente elaborados en fábrica, con la mejor tecnología existente en el mercado y garantizamos su perfecto estado de conservación y operación incluyendo el periodo de garantía técnica de (***indicar tiempo de garantía ofertado***).

..... de..... de.....2018

_____
Firma del Representante del Fabricante
Nombre y Titulo

Sección 15: Declaración jurada de instalación, capacitación y mantenimiento

(a ser presentado en papel membretado del licitante)

Señores
Programa de las Naciones Unidas para el Desarrollo
Proyecto 00100712
Presente

REF.: Invitación a Licitar PNUD/IAL-133/2018

En relación con los bienes propuestos para la Invitación a Licitar PNUD/IAL-133/2018, el licitante que suscribe declara lo siguiente:

Mediante la presente declaramos cumplir con los servicios de Intalacion, capacitación y mantenimiento de acuerdo a los requisitos establecidos en los Términos de Referencia indicando como fecha de implementación de servicios de acuerdo al siguiente detalle:

Descripcion del servicio	Fecha de implemetacion	No. de Item
Servicio de Intalación		
Servicio de Capacitacion		
Primer servicio de Mantenimiento		
Segundo servicio de Mantenimiento		

.

..... de..... de.....2018

_____
Firma del Representante del Fabricante
Nombre y Titulo